

JoeSandbox Cloud BASIC



**ID:** 745034

**Sample Name:** gdazhx1EIP.exe

**Cookbook:** default.jbs

**Time:** 18:00:18

**Date:** 13/11/2022

**Version:** 36.0.0 Rainbow Opal

# Table of Contents

|                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------|----|
| Table of Contents                                                                                   | 2  |
| Windows Analysis Report gdazhx1EIP.exe                                                              | 4  |
| Overview                                                                                            | 4  |
| General Information                                                                                 | 4  |
| Detection                                                                                           | 4  |
| Signatures                                                                                          | 4  |
| Classification                                                                                      | 4  |
| Process Tree                                                                                        | 4  |
| Malware Configuration                                                                               | 4  |
| Threatname: Emotet                                                                                  | 4  |
| Yara Signatures                                                                                     | 5  |
| Memory Dumps                                                                                        | 5  |
| Unpacked PEs                                                                                        | 5  |
| Sigma Signatures                                                                                    | 6  |
| Snort Signatures                                                                                    | 6  |
| Joe Sandbox Signatures                                                                              | 6  |
| AV Detection                                                                                        | 6  |
| Networking                                                                                          | 6  |
| E-Banking Fraud                                                                                     | 6  |
| Boot Survival                                                                                       | 6  |
| Hooking and other Techniques for Hiding and Protection                                              | 6  |
| HIPS / PFW / Operating System Protection Evasion                                                    | 6  |
| Stealing of Sensitive Information                                                                   | 7  |
| Mitre Att&ck Matrix                                                                                 | 7  |
| Behavior Graph                                                                                      | 7  |
| Screenshots                                                                                         | 8  |
| Thumbnails                                                                                          | 8  |
| Antivirus, Machine Learning and Genetic Malware Detection                                           | 9  |
| Initial Sample                                                                                      | 9  |
| Dropped Files                                                                                       | 9  |
| Unpacked PE Files                                                                                   | 9  |
| Domains                                                                                             | 10 |
| URLs                                                                                                | 10 |
| Domains and IPs                                                                                     | 10 |
| Contacted Domains                                                                                   | 10 |
| URLs from Memory and Binaries                                                                       | 10 |
| World Map of Contacted IPs                                                                          | 10 |
| Public IPs                                                                                          | 11 |
| General Information                                                                                 | 12 |
| Warnings                                                                                            | 13 |
| Simulations                                                                                         | 13 |
| Behavior and APIs                                                                                   | 13 |
| Joe Sandbox View / Context                                                                          | 13 |
| IPs                                                                                                 | 13 |
| Domains                                                                                             | 13 |
| ASNs                                                                                                | 13 |
| JA3 Fingerprints                                                                                    | 13 |
| Dropped Files                                                                                       | 13 |
| Created / dropped Files                                                                             | 14 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506  | 14 |
| C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 | 14 |
| Static File Info                                                                                    | 14 |
| General                                                                                             | 14 |
| File Icon                                                                                           | 14 |
| Static PE Info                                                                                      | 15 |
| General                                                                                             | 15 |
| Entrypoint Preview                                                                                  | 15 |
| Rich Headers                                                                                        | 17 |
| Data Directories                                                                                    | 17 |
| Sections                                                                                            | 17 |
| Resources                                                                                           | 18 |
| Imports                                                                                             | 18 |
| Exports                                                                                             | 18 |
| Possible Origin                                                                                     | 18 |
| Network Behavior                                                                                    | 18 |
| Snort IDS Alerts                                                                                    | 18 |
| Network Port Distribution                                                                           | 18 |
| TCP Packets                                                                                         | 19 |
| Statistics                                                                                          | 19 |
| Behavior                                                                                            | 19 |
| System Behavior                                                                                     | 20 |
| Analysis Process: loaddll64.exePID: 5948, Parent PID: 3452                                          | 20 |

|                                                           |    |
|-----------------------------------------------------------|----|
| General                                                   | 20 |
| File Activities                                           | 20 |
| Analysis Process: conhost.exePID: 5944, Parent PID: 5948  | 20 |
| General                                                   | 20 |
| Analysis Process: cmd.exePID: 5048, Parent PID: 5948      | 21 |
| General                                                   | 21 |
| File Activities                                           | 21 |
| Analysis Process: regsvr32.exePID: 676, Parent PID: 5948  | 21 |
| General                                                   | 21 |
| File Activities                                           | 21 |
| Analysis Process: rundll32.exePID: 2436, Parent PID: 5048 | 22 |
| General                                                   | 22 |
| File Activities                                           | 22 |
| File Deleted                                              | 22 |
| Analysis Process: rundll32.exePID: 4252, Parent PID: 5948 | 22 |
| General                                                   | 22 |
| File Activities                                           | 22 |
| Analysis Process: regsvr32.exePID: 5244, Parent PID: 2436 | 23 |
| General                                                   | 23 |
| File Activities                                           | 23 |
| Registry Activities                                       | 23 |
| Key Value Created                                         | 23 |
| Analysis Process: regsvr32.exePID: 5204, Parent PID: 676  | 23 |
| General                                                   | 23 |
| File Activities                                           | 23 |
| Analysis Process: regsvr32.exePID: 4896, Parent PID: 4252 | 24 |
| General                                                   | 24 |
| File Activities                                           | 24 |
| Analysis Process: regsvr32.exePID: 5444, Parent PID: 5948 | 24 |
| General                                                   | 24 |
| File Activities                                           | 24 |
| Analysis Process: regsvr32.exePID: 2356, Parent PID: 3452 | 24 |
| General                                                   | 24 |
| File Activities                                           | 25 |
| Analysis Process: regsvr32.exePID: 3092, Parent PID: 2356 | 25 |
| General                                                   | 25 |
| File Activities                                           | 25 |
| Disassembly                                               | 25 |

# Windows Analysis Report

gdazhx1EIP.exe

## Overview

### General Information

Sample Name:

gdazhx1EIP.exe  
(renamed file extension from exe to dll)

Analysis ID:

745034

MD5:

6b304d058ae078.

SHA1:

f416b3c02d4f174..

SHA256:

5b2039d5a1ba30.

Tags:

dll

exe

Infos:

### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Emotet

Score:

84

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Multi AV Scanner detection for subm...

Yara detected Emotet

System process connects to network...

Snort IDS alert for network traffic

Creates an autostart registry key po...

C2 URLs / IPs found in malware con...

Hides that the sample has been dow...

Queries the volume information (nam...

Contains functionality to check if a d...

Deletes files inside the Windows fol...

May sleep (evasive loops) to hinder...

Uses code obfuscation techniques (...)

### Classification

## Process Tree

System is w10x64

loadll64.exe

(PID: 5948 cmdline: loadll64.exe "C:\Users\user\Desktop\gdazhx1EIP.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)

conhost.exe

(PID: 5944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

cmd.exe

(PID: 5048 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\gdazhx1EIP.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

rundll32.exe

(PID: 2436 cmdline: rundll32.exe "C:\Users\user\Desktop\gdazhx1EIP.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)

regsvr32.exe

(PID: 5244 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\lhDzTHldHNg.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 676 cmdline: regsvr32.exe /s C:\Users\user\Desktop\gdazhx1EIP.dll MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 5204 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\VGdnyYmEzk\YPPr.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

rundll32.exe

(PID: 4252 cmdline: rundll32.exe C:\Users\user\Desktop\gdazhx1EIP.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)

regsvr32.exe

(PID: 4896 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XeFicoVt\wPzeOKW.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 5444 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MtAvdtxCdYblye\mPrkhfVupthqSBxp.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 2356 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\lhDzTHldHNg.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

regsvr32.exe

(PID: 3092 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\EHrtIMNuOOxGFcDTWQXzuCij.dll" MD5: D78B75FC68247E8A63ACBA846182740E)

