# MALICIOUS

Classifications: Injector | Spyware | Downloader

Threat Names: SmokeLoader | Mal/HTMLGen-A

Verdict Reason: -

| | |
|---|---|
| **Sample Type** | **Windows Exe (x86-32)** |
| **File Name** | **31a601a28f4a81a69c9b09d7249582b9.virus.exe** |
| ID | #3264342 |
| MD5 | 31a601a28f4a81a69c9b09d7249582b9 |
| SHA1 | 7aa415965720f2c794fd44a4f147dd7fa756b9b8 |
| SHA256 | 4a74dbaaacb20b26d7237b74ced5bd105b0ff3e2eb3ece3eba7bb93bf224b853 |
| File Size | 279.00 KB |
| Report Created | 2022-01-11 13:11 (UTC+1) |
| Target Environment | win10_64_th2_en_mso2016 \| exe |

# OVERVIEW

## VMRay Threat Identifiers (34 rules, 77 matches)

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 5/5 | YARA | Malicious content matched by YARA rules | 3 | Downloader |
| | • Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #3) explorer.exe.<br>• Rule "SmokeLoader" from ruleset "Malware" has matched on a memory dump for (process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe.<br>• Rule "SmokeLoaderStrings" from ruleset "Malware" has matched on the function strings for (process #3) explorer.exe. | | | |
| 5/5 | Data Collection | Tries to read cached credentials of various applications | 1 | Spyware |
| | • Tries to read sensitive data of: Vivaldi, Epic Privacy Browser, MultiDoge DogeCoin wallet, Google Chrome, Foxmail, Chromium, 7Star... ...currency Wallet, Comodo Dragon, Torch, Apache Directory Studio, Orbitum, Kometa, Opera, Internet Explorer, CentBrowser, BlackHawk. | | | |
| 4/5 | Defense Evasion | Obscures a file's origin | 1 | - |
| | • (Process #3) explorer.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih". | | | |
| 4/5 | Reputation | Known malicious file | 1 | - |
| | • File "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\asdfyhahsdfhasdf.dll" is a known malicious file. | | | |
| 4/5 | Reputation | Contacts known malicious URL | 3 | - |
| | • Reputation analysis labels the URL "host-data-coin-11.com/" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".<br>• Reputation analysis labels the URL "data-host-coin-8.com/files/4892_1641897821_7641.exe" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".<br>• Reputation analysis labels the URL "http://data-host-coin-8.com/files/2739_1641880829_4069.exe" which was contacted by (process #5) 8c55.exe as "Mal/HTMLGen-A". | | | |
| 4/5 | Reputation | Resolves known malicious domain | 1 | - |
| | • Reputation analysis labels the resolved domain "data-host-coin-8.com" as "Mal/HTMLGen-A". | | | |
| 4/5 | Injection | Writes into the memory of another process | 1 | Injector |
| | • (Process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe modifies memory of (process #3) explorer.exe. | | | |
| 4/5 | Injection | Modifies control flow of another process | 1 | Injector |
| | • (Process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe creates thread in (process #3) explorer.exe. | | | |
| 3/5 | Data Collection | Reads cryptocurrency wallet locations | 5 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to read the cryptocurrency wallet "mSIGNA Cryptocurrency Wallet".<br>• (Process #7) 7357_1641723530_7360.exe tries to read the cryptocurrency wallet "Ethereum" for "ETH".<br>• (Process #7) 7357_1641723530_7360.exe tries to read the cryptocurrency wallet "Electron Cash Bitcoin Cash Wallet" for "BCH".<br>• (Process #7) 7357_1641723530_7360.exe tries to read the cryptocurrency wallet "Exodus Cryptocurrency Wallet".<br>• (Process #7) 7357_1641723530_7360.exe tries to read the cryptocurrency wallet "MultiDoge DogeCoin wallet" for "DOGE". | | | |
| 3/5 | Network Connection | Uses HTTP to upload a large amount of data. | 1 | - |
| | • (Process #7) 7357_1641723530_7360.exe uploads 122.978KB data using HTTP POST. | | | |
| 2/5 | Anti Analysis | Tries to detect debugger | 1 | - |
| | • (Process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe tries to detect a debugger via API "NtQueryInformationProcess". | | | |
| 2/5 | Hide Tracks | Deletes file after execution | 2 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | • (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih".<br>• (Process #3) explorer.exe deletes executed executable "c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe". | | | |
| 2/5 | Anti Analysis | Delays execution | 1 | - |
| | • (Process #3) explorer.exe has a thread which sleeps more than 5 minutes. | | | |
| 2/5 | Discovery | Reads network adapter information | 1 | - |
| | • (Process #5) 8c55.exe reads the network adapters' addresses by API. | | | |
| 2/5 | Data Collection | Reads sensitive browser data | 19 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Google Chrome" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Chromium" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Kometa" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Amigo" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Torch" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Orbitum" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Comodo Dragon" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Epic Privacy Browser" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Vivaldi" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "CocCoc" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Uran" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "CentBrowser" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Elements Browser" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Opera" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Mozilla Firefox" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "Cyberfox" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "BlackHawk" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of web browser "7Star" by file. | | | |
| 2/5 | Data Collection | Reads sensitive mail data | 2 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of mail application "Mozilla Thunderbird" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of mail application "Foxmail" by file. | | | |
| 2/5 | Data Collection | Reads sensitive ftp data | 2 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of ftp application "AbleFTP" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of ftp application "Total Commander" by file. | | | |
| 2/5 | Data Collection | Reads sensitive application data | 1 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to read sensitive data of application "Apache Directory Studio" by file. | | | |
| 2/5 | Task Scheduling | Schedules task | 2 | - |
| | • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Logon.<br>• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih", to be triggered by Time. Task has been rescheduled by the analyzer. | | | |
| 2/5 | Injection | Writes into the memory of a process started from a created or modified executable | 1 | - |
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe modifies memory of (process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe. | | | |
| 2/5 | Injection | Modifies control flow of a process started from a created or modified executable | 1 | - |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe alters context of (process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe. | | | |
| 1/5 | Obfuscation | Reads from memory of another process | 1 | - |
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe reads from (process #2) 31a601a28f4a81a69c9b09d7249582b9.virus.exe. | | | |
| 1/5 | Obfuscation | Creates a page with write and execute permissions | 1 | - |
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. | | | |
| 1/5 | Discovery | Enumerates running processes | 1 | - |
| | • (Process #3) explorer.exe enumerates running processes. | | | |
| 1/5 | Mutex | Creates mutex | 1 | - |
| | • (Process #3) explorer.exe creates mutex with name "FE7F15060B875FB9FB2A49F08D5D03120C287F38". | | | |
| 1/5 | Hide Tracks | Creates process with hidden window | 1 | - |
| | • (Process #3) explorer.exe starts (process #5) 8c55.exe with a hidden window. | | | |
| 1/5 | Discovery | Possibly does reconnaissance | 4 | - |
| | • (Process #7) 7357_1641723530_7360.exe tries to gather information about application "Mozilla Firefox" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to gather information about application "Cyberfox" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to gather information about application "blackHawk" by file.<br>• (Process #7) 7357_1641723530_7360.exe tries to gather information about application "icecat" by file. | | | |
| 1/5 | Obfuscation | Overwrites code | 1 | - |
| | • (Process #5) 8c55.exe overwrites code to possibly hide behavior. | | | |
| 1/5 | Obfuscation | Resolves API functions dynamically | 2 | - |
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe resolves 41 API functions by name.<br>• (Process #7) 7357_1641723530_7360.exe resolves 124 API functions by name. | | | |
| 1/5 | Network Connection | Performs DNS request | 1 | - |
| | • (Process #5) 8c55.exe resolves host name "data-host-coin-8.com" to IP "5.188.88.184". | | | |
| 1/5 | Network Connection | Connects to remote host | 1 | - |
| | • (Process #5) 8c55.exe opens an outgoing TCP connection to host "5.188.88.184:80". | | | |
| 1/5 | Network Connection | Downloads executable | 9 | Downloader |
| | • (Process #3) explorer.exe downloads executable via http from data-host-coin-8.com/files/4892_1641897821_7641.exe.<br>• (Process #5) 8c55.exe downloads executable via http from http://data-host-coin-8.com/files/2739_1641880829_4069.exe.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/6.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/1.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/2.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/3.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/4.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/5.jpg.<br>• (Process #7) 7357_1641723530_7360.exe downloads executable via http from tikwish.com/7.jpg. | | | |

