
**ID:** 525020
**Sample Name:**
GQwxmGZFvtg.dll
**Cookbook:** default.jbs
**Time:** 10:11:59
**Date:** 19/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

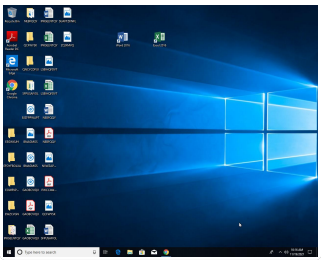
# Windows Analysis Report GQwxmGZFvtg.dll

## Overview

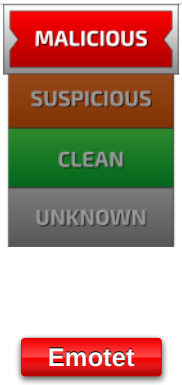
### General Information

| | |
|---|---|
| Sample Name: | GQwxmGZFvtg.dll |
| Analysis ID: | 525020 |
| MD5: | 3ecb8e8c0baaa4.. |
| SHA1: | 5de0548c74dd50.. |
| SHA256: | 7e4d240abe7a38.. |
| Infos: | |

Most interesting Screenshot:



### Detection

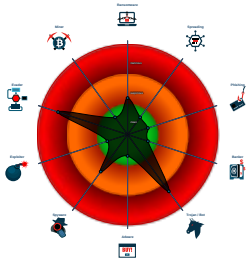



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Sigma detected: Emotet RunDLL32 …
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…

### Classification



## Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3228 cmdline: loaddll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4720 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2932 cmdline: rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5576 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5244 cmdline: rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 5480 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gbdnfdnwgwzcefyt\nlnmlmepgkdbq.udp",iHIeY MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 4928 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Gbdnfdnwgwzcefyt\nlnmlmepgkdbq.udp",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6136 cmdline: rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,abziuleoxsborpb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2224 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2016 cmdline: rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,aejkroaebsbxdnkhb MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2240 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4544 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 3716 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5320 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4128 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5740 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

## Malware Configuration

### Threatname: Emotet

```
{
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ],
  "C2 list": [
    "51.178.61.60:443",
    "168.197.250.14:80",
    "45.79.33.48:8080",
    "196.44.98.190:8080",
    "177.72.80.14:7080",
    "51.210.242.234:8080",
    "185.148.169.10:8080",
    "142.4.219.173:8080",
    "78.47.204.80:443",
    "78.46.73.125:443",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "191.252.103.16:80",
    "54.38.242.185:443",
    "85.214.67.203:8080",
    "54.37.228.122:443",
    "207.148.81.119:8080",
    "195.77.239.39:8080",
    "66.42.57.149:443",
    "195.154.146.35:443"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000000C.00000002.1195922556.00000000319A000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000002.00000002.776937820.0000000002C55000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000008.00000002.829087525.0000000002B9A000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000004.00000002.792999078.0000000002F2A000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 00000003.00000002.776035801.000000000048A000.00000004.00000020.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| Click to see the 2 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8.2.rundll32.exe.2bb5280.1.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 4.2.rundll32.exe.2f443a8.1.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.4a4148.0.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 5.2.rundll32.exe.30f42a8.0.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| 3.2.rundll32.exe.4a4148.0.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security | |
