# Virtual Analyzer Report



### Submission Context

| Logged    | 2021-05-27 11:32:17 |
|-----------|---------------------|
| Submitter | Manual Submission   |
| Туре      | HTML File           |

### Analysis Overview

| Overall risk level        | High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. |  |  |  |  |
|---------------------------|---|--|--|--|--|
| Detections                | VAN_DROPPER.UMXX, VAN_BACKDOOR.UMXX   |  |  |  |  |
| Exploited vulnerabilities |   |  |  |  |  |
| Analyzed objects          | HTML File 1 - Hawb.html F7911D858AFCCB9E871595374564EFE2D6449377  |  |  |  |  |

### Analysis Environments

|  | W7       | W10 | CentOS w Docker |
|--|----------|-----|-----------------|
| Anti-security, self-preservation                   |          |     |                 |
| Autostart or other system reconfiguration          |          |     |                 |
| Deception, social engineering                      |          |     |                 |
| File drop, download, sharing, or replication       | <b>~</b> |     |                 |
| Hijack, redirection, or data theft                 |          |     |                 |
| Malformed, defective, or with known malware traits | ~        | ~   |                 |
| Process, service, or memory object change          | ~        | ~   |                 |
| Rootkit, cloaking                                  |          |     |                 |
| Suspicious network or messaging activity           | ~        | ~   |                 |

### W7

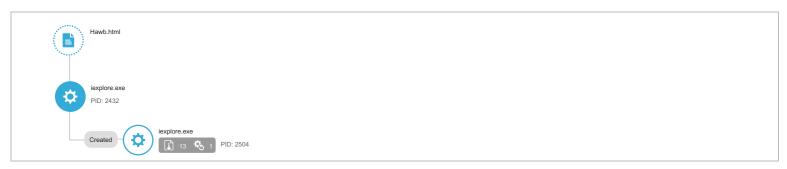
| Environment-specific risk level | High risk  The object exhibited highly suspicious characteristics that are commonly associated with malware. |  |  |  |
|---------------------------------|--|--|--|--|
| Detections                      | VAN_DROPPER.UMXX   |  |  |  |
| Exploited vulnerabilities       |  |  |  |  |
| Network connection              | Custom   |  |  |  |

#### ▼ Object 1 - Hawb.html (HTML File)

| File name | Hawb.html   |
|-----------|---|
| File type | HTML File   |
| SHA-1     | F7911D858AFCCB9E871595374564EFE2D6449377                        |
| SHA-256   | FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E9 |
| MD5       | DEE4CFA9FB0A28C29485245440EF3D50                                |
| Size      | 186357 byte(s)  |

| Risk Level                | High risk  |
|---------------------------|--|
| Detection                 | VAN_DROPPER.UMXX   |
| Exploited vulnerabilities | -  |
| Threat Characteristics    | File drop, download, sharing, or replication (13) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1) Suspicious network or messaging activity (17) |

### Process Graph



### Process Graph Legend

### MITRE ATT&CK™ Framework Tactics and Techniques

| Tactics         | Techniques    | Notable Threat Characteristics                             |
|-----------------|---------------|--|
| Defense Evasion | File Deletion | Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 |

 $\ensuremath{\text{\fontfamily MITRE}}$  Corporation.

### ▼ Notable Threat Characteristics

▼ File drop, download, sharing, or replication (13)

| Characteristic   | Significance | Details   |
|--|--------------|---|
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabED05.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabEA74.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabE9D6.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabE8CA.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabE7EE.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\CabAB48.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection | •            | Process ID: 2504 File: %TEMP%\CabAB68.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\Cab941E.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\Cab935D.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%(Cab93BE.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\Cab937E.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\Cab92BF.tmp Type: VSDT_MSCF |
| Deletes file to compromise the system or to remove traces of the infection |              | Process ID: 2504 File: %TEMP%\Cab925F.tmp Type: VSDT_MSCF |

#### ▼ Malformed, defective, or with known malware traits (1)

| Characteristic                     | Significance | Details   |
|------------------------------------|--------------|-----------|
| Web content contains phishing code |              | Hawb.html |

### ▼ Process, service, or memory object change (1)

| Characteristic  | Significance | Details   |
|-----------------|--------------|---|
| Creates process | •==          | Process ID: 2504 Image Path: %ProgramFiles%Internet Explorer\(\)iexplore.exe SCODEF:2432 CREDAT:79873 |

### ▼ Suspicious network or messaging activity (17)

| Characteristic  | Significance | Details         |
|-----------------|--------------|-----------------|
| Listens on port |              | 0.0.0.0:49184   |
| Listens on port |              | 0.0.0.0:49183   |
| Listens on port |              | 0.0.0.0:49182   |
| Listens on port |              | 0.0.0.0:49181   |
| Listens on port |              | 0.0.0.0:49180   |
| Listens on port |              | 0.0.0.0:49179   |
| Listens on port |              | 0.0.0.0:49178   |
| Listens on port |              | 0.0.0.0:49177   |
| Listens on port |              | 0.0.0.0:49176   |
| Listens on port |              | 0.0.0.0:49175   |
| Listens on port |              | 0.0.0.0:49172   |
| Listens on port |              | 0.0.0.0:49171   |
| Listens on port |              | 0.0.0.0:49170   |
| Listens on port |              | 127.0.0.1:53825 |
| Listens on port |              | 0.0.0.049169    |
| Listens on port |              | 0.0.0.0:49168   |
| Listens on port |              | 127.0.0.1:57644 |

#### ▼ Network Destinations

| Domain                         | IP Address     | Port | Location | Risk Level | Threat | Accessed By |
|--------------------------------|----------------|------|----------|------------|--------|-------------|
| www.download.windowsupdate.com | 93.184.221.240 | 53   | -        | No risk    | -      | Hawb.html   |
| crl.microsoft.com              | 81.198.165.16  | 53   | -        | No risk    | -      | Hawb.html   |
| ie9cvlist.ie.microsoft.com     | 152.199.19.161 | 53   | -        | No risk    | -      | Hawb.html   |
| fonts.googleapis.com           | 142.250.74.10  | 53   | -        | No risk    | -      | Hawb.html   |
| iecvlist.microsoft.com         | 152.199.19.161 | 53   | -        | No risk    | -      | Hawb.html   |
| ocsp.pki.goog                  | 216.58.207.227 | 53   | -        | No risk    | -      | Hawb.html   |
| fonts.gstatic.com              | 216.58.207.195 | 53   | -        | No risk    | -      | Hawb.html   |
| www.microsoft.com              | 2.22.42.141    | 53   | -        | No risk    | -      | Hawb.html   |
| ocsp.pki.goog                  | 216.58.207.227 | 80   | -        | -          | -      | Hawb.html   |
| www.microsoft.com              | 2.22.42.141    | 80   | -        | -          | -      | Hawb.html   |
| iecvlist.microsoft.com         | 152.199.19.161 | 443  | -        | -          | -      | Hawb.html   |
| www.download.windowsupdate.com | 93.184.221.240 | 80   | -        | -          | -      | Hawb.html   |
| www.download.windowsupdate.com | 13.107.4.50    | 80   | -        | -          | -      | Hawb.html   |
| crl.microsoft.com              | 81.198.165.10  | 80   | -        | -          | -      | Hawb.html   |
| fonts.gstatic.com              | 216.58.207.195 | 443  | -        | -          | -      | Hawb.html   |
| fonts.googleapis.com           | 142.250.74.10  | 443  | -        | -          | -      | Hawb.html   |
| iecvlist.microsoft.com         | 152.199.19.161 | 80   | -        | -          | -      | Hawb.html   |

| URL   | Site Category  | Risk Level | Threat | Accessed By |
|---|--|------------|--------|-------------|
| https://fonts.googleapis.com/css?family=PT+Sans:400,700   | Computers / Internet<br>Cloud Applications                       | No risk    | -      | Hawb.html   |
| https://iecvlist.microsoft.com/ie11blocklist/140174<br>6408/versionlist.xml   | Business / Economy<br>Computers / Internet<br>Cloud Applications | No risk    | -      | Hawb.html   |
| https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiT<br>o99u79D0KEww.woff  | Computers / Internet   | No risk    | -      | Hawb.html   |
| http://crl.microsoft.com/pki/crl/products/CodeSign<br>PCA2.crl  | Business / Economy<br>Computers / Internet<br>Cloud Applications | No risk    | -      | Hawb.html   |
| http://www.download.windowsupdate.com/msdow<br>nload/update/v3/static/trustedr/en/authrootstl.ca<br>b   | Software Downloads   | No risk    | -      | Hawb.html   |
| http://ocsp.pki.goog/gls1o1core/MFEwTzBNMEs<br>wSTAJBgUrDgMCGgUABBRCRijDCJxmb3nDwj%<br>2Fxz5aZtZjgXvAQUmNH4bhDrz5vsYJ8YkBug63<br>0J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E<br>%3D | Computers / Internet   | No risk    | -      | Hawb.html   |
| http://www.microsoft.com/pki/certs/MicRooCerAut<br>_2010-06-23.crt  | Business / Economy<br>Computers / Internet<br>Cloud Applications | No risk    | -      | Hawb.html   |
| http://ocsp.pki.goog/gls1o1core/MFIWUDBOMEw<br>wSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%<br>2Fxz5aZIZjgXvAQUmNH4bhDrz5vsYJ8YkBug63<br>0J%2FSsCEQCw80IEZ3xvjQUAAAAAh8vC          | Computers / Internet   | No risk    | -      | Hawb.html   |
| http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJ<br>BgUrDgMCGgUABBTgXlsxbvr2lBkPpolEVRE6g<br>HICnAQUm%2BIHV2ccHsBqBt5ZUot39wZhi4CD<br>QHjIJqhjYqpgSVpULg%3D                     | Computers / Internet   | No risk    |        | Hawb.html   |
| http://ie9cvlist.ie.microsoft.com/IE9CompatViewList.xml   | Business / Economy<br>Computers / Internet<br>Cloud Applications | No risk    | -      | Hawb.html   |
| https://fonts.gstatic.com/s/ptsans/v12/jizfRExUiTo<br>99u79B_mh0O6tKw.woff  | Computers / Internet   | No risk    | -      | Hawb.html   |

### ▼ Dropped or Downloaded Files

| File  | Risk Level | Threat | Threat Characteristics | Source URL   | Size (bytes) | SHA-1  |
|---|------------|--------|------------------------|--|--------------|--|
| {38CCAF38-BEE1-11EB-B06F-08<br>002739B404}.dat                            | No risk    | -      | -                      | -  | 4608         | BB02092AB0D145352017996CF2F2985D1B4<br>7D449 |
| RecoveryStore.{0E12DC2E-BEE1 -11EB-B06F-08002739B404}.dat                 | No risk    | -      | -                      | -  | 4608         | 8286A21E93E6DF15091AD207CA860B2F129<br>A46CC |
| {0E12DC2F-BEE1-11EB-B06F-08<br>002739B404}.dat                            | No risk    | -      | -                      | -  | 4608         | 66B7AD61E6004EA37F3A9CAF2FACDFB8A<br>6A7D995 |
| RecoveryStore.{38CCAF37-BEE1 -11EB-B06F-08002739B404}.dat                 | No risk    | -      | -                      | -  | 3584         | FBBCD6C9EE4AA3DBF515C16D2AD7402E7<br>14AF275 |
| ~DFC01FA64DF190A795.TMP   | No risk    | -      | -                      | -  | 20480        | EA4D9AF1E727D831D32193A96F8BE40290<br>29FEDD |
| ~DF1AAEFA4FE340E9FA.TMP   | No risk    | -      | -                      | -  | 16384        | BF983F1B7E16997577B6E39F3D5E0469204<br>1D210 |
| F0ACCF77CDCBFF39F6191887<br>F6D2D357                                      | No risk    | -      | -                      | -  | 242          | B5938F0F54195EC717A65E77409E71B4F1A<br>A5444 |
| jizfRExUiTo99u79B_mh0O6tKw[1]<br>.woff                                    | No risk    | -      |                        | https://fonts.gstatic.com/s/ptsans/<br>v12/jizfRExUiTo99u79B_mh0O6t<br>Kw.woff | 57524        | 27DF60E5879AA568876F747F3CFACF28564<br>F9B09 |
| CFE86DBBE02D859DC92F1E17<br>E0574EE8_46766FC45507C0B9<br>E264E4C18BC7288B | No risk    | -      |                        | -  | 394          | 5CC3EC7C82ABAA05C4DDBF1647D9744D5<br>31C8D6A |
| CC197601BE0898B7B0FCC91FA<br>15D8A69_8A59D0CC8B8124639<br>3FAF874672C0BE9 | No risk    | -      | -                      | -  | 414          | 3B7225E3FDF0ADD3C7C1A54D70D4673FF<br>E858687 |

#### ▼ Suspicious Objects

| Туре        | Object                                   | Risk Level |
|-------------|--|------------|
| File (SHA1) | F7911D858AFCCB9E871595374564EFE2D6449377 | High       |