| Score | Category | Operation | Count | Classification |
|---|---|---|---|---|
| 1/5 | Execution | Drops PE file | 1 | - |
| | • (Process #5) 8c55.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\asdfyhahsdfhasdf.dll". | | | |
| 1/5 | Execution | Executes itself | 2 | - |
| | • (Process #1) 31a601a28f4a81a69c9b09d7249582b9.virus.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe.<br>• (Process #4) svchost.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe. | | |
| - | Trusted | Known clean file | 8 | - |
| | • File "_desktop.zip" is a known clean file.<br>• File "C:\\ProgramData\\softokn3.dll" is a known clean file.<br>• File "C:\\ProgramData\\sqlite3.dll" is a known clean file.<br>• File "C:\\ProgramData\\freebl3.dll" is a known clean file.<br>• File "C:\\ProgramData\\mozglue.dll" is a known clean file.<br>• File "C:\\ProgramData\\msvcp140.dll" is a known clean file.<br>• File "C:\\ProgramData\\nss3.dll" is a known clean file.<br>• File "C:\\ProgramData\\vcruntime140.dll" is a known clean file. | | | |
| - | Trusted | Executable has a trusted signature | 4 | - |
| | • Executable C:\\ProgramData\\softokn3.dll has a trusted signature.<br>• Executable C:\\ProgramData\\freebl3.dll has a trusted signature.<br>• Executable C:\\ProgramData\\mozglue.dll has a trusted signature.<br>• Executable C:\\ProgramData\\nss3.dll has a trusted signature. | | | |

### Mitre ATT&CK Matrix

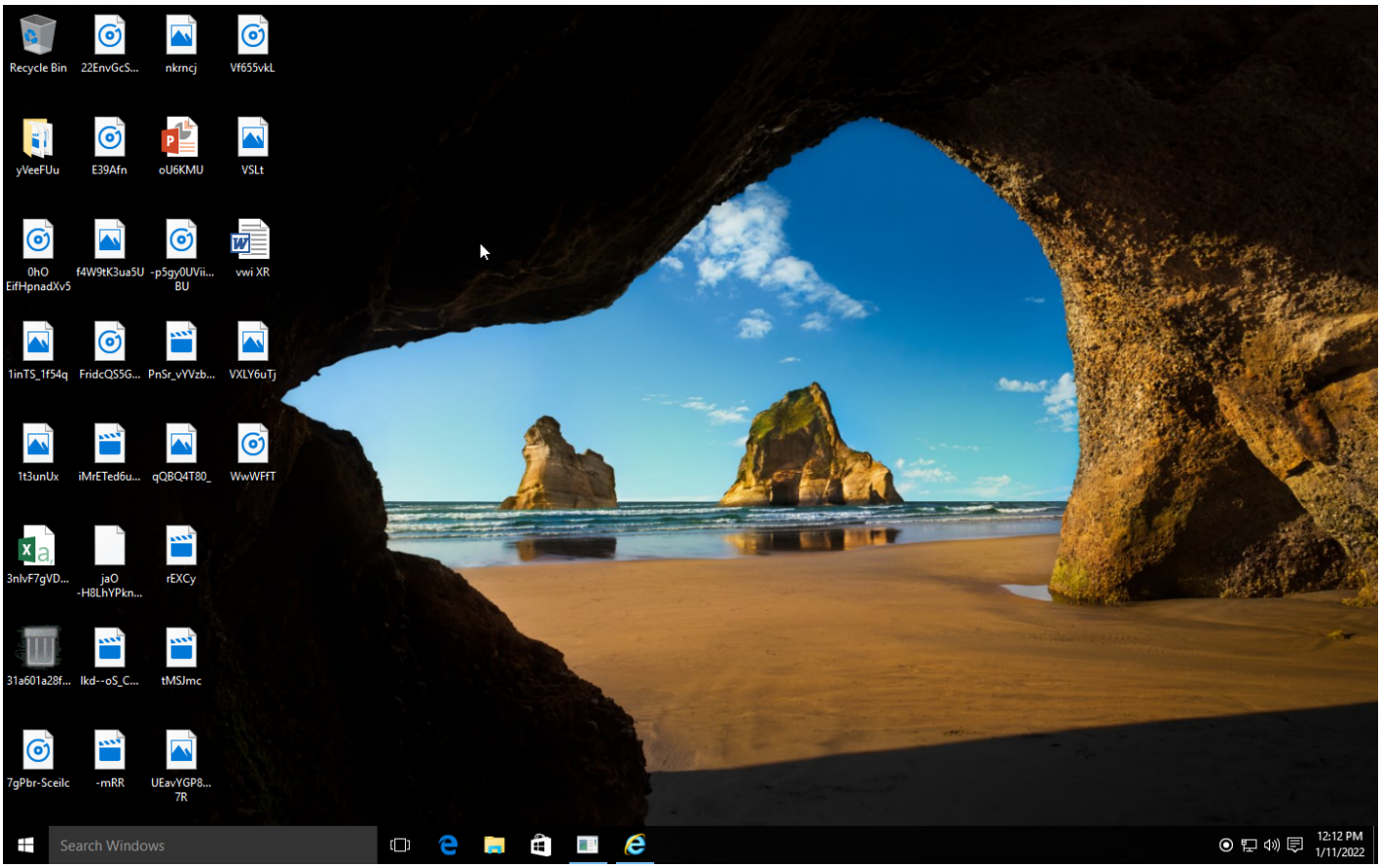
| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | #T1053 Scheduled Task | #T1053 Scheduled Task | #T1053 Scheduled Task | #T1045 Software Packing | #T1003 Credential Dumping | #T1057 Process Discovery | #T1105 Remote File Copy | #T1119 Automated Collection | #T1071 Standard Application Layer Protocol | #T1020 Automated Exfiltration | |
| | | | | #T1096 NTFS File Attributes | #T1081 Credentials in Files | #T1016 System Network Configuration Discovery | | #T1005 Data from Local System | #T1105 Remote File Copy | | |
| | | | | #T1143 Hidden Window | | #T1083 File and Directory Discovery | | | | | |