cleanup

## Malware Configuration

Threatname: Emotet

Copyright Joe Security LLC 2022

Page 4 of 25

```
{
  "C2 list": [
    "172.105.115.71:8080",
    "218.38.121.17:443",
    "186.250.48.5:443",
    "103.71.99.57:8080",
    "85.214.67.203:8080",
    "85.25.120.45:8080",
    "139.196.72.155:8080",
    "103.85.95.4:8080",
    "198.199.70.22:8080",
    "209.239.112.82:8080",
    "78.47.204.80:443",
    "36.67.23.59:443",
    "104.244.79.94:443",
    "62.171.178.147:8080",
    "195.77.239.39:8080",
    "103.56.149.105:8080",
    "80.211.107.116:8080",
    "93.104.209.107:8080",
    "174.138.33.49:7080",
    "202.28.34.99:8080",
    "178.62.112.199:8080",
    "114.79.130.68:443",
    "118.98.72.86:443",
    "103.41.204.169:8080",
    "178.238.225.252:8080",
    "83.229.80.93:8080",
    "46.101.98.60:8080",
    "82.98.180.154:7080",
    "87.106.97.83:7080",
    "196.44.98.190:8080",
    "139.59.80.108:8080",
    "103.224.241.74:8080",
    "103.254.12.236:7080",
    "185.148.169.10:8080",
    "165.22.254.236:8080",
    "37.44.244.177:8080",
    "54.37.228.122:443",
    "51.75.33.122:443",
    "128.199.217.206:443",
    "188.165.79.151:443",
    "210.57.209.142:8080",
    "160.16.143.191:8080",
    "175.126.176.79:8080",
    "202.134.4.210:7080",
    "103.126.216.86:443",
    "190.145.8.4:443",
    "128.199.242.164:8080",
    "64.227.55.231:8080"
  ]
}
```

| Yara Signatures                                                                       |                      |                      |              |         |
|---------------------------------------------------------------------------------------|----------------------|----------------------|--------------|---------|
| Memory Dumps                                                                          |                      |                      |              |         |
| Source                                                                                | Rule                 | Description          | Author       | Strings |
| 00000006.00000002.771127294.0000000180001000.00000020.00001000.00020000.00000000.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 00000004.00000002.261854248.0000018104890000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 00000006.00000002.769097156.000000000490000.00000040.00001000.00020000.00000000.sdmp  | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 00000013.00000002.415103190.00000000028E0000.00000040.00001000.00020000.00000000.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 00000013.00000002.415208554.0000000180001000.00000020.00001000.00020000.00000000.sdmp | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| Click to see the 7 entries                                                            |                      |                      |              |         |

| Unpacked PEs                              |                      |                      |              |         |
|-------------------------------------------|----------------------|----------------------|--------------|---------|
| Source                                    | Rule                 | Description          | Author       | Strings |
| 4.2.rundll32.exe.18104890000.0.raw.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 3.2.regsvr32.exe.b60000.0.raw.unpack      | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |

| Source                                  | Rule                 | Description          | Author       | Strings |
|-----------------------------------------|----------------------|----------------------|--------------|---------|
| 0.2.load.dll64.exe.1fd03f10000.0.unpack | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 6.2.regsvr32.exe.490000.0.raw.unpack    | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| 19.2.regsvr32.exe.28e0000.0.unpack      | JoeSecurity_Emotet_1 | Yara detected Emotet | Joe Security |         |
| Click to see the 7 entries              |                      |                      |              |         |

## Sigma Signatures

 No Sigma rule has matched

## Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.3 - Destination IP: 115.178.55.22

|                   |                                                                 |
|-------------------|-----------------------------------------------------------------|
| Timestamp:        | 192.168.2.3115.178.55.2249698802404304 11/13/22-18:01:59.432679 |
| SID:              | 2404304                                                         |
| Source Port:      | 49698                                                           |
| Destination Port: | 80                                                              |
| Protocol:         | TCP                                                             |
| Classtype:        | A Network Trojan was detected                                   |

## Joe Sandbox Signatures

### AV Detection



Multi AV Scanner detection for submitted file

### Networking



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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