#### ▼ Analysis

| Event Type               | Details   | Parent PID | PID  |
|--------------------------|---|------------|------|
| Detection                | Threat Characteristic: Web content contains phishing code   |            |      |
|                          | Hawb.html   |            |      |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\nternet Explorer\Main\CompatibilityFlags Value: 0   |            | 2432 |
| Call Service API         | API Name: OpenServiceA Args: (25a2e18, rasman, 4) Return: 25a2d78   |            | 2432 |
| Call Service API         | API Name: OpenServiceA Args: ( 25a2ff8, RASMAN, 4 ) Return: 25a2f58   |            | 2432 |
| Call Service API         | API Name: OpenServiceW Args: (1ba378, Sens, 4) Return: 1b9ba8   |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\\Internet Settings\ProxyEnable Value: 0   |            | 2432 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\\Internet Settings\ProxyServer Value: None  |            | 2432 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None   |            | 2432 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None   |            | 2432 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None   |            | 2432 |
| Call Network API         | API Name: socket Args: ( 23, 1, 6 ) Return: 408   |            | 2432 |
| Call Network API         | API Name: socket Args: ( 23, 1, 6 ) Return: 408   |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive\{0E12DC2E-BEE1-11EB-B06F-08002739B404\} Value: 0   |            | 2432 |
| Call Service API         | API Name: OpenServiceW Args: ( 25c7048, WSearch, 1 ) Return: 25c6fd0  |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running  |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\SecuritySafe Value: 1  |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FullScreen Value: no   |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window_Placement Value: None   |            | 2432 |
| all Process API          | API Name: CreateProcessW Args: (, "%ProgramFiles%Internet Exploreriexplore.exe" SCODEF:2432 CREDAT:79873,,,, CREATE_SUSPENDED,,,, Process:2504:%ProgramFiles%Internet Exploreriexplore.exe ) Return: 1          |            | 2432 |
| Call Thread API          | API Name: NtResumeThread Args: ( Process:2504, ) Return: ?  |            | 2432 |
| Call System API          | API Name: evtchann.SendEvent Args: ( e), pid[2504], ppid[2432 ) Return: 1   |            | 2432 |
| Call Network API         | API Name: socket Args: ( 2, 2, 0 ) Return: 518  |            | 2432 |
| Call Network API         | API Name: socket Args: ( 23, 2, 0 ) Return: 518   |            | 2432 |
| Detection                | Threat Characteristic: Creates process Process ID: 2504 Image Path: %ProgramFiles%Internet Explorer/iexplore.exe SCODEF:2432 CREDAT:79873   |            |      |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\{E7E4BC40-E76A-11CE-A9BB-00AA004AE837\} {0002 14E6-0000-0000-000000000046} 0xFFFF Value: None                         | 2432       | 2504 |
| Call Service API         | API Name: OpenServiceW Args: ( 3397050, FontCache, 14 ) Return: 3396da8   | 2432       | 2504 |
| Call Service API         | API Name: OpenServiceA Args: ( 33ef0b0, rasman, 4 ) Return: 33ef038   | 2432       | 2504 |
| Call Service API         | API Name: OpenServiceA Args: ( 33ef0b0, RASMAN, 4 ) Return: 33ef100   | 2432       | 2504 |
| Call Service API         | API Name: OpenServiceW Args: ( 33ef380, Sens, 4 ) Return: 33ef308   | 2432       | 2504 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0  | 2432       | 2504 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None   | 2432       | 2504 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None   | 2432       | 2504 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None   | 2432       | 2504 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None   | 2432       | 2504 |
| Call System API          | API Name: evtchann.SendEvent Args: ( e), pid[1416], ppid[2504 ) Return: 1   | 2432       | 2504 |
| Call Service API         | API Name: StartServiceW Args: ( 3396da8, 0, 0 ) Return: 1   | 2432       | 2504 |
| Call Service API         | API Name: StartServiceW Args: ( 3396da8, 0, 0 ) Return: 1   | 2432       | 2504 |
| Call Network API         | API Name: socket Args: ( 23, 1, 6 ) Return: 43c   |            | 2432 |
| Vrite Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\DefaultConnectionSettings Value: None   |            | 2432 |
| Call Internet Helper API | API Name: InternetGetConnectedStateExW Args: ( 3d38c24, 0, 0, 0 ) Return: 1   | 2432       | 2504 |
| Call Network API         | API Name: socket Args: ( 2, 2, 17 ) Return: 4c0   | 2432       | 2504 |
| Call Network API         | API Name: bind Args: (4c0, 127.0.0.1:57644, 16 ) Return: 0  | 2432       | 2504 |
| Detection                | Threat Characteristic: Listens on port 127.0.0.1:57644  |            |      |
| Call Internet Helper API | API Name: InternetOpenW Args: ( Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0), 0, , , 10000000 ) Return: cc0004   | 2432       | 2504 |
| Call System API          | API Name: Internet/OpenW Args: ( Mozilia/s.) (compatible; MSIE 9.0; vvindows NT 6.1; Indent/9.0), 0, , , 10000000 ) Return: ccuou4  API Name: DnsQueryExW Args: ( fonts.googleapis.com, 1, 50000000 ) Return: 0 | 2432       | 2504 |
| Call Internet Helper API | API Name: Dnsqueryexw Args: ( fonts.googleapis.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, fonts.googleapis.com, 443, , , 3, 8388608, 54933528 ) Return: cc0008                    | 2432       | 2504 |
| Call Internet Helper API |   | 2432       | 2504 |
|                          | API Name: HttpOpenRequestW Args: ( cc0008, GET, /css?family=PT+Sans:400,700, , , 64194584, 12582912, 54933528 ) Return: cc000c  |            |      |
| Call System API          | API Name: CreateDXGIFactory Args: ( (787166EC-21C7-44AE-B21A-C9AE321AE369), 3fcf874 ) Return: 0   | 2432       | 2504 |
| Call Network API         | API Name: socket Args: (2, 2, 0) Return: 5f0  | 2432       | 2504 |
| Call Mutex API           | API Name: CreateMutexW Args: (0, 0, SmartScreen_AppRepSettings_Mutex.) Return: 5e8  | 2432       | 2504 |
| Call Mutex API           | API Name: CreateMutexW Args: (0, 0, SmartScreen_ClientId_Mutex ) Return: 5f0  | 2432       | 2504 |
| Call Mutex API           | API Name: CreateMutexW Args: ( 0, 0, CommunicationManager_Mutex ) Return: 5f8   | 2432       | 2504 |
| Call Network API         | API Name: socket Args: (23, 2, 0) Return: 60c   | 2432       | 2504 |
| Call System API          | API Name: DnsQueryExW Args: ( fonts.googleapis.com, 1, 40006000 ) Return: 9701  | 2432       | 2504 |
| Call System API          | API Name: DnsQueryExW Args: ( fonts.googleapis.com, 1c, 40006000 ) Return: 0  | 2432       | 2504 |
| Call Network API         | API Name: socket Args: ( 23, 2, 0 ) Return: 628   | 2432       | 2504 |
| Call Network API         | API Name: socket Args: ( 2, 1, 6 ) Return: 628  | 2432       | 2504 |
| Call Network API         | API Name: bind Args: ( 628, 0.0.0.0:49168, 16 ) Return: 0   | 2432       | 2504 |
| Petection                | Threat Characteristic: Listens on port  |            |      |

| Call Network API      | API Name: connect Args: ( 628, 142.250.74.10:443, 16 ) Return: fffffff   | 2432 | 2504 |
|-----------------------|--|------|------|
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432 | 2504 |
| Call Network API      | API Name: socket Args: ( 2, 1, 6 ) Return: 638   | 2432 | 2504 |
| Call Network API      | API Name: bind Args: ( 638, 0.0.0.0:49169, 16 ) Return: 0  | 2432 | 2504 |
| Detection             | Threat Characteristic: Listens on port   |      |      |
| 2000000               | 0.0.0.49169  |      |      |
| Call Network API      | API Name: connect Args: ( 638, 142.250.74.10:443, 16 ) Return: ffffffff  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: send Args: (4c0, I, 1, 0) Return: 1  | 2432 | 2504 |
|                       |  |      |      |
| Call System API       | API Name: CreateDXGIFactory Args: ( \( 7\text{B7166EC-21C7-44AE-B21A-C9AE321AE369} \), \( 3\text{Cr64BO} \) \( \text{Return: 0} \)   | 2432 | 2504 |
| Call System API       | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3fcf804 ) Return: 0  | 2432 | 2504 |
| Call System API       | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3fcf804 ) Return: 0  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 628,, 133, 0 ) Return: 133  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 638,, 133, 0 ) Return: 133  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
|                       |  |      |      |
| Call Network API      | API Name: send Args: (4c0, I, 1, 0) Return: 1  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 92, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 92, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 1024, 0 ) Return: ?  | 2432 | 2504 |
|                       |  |      |      |
| Call Network API      | API Name: recv Args: ( 638, , 1024, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 628,, 134, 0 ) Return: 134  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 3072, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432 | 2504 |
| Call Network API      | API Name: send Args: ( 638,, 134, 0 ) Return: 134  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 3072, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432 | 2504 |
|                       |  |      |      |
| Call Network API      | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 628, , 3072, 0 ) Return: ?  | 2432 | 2504 |
| Call Network API      | API Name: recv Args: ( 638, , 3072, 0 ) Return: ?  | 2432 | 2504 |
| Call Service API      | API Name: OpenServiceW Args: ( 33cf500, gpsvc, 5 ) Return: 33cf8c0   | 2432 | 2504 |
| Write Registry Key    | Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\46\52C64B7E\LanguageList Value: en-US\0en\0  | 2432 | 2504 |
| Delete Registry Key   | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N  | 2432 | 2504 |
|                       | one  |      |      |
| Write Registry Key    | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None  | 2432 | 2504 |
| Delete Registry Key   | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None   | 2432 | 2504 |
| Write Registry Key    | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None  | 2432 | 2504 |
| Dalata File           |  | 0400 | 0504 |
| Delete File           | Path: %TEMP%\Cab925F.tmp Type: VSDT_MSCF   | 2432 | 2504 |
| Detection             | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504 File: %TEMP%\Cab925F.tmp Type: VSDT_MSCF   |      |      |
| Delete Registry Key   | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None   | 2432 | 2504 |
| Write Registry Key    | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None  | 2432 | 2504 |
| Delete File           | Path: %TEMP%\Cab92BF.tmp Type: VSDT_MSCF   | 2432 | 2504 |
| Detection             | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  |      |      |
| Detection             | Intest Characteristic: Deletes lite to compromise the system of to remove traces of the infection Process ID: 2504 File: %TEMP%\Cab92BF.tmp Type: VSDT_MSCF  |      |      |
| Call Service API      | API Name: OpenServiceW Args: ( 4a1f398, CryptSvc, 5 ) Return: 4a1e998  | 2432 | 2504 |
| Delete File           | Path: %TEMP%(Cab937E.tmp Type: VSDT_MSCF   | 2432 | 2504 |
| Detection             | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504  File: %TEMP%\Cab937E.tmp  Type: \SDIT MSCF  |      |      |
| Delete File           |  | 2432 | 2504 |
| Detection             | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504  File: %TEMP%(Cab93BE.tmp  Type: VSDT_MSCF   | 01   |      |
| Delete File           | Path: %TEMP%\Cab935D.tmp Type: VSDT_MSCF   | 2432 | 2504 |
| Delete File Detection | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504 File: %TEMP%\Cab937E.tmp Type: VSDT_MSCF  Path: %TEMP%\Cab938E.tmp Type: VSDT_MSCF  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504 File: %TEMP%\Cab938E.tmp Type: VSDT_MSCF | 2432 | 2504 |