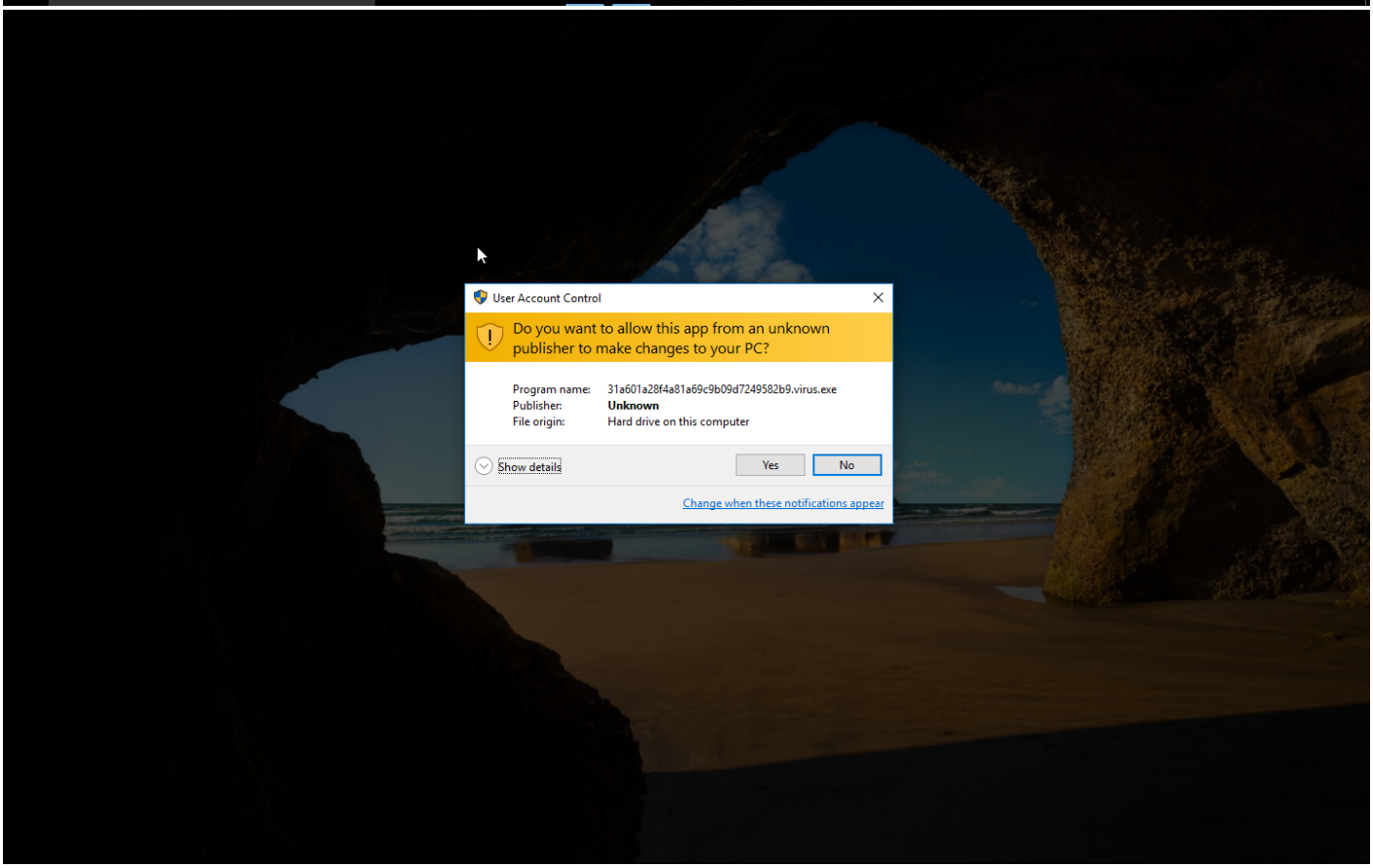
## Sample Information

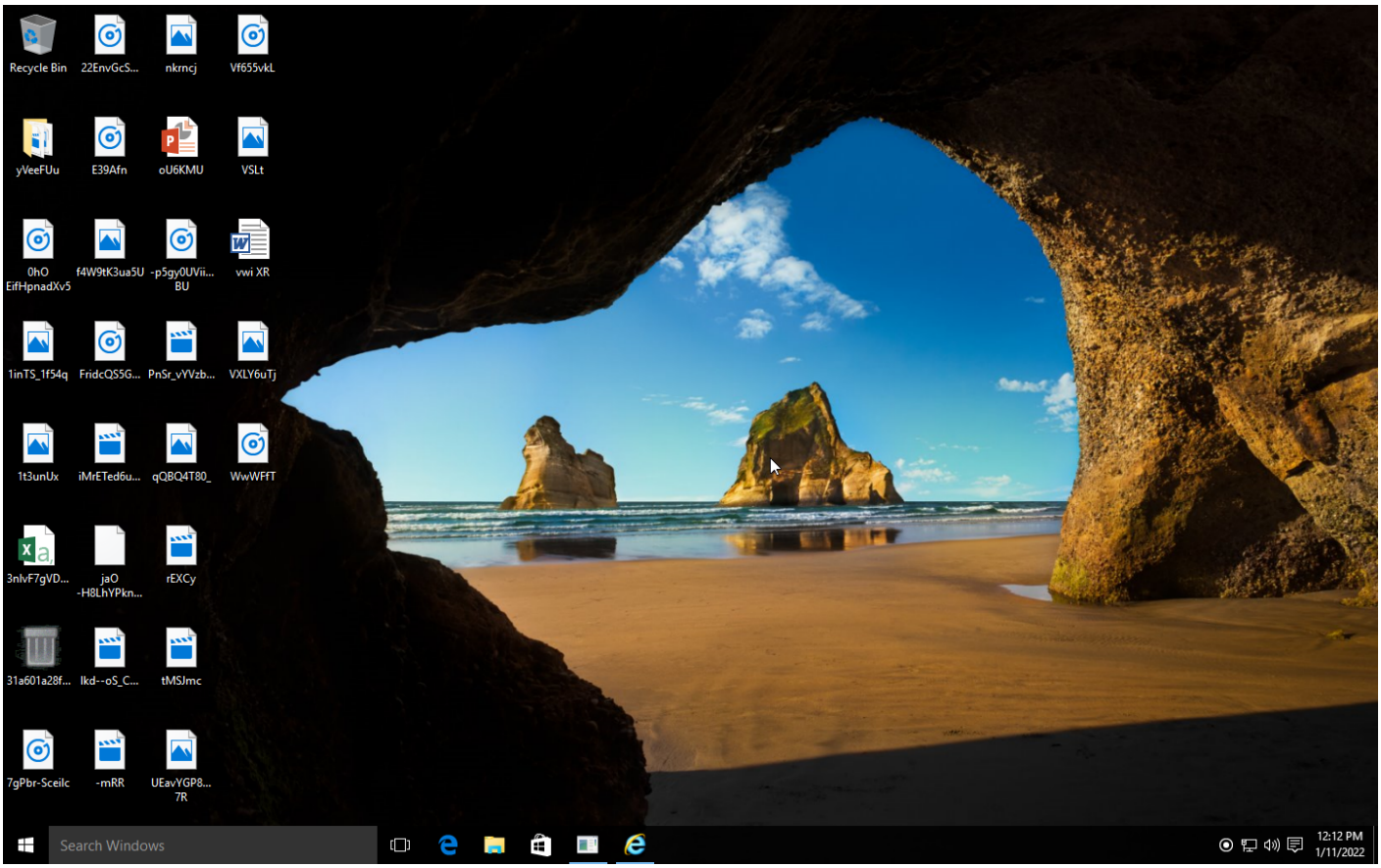
| | |
|---|---|
| ID | #3264342 |
| MD5 | 31a601a28f4a81a69c9b09d7249582b9 |
| SHA1 | 7aa415965720f2c794fd44a4f147dd7fa756b9b8 |
| SHA256 | 4a74dbaaacb20b26d7237b74ced5bd105b0ff3e2eb3ece3eba7bb93bf224b853 |
| SSDeep | 3072:74aUfB9HX64t9b47ZgNaZ330yPTk40f6rzCRYaEfF8Wrxpzbgqru:0LfWcZBS3dPTkrgKYaluzbgwu |
| ImpHash | 22d83eb8d57dfc503864047e3c9d375e |
| File Name | 31a601a28f4a81a69c9b09d7249582b9.virus.exe |
| File Size | 279.00 KB |
| Sample Type | Windows Exe (x86-32) |