| Click to see the 7 entries | | | | |

# Sigma Overview

**System Summary:**

**Sigma detected: Emotet RunDLL32 Process Creation**

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

## Networking:

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

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

**C2 URLs / IPs found in malware configuration**

## 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)**

## Malware Analysis System Evasion:

**Tries to detect virtualization through RDTSC time measurements**

## HIPS / PFW / Operating System Protection Evasion:

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

## Stealing of Sensitive Information:

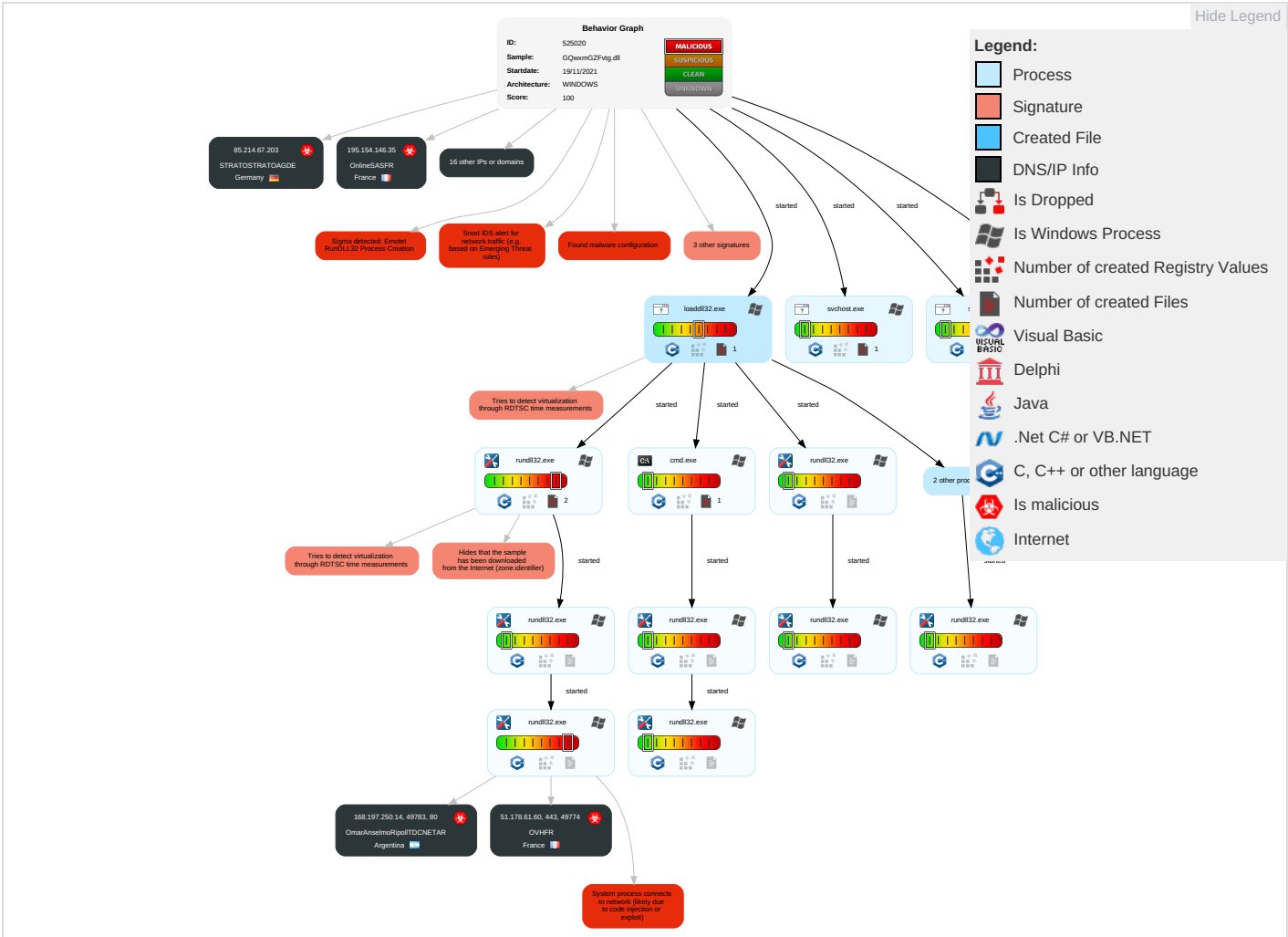
**Yara detected Emotet**

# 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 | Windows Management Instrumentation | 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 | Eavesdr Insecure Network Commur |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 | LSASS Memory | Query Registry 1 | Remote Desktop Protocol | Clipboard Data 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit S Redirect Calls/SM |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 1 2 | Security Account Manager | Security Software Discovery 1 3 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 1 | Exploit S Track De Location |

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Deobfuscate/Decode Files or Information 1 | NTDS | Virtualization/Sandbox Evasion 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 2 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Hidden Files and Directories 1 | LSA Secrets | Process Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Commun |
| 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 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 W Access F |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | File Deletion 1 | Proc Filesystem | System Information Discovery 1 3 4 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgra 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 |
|---|---|---|---|---|
| GQwxmGZFvtg.dll | 18% | Virustotal | | Browse |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| GQwxmGZFvtg.dll | 24% | ReversingLabs | Win32.Infostealer.Convagent | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.2.loaddll32.exe.1450000.1.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 8.2.rundll32.exe.a40000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 2.2.rundll32.exe.930000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 4.2.rundll32.exe.2ba0000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 5.2.rundll32.exe.32a0000.1.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 12.2.rundll32.exe.3160000.0.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 12.2.rundll32.exe.31b4780.1.unpack | 100% | Avira | HEUR/AGEN.1110387 | | Download File |
| 3.2.rundll32.exe.690000.1.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://https://www.disneyplus.com/legal/privacy-policy | 0% | URL Reputation | safe | |
| http://https://168.197.250.14:80/W4 | 0% | Avira URL Cloud | safe | |
| http://https://51.178.61.60/vIaXhjlEiVCJtvEYurwocvmNMaSkNlb | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14/GlobalSign | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14:80/D | 0% | Avira URL Cloud | safe | |
| http://https://51.178.61.60/vIaXhjlEiVCJtvEYurwocvmNMaSkNlb9 | 0% | Avira URL Cloud | safe | |