|   | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504 File: %TEMP%(Cab935D.tmp Type: VSDT_MSCF  |              |              |
|---|---|--------------|--------------|
| Delete File   | Path: %TEMP%\Cab941E.tmp Type: VSDT_MSCF  | 2432         | 2504         |
| Detection   | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504 File: %TEMP%\Cab941E.tmp Type: VSDT_MSCF   |              |              |
| Call Service API  | API Name: OpenServiceW Args: ( 4a76718, WinHttpAutoProxySvc, 94 ) Return: 4a1ec18   | 2432         | 2504         |
| Call Service API  | API Name: OpenServiceW Args: ( 33be7f0, WinHttpAutoProxySvc, 94 ) Return: 33befc0   | 2432         | 2504         |
| all Internet Helper API   | API Name: InternetGetConnectedStateExW Args: ( 37edd7c, 0, 0, 0 ) Return: 1   |              | 2432         |
| all Network API   | API Name: socket Args: ( 2, 2, 17 ) Return: 5a4   |              | 2432         |
| Call Network API  | API Name: bind Args: ( 5a4, 127.0.0.1:53825, 16 ) Return: 0   |              | 2432         |
| etection  | Threat Characteristic: Listens on port 127.0.0.1:53825  |              |              |
| Call Internet Helper API  | API Name: InternetOpenW Args: ( Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0), 0, , , 10000000 ) Return: cc0004   |              | 2432         |
| Call System API   | API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0   |              | 2432         |
| Call Internet Helper API  | API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 76528104 ) Return: cc0008  |              | 2432         |
| Call Internet Helper API  | API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644848, 4194320, 76528104 ) Return: cc000c  |              | 2432         |
| all Network API   | API Name: socket Args: (2, 2, 0) Return: 674  |              | 2432         |
| all Network API   | API Name: socket Args: (23, 2, 0) Return: 674   |              | 2432         |
| all System API  | API Name: DnsQueryExW Args: ( je9cvlist.ie.microsoft.com, 1, 40006000 ) Return: 9701  |              | 2432         |
| all System API all Network API                                      | API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket årre: ( 23, 2, 0, ) Return: 674  |              | 2432         |
| all Network API all Network API                                     | API Name: socket Args: (23, 2, 0) Return: 674  API Name: socket Args: (2, 1, 6) Return: 674   |              | 2432         |
| all Network API   | API Name: socket Args: ( 2, 1, 6 ) Return: 6/4  API Name: bind Args: ( 674, 0.0.0:49170, 16 ) Return: 0   |              | 2432         |
| etection  | API Name: bino Args: (674, 0.0.0.949170, 16) Return: 0  Threat Characteristic: Listens on port  |              | 2402         |
|   | 0.0.0.049170  |              | 2422         |
| all Network API   | API Name: connect Args: ( 674, 152.199.19.161:80, 16 ) Return: ffffffff   |              | 2432         |
| all Network API   | API Name: recv Args: (5a4, , 32, 0) Return: ?   |              | 2432         |
| Call Network API  | API Name: send Args: (544, I, 1, 0) Return: 1  API Name: send Args: (674, CET //E9Compat//joul jet vm HTTP/1 1/m Accord: */*/dn Accord: Encoding: axin, do@alolan log. Accord: Maxilla/5.0 (compatible):  |              | 2432         |
|   | API Name: send Args: (674, GET /IE9CompatViewList.xml HTTP/1.1\n'nAccept: "/"\n'nAccept-Encoding: gzip, deflate\n'n\User-Agent: Mozilla/5.0 [compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0]\n'nhost: ie9cvlist.ie.microsoft.com\n'nConnection: Keep-Alive\n'n\n'n, 219, 0 ) Return: 219 |              |              |
| all Network API   | API Name: recv Args: ( 674, , 1024, 0 ) Return: ?   |              | 2432         |
| all Network API   | API Name: send Args: (5a4, I, 1, 0) Return: 1   |              | 2432         |
| all Network API   | API Name: recv Args: ( 5a4, , 32, 0 ) Return: ?   |              | 2432         |
| all Network API   | API Name: recv Args: ( 674, , 1024, 0 ) Return: ?  API Name: recv Args: ( 674, , 8192, 0 ) Return: ?  |              | 2432         |
|   |   |              | 2432         |
| all Network API   | API Name: recv Args: ( 674, , 4969, 0 ) Return: ?  API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |              | 2432         |
| dd File   | Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9Compat\ViewList[1].xml Type: VSDT_TEXT_HTML   |              | 2432         |
| Vrite File  | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9Compat\ViewList[1].xml Type: VSDT_TEXT_HTML   |              | 2432         |
| dd File   | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_EMPTY   |              | 2432         |
| Vrite File  | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   |              | 2432         |
| Call Filesystem API   | API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\internet Explorer\iECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1  |              | 2432         |
| Vrite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Exploren\GPU\VersionHigh Value: 0  |              | 2432         |
| Vrite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\VersionLow Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\DXFeatureLevel Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-Vendorld Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DeviceId Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-SubSysld Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-Revision Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionHigh Value: 0  |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionLow Value: 0   |              | 2432         |
| /rite Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DXFeatureLevel Value: 0   |              | 2432         |
| all Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: 8d8  | 2432         | 2504         |
| all Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8d8   | 2432         | 2504         |
| all Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: 8e0  | 2432         | 2504         |
| all Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8e0   | 2432         | 2504         |
| all System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1, 40006000 ) Return: 9701  | 2432         | 2504         |
| all System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1, 40006000 ) Return: 9701  | 2432         | 2504         |
| all System API  | API Name: CreateDXGIFactory Args: ( (787166EC-21C7-44AE-821A-C9AE321AE369), 37edd90 ) Return: 0   | 2422         | 2432         |
| all System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1c, 40006000 ) Return: 0  | 2432         | 2504         |
| all Network API   | API Name: socket Args: (23, 2, 0) Return: 8e0   | 2432         | 2504         |
| all Network API   | API Name: socket Args: (2, 2, 0) Return: 8e0  API Name: socket Args: (23, 2, 0) Return: 8e0   | 2432         | 2504         |
| all Network API   | API Name: socket Args: (23, 2, 0) Return: 8e0  API Name: DecQueriEv/M Args: (uses described windows) and 1, 40006000 \ Paturn: 9701   | 2432         | 2504         |
| all System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.download.windowsupdate.com 1c, 40006000 ) Return: 0   | 2432         | 2504<br>2504 |
| all System ADI  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8e0   | 2432         | 2504         |
| Call System API   |   | 4404         | 2004         |
| all Network API   |   | 2432         | 2504         |
| all System API  all Network API  fall Network API  fall Network API | API Name: socket Args: (2, 1, 6) Return: 8e0  API Name: bind Args: (8e0, 0.0.0.049171, 128) Return: 0   | 2432<br>2432 | 2504<br>2504 |

| Call System API  | API Name: ConnectEx Args: ( 8e0, 13.107.4.50:80, 16, 0, 0, 0, 4a12590 ) Return: 0  | 2432   | 2504   |
|--|--|--|--|
| Call Network API   | API Name: send Args: ( 8e0, GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1\r\nCache-Control: max-age = 12819\r\nConnection: Kee   | 2432   | 2504   |
|  | p-AlivelnAccept: "/"nnlf-Modified-Since: Fri, 12 Sep 2014 18:47:05 GMT\nlf-None-Match: "805a83f2b9cecf1:0"\nnUser-Agent: Microsoft-CryptoAPI/6.1\nn  |  |  |
|  | Host: www.download.windowsupdate.comlr\n\r\n, 1, 303 ) Return: 0   |  |  |
| Call System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1c, 40006000 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8e4  | 2432   | 2504   |
| Call Network API   | API Name: socket Args: (2, 2, 0) Return: 8e4   | 2432   | 2504   |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8e4  | 2432   | 2504   |
|  |  |  |  |
| Call System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1, 40006000 ) Return: 9701   | 2432   | 2504   |
| Call System API  | API Name: DnsQueryExW Args: ( www.download.windowsupdate.com, 1c, 40006000 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8e4  | 2432   | 2504   |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: 8e4   | 2432   | 2504   |
| Call Network API   | API Name: bind Args: ( 8e4, 0.0.0.949172, 128 ) Return: 0  | 2432   | 2504   |
| Detection  | Threat Characteristic: Listens on port   |  |  |
| 20.00.0.1  | 0.0.0.49172  |  |  |
| Call System API  | API Name: ConnectEx Args: ( 8e4, 93.184.221.240:80, 16, 0, 0, 0, 4a12590 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: send Args: ( 8e4, GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1\r\nCache-Control: max-age = 12819\r\nConnection: Kee   | 2432   | 2504   |
| Can House III  | p-Alive\n/nAccept: "\n/\n/III-Modified-Since: Fri, 12 Sep 2014 18:47:05 GMT\n/\n/II-None-Match: "805a83/2b9cecf1:0"\n/\n/\ser-Agent: Microsoft-CryptoAPI/6.1\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\   | 2.02   | 2501   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 33/4ff0 ) Return: 1   | 2432   | 2504   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 33e4bc8 ) Return: 1   | 2432   | 2504   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4a34800 ) Return: 1   | 2432   | 2504   |
|  |  |  |  |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1   | 2432   | 2504   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4a4e260 ) Return: 1   | 2432   | 2504   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4afe630 ) Return: 1   | 2432   | 2504   |
| Delete File  | Path: %TEMP%\CabAB68.tmp Type: VSDT_MSCF   | 2432   | 2504   |
| Detection  | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504   |  |  |
|  | File: %TEMP%ICabAB68.tmp Type: VSDT_MSCF   |  |  |
| Delete File  | Path: %TEMP%\CabAB48.tmp Type: VSDT_MSCF   | 2432   | 2504   |
| Detection  | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  |  |  |
|  | Process ID: 2504 File: %TEMP%\CabAB48.tmp Type: VSDT_MSCF  |  |  |
| Call Network API   |  |  | 2432   |
|  | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |  |  |
| Call Network API   | API Name: recv Args: (674, 1, 2) Return: ?   |  | 2432   |
| Call System API  | API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  |  | 2432   |
| Call Internet Helper API   | API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 76668112 ) Return: cc0008   |  | 2432   |
| Call Internet Helper API   | API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 76668112 ) Return: cc000c   |  | 2432   |
| Add File   | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  |  | 2432   |
|  |  |  |  |
| Write File   | Path: %LOCALAPPDATA%IMicrosoftInternet ExplorerIECompatData\(\)iecompatdata.xml Type: VSDT_TEXT_HTML   |  | 2432   |
| Call Filesystem API  | API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9Compat\ViewList[1].xml, %L OCALAPPDATA%\Microsoft\Internet Explorer\IECompat\Data\iecompat\Data\iecompat\Data\iecompat\Data\iecompat\Data\iecompat\Uectrice (0, 0, 0, 0) Return: 1   |  | 2432   |
| Call Network API   | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |  | 2432   |
|  |  |  |  |
| Call Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: 8d0   | 2432   | 2504   |
|  | API Name: socket Args: ( 23, 2, 0 ) Return: 8d0  | 2432   | 2504   |
| Call Network API   |  |  |  |
|  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  | 2432   | 2504   |
| Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0   | 2432<br>2432   | 2504<br>2504   |
| Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  | 2432   |  |
| Call System API<br>Call System API<br>Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0 API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  | 2432<br>2432   | 2504<br>2504   |
| Call System API Call System API Call Network API Call Network API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 2, 2, 0 ) Return: 8d4   | 2432<br>2432<br>2432   | 2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 2, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  | 2432<br>2432<br>2432<br>2432                                 | 2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 2, 2, 0 ) Return: 8d4   | 2432<br>2432<br>2432   | 2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 2, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  | 2432<br>2432<br>2432<br>2432                                 | 2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  | 2432<br>2432<br>2432<br>2432<br>2432                         | 2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432                 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 24, 6 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.049175, 128 ) Return: 0  Threat Characteristic: Listens on port  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432         | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call Network API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 2, 1, 6 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0:49175   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call System API Call Network API Call Network API Call System API Call System API Call Network API Call System API Call System API Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.049175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.049175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call System API Call Network API Call Network API Call System API Call System API Call Network API Call System API Call System API Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0:49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.11vinConnection: Keep-Alive\nAccept: 1"\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0/49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.0/49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser-Agent: Microsoft-Crypto API/6.1\tr\inHost: www.microsoft.com\tr\in\ | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.0:49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\r\inConnection: Keep-Alive\r\inAccept: */"\r\inUser-Agent: Microsoft-Crypto API/6.1\r\inHost: www.microsoft.com\r\in\r\in\r\in, 1, 154 ) Return: 0  API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API  Call Network API  Call Network API  Call Network API  Call System API  Call System API  Call Network API  Call System API  Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0/49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.0/49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser-Agent: Microsoft-Crypto API/6.1\tr\inHost: www.microsoft.com\tr\in\ | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call Network API Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.0:49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\r\inConnection: Keep-Alive\r\inAccept: */"\r\inUser-Agent: Microsoft-Crypto API/6.1\r\inHost: www.microsoft.com\r\in\r\in\r\in, 1, 154 ) Return: 0  API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call System API  | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: Socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.049175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.049175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET/pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-Crypto API/6.1\r\nHost: www.microsoft.com\r\n\r\n\r\n, 1, 154 ) Return: 0  API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0:49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCer/Aut_2010-06-23.crt HTTP/1.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\User-Agent: Microsoft-Crypto API/6.1\tr\inHost: www.microsoft.com\tr\in\tr\in\tr\in, 1, 154 ) Return: 0  API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442490 ) Return: 1  API Name: Send Args: ( 8d4, GET /pki/certs/MicRooCer/Aut_2010-06-23.crt HTTP/1.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser-Agent: Microsoft-Crypto API/6.1\tr\inHost: www.microsoft.com\tr\in\tr\in\tr\in\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser-Agent: Microsoft-Crypto API/6.1\tr\inHost: WinHttpCloseHandle Args: ( 3442578 ) Return: 1  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCer/Aut_2010-06-23.crt HTTP/1.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser-Agent: Microsoft-Crypto API/6.1\tr\inConnection: Keep-Alive\tr\inAccept: \tau'\tr\in\tr\inUser | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 24, 1, 6 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.49175, 128 ) Return: 0  Threat Characteristic: Listens on port  0.0.0.49175  API Name: ConnectEx Args: ( 8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1VinConnection: Keep-Alive\rinAccept: */"\rinUser-Agent: Microsoft-Crypto API/6.1\rinHost: www.microsoft.com\rin\rin, 1, 154 ) Return: 0  API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1  API Name: winHttpCloseHandle Args: ( 3442290 ) Return: 1  API Name: send Args: ( 8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.1\rinConnection: Keep-Alive\rinAccept: */"\rinUser-Agent: Microsoft-Crypto API/6.1\rinHost: www.microsoft.com\rin\rin, 1, 154 ) Return: 0  Path: "TEMP%/CabETEE.tmp Type: VSDT_MSCF  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504  File: "TEMP%/CabETEE.tmp   | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call S | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 24, 1, 6 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API  | API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701  API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701  API Name: DnsQueryExW Args: (www.microsoft.com, 16, 40006000) Return: 0  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (24, 1, 6) Return: 8d4  API Name: socket Args: (8d4, 0, 0.0.0:49175, 128) Return: 0  Threat Characteristic: Listens on port 0, 0.0.49175  API Name: SonnectEx Args: (8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8) Return: 0  API Name: SonnectEx Args: (8d4, 6ET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.11/InConnection: Keep-AliveivinAccept: '/"vinUser-Agent: Microsoft-Crypto API/6.11/inHost: www.microsoft.com/ini/in, 1, 154) Return: 1  API Name: WinHttpCloseHandle Args: (3442578) Return: 1  API Name: WinHttpCloseHandle Args: (3442490) Return: 1  API Name: send Args: (8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.11/InConnection: Keep-AliveivinAccept: '/"vinUser-Agent: Microsoft-Crypto API/6.11/inHost: www.microsoft.com/ini/in, 1, 154) Return: 0  Path: %TEMP%/CabETZE:.tmp Type: VSDT_MSCF  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504  File: %TEMP%/CabETZE:.tmp Type: VSDT_MSCF  API Name: WinHttpCloseHandle Args: (495ec00) Return: 1   | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504 |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API   | API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: DnsQueryExW Args: ( www.microsoft.com, 1, 40006000 ) Return: 9701  API Name: DnsQueryExW Args: ( www.microsoft.com, 1c, 40006000 ) Return: 9701  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 23, 2, 0 ) Return: 8d4  API Name: socket Args: ( 24, 1, 6 ) Return: 8d4  API Name: bind Args: ( 8d4, 0.0.0.0:49175, 128 ) Return: 0  Threat Characteristic: Listens on port  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API   | API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701  API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701  API Name: DnsQueryExW Args: (www.microsoft.com, 16, 40006000) Return: 0  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (23, 2, 0) Return: 8d4  API Name: socket Args: (24, 1, 6) Return: 8d4  API Name: socket Args: (8d4, 0, 0.0.0:49175, 128) Return: 0  Threat Characteristic: Listens on port 0, 0.0.49175  API Name: SonnectEx Args: (8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8) Return: 0  API Name: SonnectEx Args: (8d4, 6ET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.11/InConnection: Keep-AliveivinAccept: '/"vinUser-Agent: Microsoft-Crypto API/6.11/inHost: www.microsoft.com/ini/in, 1, 154) Return: 1  API Name: WinHttpCloseHandle Args: (3442578) Return: 1  API Name: WinHttpCloseHandle Args: (3442490) Return: 1  API Name: send Args: (8d4, GET /pki/certs/MicRooCerAut_2010-06-23.crt HTTP/1.11/InConnection: Keep-AliveivinAccept: '/"vinUser-Agent: Microsoft-Crypto API/6.11/inHost: www.microsoft.com/ini/in, 1, 154) Return: 0  Path: %TEMP%/CabETZE:.tmp Type: VSDT_MSCF  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504  File: %TEMP%/CabETZE:.tmp Type: VSDT_MSCF  API Name: WinHttpCloseHandle Args: (495ec00) Return: 1   | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504 |