| Has Macros | ✓ |

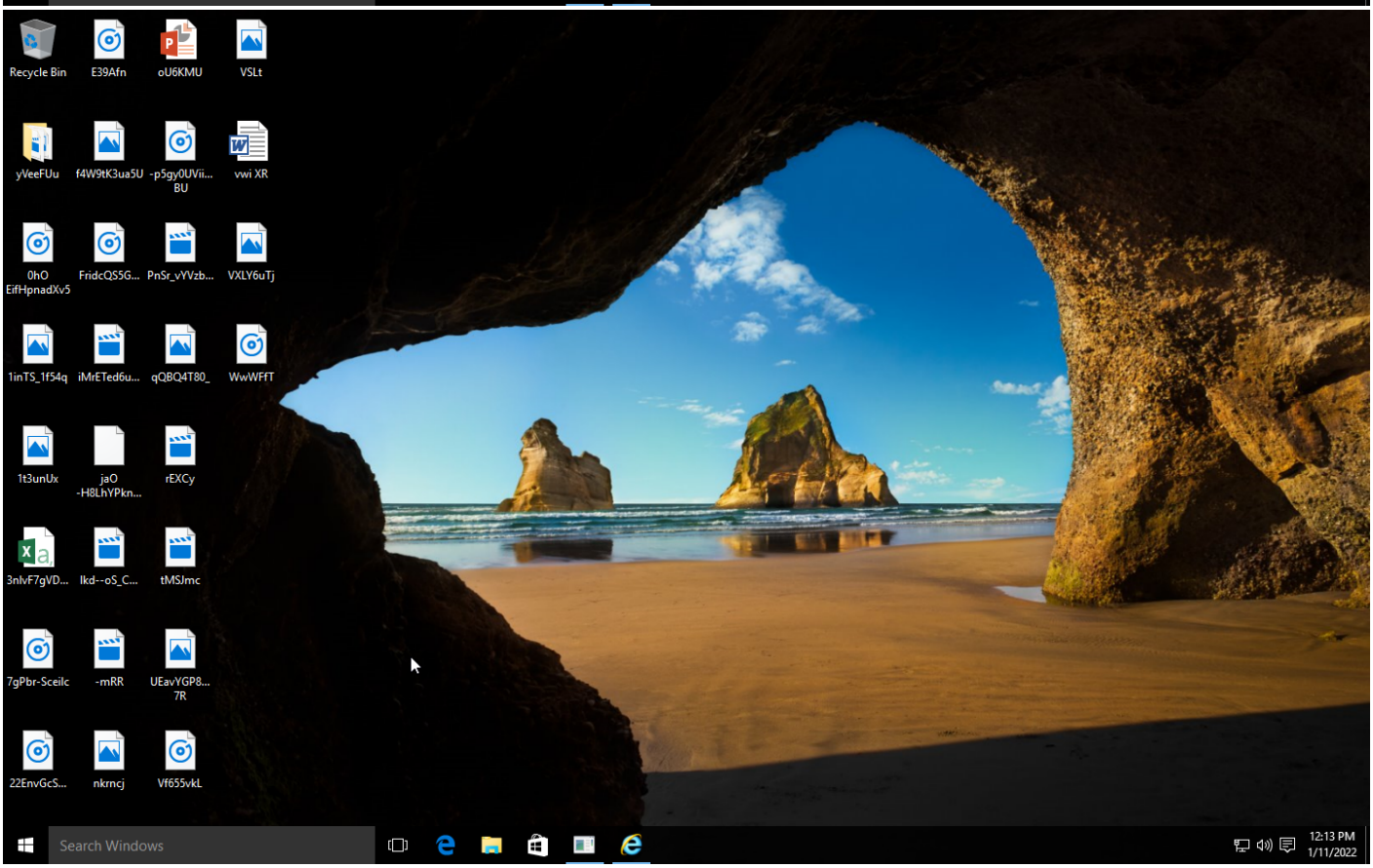
## Analysis Information

| | |
|---|---|
| Creation Time | 2022-01-11 13:11 (UTC+1) |
| Analysis Duration | 00:04:00 |
| Termination Reason | Timeout |
| Number of Monitored Processes | 7 |
| Execution Successful | False |
| Reputation Enabled | ✓ |
| WHOIS Enabled | ✓ |
| Built-in AV Enabled | ✗ |
| Built-in AV Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of AV Matches | 0 |
| YARA Enabled | ✓ |
| YARA Applied On | Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files |
| Number of YARA Matches | 3 |