### E-Banking Fraud



Yara detected Emotet

### Boot Survival



Creates an autostart registry key pointing to binary in C:\Windows

### 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)

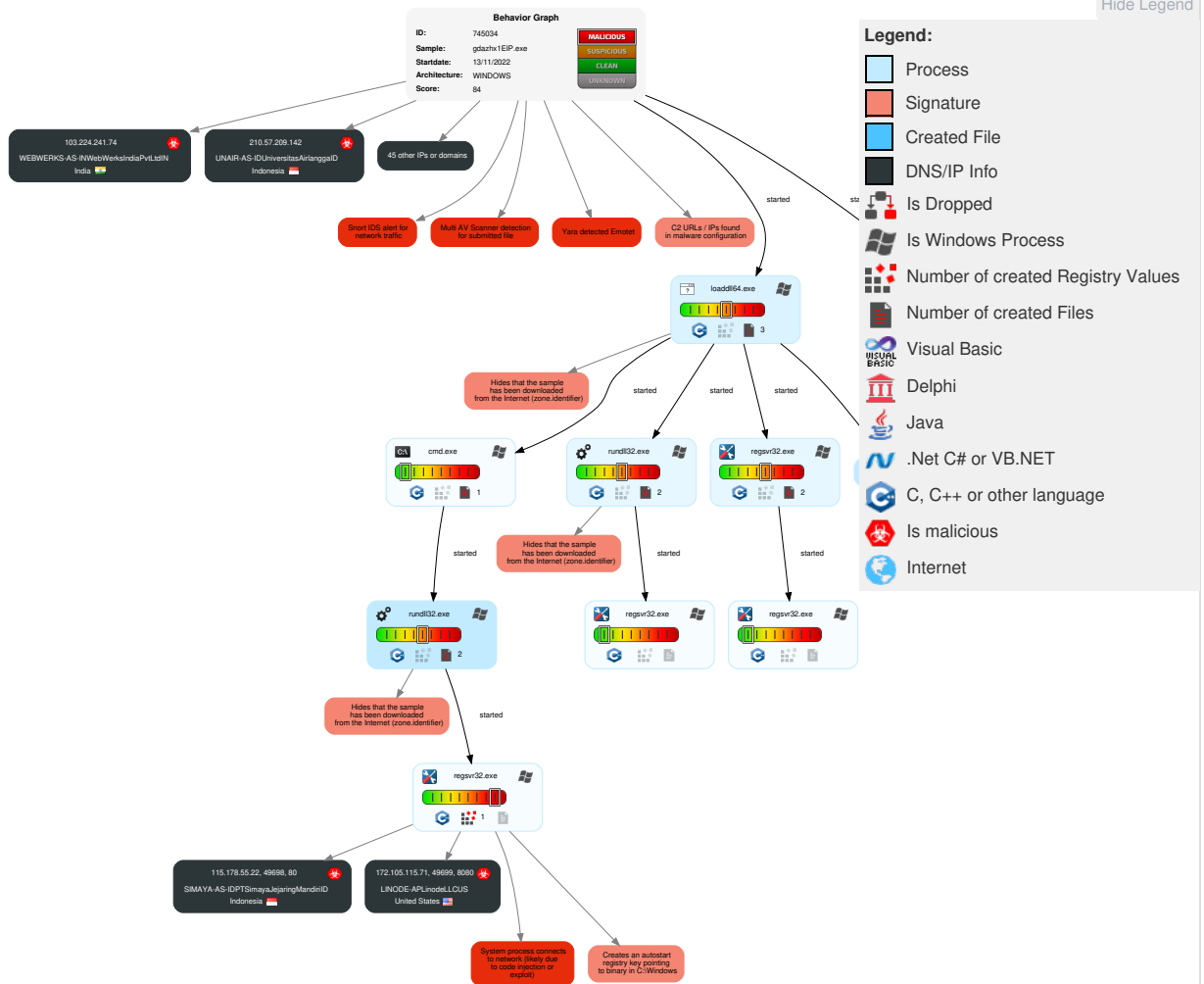


Yara detected Emotet

## Mitre Att&ck Matrix

| Initial Access                      | Execution                          | Persistence                                             | Privilege Escalation                                    | Defense Evasion                                 | Credential Access           | Discovery                                         | Lateral Movement                   | Collection                         | Exfiltration                                           | Command and Control                    | Network Effects                             | Remote Service Effects                      | Impact                                   |
|-------------------------------------|------------------------------------|---------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------|-----------------------------|---------------------------------------------------|------------------------------------|------------------------------------|--------------------------------------------------------|----------------------------------------|---------------------------------------------|---------------------------------------------|------------------------------------------|
| Valid Accounts                      | Windows Management Instrumentation | <b>1</b> <b>1</b><br>Registry Run Keys / Startup Folder | <b>1</b> <b>1</b> <b>1</b><br>Process Injection         | <b>2</b> <b>1</b><br>Masquerading               | OS Credential Dumping       | <b>1</b><br>System Time Discovery                 | Remote Services                    | <b>1</b><br>Archive Collected Data | Exfiltration Over Other Network Medium                 | <b>2</b><br>Encrypted Channel          | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition                  |
| Default Accounts                    | Scheduled Task/Job                 | <b>1</b><br>DLL Side-Loading                            | <b>1</b> <b>1</b><br>Registry Run Keys / Startup Folder | <b>1</b><br>Virtualization/Sandbox Evasion      | LSASS Memory                | <b>2</b> <b>1</b><br>Security Software Discovery  | Remote Desktop Protocol            | Data from Removable Media          | Exfiltration Over Bluetooth                            | <b>1</b><br>Application Layer Protocol | Exploit SS7 to Redirect Phone Calls/SMS     | Remotely Wipe Data Without Authorization    | Device Lockout                           |
| Domain Accounts                     | At (Linux)                         | Logon Script (Windows)                                  | <b>1</b><br>DLL Side-Loading                            | <b>1</b> <b>1</b> <b>1</b><br>Process Injection | Security Account Manager    | <b>1</b><br>Virtualization/Sandbox Evasion        | SMB/Windows Admin Shares           | Data from Network Shared Drive     | Automated Exfiltration                                 | Steganography                          | Exploit SS7 to Track Device Location        | Obtain Device Cloud Backups                 | Delete Device Data                       |
| Local Accounts                      | At (Windows)                       | Logon Script (Mac)                                      | Logon Script (Mac)                                      | <b>1</b><br>Hidden Files and Directories        | NTDS                        | <b>2</b><br>Process Discovery                     | Distributed Component Object Model | Input Capture                      | Scheduled Transfer                                     | Protocol Impersonation                 | SIM Card Swap                               |                                             | Carrier Billing Fraud                    |
| Cloud Accounts                      | Cron                               | Network Logon Script                                    | Network Logon Script                                    | <b>1</b><br>Obfuscated Files or Information     | LSA Secrets                 | <b>1</b><br>Remote System Discovery               | SSH                                | Keylogging                         | Data Transfer Size Limits                              | Fallback Channels                      | Manipulate Device Communication             |                                             | Manipulate App Store Rankings or Ratings |
| Replication Through Removable Media | Launchd                            | Rc.common                                               | Rc.common                                               | <b>1</b><br>Regsvr32                            | Cached Domain Credentials   | <b>2</b><br>File and Directory Discovery          | VNC                                | GUI Input Capture                  | Exfiltration Over C2 Channel                           | Multiband Communication                | Jamming or Denial of Service                |                                             | Abuse Accessibility Features             |
| External Remote Services            | Scheduled Task                     | Startup Items                                           | Startup Items                                           | <b>1</b><br>Rundll32                            | DCSync                      | <b>2</b> <b>4</b><br>System Information Discovery | Windows Remote Management          | Web Portal Capture                 | Exfiltration Over Alternative Protocol                 | Commonly Used Port                     | Rogue Wi-Fi Access Points                   |                                             | Data Encrypted for Impact                |
| Drive-by Compromise                 | Command and Scripting Interpreter  | Scheduled Task/Job                                      | Scheduled Task/Job                                      | <b>1</b><br>DLL Side-Loading                    | Proc Filesystem             | Network Service Scanning                          | Shared Webroot                     | Credential API Hooking             | Exfiltration Over Symmetric Encrypted Non-C2 Protocol  | Application Layer Protocol             | Downgrade to Insecure Protocols             |                                             | Generate Fraudulent Advertising Revenue  |
| Exploit Public-Facing Application   | PowerShell                         | At (Linux)                                              | At (Linux)                                              | <b>1</b><br>File Deletion                       | /etc/passwd and /etc/shadow | System Network Connections Discovery              | Software Deployment Tools          | Data Staged                        | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Web Protocols                          | Rogue Cellular Base Station                 |                                             | Data Destruction                         |

## 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                   |
|----------------|-----------|------------|-------|------------------------|
| gdazhx1EIP.dll | 44%       | Virustotal |       | <a href="#">Browse</a> |

### Dropped Files

|                      |
|----------------------|
| No Antivirus matches |
|----------------------|

### Unpacked PE Files

| Source                                 | Detection | Scanner | Label                 | Link | Download                      |
|----------------------------------------|-----------|---------|-----------------------|------|-------------------------------|
| 4.2.rundll32.exe.18104890000.0.unpack  | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |
| 19.2.regsvr32.exe.28e0000.0.unpack     | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |
| 3.2.regsvr32.exe.b60000.0.unpack       | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |
| 5.2.rundll32.exe.222d2e50000.0.unpack  | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |
| 6.2.regsvr32.exe.490000.0.unpack       | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |
| 0.2.loaddll64.exe.1fd03f10000.0.unpack | 100%      | Avira   | HEUR/AGEN.12<br>15461 |      | <a href="#">Download File</a> |

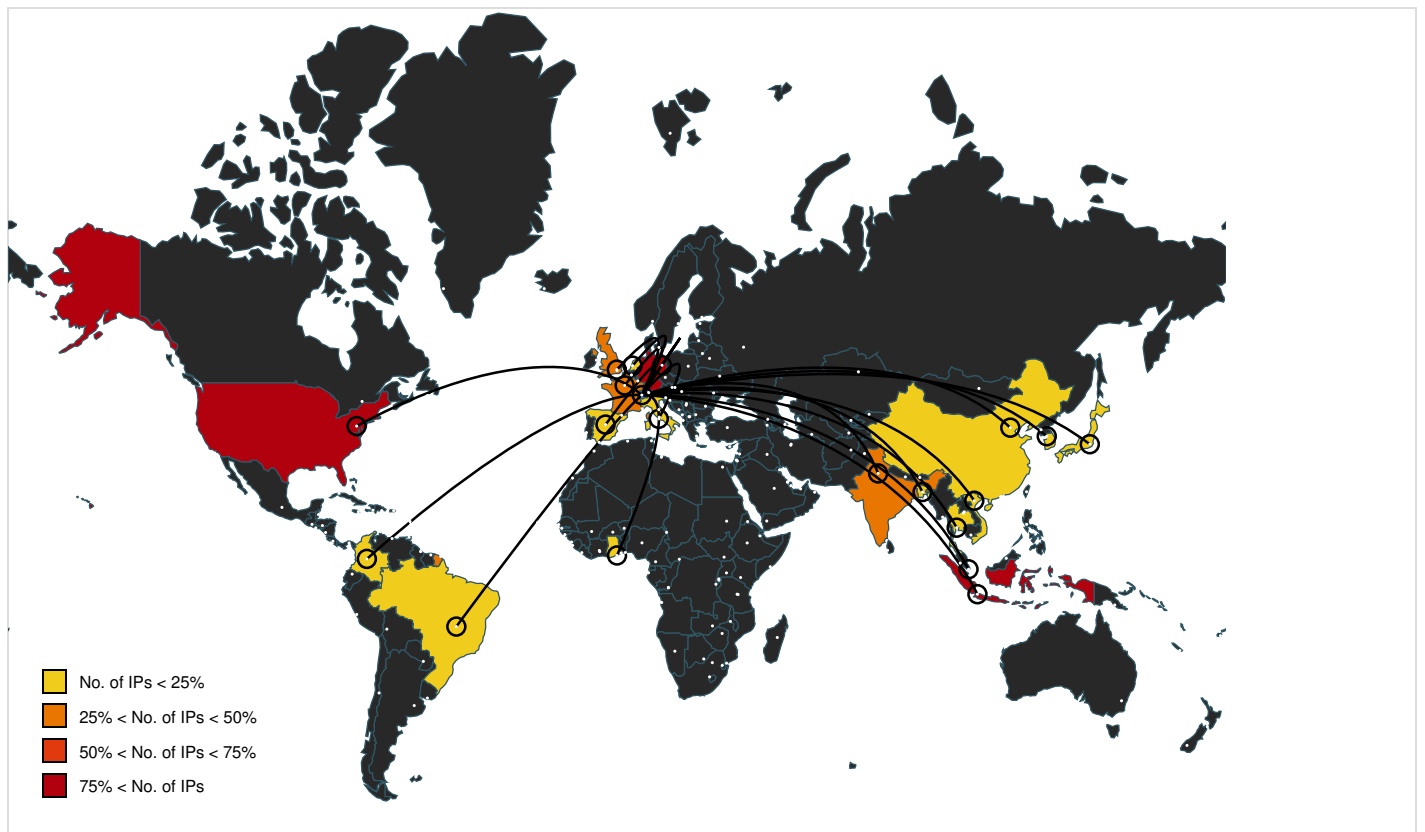
|                                                                                                        |
|--------------------------------------------------------------------------------------------------------|
| <b>Domains</b>                                                                                         |
|  No Antivirus matches |