| Detection        | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504 File: %TEMP%\CabE8CA.tmp Type: VSDT_MSCF   |      |      |
|------------------|---|------|------|
| Call Network API | API Name: send Args: ( 8e0, GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1\r\nCache-Control: max-age = 900\r\nConnection: Keep-Alive\r\nAccept: *\"\r\nIf-Modified-Since: Mon, 19 Apr 2021 20:17:25 GMT\r\nIf-None-Match: "80f8835935d71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHo st: www.download.windowsupdate.com\r\n\r\n, 1, 299 ) Return: 0  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442660 ) Return: 1  | 2432 | 2504 |
|                  |   |      |      |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1  | 2432 | 2504 |
| all Network API  | API Name: send Args: ( 8e4, GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1\r\nCache-Control: max-age = 900\r\nConnection: Keep-Alive\r\nAccept: "\"\r\nIf-Modified-Since: Mon, 19 Apr 2021 20:17:25 GMT\r\nIf-None-Match: "80/8835935d71:0\"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHo st: www.download.windowsupdate.com\r\n\r\n, 1, 299 ) Return: 0 | 2432 | 2504 |
| Delete File      | Path: %TEMP%CabE9D6.tmp Type: VSDT_MSCF   | 2432 | 2504 |
| Detection        | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2504 File: %TEMP%\CabE9D6.tmp Type: VSDT_MSCF   |      |      |
| Call System API  | API Name: WinHttpCloseHandle Args: (4b76df8 ) Return: 1   | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442748 ) Return: 1  | 2432 | 2504 |
|                  |   |      |      |
| Delection        | Path: %TEMP%(CabEA74.tmp Type: VSDT_MSCF  Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504  File: %TEMP%(CabEA74.tmp  Type: VSDT_MSCF  | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 2, 0 ) Return: 920  | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 920   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 2, 0 ) Return: 914  | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 914   | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1, 40006000 ) Return: 9701   | 2432 | 2504 |
|                  |   |      |      |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1, 40006000 ) Return: 9701   | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1c, 40006000 ) Return: 0   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 914   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 2, 0 ) Return: 914  | 2432 | 2504 |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 914   | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1c, 40006000 ) Return: 0   | 2432 | 2504 |
| Call Network API |   | 2432 | 2504 |
|                  | API Name: socket Args: (23, 2, 0) Return: 914   |      |      |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1, 40006000 ) Return: 9701   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 2, 0 ) Return: 914  | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1c, 40006000 ) Return: 0   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 8d0   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 1, 6 ) Return: 8d0  | 2432 | 2504 |
| Call Network API | API Name: bind Args: ( 8d0, 0.0.0.49176, 128 ) Return: 0  | 2432 | 2504 |
| Detection        | Threat Characteristic: Listens on port 0.0.0.0.49176  |      |      |
| Call System API  | API Name: ConnectEx Args: ( 8d0, 216.58.207.227:80, 16, 0, 0, 0, 4a11910 ) Return: 0  | 2432 | 2504 |
|                  |   |      |      |
| Call Network API | API Name: socket Args: (23, 2, 0) Return: 914   | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1, 40006000 ) Return: 9701   | 2432 | 2504 |
| Call System API  | API Name: DnsQueryExW Args: ( ocsp.pki.goog, 1c, 40006000 ) Return: 0   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 914   | 2432 | 2504 |
| Call Network API | API Name: socket Args: ( 2, 1, 6 ) Return: 914  | 2432 | 2504 |
| Call Network API | API Name: bind Args: ( 914, 0.0.0.0:49177, 128 ) Return: 0  | 2432 | 2504 |
| Detection        | Threat Characteristic: Listens on port 0.0.0.0:49177  |      |      |
| Call System API  | API Name: ConnectEx Args: ( 914, 216.58.207.227:80, 16, 0, 0, 0, 4a119d8 ) Return: 0  | 2432 | 2504 |
| Call Network API | API Name: send Args: ( 8d0, GET /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXlsxbvr2lBkPpolEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4 CDQHjtJqhjYqpgSVpULg%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPl/6.1\r\nhots: ocsp.pki.goog\r\n\r\n, 1, 23 0 ) Return: 0  | 2432 | 2504 |
| Call Network API | API Name: send Args: ( 914, GET /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXlsxbvr2/lBkPpolEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZiJot39wZhi4 CDQHjtJqhjYqpgSVpULg%3D HTTP/1.1\r/inConnection: Keep-AlivelvinAccept: */"\r/inUser-Agent: Microsoft-CryptoAPl/6.1\r/inhtost: ocsp.pki.goog\r/in\r/in, 1, 23 0 ) Return: 0   | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1  | 2432 | 2504 |
|                  | API Name: WinHttpCloseHandle Args. ( 4402600 ) Return: 1  API Name: WinHttpCloseHandle Args. ( 3442578 ) Return: 1  | 2432 | 2504 |
| Call System API  |   |      |      |
| Call System API  | API Name: WinHttpCloseHandle Args: (3442748 ) Return: 1   | 2432 | 2504 |
| Call Network API | API Name: send Args: ( 8d0, GET /gts1o1core/MFlwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZf2jgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEQCw80IEZ3xvjQUAAAAAh8vC HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.pki.g oog\r\n\r\n, 1, 240 ) Return: 0  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4b91e50 ) Return: 1  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442918 ) Return: 1  | 2432 | 2504 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  | 2432 | 2504 |
|                  |   |      |      |
| Call System API  | API Name: WinHttpCloseHandle Args: (4abca80 ) Return: 1   | 2432 | 2504 |
|                  | API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1  | 2432 | 2504 |
|                  |   |      |      |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442748 ) Return: 1  | 2432 | 2504 |

| Detection                         | Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 2504  |              |              |
|-----------------------------------|--|--------------|--------------|
|                                   | File: %TEMP%\CabED05.tmp Type: VSDT_MSCF   |              |              |
| Call Network API                  | API Name: send Args: ( 914, GET /gls1o1core/MFlwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEQCw80IEZ3xvjQUAAAAAh8vC HTTP/1.1\r\nCache-Control: max-age = 86400\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Micros oft-CryptoAPli6.1\r\nHotst: ocsp.pki.goog\r\n\r\n, 1, 272 ) Return: 0  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: (638, , 1, 2) Return: ?   | 2432         | 2504         |
| Call System API                   | API Name: WinHttpCloseHandle Args: ( 4abca80 ) Return: 1   | 2432         | 2504         |
| Call System API                   | API Name: WinHttpCloseHandle Args: ( 3442578 ) Return: 1   | 2432         | 2504         |
| Call System API                   | API Name: WinHttpCloseHandle Args: ( 3442748 ) Return: 1   | 2432         | 2504         |
| Call Network API                  | API Name: send Args: (628,RANAVtbz[.e.U3wU.&V.S,4*<]   | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 628, , 1500, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 628, , 1500, 0 ) Return: ?  | 2432         | 2504         |
| Call System API                   | API Name: BCryptDecrypt Args: (4a1ceo), HTTP/1.1 200 OKt/nContent-Type: text/css; charset=utf-8l/nAccess-Control-Allow-Origin: "n/nTming-Allow-Origin: "n/nExpires: Thu, 27 May 2021 11:56:26 GMTn/nDate: Thu, 27 May 2021 11:56:26 GMTn/nDate: Thu, 27 May 2021 11:56:26 GMTn/nDate: Drivate, max-age=86400\tinCross-Origin-Resource-Policy: cross-origin\tinContent-Encoding: gzip\tinServer: ESF\tinX-XSS-Protection: 0\tinNx-Frame-Options: SAMEORIGIN\tinNx-Content-Type-Options: no sniff\tin\tinL\tinSvc: h3-29=":443"; ma=2592000, h3-D045=":443"; ma=2592000, h3-Q045=":443"; ma=2592000, n3-Q045=":443"; ma=2592000, quic=":443"; ma=2592000, v="46, 43"\tinTransfer-Encoding: chunked\tin\tin\tin00000001\tin, 944, 0, , 0, HTTP/1.1 200 OK\tinContent-Type: text/c ss; charset=utf-8\tin\tinAccess-Control-Allow-Origin: "\tin\tinTiming-Allow-Origin: "\tin\tinExpires: Thu, 27 May 2021 11:56:26 GMT\tinDate: Thu, 27 May 2021 11:56: | 2432         | 2504         |
| Call System API                   | API Name: BCryptDecrypt Args: ( 4a1cec0, 00000001\r\n, 80, 0, , 0, 00000001\r\n, 117, 85325176, 0 ) Return: 0  | 2432         | 2504         |
| Call System API                   | API Name: BCryptDecrypt Args: ( 4a1cec0, 0\r\n\r\nH'Z\rangle^*, 32, 0, , 0, 0\r\n\r\nH'Z\rangle^*, 32, 85325176, 0 ) Return: 0   | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 628, , 1, 2 ) Return: ?   | 2432         | 2504         |
| Add File                          | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\css[1].css Type: VSDT_ASCII   | 2432         | 2504         |
| Write File                        | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\css[1].css Type: VSDT_ASCII   | 2432         | 2504         |
| Call System API                   | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft ) Return: 1   | 2432         | 2504         |
| Call System API                   | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer ) Return: 1   | 2432         | 2504         |
| Call System API                   | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer ) Return: 1   | 2432         | 2504         |
| Call System API                   | API Name: DnsQueryExW Args: ( fonts.gstatic.com, 1, 50000000 ) Return: 0   | 2432         | 2504         |
| Call Internet Helper API          | API Name: InternetConnectW Args: ( cc0004, fonts.gstatic.com, 443, , , 3, 8388608, 54933528 ) Return: cc0008   | 2432         | 2504         |
| Call Internet Helper API          | API Name: HttpOpenRequestW Args: ( cc0008, GET, /s/ptsans/v12/jizaRExUiTo99u79D0KEww.woff, , , 64207332, 12582912, 54933528 ) Return: cc000c   | 2432         | 2504         |
| Call Network API                  | API Name: socket Args: ( 2, 2, 0 ) Return: 760   | 2432         | 2504         |
| Call Network API                  | API Name: socket Args: ( 23, 2, 0 ) Return: 760  | 2432         | 2504         |
| Call System API                   | API Name: DnsQueryExW Args: ( fonts.gstatic.com, 1, 40006000 ) Return: 9701  | 2432         | 2504         |
| Call System API                   | API Name: DnsQueryExW Args: ( fonts.gstatic.com, 1c, 40006000 ) Return: 0  | 2432         | 2504         |
| Call Network API                  | API Name: socket Args: ( 23, 2, 0 ) Return: 8f8  | 2432         | 2504         |
| Call Network API                  | API Name: socket Args: ( 2, 1, 6 ) Return: 8f8   | 2432         | 2504         |
| Call Network API                  | API Name: bind Args: ( 8f8, 0.0.0.0:49178, 16 ) Return: 0  | 2432         | 2504         |
| Detection                         | Threat Characteristic: Listens on port 0.0.0.0.49178   |              |              |
| Call Network API                  | API Name: connect Args: ( 8f8, 216.58.207.195:443, 16 ) Return: fffffff  | 2432         | 2504         |
| Call Network API                  | API Name: send Args: ( 4c0, 1, 1, 0 ) Return: 1  | 2432         | 2504         |
| Call Network API                  | API Name: socket Args: ( 2, 1, 6 ) Return: 928   | 2432         | 2504         |
| Call Network API  Detection       | API Name: bind Args: (928, 0.0.0.49179, 16) Return: 0  Threat Characteristic: Listens on port  | 2432         | 2504         |
| 0.884                             | 0.0.0.49179  | 0400         | 0504         |
| Call Network API                  | API Name: connect Args: ( 928, 216.58.207.195:443, 16 ) Return: ffffffff   | 2432         | 2504         |
| Call Network API                  | API Name: send Args: (4c0, 1, 1, 0) Return: 1  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: (4c0, 32, 0) Return: ?  API Name: recv Args: (4c0, 32, 0) Return: ?   | 2432         | 2504         |
| Call Network API Call Network API | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  API Name: send Args: ( 8f8,, 130, 0 ) Return: 130   | 2432         | 2504<br>2504 |
| Call Network API                  | API Name: Seno Args: ( 8/8, , 1024, 0 ) Return: 130  API Name: recv Args: ( 8/8, , 1024, 0 ) Return: ?   | 2432         | 2504         |
| Call Network API                  | API Name: send Args: ( 4c0, I, 1, 0 ) Return: 1  | 2432         | 2504         |
| Call Network API                  | API Name: send Args. ( 4c0, ; , 1, 0 ) Return. 1  API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: send Args: ( 928,, 130, 0 ) Return: 130  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: (928, , 1024, 0) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: send Args: ( 4c0, 1, 1, 0 ) Return: 1  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?  | 2432         | 2504         |
| Call System API                   | API Name: DnsQueryExW Args: ( fonts.gstatic.com, 1, 50000000 ) Return: 0   | 2432         | 2504         |
| Call Internet Helper API          | API Name: InternetConnectW Args: ( cc0004, fonts.gstatic.com, 443, , , 3, 8388608, 78349192 ) Return: cc0010   | 2432         | 2504         |
| Call Internet Helper API          | API Name: HttpOpenRequestW Args: ( cc0010, GET, /s/ptsans/v12/jiz/RExUITo99u79B_mh006tKw.woff, , , 64207332, 12582912, 78349192 ) Return: cc001 4  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 8f8, , 1024, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 928, , 1024, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  | API Name: recv Args: ( 8f8, , 92, 0 ) Return: ?  | 2432         | 2504         |
|                                   | API Name: recv Args: ( 928, , 92, 0 ) Return: ?  | 2432         | 2504         |
| Call Network API                  |  |              |              |
| Call Network API                  | API Name: recv Args: ( 8f8, , 1024, 0 ) Return: ?  | 2432         | 2504         |
|                                   | API Name: recv Args: ( 8f8, , 1024, 0 ) Return: ?  API Name: recv Args: ( 928, , 1024, 0 ) Return: ?   | 2432<br>2432 | 2504<br>2504 |