Recycle Bin
22EnvGcS...
nkrncj
Vf655vkL
yVeeFUu
E39Afn
oU6KMU
VSLt
0hO EifHpnadXv5
f4W9tK3ua5U
-p5gy0UVii... BU
vwi XR
1inTS_1f54q
FridcQS5G...
PnSr_vYVzb...
VXLY6uTj
1t3unUx
iMrETed6u...
qQBQ4T80_
WwWFfT
3nlvF7gVD...
jaO -H8LhYPkn...
rEXCy
31a601a28f...
lkd--oS_C...
tMSJmc
7gPbr-Sceilc
-mRR
UEavYGP8... 7R
Search Windows
12:12 PM
1/11/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 31a601a28f4a81a69c9b09d7249582b9.virus.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear




Screenshots truncated

# NETWORK

## General

151.08 KB total sent

3679.54 KB total received

1 ports 80

3 contacted IP addresses

0 URLs extracted

10 files downloaded

0 malicious hosts detected

## DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

## HTTP/S

12 URLs contacted, 2 servers

24 sessions, 151.08 KB sent, 3679.54 KB received

## HTTP Requests

| Method | URL | Dest. IP | Dest. Port | Status Code | Response Size | Verdict |
|---|---|---|---|---|---|---|
| POST | host-data-coin-11.com/ | - | - | | 0 bytes | NA |
| GET | data-host-coin-8.com/files/4892_1641897821_7641.exe | - | - | | 0 bytes | NA |
| GET | http://data-host-coin-8.com/files/2739_1641880829_4069.exe | - | - | | 0 bytes | NA |
| POST | tikwish.com/6.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/1.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/2.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/3.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/4.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/5.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/7.jpg | - | - | | 0 bytes | NA |
| POST | tikwish.com/main.php | - | - | | 0 bytes | NA |
| POST | tikwish.com/ | - | - | | 0 bytes | NA |

## DNS Requests

| Type | Hostname | Response Code | Resolved IPs | CNames | Verdict |
|---|---|---|---|---|---|
| - | data-host-coin-8.com | - | 5.188.88.184 | | NA |

## BEHAVIOR

### Process Graph

### Process #1: 31a601a28f4a81a69c9b09d7249582b9.virus.exe

| | |
|---|---|
| ID | 1 |
| File Name | c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 70331, Reason: Analysis Target |
| Unmonitor End Time | End Time: 94980, Reason: Terminated |
| Monitor duration | 24.65s |
| Return Code | 0 |
| PID | 3396 |
| Parent PID | 1560 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 72 |
| File | 6 |
| Environment | 1 |
| Window | 1 |
| Process | 1 |
| - | 3 |
| - | 5 |

### Process #2: 31a601a28f4a81a69c9b09d7249582b9.virus.exe

| | |
|---|---|
| ID | 2 |
| File Name | c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe |
| Command Line | "C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe" |
| Initial Working Directory | C:\Users\RDhJ0CNFevzX\Desktop\ |
| Monitor Start Time | Start Time: 88456, Reason: Child Process |
| Unmonitor End Time | End Time: 107994, Reason: Terminated |
| Monitor duration | 19.54s |
| Return Code | 0 |
| PID | 748 |
| Parent PID | 3396 |
| Bitness | 32 Bit |

### Injection Information (4)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #1: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0xdbc | 0x400000(4194304) | 0x200 | ✓ | 1 |
| Modify Memory | #1: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0xdbc | 0x401000(4198400) | 0x7200 | ✓ | 1 |
| Modify Memory | #1: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0xdbc | 0x34c008(3457032) | 0x4 | ✓ | 1 |
| Modify Control Flow | #1: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0xdbc / 0x518 | 0x77c08fe0(2009108448) | - | ✓ | 1 |

### Host Behavior

| Type | Count |
|---|---|
| Module | 17 |
| Keyboard | 2 |
| Process | 1 |
| File | 1 |
| System | 6 |
| - | 1 |
| Registry | 12 |
| - | 1 |

### Process #3: explorer.exe

| | |
|---|---|
| ID | 3 |
| File Name | c:\windows\explorer.exe |
| Command Line | C:\Windows\Explorer.EXE |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 102978, Reason: Injection |
| Unmonitor End Time | End Time: 311010, Reason: Terminated by Timeout |
| Monitor duration | 208.03s |
| Return Code | Unknown |
| PID | 1560 |
| Parent PID | 18446744073709551615 |
| Bitness | 64 Bit |

### Injection Information (3)

| Injection Type | Source Process | Source / Target TID | Address / Name | Size | Success | Count |
|---|---|---|---|---|---|---|
| Modify Memory | #2: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0x518 | 0x410000(4259840) | 0x5000 | ✓ | 1 |
| Modify Memory | #2: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0x518 | 0x420000(4325376) | 0x16000 | ✓ | 1 |
| Create Remote Thread | #2: c:\users\rdhj0cnfevzx\desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | 0x518 | 0x421930(4331824) | - | ✓ | 1 |

### Dropped Files (2)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih | 279.00 KB | 4a74dbaaacb20b26d7237b74ced5bd105b0ff3e2eb3ece3eba7bb93bf224b853 | ✗ |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.exe | 213.50 KB | 2060c534b8b1d2b20a49ed055b864fb2fd5cfd6371ddf8e92436fb889f3d852d | ✗ |

### Host Behavior

| Type | Count |
|---|---|
| Module | 47 |
| Process | 8429 |
| System | 37557 |
| Mutex | 1 |
| Registry | 2 |
| File | 41 |
| User | 1 |
| COM | 1 |

### Network Behavior

| Type | Count |
|---|---|
| HTTP | 19 |
| TCP | 19 |

### Process #4: svchost.exe

| | |
|---|---|
| ID | 4 |
| File Name | c:\windows\system32\svchost.exe |
| Command Line | C:\Windows\system32\svchost.exe -k netsvcs |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 143134, Reason: Created Scheduled Job |
| Unmonitor End Time | End Time: 311010, Reason: Terminated by Timeout |
| Monitor duration | 167.88s |
| Return Code | Unknown |
| PID | 860 |
| Parent PID | 532 |
| Bitness | 64 Bit |

### Process #5: 8c55.exe

| | |
|---|---|
| ID | 5 |
| File Name | c:\users\rdhj0cnfevzx\appdata\local\temp\8c55.exe |
| Command Line | C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.exe |
| Initial Working Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp\ |
| Monitor Start Time | Start Time: 146100, Reason: Child Process |
| Unmonitor End Time | End Time: 221204, Reason: Terminated |
| Monitor duration | 75.10s |
| Return Code | 0 |
| PID | 1516 |
| Parent PID | 1560 |
| Bitness | 32 Bit |