| http://https://www.tiktok.c | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14:80/OtSInaOjcxTpmnaQwecTWVLWIJIlRyonuNIIpOexeLeibZsTuTWRBEaFrFZGFyKC | 0% | Avira URL Cloud | safe | |
| http://https://disneyplus.com/legal. | 0% | URL Reputation | safe | |
| http://https://168.197.250.14/rosoft | 0% | Avira URL Cloud | safe | |
| http://https://www.tiktok.com/legal/report/feedback | 0% | URL Reputation | safe | |
| http://https://168.197.250.14/ | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14:80/OtSInaOjcxTpmnaQwecTWVLWIJIlRyonuNIIpOexeLeibZsTuTWRBEaFrFZGFy | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14:80/OtSInaOjcxTpmnaQwecTWVLWIJIlRyonuNIIpOexeLeibZsTuTWRBEaFrFZGFy-0 | 0% | Avira URL Cloud | safe | |
| http://help.disneyplus.com. | 0% | URL Reputation | safe | |
| http://https://168.197.250.14:80/ | 0% | Avira URL Cloud | safe | |
| http://https://168.197.250.14:80/OtSInaOjcxTpmnaQwecTWVLWIJIlRyonuNIIpOexeLeibZsTuTWRBEaFrFZGFy3 | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

No contacted domains info

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://51.178.61.60/vIaXhjlEiVCJtvEYurwocvmNMaSkNlb | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 207.148.81.119 | unknown | United States | | 20473 | AS-CHOOPAUS | true |
| 196.44.98.190 | unknown | Ghana | | 327814 | EcobandGH | true |
| 78.46.73.125 | unknown | Germany | | 24940 | HETZNER-ASDE | true |
| 37.59.209.141 | unknown | France | | 16276 | OVHFR | true |
| 85.214.67.203 | unknown | Germany | | 6724 | STRATOSTRATOAGDE | true |
| 191.252.103.16 | unknown | Brazil | | 27715 | LocawebServicosdeInternet SABR | true |
| 45.79.33.48 | unknown | United States | | 63949 | LINODE-APLinodeLLCUS | true |
| 54.37.228.122 | unknown | France | | 16276 | OVHFR | true |
| 185.148.169.10 | unknown | Germany | | 44780 | EVERSCALE-ASDE | true |
| 142.4.219.173 | unknown | Canada | | 16276 | OVHFR | true |
| 54.38.242.185 | unknown | France | | 16276 | OVHFR | true |
| 195.154.146.35 | unknown | France | | 12876 | OnlineSASFR | true |
| 195.77.239.39 | unknown | Spain | | 60493 | FICOSA-ASES | true |
| 78.47.204.80 | unknown | Germany | | 24940 | HETZNER-ASDE | true |
| 168.197.250.14 | unknown | Argentina | | 264776 | OmarAnselmoRipollTDCNET AR | true |
| 51.178.61.60 | unknown | France | | 16276 | OVHFR | true |
| 177.72.80.14 | unknown | Brazil | | 262543 | NewLifeFibraBR | true |
| 66.42.57.149 | unknown | United States | | 20473 | AS-CHOOPAUS | true |
| 37.44.244.177 | unknown | Germany | | 47583 | AS-HOSTINGERLT | true |
| 51.210.242.234 | unknown | France | | 16276 | OVHFR | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 525020 |
| Start date: | 19.11.2021 |
| Start time: | 10:11:59 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 13m 30s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | GQwxmGZFvtg.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: | 25 |
| 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: | mal100.troj.evad.winDLL@27/2@0/20 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 45.6% (good quality ratio 40.5%)<br>• Quality average: 68.2%<br>• Quality standard deviation: 31% |

| | |
|---|---|
| HCA Information: | • Successful, ratio: 61%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .dll<br>• Override analysis time to 240s for rundll32 |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 10:15:27 | API Interceptor | 8x Sleep call for process: svchost.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 207.148.81.119 | wNjqkrm8pH.dll | Get hash | malicious | Browse | |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | |
| | V0gZWRXv8d.dll | Get hash | malicious | Browse | |
| | t5EuQW2GUF.dll | Get hash | malicious | Browse | |