| Call Network API  |   |  |  |
|---|---|--|--|
|   | API Name: recv Args: ( 928, , 1024, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 8f8,, 134, 0 ) Return: 134   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 8f8, , 3072, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 4c0, I, 1, 0 ) Return: 1   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 8f8, , 3072, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: (928,, 134, 0 ) Return: 134  | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 928, , 3072, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: (4c0, !, 1, 0 ) Return: 1  | 2432   | 2504   |
|   |   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?   |  |  |
| Call Network API  | API Name: recv Args: ( 928, , 3072, 0 ) Return: ?   | 2432   | 2504   |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3d3c094 ) Return: 0   | 2432   | 2504   |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3d3c024 ) Return: 0   | 2432   | 2504   |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3d3c024 ) Return: 0   | 2432   | 2504   |
| Call System API   | API Name: DnsQueryExW Args: ( fonts.gstatic.com, 1, 50000000 ) Return: 0  | 2432   | 2504   |
| Call Internet Helper API  | API Name: InternetConnectW Args: ( cc0004, fonts.gstatic.com, 80, , , 3, 0, 1995256424 ) Return: cc0018   | 2432   | 2504   |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 960  | 2432   | 2504   |
| Call Network API  | API Name: bind Args: ( 960, 0.0.0.49180, 16 ) Return: 0   | 2432   | 2504   |
| Detection   | Threat Characteristic: Listens on port  |  |  |
| 0.000   | 0.0.0.49180   | 0400   | 0504   |
| Call Network API  | API Name: connect Args: ( 960, 216.58.207.195:443, 16 ) Return: fffffff   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 960,, 162, 0 ) Return: 162   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 960, , 1024, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 4c0, , 32, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1   | 2432   | 2504   |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3d3c024 ) Return: 0   | 2432   | 2504   |
| Call Network API  | API Name: recv Args: ( 960, , 1024, 0 ) Return: ?   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 960,, 59, 0 ) Return: 59   | 2432   | 2504   |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3d3c0e4 ) Return: 0   | 2432   | 2504   |
| Call Network API  | API Name: send Args: ( 8d0, GET /gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBu   | 2432   | 2504   |
|   | g630J%2FSsCEBow%2FX18SvRyAwAAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: o csp.pki.goog\r\n\r\n, 1, 244 ) Return: 0  |  |  |
| Call Network API  | API Name: send Args: (914, GET /gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: o csp.pki.goog\r\n\r\n, 1, 244 ) Return: 0   | 2432   | 2504   |
|   | API Name: WinHttpCloseHandle Args: ( 49e79b0 ) Return: 1  | 2432   | 2504   |
| Call System API   | AFT Name. Will http://oserianule.aigs. ( 496/900 ) Neturn. 1  |  | 2001   |
| Call System API  Call System API  | API Name: WinHttpCloseHandle Args. ( 4342a00 ) Return: 1  | 2432   | 2504   |
|   |   | 2432<br>2432   |  |
| Call System API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  |  | 2504   |
| Call System API Call System API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1 API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1   | 2432   | 2504<br>2504   |
| Call System API Call System API Call Network API  | API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  API Name: send Args: ( 8f8,0,  &V.Y3,'a.qV.\nls53\r?b\%.Mp?"G.mABeGKC*a`C.Uo\zKG\t.\rV, 309, 0 ) Return: 309  | 2432   | 2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 818,0. &V.Y3'aqV.\nts53\r'?b%.Mp?"G.mABeGKC*a'C.Uo\zKG\t.\rV, 309, 0 ) Return: 309  API Name: recv Args: ( 818,10, 0 ) Return: ?  API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  | 2432<br>2432<br>2432   | 2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 8f8,0,&V.Y3'a.,,V.\nts53ir'?b%.Mp?"G.mABeGKC*a'C.Uo\zKG\t.\rV, 309, 0 ) Return: 309  API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?  API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  API Name: recv Args: ( 4c0, ., 32, 0 ) Return: ?  | 2432<br>2432<br>2432<br>2432<br>2432                         | 2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 8f8,0,   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432                 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API   | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 8f8,0,&V.Y3'a.,,V.\nts53ir'?b%.Mp?"G.mABeGKC*a'C.Uo\zKG\t.\rV, 309, 0 ) Return: 309  API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?  API Name: send Args: ( 4c0, !, 1, 0 ) Return: 1  API Name: recv Args: ( 4c0, ., 32, 0 ) Return: ?  | 2432<br>2432<br>2432<br>2432<br>2432                         | 2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API  | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 8f8,0,   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432         | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API  | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  API Name: WinHttpCloseHandle Args: ( 3442a30 ) Return: 1  API Name: send Args: ( 8f8,o.,  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API Call System API   | API Name: WinHttpCloseHandle Args: (3442a00) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0. &V.Y3'aqV.\nts53ir'.?b%.Mp?"G.mABeGKC*a`C.Uo\zKG\t\rV, 309, 0) Return: 309  API Name: recv Args: (8f8,1500, 0) Return: ?  API Name: send Args: (4c0, !, 1, 0) Return: 1  API Name: recv Args: (4c0, ., 32, 0) Return: ?  API Name: recv Args: (638, ., 1, 2) Return: ?  API Name: recv Args: (688, ., 1, 2) Return: ?  API Name: recv Args: (688, ., 1, 2) Return: ?  API Name: recv Args: (688, ., 1, 2) Return: ?  API Name: Recv Args: (4c0, ., 32, 0) Return: ?  API Name: BCryptDecrypt Args: (4c03d00, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font/woff\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nContent-Type-Options: nosniff\r\nServer: sffeir\nX-XSS-Protection: 0\r\nAge: 184705\r\nCache-Control: public, max-age=315360 00\r\nAlt-Svc: h3-29=".443"; ma=2592000, r\square\forall-443"; ma=2592000, r\square\forall-43"; ma=2592000, r\square\forall-43"; ma=2592000; w="46, 43"\r\nh\r\nr\nContent-Length: 55340\r\nAlthacept-Ranges: bytes\r\nContent-Type: font/woff\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin:   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API   | API Name: WinHttpCloseHandle Args: (3442a00) Return: 1  API Name: WinHttpCloseHandle Args: (3442a30) Return: 1  API Name: send Args: (8f8,0. &V.Y3'aqV.\nts53ir'.?b%.Mp?"G.mABeGKC*a`C.Uo\zKG\t\rV, 309, 0) Return: 309  API Name: send Args: (8f8,1500, 0) Return: ?  API Name: recv Args: (460, .1, 1, 0) Return: 1  API Name: recv Args: (4c0, .32, 0) Return: ?  API Name: recv Args: (638, .1, 2) Return: ?  API Name: recv Args: (68, .1, 2) Return: ?  API Name: recv Args: (68, .1, 2) Return: ?  API Name: recv Args: (68, .1, 2) Return: ?  API Name: BCryptDecrypt Args: (4c03d00, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font\woff\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nContent-Type-Options: nosniff\r\nServer: sffe\r\nX-XSS-Protection: 0\r\nAge: 184705\r\nCache-Control: public, max-age=315360 00\r\nAlt-Svc: h3-29="\443"; ma=2592000, r3-T051="\443"; ma=2592000, r3-Q045="\443"; ma=2592000, r3-Q043="\443"; ma=2592000, r3-Q045="\443"; ma=2592000, r3-Q050="\443"; ma=2592000, r3-Q0 | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API  | API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  API Name: winHttpCloseHandle Args: ( 3442830 ) Return: 1  API Name: send Args: ( 818,0. &V.Y3'aqV.\nts53ir'.?b%.Mp?"G.mABeGKC*a'C.Uo\zKG\t\rV, 309, 0 ) Return: 309  API Name: recv Args: ( 818,1500, 0 ) Return: ?  API Name: send Args: ( 4c0, .1, 1, 0 ) Return: ?  API Name: recv Args: ( 4c0, .32, 0 ) Return: ?  API Name: recv Args: ( 638, .1, 2 ) Return: ?  API Name: recv Args: ( 628, .1, 2 ) Return: ?  API Name: recv Args: ( 688, .1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 4c03d00, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font\wof\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nContent-Type-Options: nosniff\r\nServer: sffe\r\nX-XSS-Protection: 0\r\nAge: 184705\r\nContent-Type: font\wof\r\nAccept-Ranges: 19406\r\nage: 315360  00\r\nAll: Svc: h3-29="'443"; ma=2592000, h3-Qoi-5="'443"; ma=2592000, h3-Qoi-6="'443"; ma | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call Network API  | API Name: WinHttpCloseHandle Args: (3442800 ) Return: 1  API Name: WinHttpCloseHandle Args: (3442830 ) Return: 1  API Name: send Args: (8f8,0.  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call Network API Call System API   | API Name: WinHttpCloseHandle Args: (344280 ) Return: 1  API Name: WinHttpCloseHandle Args: (3442830 ) Return: 1  API Name: send Args: (8f8,0,   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API   | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0,1,,8V.Y3,,*a,q,V.\nls53\r\;?b\%.M.,p?'G.mABeGKC,*a'C.Uo\z.KGit.\rV,309, 0) Return: 309  API Name: send Args: (8f8,1500, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (68,1, 2) Return: 7  API Name: recv Args: (68,1, 2) Return: 7  API Name: recv Args: (68,1, 2) Return: 7  API Name: recv Args: (8f8,1500, 0) Return: 7  API Name: BCryptDecrypt Args: (4c03d00, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font\woff\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nTontent-Length: 55340\r\nDate: Tue, 25 May 2021 08:38:03 GMT\r\nLsx-Modified: Tue, 15 S ep 2020 18:09:19 GMT\r\nX-Content-Type-Options: nosnifit\r\nSevers: sffev\r\nX-XSS-Protection: 0\r\nAge: 1847\signale-1843\r\na=2592000, \rangle-2000, \rangle-1051="443"; ma=2592000, \rangle-3050="7-443"; ma=2592000, \rangle-2000, \rangle-     | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API   | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,,0. 8V.Y3a.qV.\nts53\r\?b\%.Mp?'G.mABeGKC*a' C.Uo\z.KG\t\\rV,309, 0) Return: 309  API Name: send Args: (8f8,,1500, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (68,,12) Return: 7  API Name: recv Args: (68,,12) Return: 7  API Name: recv Args: (68,,12) Return: 7  API Name: recv Args: (8f8,,1500, 0) Return: 7  API Name: BCryptDecrypt Args: (4c03400, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font\woff\r\nAccess-Control-Allow-Origin: "\r\nTiming-Allow-Origin: "\r\nTontent-Length: 55340\r\nDate: Tue, 25 May 2021 08.38.03 GMT\r\nLsx\r\nSs-Protection: 0\r\nAge: 1847\s\notation\r\nCacept-Ad3\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000, n3-Q046="443\r\na=2592000\r\nAllow-Origin: "\r\nTiming-Allow-Origin: "\r\nTiming-Allow-Ori               | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API  | API Name: WinHttpCloseHandle Args: (3442a00) Return: 1  API Name: winHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (818,0,  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call Network API Call System API Call Network API  | API Name: WinHttpCloseHandle Args: (344280) Return: 1  API Name: winHttpCloseHandle Args: (344280) Return: 1  API Name: send Args: (8f8,0,18V,Y3  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API  | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: winHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0.1,8V.Y3   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API  | API Name: WinHttpCloseHandle Args: (344280) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0. &V.Y3'aqV.\nts53v'.?b%.Mp?'G.mABeGKC'a' C.Uo\zKG\t\tV, 309, 0) Return: 309  API Name: send Args: (8f8,1500, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (638,12) Return: 7  API Name: recv Args: (638,12) Return: 7  API Name: recv Args: (628, 1, 2) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: BC/typlDecrypt Args: (4c03400, HTTP/1.1 200 OK\t\nAccept-Ranges: bytes\nContent-Type: font\woff\nAccess-Control-Allow-Origin: "\nTiming-Allow-Origin: \nTimi                    | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call Network API Call Network API Call System API  | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: winHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,01,8V.Y3  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call Network API   | API Name: WinHttpCloseHandle Args: (344280) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0. &V.Y3'aqV.\nts53v'.?b%.Mp?'G.mABeGKC'a' C.Uo\zKG\t\tV, 309, 0) Return: 309  API Name: send Args: (8f8,1500, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (638,12) Return: 7  API Name: recv Args: (638,12) Return: 7  API Name: recv Args: (628, 1, 2) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: recv Args: (688,120) Return: 7  API Name: BC/typlDecrypt Args: (4c03400, HTTP/1.1 200 OK\t\nAccept-Ranges: bytes\nContent-Type: font\woff\nAccess-Control-Allow-Origin: "\nTiming-Allow-Origin: \nTimi                    | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call Network API Call System API Call System API Call Network API Call System API Call Network API Call System API  | API Name: WinHttpCloseHandle Args: (344280) Return: 1  API Name: WinHttpCloseHandle Args: (3442830) Return: 1  API Name: send Args: (8f8,0. &V.Y3'aqV.\nts53v'.?b%.Mp?G.mABeGKC'a'C.UoizKGit.lvV, 309, 0) Return: 309  API Name: send Args: (8f8,1500, 0) Return: 7  API Name: send Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (4c0, 1, 1, 0) Return: 7  API Name: recv Args: (638,1, 2) Return: 7  API Name: recv Args: (638,1, 2) Return: 7  API Name: recv Args: (638,1, 2) Return: 7  API Name: recv Args: (629, 1, 2) Return: 7  API Name: recv Args: (681,1500, 0) Return: 7  API Name: recv Args: (818,1500, 0) Return: 7  API Name: Recv Pribe Recvire Recvir   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API   | API Name: WinHttpCloseHandle Args: (3442800 ) Return: 1  API Name: send Args: (818,0.1,&V.Y3'aqV.Ints53ir.'.7b%.Mp?'G.mABeGK.C"a'C.Uo\z.KGit.\vV309, 0 ) Return: 309  API Name: send Args: (818,1900, 0 ) Return: ?  API Name: serv Args: (818,1900, 0 ) Return: ?  API Name: recv Args: (400,1, 0 ) Return: ?  API Name: recv Args: (400,3, 0 ) Return: ?  API Name: recv Args: (628,1, 2 ) Return: ?  API Name: recv Args: (628,1, 2 ) Return: ?  API Name: recv Args: (628,1, 2 ) Return: ?  API Name: recv Args: (628,1, 2 ) Return: ?  API Name: Recv Args: (628,1, 2 ) Return: ?  API Name: Recv Args: (628,1, 2 ) Return: ?  API Name: Recv Args: (628,1, 2 ) Return: ?  API Name: SCryptDecrypt Args: (403000, HTTP1.1 200 OK\n/nAccept-Ranges: bytesi/n/Content-Type: font/wof/n/nAccess-Control-Allow-Origin: "\n/nTiming-Allow-Origin: "\n/nTiming-Souther South                                   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API  | API Name: WinHttpCloseHandle Args: (3442800 ) Return: 1  API Name: send Args: (88,0.1,&V.Y3'aqV.IntsS3ir.'.7b%.Mp?G.mABeGK.C"a'C.Uo\z.KGtt.VV, 308, 0 ) Return: 309  API Name: send Args: (88,1500, 0 ) Return: 7  API Name: send Args: (460,12, 0 ) Return: 7  API Name: recv Args: (460,32, 0 ) Return: 7  API Name: recv Args: (460,32, 0 ) Return: 7  API Name: recv Args: (628,1, 2 ) Return: 7  API Name: recv Args: (628,1, 2 ) Return: 7  API Name: recv Args: (628,1, 2 ) Return: 7  API Name: recv Args: (628,1, 2 ) Return: 7  API Name: recv Args: (628,1, 2 ) Return: 7  API Name: Poyrpticecypt Args: (403000, HTTP11, 1200 OKInnAccept-Ranges: bytesinnContent-Type: font/woffnnAccess-Control-Allow-Origin: "ninTiming-Allow-Origin: "south-Content-Type-Options: mosniffnnAccept-Ranges: bytesinnContent-Type: font/woffnnAccess-Control-Allow-Origin: "ninTiming-Allow-Origin: "ninContent-Length: 55340/inDale: Tue, 25 May 2021 08.38.03 GMT/ninExpires: Wed, 25 May 2022 08.38.03 GMT/                          | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call System API Call Network API Call System API Call Network API Call Network API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call Network API  | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: send Args: (88,   | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API Call System API Call Network API Call System API Call System API Call Network API Call System API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API | API Name: WinHttpCloseHandle Args: (3442800) Return: 1  API Name: send Args: (88, 0,  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call System API Call Network API Call System API Call System API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call Network API Call System API Call System API Call Network API Call Network API Call System API Call Network API Call Network API     | API Name: WinHttpCloseHandle Args: (3442800 ) Return: 1  API Name: send Args: (88,0,  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504 |