| <b>URLs</b>                                              |           |                 |       |      |
|----------------------------------------------------------|-----------|-----------------|-------|------|
| Source                                                   | Detection | Scanner         | Label | Link |
| http://https://172.105.115.71:8080/lsug/nhhwenwy/qahixm/ | 0%        | Avira URL Cloud | safe  |      |
| http://https://172.105.115.71:8080/                      | 0%        | Avira URL Cloud | safe  |      |
| http://https://112.105.115.71:8080/                      | 0%        | Avira URL Cloud | safe  |      |

|                                                                                                             |
|-------------------------------------------------------------------------------------------------------------|
| <b>Domains and IPs</b>                                                                                      |
| <b>Contacted Domains</b>                                                                                    |
|  No contacted domains info |

| <b>URLs from Memory and Binaries</b>                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |                                                                         |            |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------|------------|
| Name                                                         | Source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Malicious | Antivirus Detection                                                     | Reputation |
| http://https://172.105.115.71:8080/                          | regsvr32.exe, 00000006.00000003.50545383<br>6.000000000051A000.00000004.00000020.000<br>20000.00000000.sdmp, regsvr32.exe, 00000<br>006.00000003.382745999.000000000051A000.<br>00000004.00000020.00020000.00000000.sdmp,<br>regsvr32.exe, 00000006.00000003.504752<br>110.000000000051A000.00000004.00000020.0<br>0020000.00000000.sdmp, regsvr32.exe, 000<br>00006.00000002.769713040.000000000051A00<br>0.00000004.00000020.00020000.00000000.sdmp                                                                                                                 | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| http://https://112.105.115.71:8080/                          | regsvr32.exe, 00000006.00000003.50519030<br>2.000000000053B000.00000004.00000020.000<br>20000.00000000.sdmp, regsvr32.exe, 00000<br>006.00000003.383008257.0000000000533000.<br>00000004.00000020.00020000.00000000.sdmp,<br>regsvr32.exe, 00000006.00000003.505078<br>011.0000000000534000.00000004.00000020.0<br>0020000.00000000.sdmp                                                                                                                                                                                                                              | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |
| http://<br>https://172.105.115.71:8080/lsug/nhhwenwy/qahixm/ | regsvr32.exe, 00000006.00000003.38300825<br>7.0000000000533000.00000004.00000020.000<br>20000.00000000.sdmp, regsvr32.exe, 00000<br>006.00000003.505360051.0000000000534000.<br>00000004.00000020.00020000.00000000.sdmp,<br>regsvr32.exe, 00000006.00000003.505078<br>011.0000000000534000.00000004.00000020.0<br>0020000.00000000.sdmp, regsvr32.exe, 000<br>00006.00000002.769331647.00000000004C800<br>0.00000004.00000020.00020000.00000000.sdmp,<br>regsvr32.exe, 00000006.00000002.769796168.0000<br>000000534000.00000004.00000020.00020000.<br>00000000.sdmp | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |

|                                   |
|-----------------------------------|
| <b>World Map of Contacted IPs</b> |
|-----------------------------------|



| Public IPs      |         |                   |      |        |                                                   |           |
|-----------------|---------|-------------------|------|--------|---------------------------------------------------|-----------|
| IP              | Domain  | Country           | Flag | ASN    | ASN Name                                          | Malicious |
| 172.105.115.71  | unknown | United States     |      | 63949  | LINODE-APLinodeLLCUS                              | true      |
| 188.165.79.151  | unknown | France            |      | 16276  | OVHFR                                             | true      |
| 196.44.98.190   | unknown | Ghana             |      | 327814 | EcobandGH                                         | true      |
| 174.138.33.49   | unknown | United States     |      | 14061  | DIGITALOCEAN-ASNUS                                | true      |
| 36.67.23.59     | unknown | Indonesia         |      | 17974  | TELKOMNET-AS2-APPTTelekomunikasiIndonesialD       | true      |
| 103.41.204.169  | unknown | Indonesia         |      | 58397  | INFINYS-AS-IDPTInfynsSystemIndonesiaID            | true      |
| 85.214.67.203   | unknown | Germany           |      | 6724   | STRATOSTRATOAGDE                                  | true      |
| 83.229.80.93    | unknown | United Kingdom    |      | 8513   | SKYVISIONGB                                       | true      |
| 198.199.70.22   | unknown | United States     |      | 14061  | DIGITALOCEAN-ASNUS                                | true      |
| 93.104.209.107  | unknown | Germany           |      | 8767   | MNET-ASGermanyDE                                  | true      |
| 186.250.48.5    | unknown | Brazil            |      | 262807 | RedfoxTelecomunicacoesLtdaBR                      | true      |
| 209.239.112.82  | unknown | United States     |      | 30083  | AS-30083-GO-DADDY-COM-LLCUS                       | true      |
| 175.126.176.79  | unknown | Korea Republic of |      | 9523   | MOKWON-AS-KRMokwonUniversityKR                    | true      |
| 128.199.242.164 | unknown | United Kingdom    |      | 14061  | DIGITALOCEAN-ASNUS                                | true      |
| 178.238.225.252 | unknown | Germany           |      | 51167  | CONTABODE                                         | true      |
| 46.101.98.60    | unknown | Netherlands       |      | 14061  | DIGITALOCEAN-ASNUS                                | true      |
| 190.145.8.4     | unknown | Colombia          |      | 14080  | TelmexColombiaSACO                                | true      |
| 82.98.180.154   | unknown | Spain             |      | 42612  | DINAHOSTING-ASES                                  | true      |
| 103.71.99.57    | unknown | India             |      | 135682 | AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN  | true      |
| 87.106.97.83    | unknown | Germany           |      | 8560   | ONEANDONE-ASBrauerstrasse48DE                     | true      |
| 103.254.12.236  | unknown | Viet Nam          |      | 56151  | DIGISTAR-VNDigiStarCompanyLimitedVN               | true      |
| 103.85.95.4     | unknown | Indonesia         |      | 136077 | IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID | true      |