| | uh1WyesPlh.dll | Get hash | malicious | Browse | |
| | 8rryPzJR1p.dll | Get hash | malicious | Browse | |
| | a65FgjVus4.dll | Get hash | malicious | Browse | |
| | bWjYh6H8wk.dll | Get hash | malicious | Browse | |
| | ZJOHKItBoJ.dll | Get hash | malicious | Browse | |
| | eyPPiz3W6u.dll | Get hash | malicious | Browse | |
| | HjYSwxqyUn.dll | Get hash | malicious | Browse | |
| | f47YPsvRI3.dll | Get hash | malicious | Browse | |
| | 2n64VXT08V.dll | Get hash | malicious | Browse | |
| | qUr4bXsweR.dll | Get hash | malicious | Browse | |
| | 52O6evfqQT.dll | Get hash | malicious | Browse | |
| | ONEitXKvz6.dll | Get hash | malicious | Browse | |
| 196.44.98.190 | wNjqkrm8pH.dll | Get hash | malicious | Browse | |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | |
| | V0gZWRXv8d.dll | Get hash | malicious | Browse | |
| | t5EuQW2GUF.dll | Get hash | malicious | Browse | |
| | uh1WyesPlh.dll | Get hash | malicious | Browse | |
| | 8rryPzJR1p.dll | Get hash | malicious | Browse | |
| | a65FgjVus4.dll | Get hash | malicious | Browse | |
| | bWjYh6H8wk.dll | Get hash | malicious | Browse | |
| | ZJOHKItBoJ.dll | Get hash | malicious | Browse | |
| | eyPPiz3W6u.dll | Get hash | malicious | Browse | |
| | HjYSwxqyUn.dll | Get hash | malicious | Browse | |
| | f47YPsvRI3.dll | Get hash | malicious | Browse | |
| | 2n64VXT08V.dll | Get hash | malicious | Browse | |
| | qUr4bXsweR.dll | Get hash | malicious | Browse | |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 52O6evfqQT.dll | Get hash | malicious | Browse | |
| | ONEitXKvz6.dll | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AS-CHOOPAUS | RFQ DETAILS.xlsx | Get hash | malicious | Browse | • 149.28.171.238 |
| | vgVQ5S6MxN.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | vgVQ5S6MxN.exe | Get hash | malicious | Browse | • 149.28.253.196 |
| | qa7tRJ7QVe.exe | Get hash | malicious | Browse | • 216.128.137.31 |
| | DHL_AWB_NO907853880911.xlsx | Get hash | malicious | Browse | • 185.175.156.30 |
| | wNjqkrm8pH.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | V0gZWRXv8d.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | t5EuQW2GUF.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | uh1WyesPlh.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | 8rryPzJR1p.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | a65FgjVus4.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | bWjYh6H8wk.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | ZJOHKItBoJ.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | eyPPiz3W6u.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| | HjYSwxqyUn.dll | Get hash | malicious | Browse | • 66.42.57.149 |
| EcobandGH | wNjqkrm8pH.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | V0gZWRXv8d.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | t5EuQW2GUF.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | uh1WyesPlh.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | 8rryPzJR1p.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | a65FgjVus4.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | bWjYh6H8wk.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | ZJOHKItBoJ.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | eyPPiz3W6u.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | HjYSwxqyUn.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | f47YPsvRI3.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | 2n64VXT08V.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | qUr4bXsweR.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | 52O6evfqQT.dll | Get hash | malicious | Browse | • 196.44.98.190 |