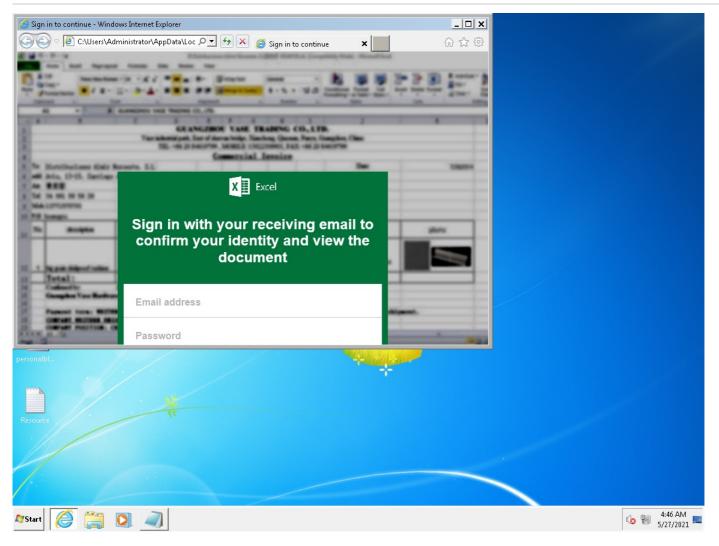
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
|------------------|---|------|----------------------|
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ]6¡ñXLA, 1408, 0, , 0, ]6¡ñXLA, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ççÇ, 1408, 0, , 0, ççÇ, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ™^, 1408, 0, , 0, ™^, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, Lò°bq, 1408, 0, , 0, Lò°bq, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ù©WW"-ý°\$ā, 1408, 0, , 0, ù©WW"-ý°\$ā, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: (8f8, , 1500, 0 ) Return: ?  | 2432 | 2504                 |
| Call System API  |   |      |                      |
| •                | API Name: BCryptDecrypt Args: ( 4c03d00, èÑ8JšÝā°‰Y'.'FI''ÆÓD7ϵ, 1408, 0, , 0, èÑ8JšÝā°‰Y'.'FI''ÆÓD7ϵ, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, t, 1408, 0, , 0, t, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, 'T'M»ß°b;q'ß³"\ršdjBbë!Ü©, 1408, 0, , 0, 'T'M»ß°b;q'ß³"\ršdjBbë!Ü©, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ®¬™é→>6M5Mz, 1408, 0, , 0, ®¬™é→>6M5Mz, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, 7ù,ê, 1408, 0, , 0, 7ù,ê, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, [ý/3]]ÝaŐ, 1408, 0, , 0, [ý/3]]ÝaŐ, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: (8f8, , 1500, 0) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, 6°ĒÉK"±X\$, 1408, 0, , 0, 6°ĒÉK"±X\$, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
|                  |   |      | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 |                      |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, , 1408, 0, , 0, , 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, @äqSáÝóG¿0cRV,«i, 320, 0, , 0, @äqSáÝóG¿0cRV,«i, 1495, 70770992, 0 ) Return: 0   | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 238, 0 ) Return: ?  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, 8çB7•, 1408, 0, , 0, 8çB7•, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ( 'tZ, 1408, 0, , 0, ( 'tZ, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, YPÚ[>ÞÑQ€1ŒÄâA', 1408, 0, , 0, YPÚ[>ÞÑQ€1ŒÄâA', 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ÿμβιβ*, 1408, 0, , 0, ÿμβιβ*, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, þÊÊ(8¶€1`¬1Ö'ŌŒ~d'é#, 1408, 0, , 0, þÊÊ(8¶€1`¬1Ö'ŌŒ~d'é#, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
|                  |   | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1500, 0 ) Return: ?   |      |                      |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ÚU^, 1408, 0, , 0, ÚU^, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, Î ŒpV Û@;'â?, 1408, 0, , 0, Î ŒpV Û@;'â?, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, -^å, 1408, 0, , 0, -^å, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, t†±m, 1408, 0, , 0, t†±m, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ×5A°, 1408, 0, , 0, ×5A°, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1326, 0 ) Return: ?   | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, 1 J, 1408, 0, , 0, 1 J, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, aÑ, 1408, 0, , 0, aÑ, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, вJW-«Šjç®ò²Ö*jA"="\$UeZeŒ-, 1408, 0, , 0, вJW-«Šjç®ò²Ö*jA"="\$UeZeŒ-, 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ?ùÃèœ:ÃûiÅ, 1408, 0, , 0, ?ùÃèœ:ÃûiÅ, 1495, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, Ife"U[iuemQ"r², 1408, 0, , 0, Ife"U[iuemQ"r², 1408, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call System API  | API Name: BCtyptDecrypt Args: ( 4c03d00, 12 O[toeffice F; 1406, 0, 10, 12 O[toeffice F; 1406, 70770992, 0 ) Return: 0   | 2432 | 2504                 |
|                  |   |      |                      |
| Call Network API | API Name: recv Args: ( 8f8, , 494, 0 ) Return: ?  | 2432 | 2504                 |
| Call System API  | API Name: BCryptDecrypt Args: ( 4c03d00, ¾, 576, 0, , 0, ¾, 576, 70770992, 0 ) Return: 0  | 2432 | 2504                 |
| Call Network API | API Name: recv Args: ( 8f8, , 1, 2 ) Return: ?  | 2432 | 2504                 |
| Call Network API | API Name: send Args: (8d0, GET /gls1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfzjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E%3D HTTP/1.1\r\nCache-Control: max-age = 86400\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Age nt: Microsoft-CryptoAPl/6.1\r\nHost: ocsp.pki.goog\r\n\r\n, 1, 276 ) Return: 0 | 2432 | 2504                 |
| Add File         | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4Y300HM3\jizaRExUiTo99u79D0KEww[1].woff Type: VSDT_COM_DO S   | 2432 | 2504                 |
| Write File       | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4Y300HM3\jjzaRExUiTo99u79D0KEww[1].woff Type: VSDT_COM_DO S   | 2432 | 2504                 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 4b8c518 ) Return: 1  | 2432 | 2504                 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442a00 ) Return: 1  | 2432 | 2504                 |
| Call System API  | API Name: WinHttpCloseHandle Args: ( 3442830 ) Return: 1  | 2432 | 2504                 |
| Call Network API | API Name: send Args: ( 960,0.z.>L~U.iikU.ffw.#.etaa.8a3.&  q.{S5"%r@*E'.SAA.f&^\vZ.&&".fy{M.t.K.\t[N.9.vlwEax.\$tc.H\y = K.t.ulf:6.H32.2.l*g&uiN5{#yU#.b}@!\$.q[.8.*.bTtlxPY.f.y.V.l."JW5.D.';aA.N.QSM.?G1S, 309, 0 ) Return: 30  | 2432 | 2504                 |
|                  |   | 2432 | 2504                 |
| Call Network API | API Name: recy Args; ( 960, , 1500, 0 ) Return; ?   |      |                      |
| Call Network API | API Name: recv Args: (960, , 1500, 0 ) Return: ?  API Name: sent Arre: (4c0, 1, 1, 0, ) Return: 1   |      | 2504                 |
| Call Network API | API Name: send Args: ( 4c0, I, 1, 0 ) Return: 1   | 2432 | 2504                 |
|                  |   |      | 2504<br>2504<br>2504 |