| IP              | Domain  | Country           | Flag                                                                                | ASN    | ASN Name                                               | Malicious |
|-----------------|---------|-------------------|-------------------------------------------------------------------------------------|--------|--------------------------------------------------------|-----------|
| 202.134.4.210   | unknown | Indonesia         |    | 7713   | TELKOMNET-AS-APPTTelekomunikasiIndonesiaID             | true      |
| 165.22.254.236  | unknown | United States     |    | 14061  | DIGITALOCEAN-ASNUS                                     | true      |
| 78.47.204.80    | unknown | Germany           |    | 24940  | HETZNER-ASDE                                           | true      |
| 118.98.72.86    | unknown | Indonesia         |    | 7713   | TELKOMNET-AS-APPTTelekomunikasiIndonesiaID             | true      |
| 139.59.80.108   | unknown | Singapore         |    | 14061  | DIGITALOCEAN-ASNUS                                     | true      |
| 104.244.79.94   | unknown | United States     |    | 53667  | PONYNETUS                                              | true      |
| 37.44.244.177   | unknown | Germany           |    | 47583  | AS-HOSTINGERLT                                         | true      |
| 51.75.33.122    | unknown | France            |    | 16276  | OVHFR                                                  | true      |
| 160.16.143.191  | unknown | Japan             |    | 9370   | SAKURA-BSAKURAInternetIncJP                            | true      |
| 103.56.149.105  | unknown | Indonesia         |    | 55688  | BEON-AS-IDPTBeonIntermediaID                           | true      |
| 85.25.120.45    | unknown | Germany           |    | 8972   | GD-EMEA-DC-SXB1DE                                      | true      |
| 139.196.72.155  | unknown | China             |    | 37963  | CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd | true      |
| 115.178.55.22   | unknown | Indonesia         |    | 38783  | SIMAYA-AS-IDPTSimayaJaringanMandiriID                  | true      |
| 103.126.216.86  | unknown | Bangladesh        |    | 138482 | SKYVIEW-AS-APSKYVIEWONLINELTDBD                        | true      |
| 128.199.217.206 | unknown | United Kingdom    |    | 14061  | DIGITALOCEAN-ASNUS                                     | true      |
| 114.79.130.68   | unknown | India             |    | 45769  | DVOIS-IND-VoisBroadbandPvtLtdIN                        | true      |
| 103.224.241.74  | unknown | India             |   | 133296 | WEBWERKS-AS-INWebWerksIndiaPvtLtdIN                    | true      |
| 210.57.209.142  | unknown | Indonesia         |  | 38142  | UNAIR-AS-IDUniversitasAirlanggaID                      | true      |
| 202.28.34.99    | unknown | Thailand          |  | 9562   | MSU-TH-APMaharakhamUniversityTH                        | true      |
| 80.211.107.116  | unknown | Italy             |  | 31034  | ARUBA-ASNIT                                            | true      |
| 54.37.228.122   | unknown | France            |  | 16276  | OVHFR                                                  | true      |
| 218.38.121.17   | unknown | Korea Republic of |  | 9318   | SKB-ASSKBBroadbandCoLtdKR                              | true      |
| 185.148.169.10  | unknown | Germany           |  | 44780  | EVERSCALE-ASDE                                         | true      |
| 195.77.239.39   | unknown | Spain             |  | 60493  | FICOSA-ASES                                            | true      |
| 178.62.112.199  | unknown | European Union    |  | 14061  | DIGITALOCEAN-ASNUS                                     | true      |
| 62.171.178.147  | unknown | United Kingdom    |  | 51167  | CONTABODE                                              | true      |
| 64.227.55.231   | unknown | United States     |  | 14061  | DIGITALOCEAN-ASNUS                                     | true      |

## General Information

|                                                    |                                                                                                                      |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 36.0.0 Rainbow Opal                                                                                                  |
| Analysis ID:                                       | 745034                                                                                                               |
| Start date and time:                               | 2022-11-13 18:00:18 +01:00                                                                                           |
| Joe Sandbox Product:                               | CloudBasic                                                                                                           |
| Overall analysis duration:                         | 0h 10m 4s                                                                                                            |
| Hypervisor based Inspection enabled:               | false                                                                                                                |
| Report type:                                       | light                                                                                                                |
| Sample file name:                                  | gdazhx1EIP.exe (renamed file extension from exe to dll)                                                              |
| Cookbook file name:                                | default.jbs                                                                                                          |
| Analysis system description:                       | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 26                                                                                                                   |
| Number of new started drivers analysed:            | 0                                                                                                                    |
| Number of existing processes analysed:             | 0                                                                                                                    |
| Number of existing drivers analysed:               | 0                                                                                                                    |

|                                        |                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of injected processes analysed: | 0                                                                                                                                                                                  |
| Technologies:                          | <ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>                                                   |
| Analysis Mode:                         | default                                                                                                                                                                            |
| Analysis stop reason:                  | Timeout                                                                                                                                                                            |
| Detection:                             | MAL                                                                                                                                                                                |
| Classification:                        | mal84.troj.evad.winDLL@21/2@0/49                                                                                                                                                   |
| EGA Information:                       | <ul style="list-style-type: none"><li>• Successful, ratio: 100%</li></ul>                                                                                                          |
| HDC Information:                       | <ul style="list-style-type: none"><li>• Successful, ratio: 58.8% (good quality ratio 53.4%)</li><li>• Quality average: 60.9%</li><li>• Quality standard deviation: 31.8%</li></ul> |
| HCA Information:                       | <ul style="list-style-type: none"><li>• Successful, ratio: 99%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>                   |
| Cookbook Comments:                     | <ul style="list-style-type: none"><li>• Override analysis time to 240s for rundll32</li></ul>                                                                                      |

### Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 8.238.189.126, 8.241.126.121, 67.26.137.254, 8.238.191.126, 8.248.113.254, 93.184.221.240, 209.197.3.8
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ocsp.digicert.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

### Simulations

#### Behavior and APIs

| Time     | Type            | Description                                                                                                                                                  |
|----------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18:02:53 | API Interceptor | 2x Sleep call for process: regsvr32.exe modified                                                                                                             |
| 18:03:08 | Autostart       | Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run lhDzTIHIdHNg.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\lhDzTIHIdHNg.dll" |

### Joe Sandbox View / Context

#### IPs

 No context

#### Domains

 No context

#### ASNs

 No context

#### JA3 Fingerprints

 No context

#### Dropped Files

 No context

## Created / dropped Files

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



|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Windows\System32\regsvr32.exe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Category:       | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes):   | 62919                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Entropy (8bit): | 7.995280921994772                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Encrypted:      | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:         | 1536:d+OrVxHI7WYf11Yom3xQcRVotPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| MD5:            | 3DCF580A93972319E82CAFBC047D34D5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA1:           | 8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| SHA-256:        | 40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SHA-512:        | 98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Malicious:      | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Preview:        | MSCF.....l.....Q.....GU.....\authroot.stl..O..5..CK..<Tk...c_d....A.K...+d..-%.BJIII.QIR..\$t)Kd.-QQ*...g.....^..~ N=...y....{.4{...W....b.i..j.l.....1...b\0....<br>.Ait.2t.....w.%.&."tL_...4.8L[G...;57....AT.K.....V..K.....(....mzS...G....r."=H.?>.....x&...S%....X.M^..j...A..x.9'.9...A../s..#..4#.....ld.w...B....s.8..(..dj....=L..)s.d.]NxQX8<br>...stV#..K.'7.tH..9u~-2..!..2./.....!..9C./...mP \$.../y.....@p.6.)`...5. 0r.w....@(.. Q....)g.....m..z*.8rR..).].T9r<L....0..`.....c.....;-g...;wk.).....i.c5....{v.u...AS..=.....&:..<br>.....+..P.N..9..EAQ.V.\$s.....B.`Mfe..8.....\$..y.-q9J.....W...2.Q8...O.....i..@'^=X.dG\$.M..#=#...m.h..{9.'...-v..Z...!...z....N...i..^.....d...%Xa~q.@D 0...Y.m.....<br>...&d.4..A..{t=...../t.3_.....?-.....uroP?.d.Z.S..{...\$i....X.\$O..4..N.)....U.Z..P....X,... ..Lg..35..W..s..lc..Ap.]P..8..M..W.....U,...m.u.. =m1...~..!..b...._. |