| | ONEitXKvz6.dll | Get hash | malicious | Browse | • 196.44.98.190 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 51c64c77e60f3980eea90869b68c58a8 | Fuutbqvhmc.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | wNjqkrm8pH.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | V0gZWRXv8d.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | t5EuQW2GUF.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | uh1WyesPlh.dll | Get hash | malicious | Browse | • 51.178.61.60 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 8rryPzJR1p.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | a65FgjVus4.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | bWjYh6H8wk.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | ZJOHKItBoJ.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | eyPPiz3W6u.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | 02D6463C8D80183F843D874AB427C11FC47B6B9CE4726.exe | Get hash | malicious | Browse | • 51.178.61.60 |
| | HjYSwxqyUn.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | f47YPsvRI3.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | 2n64VXT08V.dll | Get hash | malicious | Browse | • 51.178.61.60 |
| | qUr4bXsweR.dll | Get hash | malicious | Browse | • 51.178.61.60 |

## Dropped Files

**No context**

# Created / dropped Files

**C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\rundll32.exe |
| File Type: | Microsoft Cabinet archive data, 61414 bytes, 1 file |
| Category: | dropped |
| Size (bytes): | 61414 |
| Entropy (8bit): | **7.995245868798237** |
| Encrypted: | **true** |
| SSDEEP: | 1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP |
| MD5: | ACAEDA60C79C6BCAC925EEB3653F45E0 |
| SHA1: | 2AAAE490BCDACCC6172240FF1697753B37AC5578 |
| SHA-256: | 6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658 |
| SHA-512: | FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 |
| Malicious: | false |
| Preview: | MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F..._..z....._...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y...,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&..... |

**C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\rundll32.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 328 |
| Entropy (8bit): | 3.118359240275542 |
| Encrypted: | false |
| SSDEEP: | 6:kKnNhk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:z9kPlE99SNxAhUeYlUSA/t |
| MD5: | 92A36CDA1A0A1B0958C46813CFB34973 |
| SHA1: | C532833FEA2C377FCED884D14FCB0DC427A08A73 |
| SHA-256: | 1CD5D904F36CE42BF800D2EFCA13E67337F65207C5C4BF1796247B5D56F8102F |
| SHA-512: | F8D866CA0C4463202F1CE581EE0CB38E5668BA69E0942D7DCECD450FD67B4E6091D2CA858A745397624678BC3A0BB1D2A3BC5191C8B6E0F306C23E8C8DA7DA90 |
| Malicious: | false |
| Preview: | p..... .....%...(..... .....q.\}.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."... |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.178855934216584 |

## General

| | |
|---|---|
| TrID: | • Win32 Dynamic Link Library (generic) (1002004/3) 99.40%<br>• Clipper DOS Executable (2020/12) 0.20%<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: | GQwxmGZFvtg.dll |
| File size: | 485376 |
| MD5: | 3ecb8e8c0baaa4acf5ca647a29ad2989 |
| SHA1: | 5de0548c74dd501454c949dc13a7a4e37e35aceb |
| SHA256: | 7e4d240abe7a3835a088482d21e8f308c678035513631543e370f0f028a2f40e |
| SHA512: | c14b19634604112fd95cef0118b9f8fbdb53102eb1edfdea3c35afb362d6a5a6f1b1dab3334ed2250e36ee125dab794d3eebaa5f86d051ce75dc46fd2cbe0324 |
| SSDEEP: | 12288:bdv8jkvzqZvv2wLBymTi12yD88kYwZ1h1:b2Zvv2c1Ti1v0Z1h |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<br>.....<br>..... |

## File Icon

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