| Call System API  | API Name: BCryptDecrypt Args: ( 49494/0, HTTP/1.1 200 OKI/nAccept-Ranges: bytesi/nContent-Type: font/woff\(\)rnAccess-Control-Allow-Origin: "\r/nTiming-Allow-Origin: "\r/nContent-Length: 57524\r/nDate: Tue, 25 May 2021 16:40:59 GMT\r/nExpires: Wed, 25 May 2022 16:40:59 GMT\r/nLast-Modified: Tue, 15 S ep 2020 18:10:09 GMT\r/nX-Content-Type-Options: nosniff\(\)rnServer: sffe\(\)rnX-XSS-Protection: 0\r/nAge: 155729\r/nCache-Control: public, max-age=315360 00\r/nAlt-Svc: h3-29=":443"; ma=2592000, h3-T051=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, rn-46, 43"\r/n\r/n\r/nwOFF, 1408, 0, 0, HTTP/1.1 200 OK\r/nAccept-Ranges: bytesir\r/nContent-Type: font/woff\r/nAccess-Control-Allow-Origin: "\r/nTiming-Allow-Origin: "\r/nTiming-Allow-Ori | 2432   | 2504   |
|--|--|--|--|
|  | ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="46, 43"\r\n\r\n\wOFF, 1495, 68154652, 0 ) Return: 0  |  |  |
| Call Network API   | API Name: recv Args: (960, , 1326, 0) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ¬ççÆnçe} ÉGâUÕÕ´<ø<‰ÞüÄ[§Bð¤, 1408, 0, , 0, ¬ççÆnçe} ÉGâUÕÕ´<ø<‰ÞüÄ[§Bð¤, 1408, 68149768, 0 ) R eturn: 0  | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, àÿþĬ9®{P@, 1408, 0, , 0, àÿþĬ9®{P@, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ÒÂ8±>%>)ÌÇÎc)ì:ĐZĐ¯@, 1408, 0, , 0, ÒÂ8±>%>)ÌÇÎc)ì:ĐZĐ¯@, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: (960, , 1500, 0) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ÓðpjØö⁰,Œ%{, 1408, 0, , 0, ÓðpjØö⁰,Œ%{, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ,Tég:lqÇ, 1408, 0, , 0, ,Tég:lqÇ, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, Ð, ÐBÐjú€átÆ8óöp*®ā#E^;, 1408, 0, , 0, Ð, ÐBÐjú€átÆ8óöp*®ā#E^;, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: (960, , 1500, 0) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, 'ÕÃÔ-jL¢¤qĩ') Þieṭ∱å&\n'°E;, 1408, 0, , 0, 'ÕÃÔ-jL¢¤qĩ') Þieṭ∱å&\n'°E;, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: (960, , 1326, 0) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, þ\n3۲ǹ)ØÝ¼i¶jēfz%»_B@g¥—%°D4āQæ#, 1408, 0, , 0, þ\n3۳ǹ)ØÝ¼i¶jēfz%»_B@g¥—%°D4āQæ#, 1408, 6   | 2432   | 2504   |
| •••  | 8149768, 0 ) Return: 0   |  |  |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, nvÜå, 1408, 0, , 0, nvŬå, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, žÝŮĀ¢¯, 1408, 0, , 0, žÝŮĀ¢¯, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, <àÉýVhÞCêg, 1408, 0, , 0, <àÉýVhÞCêg, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, × åu ¶ZÅ), 1408, 0, , 0, × åu ¶ZÅ), 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ñô%;læÓ,ÿçY";,q'è8OG‰ÎJÝfé<, 1408, 0, , 0, ñô%;læÓ,ÿçY";,q'è8OG‰ÎJÝfé<, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, "e;W"eß)))fW, 1408, 0, , 0, "e;W"eß)))fW, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   | 2504   |
| Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, (ekòōz'ō,÷UolÀŒL_™W, 1408, 0, , 0, (ekòōz'ō,÷UolÀŒL_™W, 1408, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call Network API   | API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432   | 2504   |
|  | API Name: BCryptDecrypt Args: ( 49494f0, ÚSíþÁ×+_ø™, 1408, 0, , 0, ÚSíþÁ×+_ø™, 1495, 68149768, 0 ) Return: 0   | 2432   | 2504   |
| Call System API  |  |  | 2504   |
| Call System API Call Network API   | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  | 2432   |  |
|  | API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ZÌOó@, 1408, 0, , 0, ZÌOó@, 1408, 68149768, 0 ) Return: 0  | 2432   | 2504   |
| Call Network API   |  |  | 2504<br>2504   |
| Call Network API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZÌOó@, 1408, 0, , 0, ZÌOó@, 1408, 68149768, 0 ) Return: 0   | 2432   |  |
| Call Network API Call System API Call Network API  | API Name: BCryptDecrypt Args: ( 49494f0, ZİOó@, 1408, 0, , 0, ZİOó@, 1408, 68149768, 0 ) Return: 0 API Name: recv Args: ( 960, , 1500, 0 ) Return: ?   | 2432<br>2432   | 2504   |
| Call Network API Call System API Call Network API Call System API  | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  | 2432<br>2432<br>2432   | 2504<br>2504   |
| Call Network API Call System API Call Network API Call System API Call Network API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?   | 2432<br>2432<br>2432<br>2432                                 | 2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ™ūjóøŸõlyGUáĬ, 1408, 0, , 0, ™ūjóøŸõlyGUáĬ, 1408, 68149768, 0 ) Return: 0   | 2432<br>2432<br>2432<br>2432<br>2432                         | 2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call Network API  | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ™ūjó¢ÝðlyGUåĨ, 1408, 0, , 0, ™ūjó¢ÝðlyGUåĨ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432                 | 2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢ŶŏlyGUāĨ, 1408, 0, , 0, ™ūjó¢ŶŏlyGUāĨ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™ūjó¢ŶŏlyGUāĨ, 1408, 0, , 0, ™ūjó¢ŶŏlyGUāĨ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YðiyGUâĬ, 1408, 0, , 0, ™üjó¢YðiyGUâĬ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YðlyGUáĬ, 1408, 0, , 0, ™üjó¢YðlyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YðlyGUáĬ, 1408, 0, , 0, ™ūjó¢YðlyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0 ) Return: 0   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call Network API Call System API Call Network API  | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™üjóṣŶŏiyGUáĭ, 1408, 0, , 0, ™üjó¢ŶŏiyGUáĭ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™ijóṣŶōiyGUáĭ, 1408, 0, , 0, ™üjó¢ŶŏiyGUáĭ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 238, 0) Return: ?  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API  | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™üjó¢YŏiyGUãĭ, 1408, 0, , 0, ™üjó¢YŏiyGUãĭ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™ijó¢YŏiyGUãĭ, 1408, 0, ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0) Return: 0  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API   | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, 1408, 0, 0, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™üjó¢ŶólyGUáĬ, 1408, 0, 0, ™üjó¢ŶólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, 0, ¬, 1495, 68149768, 0) Return: 0  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API  | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™üjó¢YólyGUáĬ, 1408, 0, 0, ™üjó¢YólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™üjó¢YólyGUáĬ, 1408, 0, 0, ™üjó¢YólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™ijó¢YólyGUáĬ, 1408, 0, 0, ™ijó¢YólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ijó¢YólyGUáĬ, 1408, 0, 0, ™ijó¢YólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ijó¢YólyGUáĬ, 1408, 0, 0, √vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ijótygiál) Return: ?   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call Network API  | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, 1408, 0, 0, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™üjó¢ŶólyGUáĬ, 1408, 0, 0, ™üjó¢ŶólyGUáĬ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, ¬, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 520, 0, 0, 0, ¬, 1495, 68149768, 0) Return: 0  | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call Network API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ™űjó¢ŸőlyGUáĬ, 1408, 0, , 0, ™űjó¢ŸölyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ", 320, 0, , 0, ", 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÅ"–A=ùFDÃ@sR, 1408, 0, , 0, "ÉÅ"–A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÅ"–A=ùFDÃ@sR, 1408, 0, , 0, "ÉÅ"–A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÅ"–A=ùFDÃ@sR, 1408, 0, , 0, \"ÉÅ"–A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API Call Network API Call Network API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™ūjóṣYōlyGUāĬ, 1408, 0, , 0, ™ūjóṣYòlyGUāĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™ūjóṣYōlyGUāĬ, 1408, 0, , 0, ™ūjóṣYòlyGUāĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, vç+5xÅ, 1408, 0, , 0, vç+5xÅ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "c, 320, 0, , 0, "., 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "c, 320, 0, , 0, "., 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÅ"-A=ùFDÃ@sR, 1408, 0, , 0, "ÉÁ"-A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÅ"-A=ùFDÃ@sR, 1408, 0, , 0, "ÉÁ"-A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÁ"-A=ùFDÃ@sR, 1408, 0, , 0, "ÉÁ"-A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÁ"-A=ùFDÃ@sR, 1408, 0, , 0, "ÉÁ"-A=ùFDÃ@sR, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, "ÉÁ"-A=ùFDÃ@sR, 1408, 0, , 0, \déā0ž¥U¢¿l/›QÉt-7+, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, \déā0ž¥U¢¿l/›QÉt-7+, 1408, 0, , 0, \déā0ž¥U¢¿l/›QÉt-7+, 1495, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1326, 0 ) Return: ?   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call Network API Call System API  | API Name: BCryptDecrypt Args: (49494f0, ZlOó@, 1408, 0, 0, ZlOó@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, 0, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūjóęYōlyGUāĬ, 1408, 0, 0, ™ūjóęYòlyGUāĬ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™ūjóęYōlyGUāĬ, 1408, 0, 0, ™ūjóęYòlyGUāĬ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, vç+5xÅ, 1408, 0, 0, 0, vç+5xÅ, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ", 320, 0, 0, ", 1495, 68149768, 0) Return: 0  API Name: recv Args: (960, , 238, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, "ÉÅ"-A=üFDÄ@sR, 1408, 0, 0, 0, "ÉÅ"-A=üFDÄ@sR, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, "ÉÅ"-A=üFDÄ@sR, 1408, 0, 0, 0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1408, 0, 0, 0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1408, 0, 0, 0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1408, 0, 0, 0, \d¢ā0ž¥U¢¿l⅓QÉt-7+, 1495, 68149768, 0) Return: 0   | 2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call Network API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Network API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YöyGUáĬ, 1408, 0, , 0, ™üjó¢YöyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YöyGUáĬ, 1408, 0, , 0, ™üjó¢YöyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, v, ¢+5xÅ, 1408, 0, , 0, v, v+5xÅ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 464—A=üFDĀ@sR, 1408, 0, , 0, ¬, ¬, ¬, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 49494f0, ¬, 404  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call System API Call Network API Call Network API Call System API   | API Name: BCryptDecrypt Args: (49494f0, ZlOo@, 1408, 0, , 0, ZlOo@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūijo¢YòlyGUāi, 1408, 0, , 0, ™ūjo¢YòlyGUāi, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūijo¢YòlyGUāi, 1408, 0, , 0, ™ūjo¢YòlyGUāi, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ī, 1408, 0, , 0, ī, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ī, 1408, 0, , 0, ī, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, v, v, +5xÅ, 1408, 0, , 0, v, v, +5xÅ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™, 320, 0, , 0, ™, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™, 320, 0, , 0, ™, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™, 520, 0, , 0, ™, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™, 520, 0, , 0, ™, 1495, 68149768, 0) Return: 0  API Name: Recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ™, 64*-A=üFDĀ@sR, 1408, 0, , 0, ™, 64*-A=üFDĀ@sR, 1408, 68149768, 0) Return: 0  API Name: Recv Args: (960, , 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ½f¥n, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0  API Name: Recv Args: (960, , 1326, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, ½f*Pnf6, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ½f*Pnf6, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ½f*Pnf6, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ½f*Pnf6, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ½f*N, 1408, 0, , 0, ½f*N, 1408, 68149768, 0) Return: 0   | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504 |
| Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ZlOó@, 1408, 0, , 0, ZlOó@, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YöyGUáĬ, 1408, 0, , 0, ™üjó¢YöyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ™üjó¢YöyGUáĬ, 1408, 0, , 0, ™üjó¢YöyGUáĬ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ĭ, 1408, 0, , 0, ĭ, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, v, ¢+5xÅ, 1408, 0, , 0, v, v+5xÅ, 1408, 68149768, 0 ) Return: 0  API Name: recv Args: ( 960, , 1500, 0 ) Return: ?  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 320, 0, , 0, ¬, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 464—A=üFDĀ@sR, 1408, 0, , 0, ¬, ¬, ¬, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 49494f0, ¬, 49494f0, ¬, 404  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call System API Call System API Call Network API Call System API                  | API Name: BCryptDecrypt Args: (49494f0, ZIOo@, 1408, 0, 0, ZIOo@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, 1408, 0, 0, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūjó¢∀ðiyGUāÍ, 1408, 0, 0, ™ūjó¢∀ðiyGUāĨ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūjó¢∀ðiyGUāÍ, 1408, 0, 0, ™ūjó¢∀ðiyGUāĨ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, 0, v,  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |
| Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API | API Name: BCryptDecrypt Args: (49494f0, ZlO6@, 1408, 0, , 0, ZlO6@, 1408, 68149768, 0 ) Return: 0  API Name: RCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™u)6yF0tyGUal, 1408, 0, , 0, ™u)6yF0tyGUal, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, 1, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, 1, 1408, 0, , 0, 1, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, 1, 1408, 0, , 0, 1, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 320, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1476, 1408, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ¬, 1408, 0, , 0, ¬, 1495, 68149768, 0 ) Return: 0  API Name: BCryptD  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504 |
| Call Network API Call System API Call System API Call System API Call System API Call Network API Call System API Call Network API Call System API | API Name: BCryptDecrypt Args: (49494f0, ZIOo@, 1408, 0, 0, ZIOo@, 1408, 68149768, 0) Return: 0  API Name: recv Args: (960, 1500, 0) Return: ?  API Name: BCryptDecrypt Args: (49494f0, 1408, 0, 0, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūjó¢∀ðiyGUāÍ, 1408, 0, 0, ™ūjó¢∀ðiyGUāĨ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ™ūjó¢∀ðiyGUāÍ, 1408, 0, 0, ™ūjó¢∀ðiyGUāĨ, 1408, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, ĭ, 1495, 68149768, 0) Return: 0  API Name: BCryptDecrypt Args: (49494f0, ĭ, 1408, 0, 0, 0, v,  | 2432 2432 2432 2432 2432 2432 2432 2432                      | 2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504<br>2504   |