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

|                 |                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:        | C:\Windows\System32\regsvr32.exe                                                                                                                                                                                                     |
| File Type:      | data                                                                                                                                                                                                                                 |
| Category:       | modified                                                                                                                                                                                                                             |
| Size (bytes):   | 328                                                                                                                                                                                                                                  |
| Entropy (8bit): | 3.1108374798811247                                                                                                                                                                                                                   |
| Encrypted:      | false                                                                                                                                                                                                                                |
| SSDEEP:         | 6:kKehN1HINiN+SkQPIEGYRMY9z+4KIDA3RUeKITAIWRyf1:G/kPIE99SNxAhUexYo1                                                                                                                                                                  |
| MD5:            | 7E8432D99C3E675A0B970703245CE46A                                                                                                                                                                                                     |
| SHA1:           | 1062493A0F10E295E8027BDDD22BE2F9DF3A3485                                                                                                                                                                                             |
| SHA-256:        | A16E46D34FDD97BF2FE6E063F5D7D8A6546BD59FB68737C15F433101675C368A                                                                                                                                                                     |
| SHA-512:        | B58AE9FE660720AD514D1C82B8A5F2C2D3CA6E124B8E9076A85335004DA1125C33D6B22274FFD7CA33766D7D91EFF73BF144690220484DF260BD56D5EEC60F5                                                                                                      |
| Malicious:      | false                                                                                                                                                                                                                                |
| Preview:        | p..... ..L..(.....&.....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.<br>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.e.d.e.4.d.3.9.b.e.8.d.8.1.:0..." |

## Static File Info

### General

|                       |                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File type:            | PE32+ executable (DLL) (GUI) x86-64, for MS Windows                                                                                                                                                                                                                                                                                 |
| Entropy (8bit):       | 6.619145958407103                                                                                                                                                                                                                                                                                                                   |
| TrID:                 | <ul style="list-style-type: none"><li>Win64 Dynamic Link Library (generic) (102004/3) 86.43%</li><li>Win64 Executable (generic) (12005/4) 10.17%</li><li>Generic Win/DOS Executable (2004/3) 1.70%</li><li>DOS Executable Generic (2002/1) 1.70%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%</li></ul> |
| File name:            | gdazhx1EIP.dll                                                                                                                                                                                                                                                                                                                      |
| File size:            | 528896                                                                                                                                                                                                                                                                                                                              |
| MD5:                  | 6b304d058ae0788762f8924d2cad7ef5                                                                                                                                                                                                                                                                                                    |
| SHA1:                 | f416b3c02d4f1746f8a642af253ee0d903b7b083                                                                                                                                                                                                                                                                                            |
| SHA256:               | 5b2039d5a1ba30d90ecd085eb135635f9830f4ae88472e779267e033f7eb4547                                                                                                                                                                                                                                                                    |
| SHA512:               | bb942317497f33c6ba9dfec3e824dacfd59329c1c70949623c0a7850bbfed66ddc8a839814e1e0265de111551a658288c40caa04fc7d3419b35e70afec198706                                                                                                                                                                                                    |
| SSDEEP:               | 6144:mW1239bnTe+Qv7NSEBJ43USaI6Y/jOpXhRikSYI+QALgJlJ1divndEX0n:mW1e9PeexPbjvKSpuvYI+TLgs1dcEX0                                                                                                                                                                                                                                      |
| TLSH:                 | 23B4F829A59E76F0C951A1F5A0420B1595F33C88FEF68EAF03502F296F6F24425F768C                                                                                                                                                                                                                                                              |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS<br>mode....\$......\$.s...\$......\$......\$......e.h.....Rich.....                                                                                                                                                                                                            |

### File Icon



Icon Hash: 74f0e4ecccdce0e4

## Static PE Info

### General

|                             |                                            |
|-----------------------------|--------------------------------------------|
| Entrypoint:                 | 0x1800044e0                                |
| Entrypoint Section:         | .text                                      |
| Digitally signed:           | false                                      |
| Imagebase:                  | 0x180000000                                |
| Subsystem:                  | windows gui                                |
| Image File Characteristics: | EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL |
| DLL Characteristics:        | HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT   |
| Time Stamp:                 | 0x636D6724 [Thu Nov 10 21:03:32 2022 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:                | 81146e0614ccc4eb7174ad2ad695dedb           |

## Entrypoint Preview

### Instruction

```
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FAFC4C55267h
call 00007FAFC4C557F8h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FAFC4C550DCh
int3
int3
int3
inc eax
```

| Instruction                    |
|--------------------------------|
| push ebx                       |
| dec eax                        |
| sub esp, 20h                   |
| dec eax                        |
| mov ebx, ecx                   |
| dec eax                        |
| mov eax, edx                   |
| dec eax                        |
| lea ecx, dword ptr [00033F0Dh] |
| dec eax                        |
| mov dword ptr [ebx], ecx       |
| dec eax                        |
| lea edx, dword ptr [ebx+08h]   |
| xor ecx, ecx                   |
| dec eax                        |
| mov dword ptr [edx], ecx       |
| dec eax                        |
| mov dword ptr [edx+08h], ecx   |
| dec eax                        |
| lea ecx, dword ptr [eax+08h]   |
| call 00007FAFC4C57A61h         |
| dec eax                        |
| lea eax, dword ptr [00033F1Dh] |
| dec eax                        |
| mov dword ptr [ebx], eax       |
| dec eax                        |
| mov eax, ebx                   |
| dec eax                        |
| add esp, 20h                   |
| pop ebx                        |
| ret                            |
| int3                           |
| xor eax, eax                   |
| dec eax                        |
| mov dword ptr [ecx+10h], eax   |
| dec eax                        |
| lea eax, dword ptr [00033F13h] |
| dec eax                        |
| mov dword ptr [ecx+08h], eax   |
| dec eax                        |
| lea eax, dword ptr [00033EF8h] |
| dec eax                        |
| mov dword ptr [ecx], eax       |
| dec eax                        |
| mov eax, ecx                   |
| ret                            |
| int3                           |
| inc eax                        |
| push ebx                       |
| dec eax                        |
| sub esp, 20h                   |
| dec eax                        |
| mov ebx, ecx                   |
| dec eax                        |
| mov eax, edx                   |
| dec eax                        |
| lea ecx, dword ptr [00033EADh] |
| dec eax                        |
| mov dword ptr [ebx], ecx       |

| Instruction                  |
|------------------------------|
| dec eax                      |
| lea edx, dword ptr [ebx+08h] |
| xor ecx, ecx                 |
| dec eax                      |
| mov dword ptr [edx], ecx     |
| dec eax                      |
| mov dword ptr [edx+08h], ecx |
| dec eax                      |
| lea ecx, dword ptr [eax+08h] |

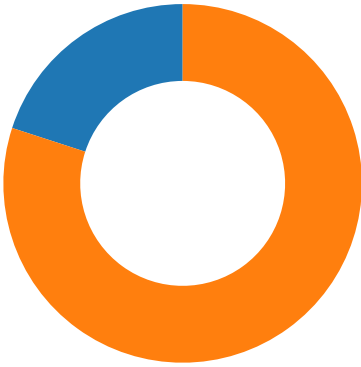
| Rich Headers                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div> <div>Programming Language:</div> <div> <ul style="list-style-type: none"> <li>[EXP] VS2015 UPD3.1 build 24215</li> <li>[RES] VS2015 UPD3 build 24213</li> <li>[LNK] VS2015 UPD3.1 build 24215</li> </ul> </div> </div> |