### Dropped Files (2)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\asdfyhahsdfhasdf.dll | 140.11 KB | 55ff1e0a4e5866d565ceeb9baafac73fdcb4464160fc6c78104d935009935cd7 | ✕ |
| C:\ProgramData\7357_1641723530_7360.exe | 200.00 KB | fc2b7524cb96be03fbb8fe44f1c03d640ffa628397a7af53690d168ede030771 | ✕ |

### Host Behavior

| Type | Count |
|---|---|
| Process | 1 |
| File | 43 |
| Module | 11 |
| - | 13 |
| System | 365 |
| Environment | 13 |
| Registry | 21 |

### Network Behavior

| Type | Count |
|---|---|
| HTTP | 1 |
| DNS | 1 |
| TCP | 1 |

### Process #6: bcatcih

| | |
|---|---|
| ID | 6 |
| File Name | c:\users\rdhj0cnfevzx\appdata\roaming\bcatcih |
| Command Line | C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih |
| Initial Working Directory | C:\Windows\system32\ |
| Monitor Start Time | Start Time: 153050, Reason: Child Process |
| Unmonitor End Time | End Time: 311010, Reason: Terminated by Timeout |
| Monitor duration | 157.96s |
| Return Code | Unknown |
| PID | 1916 |
| Parent PID | 860 |
| Bitness | 32 Bit |

### Host Behavior

| Type | Count |
|---|---|
| Module | 29 |
| File | 3 |
| Environment | 1 |

### Process #7: 7357_1641723530_7360.exe

| | |
|---|---|
| ID | 7 |
| File Name | c:\programdata\7357_1641723530_7360.exe |
| Command Line | "C:\ProgramData\7357_1641723530_7360.exe" |
| Initial Working Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp\ |
| Monitor Start Time | Start Time: 213443, Reason: Child Process |
| Unmonitor End Time | End Time: 311010, Reason: Terminated by Timeout |
| Monitor duration | 97.57s |
| Return Code | Unknown |
| PID | 3052 |
| Parent PID | 1516 |
| Bitness | 32 Bit |

### Dropped Files (13)

| File Name | File Size | SHA256 | YARA Match |
|---|---|---|---|
| - | 0 bytes | e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 | ✕ |
| C:\\ProgramData\\softokn3.dll | 141.45 KB | 43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083 | ✕ |
| C:\\ProgramData\\sqlite3.dll | 630.46 KB | 16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660 | ✕ |
| C:\\ProgramData\\freebl3.dll | 326.45 KB | a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba | ✕ |
| C:\\ProgramData\\mozglue.dll | 133.95 KB | 3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd | ✕ |
| C:\\ProgramData\\msvcp140.dll | 429.80 KB | 334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4 | ✕ |
| C:\\ProgramData\\nss3.dll | 1216.95 KB | e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78 | ✕ |
| C:\\ProgramData\\vcruntime140.dll | 81.82 KB | c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d | ✕ |
| _desktop.zip | 22 bytes | 8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85 | ✕ |
| system.txt | 2.01 KB | afad4e3d3d6460731c2ddfe2a5b07a8a0ff046cb94fe2da2f5056157d5fc7b00 | ✕ |
| C:\\ProgramData\\614533357526747\screenshot.jpg | 122.57 KB | b99407f512e3d56511540d48a4425e6f98e055882f5211a3a1dc406cf97dac49 | ✕ |
| outlook.txt | 527 bytes | 1ddf9ccdf8405a70cb261c09df1cafcdcf0f980e03c441a841d3543b42879259 | ✕ |
| _6452595239.zip | 119.76 KB | 2ff6c82786ef2ea28345077f4852b2d2c8d9b93532876457bb416865c8c501f9 | ✕ |

### Host Behavior

| Type | Count |
|---|---|
| Module | 143 |
| File | 1008 |
| Environment | 1 |
| System | 15 |
| Registry | 205 |
| User | 1 |

| Type | Count |
| --- | --- |
| Keyboard | 2 |

### Network Behavior

| Type | Count |
| --- | --- |
| HTTP | 9 |
| TCP | 4 |

# ARTIFACTS

## File

| SHA256 | File Names | Category | File Size | MIME Type | Operations | Verdict |
|---|---|---|---|---|---|---|
| 4a74dbaaacb20b26d7237b74ced5bd105b0ff3e2eb3ece3eba7bb93bf224b853 | C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih | Sample File | 279.00 KB | application/vnd.microsoft.portable-executable | Delete, Create, Write, Access | MALICIOUS |
| 55ff1e0a4e5866d565ceeb9baafac73fdcb4464160fc6c78104d935009935cd7 | C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\asdfyhahsdfhasdf.dll | Dropped File | 140.11 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | MALICIOUS |
| 2060c534b8b1d2b20a49ed055b864fb2fd5cfd6371ddf8e92436fb889f3d852d | C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.exe | Downloaded File | 213.50 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | MALICIOUS |
| fc2b7524cb96be03fbb8fe44f1c03d640ffa628397a7af53690d168ede030771 | C:\ProgramData\7357_1641723530_7360.exe | Downloaded File | 200.00 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | MALICIOUS |
| c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858 | c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat | Modified File | 128 bytes | application/octet-stream | - | CLEAN |
| 8739c76e681f900923b900c9df0ef75cf421d39cabb54650c4b9ad19b6a76d85 | _desktop.zip, C:\\ProgramData\\614533357526747_desktop.zip, _docs.zip, C:\\ProgramData\\614533357526747_docs.zip | Dropped File | 22 bytes | application/zip | Access, Delete, Read, Create, Write | CLEAN |
| afad4e3d3d6460731c2ddfe2a5b07a8a0ff046cb94fe2da2f5056157d5fc7b00 | C:\\ProgramData\\614533357526747\system.txt, system.txt | Dropped File | 2.01 KB | text/plain | Access, Delete, Read, Create, Write | CLEAN |
| b99407f512e3d56511540d48a4425e6f98e055882f5211a3a1dc406cf97dac49 | screenshot.jpg, C:\\ProgramData\\614533357526747\screenshot.jpg | Dropped File | 122.57 KB | image/jpeg | Delete, Read, Access | CLEAN |
| 1ddf9ccdf8405a70cb261c09df1cafcdcf0f980e03c441a841d3543b42879259 | outlook.txt, C:\\ProgramData\\614533357526747\outlook.txt | Embedded File | 527 bytes | text/plain | Access, Delete, Read, Create, Write | CLEAN |
| 43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083 | C:\\ProgramData\\softokn3.dll | Downloaded File | 141.45 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| 16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660 | C:\\ProgramData\\sqlite3.dll | Downloaded File | 630.46 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba | C:\\ProgramData\\freebl3.dll | Downloaded File | 326.45 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| 3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd | C:\\ProgramData\\mozglue.dll | Downloaded File | 133.95 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| 334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4 | C:\\ProgramData\\msvcp140.dll | Downloaded File | 429.80 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78 | C:\\ProgramData\\nss3.dll | Downloaded File | 1216.95 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d | C:\\ProgramData\\vcruntime140.dll | Downloaded File | 81.82 KB | application/vnd.microsoft.portable-executable | Create, Write, Access | CLEAN |
| 2ff6c82786ef2ea28345077f4852b2d2c8d9b93532876457bb416865c8c501f9 | _6452595239.zip, C:\\ProgramData\\614533357526747_6452595239.zip | Downloaded File | 119.76 KB | application/zip | Access, Delete, Read, Create, Write | CLEAN |