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x10015826 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x10000000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL |
| DLL Characteristics: | DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x61964C08 [Thu Nov 18 12:50:16 2021 UTC] |
| TLS Callbacks: | |
| 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: | 261bae8b02d2e7bf979e55d76b9dc786 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x3930c | 0x39400 | False | 0.530729735262 | data | 6.66187646144 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x3b000 | 0x13cfe | 0x13e00 | False | 0.464512087264 | data | 5.41556152438 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x4f000 | 0x252c | 0x1800 | False | 0.223795572917 | data | 3.845062089 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x52000 | 0x24410 | 0x24600 | False | 0.818520457474 | data | 7.74951937622 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .reloc | 0x77000 | 0x33a0 | 0x3400 | False | 0.71484375 | data | 6.58405020621 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Exports

### Version Infos

### Possible Origin

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

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 11/19/21-10:14:40.027395 | TCP | 2404334 | ET CNC Feodo Tracker Reported CnC Server TCP group 18 | 49774 | 443 | 192.168.2.4 | 51.178.61.60 |
| 11/19/21-10:15:13.169990 | TCP | 2404312 | ET CNC Feodo Tracker Reported CnC Server TCP group 7 | 49783 | 80 | 192.168.2.4 | 168.197.250.14 |
| 11/19/21-10:15:13.697104 | TCP | 2021013 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC) | 80 | 49783 | 168.197.250.14 | 192.168.2.4 |

## Network Port Distribution

### TCP Packets

### HTTP Request Dependency Graph

- 51.178.61.60

### HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.4 | 49774 | 51.178.61.60 | 443 | C:\Windows\SysWOW64\rundll32.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-11-19 09:14:40 UTC | 0 | OUT | GET /vIaXhjlEiVCJtvEYurwocvmNMaSkNlb HTTP/1.1<br>Cookie: DGOfLuguTgt=UBN56B3QU+Tc+Xgq31bg3f9Hc8SeJtGwRW8cIQG0AjCXtu7IVNtnsz2CZP6/nHbvDL2M+GXz6pqgLLehfHZd2GGYpuU8uQKdmhGRacOnQW/ucq9cf8VNNBbQNPbhaJyv0XRSuZSYFPtFB7LZ1OorndJDYNrS7ph90Fj+KdcaTImxvaL1Qs5Z6UL4ThHUhcfK77E//BWfq9+pJEy7ddTtLK+8K0+70BY+tADtOTnA6uo2ueeAlbD3B8i85HcUUZx7mjc28/XQaTOUj2m814xjTOmgG7kxOyfQBdcReokKXCbScsmno86poBr9V773eA2kw1LMUwfE<br>Host: 51.178.61.60<br>Connection: Keep-Alive<br>Cache-Control: no-cache |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: loaddll32.exe PID: 3228 Parent PID: 5664

### General

| | |
|---|---|
| Start time: | 10:12:58 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\System32\loaddll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | loaddll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll" |
| Imagebase: | 0x1320000 |
| 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_1, Description: Yara detected Emotet, Source: 00000000.00000002.796379773.0000000000F4A000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: cmd.exe PID: 4720 Parent PID: 3228

### General

| | |
|---|---|
| Start time: | 10:12:58 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.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: 5244 Parent PID: 3228

### General

| | |
|---|---|
| Start time: | 10:12:58 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,Control_RunDLL |
| Imagebase: | 0xa70000 |
| 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: 00000002.00000002.776937820.0000000002C55000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: rundll32.exe PID: 2932 Parent PID: 4720

### General

| | |
|---|---|