| Data Directories                     |                 |              |               |
|--------------------------------------|-----------------|--------------|---------------|
| Name                                 | Virtual Address | Virtual Size | Is in Section |
| IMAGE_DIRECTORY_ENTRY_EXPORT         | 0x7cda0         | 0x58         | .rdata        |
| IMAGE_DIRECTORY_ENTRY_IMPORT         | 0x7cdf8         | 0x78         | .rdata        |
| IMAGE_DIRECTORY_ENTRY_RESOURCE       | 0x87000         | 0x1e0        | .rsrc         |
| IMAGE_DIRECTORY_ENTRY_EXCEPTION      | 0x82000         | 0x192c       | .pdata        |
| IMAGE_DIRECTORY_ENTRY_SECURITY       | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_BASERELOC      | 0x88000         | 0x66c        | .reloc        |
| IMAGE_DIRECTORY_ENTRY_DEBUG          | 0x7a410         | 0x1c         | .rdata        |
| IMAGE_DIRECTORY_ENTRY_COPYRIGHT      | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_GLOBALPTR      | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_TLS            | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG    | 0x7a430         | 0x94         | .rdata        |
| IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT   | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_IAT            | 0x38000         | 0x370        | .rdata        |
| IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT   | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR | 0x0             | 0x0          |               |
| IMAGE_DIRECTORY_ENTRY_RESERVED       | 0x0             | 0x0          |               |

| Sections |                 |              |          |          |                     |                                                  |                     |                                                                         |
|----------|-----------------|--------------|----------|----------|---------------------|--------------------------------------------------|---------------------|-------------------------------------------------------------------------|
| Name     | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity     | File Type                                        | Entropy             | Characteristics                                                         |
| .text    | 0x1000          | 0x36fd5      | 0x37000  | False    | 0.38967507102272725 | data                                             | 5.930785005703424   | IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ           |
| .rdata   | 0x38000         | 0x4597a      | 0x45a00  | False    | 0.6705214878815081  | data                                             | 6.27546801719427    | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |
| .data    | 0x7e000         | 0x3394       | 0xc00    | False    | 0.18294270833333334 | DOS executable (block device driver \337-1231+)) | 2.573523630872546   | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE |
| .pdata   | 0x82000         | 0x192c       | 0x1a00   | False    | 0.4794170673076923  | data                                             | 5.1711441720039435  | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |
| .gfids   | 0x84000         | 0xdc         | 0x200    | False    | 0.244140625         | Spectrum .TAP data "6" - BASIC program           | 1.1531659578770692  | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |
| .gxfg    | 0x85000         | 0x1000       | 0x1000   | False    | 0.44091796875       | data                                             | 5.088628746947821   | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |
| .gehcont | 0x86000         | 0xc          | 0x200    | False    | 0.0390625           | data                                             | 0.06116285224115448 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |
| .rsrc    | 0x87000         | 0x1e0        | 0x200    | False    | 0.52734375          | data                                             | 4.724728911998389   | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ                      |



8080 undefined  
80 (HTTP)



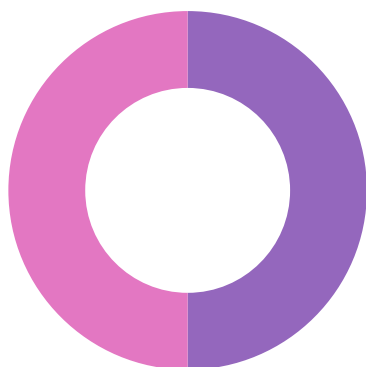
TCP Packets

| Timestamp                           | Source Port | Dest Port | Source IP      | Dest IP        |
|-------------------------------------|-------------|-----------|----------------|----------------|
| Nov 13, 2022 18:01:59.432678938 CET | 49698       | 80        | 192.168.2.3    | 115.178.55.22  |
| Nov 13, 2022 18:01:59.724894047 CET | 80          | 49698     | 115.178.55.22  | 192.168.2.3    |
| Nov 13, 2022 18:02:00.235091925 CET | 49698       | 80        | 192.168.2.3    | 115.178.55.22  |
| Nov 13, 2022 18:02:00.527365923 CET | 80          | 49698     | 115.178.55.22  | 192.168.2.3    |
| Nov 13, 2022 18:02:01.032000065 CET | 49698       | 80        | 192.168.2.3    | 115.178.55.22  |
| Nov 13, 2022 18:02:01.324109077 CET | 80          | 49698     | 115.178.55.22  | 192.168.2.3    |
| Nov 13, 2022 18:02:06.625338078 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:06.791755915 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:06.791997910 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:06.797142982 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:06.963495016 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:06.977639914 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:06.977679968 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:06.977808952 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:07.023405075 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:07.189626932 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:07.194511890 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:07.235672951 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:12.350394964 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:12.350476027 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:12.516810894 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:12.516870975 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:13.145853996 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:13.237636089 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:16.148930073 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:16.148992062 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:16.149166107 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:16.199492931 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:16.199572086 CET | 49699       | 8080      | 192.168.2.3    | 172.105.115.71 |
| Nov 13, 2022 18:02:16.365994930 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |
| Nov 13, 2022 18:02:16.366080046 CET | 8080        | 49699     | 172.105.115.71 | 192.168.2.3    |

Statistics

Behavior

loaddll64.exe



- conhost.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe
- regsvr32.exe

Click to jump to process

## System Behavior

Analysis Process: loadll64.exe    PID: 5948, Parent PID: 3452

### General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 0                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Start time:                   | 18:02:06                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Start date:                   | 13/11/2022                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Path:                         | C:\Windows\System32\loadll64.exe                                                                                                                                                                                                                                                                                                                                                                                              |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Commandline:                  | loadll64.exe "C:\Users\user\Desktop\gdazhx1EIP.dll"                                                                                                                                                                                                                                                                                                                                                                           |
| Imagebase:                    | 0x7ff683360000                                                                                                                                                                                                                                                                                                                                                                                                                |
| File size:                    | 139776 bytes                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MD5 hash:                     | C676FC0263EDD17D4CE7D644B8F3FCD6                                                                                                                                                                                                                                                                                                                                                                                              |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.267349016.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.268048394.000001FD03F10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                                                                                                                          |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Analysis Process: conhost.exe    PID: 5944, Parent PID: 5948

### General

|                        |                                                     |
|------------------------|-----------------------------------------------------|
| Target ID:             | 1                                                   |
| Start time:            | 18:02:06                                            |
| Start date:            | 13/11/2022                                          |
| Path:                  | C:\Windows\System32\conhost.exe                     |
| Wow64 process (32bit): | false                                               |
| Commandline:           | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase:             | 0x7ff745070000                                      |

|                               |                                  |
|-------------------------------|----------------------------------|
| File size:                    | 625664 bytes                     |
| MD5 hash:                     | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges:      | true                             |
| Has administrator privileges: | true                             |
| Programmed in:                | C, C++ or other language         |
| Reputation:                   | high                             |

Analysis Process: cmd.exe    PID: 5048, Parent PID: 5948

General

|                               |                                                                   |
|-------------------------------|-------------------------------------------------------------------|
| Target ID:                    | 2                                                                 |
| Start time:                   | 18:02:06                                                          |
| Start date:                   | 13/11/2022                                                        |
| Path:                         | C:\Windows\System32\cmd.exe                                       |
| Wow64 process (32bit):        | false                                                             |
| Commandline:                  | cmd.exe /C rundll32.exe "C:\Users\user\Desktop\gdazhx1EIP.dll",#1 |
| Imagebase:                    | 0x7ff707bb0000                                                    |
| File size:                    | 273920 bytes                                                      |
| MD5 hash:                     | 4E2ACF4F8A396486AB4268C94A6A245F                                  |
| Has elevated privileges:      | true                                                              |
| Has administrator privileges: | true                                                              |
| Programmed in:                | C, C++ or other language                                          |
| Reputation:                   | high                                                              |

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

Analysis Process: regsvr32.exe    PID: 676, Parent PID: 5948

General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 3                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Start time:                   | 18:02:06                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Start date:                   | 13/11/2022                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Path:                         | C:\Windows\System32\regsvr32.exe                                                                                                                                                                                                                                                                                                                                                                                              |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Commandline:                  | regsvr32.exe /s C:\Users\user\Desktop\gdazhx1EIP.dll                                                                                                                                                                                                                                                                                                                                                                          |
| Imagebase:                    | 0x7ff72a9a0000                                                                                                                                                                                                                                                                                                                                                                                                                |
| File size:                    | 24064 bytes                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                                                                                                                                                                                                                                                                                                                                                                              |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.261058866.0000000000B60000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.261968375.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                                                                                                                          |