## Filename

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe | Sample File | Delete, Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| apfHQ | Accessed File | Access | CLEAN |
| C:\Windows\system32\ntdll.dll | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih | Sample File | Delete, Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih:Zone.Identifier | Accessed File | Delete, Access | CLEAN |
| C:\Windows\system32\advapi32.dll | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\wvhwbfa | Accessed File | Access | CLEAN |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.tmp | Accessed File | Create, Delete, Access | CLEAN |
| C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.exe | Downloaded File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\ | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b | Accessed File | Create, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\5dc1a099-4b82-4c89-943c-0b2755346b5b\asdfyhahsdfhasdf.dll | Dropped File | Create, Write, Access | CLEAN |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll | Accessed File | Read, Access | CLEAN |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config | Accessed File | Read, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\8C55.exe.config | Accessed File | Access | CLEAN |
| C:\ProgramData\7357_1641723530_7360.exe | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\softokn3.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\sqlite3.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\freebl3.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\mozglue.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\msvcp140.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\nss3.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\vcruntime140.dll | Downloaded File | Create, Write, Access | CLEAN |
| C:\\ProgramData\\614533357526747 | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\cookies | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\cc | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\autofill | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto | Accessed File | Create, Access | CLEAN |
| passwords.txt | Accessed File | Create, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Google\\Chrome\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Chromium\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Kometa\\User Data\Local State | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Amigo\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Torch\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Orbitum\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Comodo\\Dragon\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Nichrome\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Maxthon5\\Users\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Sputnik\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Epic Privacy Browser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Vivaldi\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\CocCoc\\Browser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\uCozMedia\\Uran\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\QIP Surf\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\CentBrowser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\Elements Browser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\TorBro\\Profile\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\Edge\User Data\\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\CryptoTab Browser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Local\\BraveSoftware\\Brave-Browser\\User Data\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Opera Software\\Opera Stable\\\Local State | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Mozilla\\Firefox\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Moonchild Productions\\Pale Moon\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Waterfox\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\8pecxstudios\\Cyberfox\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\NETGATE Technologies\\BlackHawk\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Mozilla\\icecat\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\K-Meleon\\..\\profiles.ini | Accessed File | Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\Thunderbird\\Profiles\\..\\profiles.ini | Accessed File | Access | CLEAN |
| outlook.txt | Dropped File, Embedded File | Create, Read, Write, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Bitcoin\\ | Accessed File | Create, Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\\ProgramData\\614533357526747\\crypto\\Ethereum\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Electrum | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Electrum-LTC | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\ElectronCash | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Exodus\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\MultiDoge\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Zcash\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\DashCore\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Litecoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Anoncoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\BBQCoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\devcoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\digitalcoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Florincoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Franko\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Freicoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\GoldCoinGLD | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Infinitecoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\IOCoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Ixcoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Megacoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Mincoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Namecoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Primecoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\Terracoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\YACoin\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\ | Accessed File | Create, Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\. | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\. | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\.. | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\.. | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\autofill | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\autofill | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\cc | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\cc | Accessed File | Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\cookies | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\cookies | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\crypto | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\crypto | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\outlook.txt | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\outlook.txt | Accessed File | Access | CLEAN |
| C:\\ProgramData\\614533357526747\\crypto\\jaxx\\passwords.txt | Accessed File | Create, Write, Access | CLEAN |
| C:\Users\RDhJ0CNFevzX\AppData\Roaming\\com.liberty.jaxx\\IndexedDB\\file__0.indexeddb.leveldb\\passwords.txt | Accessed File | Access | CLEAN |
| _desktop.zip | Dropped File | Create, Write, Access | CLEAN |
| _docs.zip | Dropped File | Create, Write, Access | CLEAN |
| system.txt | Dropped File | Create, Write, Access | CLEAN |
| _6452595239.zip | Downloaded File | Create, Read, Write, Access | CLEAN |
| C:\\ProgramData\\614533357526747\autofill | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\cc | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\cookies | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Anoncoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\BBQCoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Bitcoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\DashCore | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\devcoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\digitalcoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\ElectronCash | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Electrum | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Electrum-LTC | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Ethereum | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Exodus | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Florincoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Franko | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Freicoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\GoldCoinGLD | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Infinitecoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\IOCoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Ixcoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\jaxx | Accessed File | Delete, Access | CLEAN |

| File Name | Category | Operations | Verdict |
|---|---|---|---|
| C:\\ProgramData\\614533357526747\crypto\Litecoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Megacoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Mincoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\MultiDoge | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Namecoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Primecoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Terracoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\YACoin | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\crypto\Zcash | Accessed File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747\outlook.txt | Dropped File, Embedded File | Delete, Read, Access | CLEAN |
| C:\\ProgramData\\614533357526747\passwords.txt | Accessed File | Delete, Read, Access | CLEAN |
| C:\\ProgramData\\614533357526747\screenshot.jpg | Dropped File | Delete, Read, Access | CLEAN |
| C:\\ProgramData\\614533357526747\system.txt | Dropped File | Delete, Read, Access | CLEAN |
| C:\\ProgramData\\614533357526747_6452595239.zip | Downloaded File | Delete, Access | CLEAN |
| C:\\ProgramData\\614533357526747_desktop.zip | Dropped File | Delete, Read, Access | CLEAN |
| C:\\ProgramData\\614533357526747_docs.zip | Dropped File | Delete, Read, Access | CLEAN |

## URL

| URL | Category | IP Address | Country | HTTP Methods | Verdict |
|---|---|---|---|---|---|
| http://host-data-coin-11.com | - | 5.188.88.184 | - | POST | MALICIOUS |
| http://data-host-coin-8.com/files/4892_1641897821_7641.exe | - | 5.188.88.184 | - | GET | MALICIOUS |
| http://data-host-coin-8.com/files/2739_1641880829_4069.exe | - | 5.188.88.184 | - | GET | MALICIOUS |
| http://tikwish.com/6.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/1.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/2.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/3.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/4.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/5.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/7.jpg | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com/main.php | - | 192.185.129.112 | - | POST | CLEAN |
| http://tikwish.com | - | 192.185.129.112 | - | POST | CLEAN |