| Start time: | 10:12:58 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",#1 |
| Imagebase: | 0xa70000 |
| 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: 00000003.00000002.776035801.000000000048A000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 6136 Parent PID: 3228

### General

| | |
|---|---|
| Start time: | 10:13:03 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,abziuleoxsborpb |
| Imagebase: | 0xa70000 |
| 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: 00000004.00000002.792999078.0000000002F2A000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 2016 Parent PID: 3228

### General

| | |
|---|---|
| Start time: | 10:13:07 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | rundll32.exe C:\Users\user\Desktop\GQwxmGZFvtg.dll,aejkroaebsbxdnkhb |
| Imagebase: | 0xa70000 |
| 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: 00000005.00000002.795842266.00000000030DA000.00000004.00000020.sdmp, Author: Joe Security |
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 5576 Parent PID: 2932

### General

| | |
|---|---|
| Start time: | 10:13:38 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL |
| Imagebase: | 0xa70000 |
| 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: 5480 Parent PID: 5244

### General

| | |
|---|---|
| Start time: | 10:13:39 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Gbdnfdnwgwzcefyt\nlnmlmepgkdbq.udp",iHIeY |
| Imagebase: | 0xa70000 |
| 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: 00000008.00000002.829087525.0000000002B9A000.00000004.00000020.sdmp, Author: Joe Security |

| | |
|---|---|
| Reputation: | high |

## Analysis Process: rundll32.exe PID: 2224 Parent PID: 6136

### General

| | |
|---|---|
| Start time: | 10:13:47 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL |
| Imagebase: | 0xa70000 |
| 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: 2240 Parent PID: 2016

### General

| | |
|---|---|
| Start time: | 10:13:55 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL |
| Imagebase: | 0xa70000 |
| 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: 4544 Parent PID: 3228

### General

| | |
|---|---|
| Start time: | 10:13:55 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\GQwxmGZFvtg.dll",Control_RunDLL |
| Imagebase: | 0xa70000 |
| File size: | 61952 bytes |
| MD5 hash: | D7CA562B0DB4F4DD0F03A89A1FDAD63D |
| 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: 4928 Parent PID: 5480

### General

| | |
|---|---|
| Start time: | 10:14:10 |
| Start date: | 19/11/2021 |
| Path: | C:\Windows\SysWOW64\rundll32.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Gbdnfdnwgwzcefyt\nlnmlmepgkdbq.udp",Control_RunDLL |
| Imagebase: | 0xa70000 |
| 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.00000002.1195922556.000000000319A000.00000004.00000020.sdmp, Author: Joe Security |

File Activities | Show Windows behavior

## Analysis Process: svchost.exe PID: 3716 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 10:14:25 |
| Start date: | 19/11/2021 |
| 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: svchost.exe PID: 5320 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 10:14:53 |
| Start date: | 19/11/2021 |
| 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: svchost.exe PID: 4128 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 10:15:14 |
| Start date: | 19/11/2021 |
| 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: svchost.exe PID: 5740 Parent PID: 568

### General

| | |
|---|---|
| Start time: | 10:15:25 |
| Start date: | 19/11/2021 |
| 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

# Disassembly

## Code Analysis