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Analysis Process: rundll32.exe PID: 2436, Parent PID: 5048

General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 4                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Start time:                   | 18:02:06                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Start date:                   | 13/11/2022                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                                                                                                                                                                                                              |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Commandline:                  | rundll32.exe "C:\Users\user\Desktop\gdazhx1EIP.dll",#1                                                                                                                                                                                                                                                                                                                                                                        |
| Imagebase:                    | 0x7ff780fd0000                                                                                                                                                                                                                                                                                                                                                                                                                |
| File size:                    | 69632 bytes                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                                                                                                                                                                                                              |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.261854248.0000018104890000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.260138697.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                                                                                                                          |

File Activities

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

File Deleted

| File Path                                                    | Completion      | Count | Source Address | Symbol      |
|--------------------------------------------------------------|-----------------|-------|----------------|-------------|
| C:\Windows\System32\RSNLKxhQH\hDzTIHdHNg.dll:Zone.Identifier | success or wait | 1     | 180020786      | DeleteFileW |

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---------------|---------------|------------|-------|----------------|--------|
|---------------|---------------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Analysis Process: rundll32.exe PID: 4252, Parent PID: 5948

General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 5                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Start time:                   | 18:02:06                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Start date:                   | 13/11/2022                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Path:                         | C:\Windows\System32\rundll32.exe                                                                                                                                                                                                                                                                                                                                                                                              |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Commandline:                  | rundll32.exe C:\Users\user\Desktop\gdazhx1EIP.dll,DllRegisterServer                                                                                                                                                                                                                                                                                                                                                           |
| Imagebase:                    | 0x7ff780fd0000                                                                                                                                                                                                                                                                                                                                                                                                                |
| File size:                    | 69632 bytes                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5 hash:                     | 73C519F050C20580F8A62C849D49215A                                                                                                                                                                                                                                                                                                                                                                                              |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.262113824.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.262654779.00000222D2E50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                                                                                                                          |

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Analysis Process: regsvr32.exe    PID: 5244, Parent PID: 2436

General

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target ID:                    | 6                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Start time:                   | 18:02:10                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Start date:                   | 13/11/2022                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Path:                         | C:\Windows\System32\regsvr32.exe                                                                                                                                                                                                                                                                                                                                                                                              |
| Wow64 process (32bit):        | false                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\lhDzTIHldHNg.dll"                                                                                                                                                                                                                                                                                                                                             |
| Imagebase:                    | 0x7ff72a9a0000                                                                                                                                                                                                                                                                                                                                                                                                                |
| File size:                    | 24064 bytes                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                                                                                                                                                                                                                                                                                                                                                                              |
| Has elevated privileges:      | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Has administrator privileges: | true                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Programmed in:                | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:                 | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.771127294.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.769097156.0000000000490000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |
| Reputation:                   | high                                                                                                                                                                                                                                                                                                                                                                                                                          |

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|-------|-------|------------|-------|----------------|--------|
|-----------|--------|--------|-------|-------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Registry Activities

Key Value Created

| Key Path                                                         | Name             | Type    | Data                                                                              | Completion      | Count | Source Address | Symbol         |
|------------------------------------------------------------------|------------------|---------|-----------------------------------------------------------------------------------|-----------------|-------|----------------|----------------|
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run | lhDzTIHldHNg.dll | unicode | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\lhDzTIHldHNg.dll" | success or wait | 1     | 180003442      | RegSetValueExW |

Analysis Process: regsvr32.exe    PID: 5204, Parent PID: 676

General

|                               |                                                                            |
|-------------------------------|----------------------------------------------------------------------------|
| Target ID:                    | 7                                                                          |
| Start time:                   | 18:02:10                                                                   |
| Start date:                   | 13/11/2022                                                                 |
| Path:                         | C:\Windows\System32\regsvr32.exe                                           |
| Wow64 process (32bit):        | false                                                                      |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\VGdnyYmEzk\YPrp.dll" |
| Imagebase:                    | 0x7ff72a9a0000                                                             |
| File size:                    | 24064 bytes                                                                |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                           |
| Has elevated privileges:      | true                                                                       |
| Has administrator privileges: | true                                                                       |
| Programmed in:                | C, C++ or other language                                                   |
| Reputation:                   | high                                                                       |

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

**Analysis Process: regsvr32.exe**    PID: 4896, Parent PID: 4252

**General**

|                               |                                                                             |
|-------------------------------|-----------------------------------------------------------------------------|
| Target ID:                    | 8                                                                           |
| Start time:                   | 18:02:11                                                                    |
| Start date:                   | 13/11/2022                                                                  |
| Path:                         | C:\Windows\System32\regsvr32.exe                                            |
| Wow64 process (32bit):        | false                                                                       |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XeFlcoVtIwPzeOKW.dll" |
| Imagebase:                    | 0x7ff72a9a0000                                                              |
| File size:                    | 24064 bytes                                                                 |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                            |
| Has elevated privileges:      | true                                                                        |
| Has administrator privileges: | true                                                                        |
| Programmed in:                | C, C++ or other language                                                    |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

**Analysis Process: regsvr32.exe**    PID: 5444, Parent PID: 5948

**General**

|                               |                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------|
| Target ID:                    | 9                                                                                           |
| Start time:                   | 18:02:14                                                                                    |
| Start date:                   | 13/11/2022                                                                                  |
| Path:                         | C:\Windows\System32\regsvr32.exe                                                            |
| Wow64 process (32bit):        | false                                                                                       |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MtAvdtxCDyblyei\mPrhkfVupthqSBxp.dll" |
| Imagebase:                    | 0x7ff72a9a0000                                                                              |
| File size:                    | 24064 bytes                                                                                 |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                                            |
| Has elevated privileges:      | true                                                                                        |
| Has administrator privileges: | true                                                                                        |
| Programmed in:                | C, C++ or other language                                                                    |

**File Activities**

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

**Analysis Process: regsvr32.exe**    PID: 2356, Parent PID: 3452

**General**

|                               |                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------|
| Target ID:                    | 19                                                                                |
| Start time:                   | 18:03:16                                                                          |
| Start date:                   | 13/11/2022                                                                        |
| Path:                         | C:\Windows\System32\regsvr32.exe                                                  |
| Wow64 process (32bit):        | false                                                                             |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RSNLKxhQH\IhDzTIHIdHNg.dll" |
| Imagebase:                    | 0x7ff72a9a0000                                                                    |
| File size:                    | 24064 bytes                                                                       |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                                  |
| Has elevated privileges:      | false                                                                             |
| Has administrator privileges: | false                                                                             |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Programmed in: | C, C++ or other language                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yara matches:  | <ul style="list-style-type: none"><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.415103190.00000000028E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000013.00000002.415208554.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security</li></ul> |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|-----------|--------|------------|---------|------------|-------|----------------|--------|
|-----------|--------|------------|---------|------------|-------|----------------|--------|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

### Analysis Process: regsvr32.exe PID: 3092, Parent PID: 2356

#### General

|                               |                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------|
| Target ID:                    | 20                                                                                           |
| Start time:                   | 18:03:23                                                                                     |
| Start date:                   | 13/11/2022                                                                                   |
| Path:                         | C:\Windows\System32\regsvr32.exe                                                             |
| Wow64 process (32bit):        | false                                                                                        |
| Commandline:                  | C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\EHrtIMNuOOxGF\cDTWQXzuC\j.dll" |
| Imagebase:                    | 0x7ff72a9a0000                                                                               |
| File size:                    | 24064 bytes                                                                                  |
| MD5 hash:                     | D78B75FC68247E8A63ACBA846182740E                                                             |
| Has elevated privileges:      | false                                                                                        |
| Has administrator privileges: | false                                                                                        |
| Programmed in:                | C, C++ or other language                                                                     |

### File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

## Disassembly

 No disassembly