## Domain

| Domain | IP Address | Country | Protocols | Verdict |
|---|---|---|---|---|
| data-host-coin-8.com | 5.188.88.184 | - | DNS, HTTP | MALICIOUS |
| host-data-coin-11.com | 5.188.88.184 | - | HTTP | CLEAN |
| tikwish.com | 192.185.129.112 | - | HTTP | CLEAN |

### IP

| IP Address | Domains | Country | Protocols | Verdict |
|---|---|---|---|---|
| 192.168.0.1 | - | - | UDP, DNS | CLEAN |
| 5.188.88.184 | data-host-coin-8.com, host-data-coin-11.com | Russia | DNS, HTTP, TCP | CLEAN |
| 192.185.129.112 | tikwish.com | United States | DNS, HTTP, TCP | CLEAN |

### Mutex

| Name | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| FE7F15060B875FB9FB2A49F08D5D03120C287F38 | access | explorer.exe | CLEAN |

### Registry

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| \REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE | access | 31a601a28f4a81a69c9b09d7249582b9.virus.exe | CLEAN |
| \REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI | access | 31a601a28f4a81a69c9b09d7249582b9.virus.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer | access | explorer.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion | read, access | explorer.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType | read, access | 8c55.exe | CLEAN |
| HKEY_CURRENT_USER | access | 8c55.exe | CLEAN |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Connections | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Internet Settings\Connections | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows \CurrentVersion\Internet Settings | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ LegacyWPADSupport | read, access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI | read, access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display | read, access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std | read, access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt | read, access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ v4.0.30319 | access | 8c55.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\ v4.0.30319\HWRPortReuseOnSocketBind | read, access | 8c55.exe | CLEAN |
| HKEY_PERFORMANCE_DATA | access | 8c55.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows NT\ \CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\ \9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\13.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\14.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676\\00000001 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676\\00000002 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676\\00000003 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_CURRENT_USER\Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\\9375CFF0413111d3B88A00104B2A6676\\00000004 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\ProductName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Cryptography | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Cryptography\MachineGuid | read, access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{0FA68574-690B-4B00-89AA-B28946231449}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{3c3aafc8-d898-43ec-998f-965ffdae065a}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{65e650ff-30be-469d-b63a-418d71ea1765}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{6913e92a-b64e-41c9-a5e6-cef39207fe89}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{710f4c1c-cc18-4c49-8cbf-51240c89a1a2}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0000-0000-0000000FF1CE}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\ \Uninstall\{90160000-008C-0409-0000-0000000FF1CE}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F} | access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{9BE518E6-ECC6-35A9-88E4-87755C07200F}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {B175520C-86A2-35A7-8619-86DC379688B9}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {BD95A8CD-1D9F-35AD-981A-3E7925026EBB}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d} \DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\{e6e75766-da0f-4ba2-9788-6ea593ce702d} \DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5} | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayName | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}\DisplayVersion | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757\Display Name | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173\Display Name | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860 | access | 7357_1641723530_7360.exe | CLEAN |

| Registry Key | Operations | Parent Process Name | Verdict |
|---|---|---|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860\Display Name | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655\Display Name | read, access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743 | access | 7357_1641723530_7360.exe | CLEAN |
| HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\ \CurrentVersion\\Uninstall\ {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743\Display Name | read, access | 7357_1641723530_7360.exe | CLEAN |

## Reduced dataset

### Process

| Process Name | Commandline | Verdict |
|---|---|---|
| 31a601a28f4a81a69c9b09d7249582b9.virus.exe | "C:\Users\RDhJ0CNFevzX\Desktop\31a601a28f4a81a69c9b09d7249582b9.virus.exe" | MALICIOUS |
| 8c55.exe | C:\Users\RDHJ0C~1\AppData\Local\Temp\8C55.exe | MALICIOUS |
| 7357_1641723530_7360.exe | "C:\ProgramData\7357_1641723530_7360.exe" | MALICIOUS |
| explorer.exe | C:\Windows\Explorer.EXE | SUSPICIOUS |
| svchost.exe | C:\Windows\system32\svchost.exe -k netsvcs | CLEAN |
| bcatcih | C:\Users\RDhJ0CNFevzX\AppData\Roaming\bcatcih | CLEAN |

## YARA / AV

### YARA (3)

| Ruleset Name | Rule Name | Rule Description | File Type | File Name | Classification | Verdict |
|---|---|---|---|---|---|---|
| Malware | SmokeLoader | SmokeLoader memory dump | Memory Dump | - | Downloader | 5/5 |
| Malware | SmokeLoader | SmokeLoader memory dump | Memory Dump | - | Downloader | 5/5 |
| Malware | SmokeLoaderStrings | SmokeLoader strings | Function Strings | function_strings_process_3.txt | Downloader | 5/5 |

# ENVIRONMENT

### Virtual Machine Information

| | |
|---|---|
| Name | win10_64_th2_en_mso2016 |
| Description | win10_64_th2_en_mso2016 |
| Architecture | x86 64-bit |
| Operating System | Windows 10 Threshold 2 |
| Kernel Version | 10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379) |
| Network Scheme Name | Local Gateway |
| Network Config Name | Local Gateway |

### Platform Information

| | |
|---|---|
| Platform Version | 4.4.0 |
| Dynamic Engine Version | 4.4.0 / 12/08/2021 19:04 |
| Static Engine Version | 4.4.0.0 / 2021-12-08 18:00:20 |
| AV Exceptions Version | 4.4.1.6 / 2021-12-14 15:06:27 |
| Link Detonation Heuristics Version | 4.4.1.7 / 2021-12-15 19:11:26 |
| Smart Memory Dumping Rules Version | 4.4.0.0 / 2021-12-08 18:00:20 |
| Signature Trust Store Version | 4.4.1.6 / 2021-12-14 15:06:27 |
| VMRay Threat Identifiers Version | 4.4.1.7 / 2021-12-15 19:11:26 |
| YARA Built-in Ruleset Version | 4.4.1.7 |

### Software Information

| | |
|---|---|
| Adobe Acrobat Reader Version | Not installed |
| Microsoft Office | 2016 |
| Microsoft Office Version | 16.0.4266.1003 |
| Hangul Office | Not installed |
| Hangul Office Version | Not installed |
| Internet Explorer Version | 11.0.10586.0 |
| Chrome Version | Not installed |
| Firefox Version | Not installed |
| Flash Version | Not installed |
| Java Version | Not installed |

### System Information

| | |
|---|---|
| Sample Directory | C:\Users\RDhJ0CNFevzX\Desktop |
| Computer Name | XC64ZB |
| User Domain | XC64ZB |
| User Name | RDhJ0CNFevzX |
| User Profile | C:\Users\RDhJ0CNFevzX |
| Temp Directory | C:\Users\RDHJ0C~1\AppData\Local\Temp |
| System Root | C:\Windows |