| Call System API   | API Name: WinHttpCloseHandle Args: ( 3442660 ) Return: 1   | 2432 | 2504   |
|---|--|------|--|
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, y SVÎiV²dDPT~Ãf<, 1408, 0, , 0, y SVÎiV²dDPT~Ãf<, 1495, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, /+ĪÉJN•k?\n, 1408, 0, , 0, /+ĪÉJN•k?\n, 1408, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, 1%=8silYݰ8rjj]]M×RU^ y}èŠp¯ÙQ, 1408, 0, , 0, 1%=8silYݰ8rjj]]M×RU^ y}èŠp¯ÙQ, 1495, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, Ùilò°Â¹, 1408, 0, , 0, Ùilò°Â¹, 1408, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, 'k', C", 1408, 0, , 0, 'k', C", 1495, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, w@, 1408, 0, , 0, w@, 1408, 68149768, 0 ) Return: 0   | 2432 | 2504   |
|   |  | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, 6, 1408, 0, , 0, 6, 1495, 68149768, 0 ) Return: 0   |      |  |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, N±Ö (Ü' »çcμšñ, 1408, 0, , 0, N±Ö (Ü' »çcμšñ, 1408, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Call System API   | API Name: BCryptDecrypt Args: ( 49494f0, ¬, 1376, 0, , 0, ¬, 1376, 68149768, 0 ) Return: 0   | 2432 | 2504   |
| Add File  | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\EY6ZFZU4\jizfRExUiTo99u79B_mh006tKw[1].woff Type: VSDT_COM_DOS   | 2432 | 2504   |
| Write File  | Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\EY6ZFZU4\jizfRExUiTo99u79B_mh0O6tKw[1].woff Type: VSDT_COM_DOS   | 2432 | 2504   |
| Call Service API  | API Name: OpenServiceW Args: ( 4b5aa20, WSearch, 1 ) Return: 4b5a9f8   | 2432 | 2504   |
| Write Registry Key  | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running   | 2432 | 2504   |
| Delete Registry Key   | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Suggested Sites\SlicePath Value: None  |      | 2432   |
|   |  |      |  |
| Call Network API  | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |      | 2432   |
| Call Internet Helper API  | API Name: InternetOpenW Args: ( , 0, , , , 0 ) Return: cc0008  | 2432 | 2504   |
| Call System API   | API Name: DnsQueryExW Args: ( iecvlist.microsoft.com, 1, 50000000 ) Return: 0  | 2432 | 2504   |
| Call Internet Helper API  | API Name: InternetConnectW Args: ( cc0008, iecvlist.microsoft.com, 443, , , 3, 0, 0 ) Return: cc000c   | 2432 | 2504   |
| Call Internet Helper API  | API Name: HttpOpenRequestW Args: ( cc000c, GET, /ie11blocklist/1401746408/versionlist.xml, , , 85325396, 79692288, 0 ) Return: cc0010  | 2432 | 2504   |
| Call Network API  | API Name: socket Args: ( 2, 2, 0 ) Return: 968   | 2432 | 2504   |
| Call Network API  | API Name: socket Args: (23, 2, 0) Return: 968  | 2432 | 2504   |
|   |  |      |  |
| Call System API   | API Name: DnsQueryExW Args: (iecvlist.microsoft.com, 1, 40006000) Return: 9701   | 2432 | 2504   |
| Call System API   | API Name: DnsQueryExW Args: ( iecvlist.microsoft.com, 1c, 40006000 ) Return: 0   | 2432 | 2504   |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: 968  | 2432 | 2504   |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 968   | 2432 | 2504   |
| Call Network API  | API Name: bind Args: ( 968, 0.0.0.0:49181, 16 ) Return: 0  | 2432 | 2504   |
| Detection   | Threat Characteristic: Listens on port 0.0.0.0.49181   |      |  |
| Call Network API  | API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff   | 2432 | 2504   |
|   |  |      |  |
| Call Network API  | API Name: send Args: ( 968,, 135, 0 ) Return: 135  | 2432 | 2504   |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 968   | 2432 | 2504   |
| Call Network API  | API Name: bind Args: ( 968, 0.0.0.0:49182, 16 ) Return: 0  | 2432 | 2504   |
| Detection   | Threat Characteristic: Listens on port 0.0.0.049182  |      |  |
| Call Network API  | API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: fffffff  | 2432 | 2504   |
| Call Network API  | API Name: send Args: ( 968,, 135, 0 ) Return: 135  | 2432 | 2504   |
| Call Network API  | API Name: socket Args; ( 2, 1, 6 ) Return: 968   | 2432 | 2504   |
|   | •  | 2432 | 2504   |
| Call Network API  Detection   | API Name: bind Args: ( 968, 0.0.0.049183, 16 ) Return: 0  Threat Characteristic: Listens on port   | 2432 | 2304   |
| Call Network API  | 0.0.0.0:49183  | 0400 | 0504   |
|   | API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: fffffff  | 2432 | 2504   |
| Call Network API  | API Name: send Args: ( 968,, 58, 0 ) Return: 58  | 2432 | 2504   |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 968   | 2432 | 2504   |
| Call Network API  | API Name: bind Args: ( 968, 0.0.0.0:49184, 16 ) Return: 0  |      |  |
|   |  | 2432 | 2504   |
| Detection   | Threat Characteristic: Listens on port   | 2432 | 2504   |
|   |  | 2432 | 2504   |
| Call Network API  | Threat Characteristic: Listens on port 0.0.0.0:49184   |      |  |
| Call Network API<br>Call System API   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff   |      | 2504   |
| Call Network API Call System API Call Internet Helper API   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  |      | 2504<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API  | Threat Characteristic: Listens on port 0.0.0.d:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  |      | 2504<br>2432<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File  | Threat Characteristic: Listens on port 0.00.0:49184  API Name: connect Args: (968, 152.199.19.161:443, 16) Return: ffffffff  API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008  API Name: HttpOpenRequestW Args: (cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File  | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432   |
| Detection  Call Network API  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Call Filesystem API  Write Registry Key   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IES\MXNZOZKK\IE9CompatViewList[1].xml, %L   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: (968, 152.199.19.161:443, 16) Return: ffffffff  API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008  API Name: HttpOpenRequestW Args: (cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %L OCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API  | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\tiecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\tiecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\timerosoft\ |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API   | Threat Characteristic: Listens on port 0.0.0.0.49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Vindows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  API Name: recv Args: ( 674, , 1, 2 ) Return: ?  API Name: recv Args: ( 674, , 1, 2 ) Return: ?  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DrsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\imXNZOZKK\IE9CompatViewList[1].xml, %L OCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0 ) Return: 2  API Name: recv Args: ( 674, , 1, 2 ) Return: 7  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API  | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %L OCALAPPDATA%\Microsoft\Underrosoft\Un |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API Call Internet Helper API   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IES\imXNZOZKK\IE9Compat\ViewList[1].xml, %L OCALAPPDATA%\Microsoft\Vinternet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DownloadRetries Value: 0  API Name: recv Args: ( 674, , 1, 2 ) Return: ?  API Name: consqueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API Call Internet Helper API   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %L OCALAPPDATA%\Microsoft\Underrosoft\Un |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File  | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IES\imXNZOZKK\IE9Compat\ViewList[1].xml, %L OCALAPPDATA%\Microsoft\Vinternet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DownloadRetries Value: 0  API Name: recv Args: ( 674, , 1, 2 ) Return: ?  API Name: consqueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API Add File Write File Write File   | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IES\imXNZOZKK\IE9Compat\ViewList[1].xml, %L OCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DownloadRetries Value: 0  API Name: recv Args: ( 674, , 1, 2 ) Return: ?  API Name: consqueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0000  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API   | Threat Characteristic: Listens on port 0.0.0.0.49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 5000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDataliecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDataliecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %LOCALAPPDATA%MicrosoftInternet Explorer/IECompatDataliecompatdata.xml, 0, 0, 0, 0) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DownloadRetries Value: 0  API Name: recv Args: (674, , 1, 2) Return: ?  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0000  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\Iecompatdata.xml Type: VSDT_TEXT_HTML   |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call Internet Helper API Add File Write File Call Filesystem API Call Internet Helper API Call Internet Helper API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API  | Threat Characteristic: Listens on port 0.0.0.0/49184  API Name: connect Args: (968, 152.199.19.161:443, 16) Return: ffffffff  API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 5000000) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, ., .3, 0, 39568160) Return: cc00008  API Name: HttpOpenRequestW Args: (cc0008, GET, //E9CompatViewList.xml, ., .58644852, 4194320, 39568160) Return: cc0000c  Path: %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatData\/iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: (%LOCALAPPDATA%IMicrosoftIvindows\/Temporary Internet Files\/Content.IE5iMXNZOZKK\/IE9CompatViewList\/[1].xml, %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatdata.xml, 0, 0, 0, 0) Return: 1  Key: HKEY_CURRENT_USER\/SoftwareIMicrosoftInternet Explorer\/SearchScopes\/DownloadRetries Value: 0  API Name: recv Args: (674, 1, 2) Return: ?  API Name: recv Args: (674, 1, 1, 2) Return: ?  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, ., 3, 0, 39568160) Return: cc00008  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, ., 3, 0, 39568160) Return: cc00006  Path: %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: (%LOCALAPPDATA%IMicrosoftIvindows\/Temporary Internet Files\/Content.IE5iMXNZOZKK\/IE9CompatViewList\/[1].xml, %LOCALAPPDATA%IMicrosoftInternet Explorer\/IECompatData\/iecompatdata.xml, 0, 0, 0, 0) Return: 1  API Name: recv Args: (674, 1, 1, 2) Return: 7  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432 |
| Call Network API Call System API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call Network API Call Internet Helper API Add File Write File Call Filesystem API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Network API Call Network API Call Network API                           | Threat Characteristic: Listens on port 0.0.0.0/49184  API Name: connect Args: (968, 152.199.19.161:443, 16) Return: ffffffff  API Name: DnsQueryExW Args: (ie9cviist.ie.microsoft.com, 1, 50000000) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cviist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008  API Name: HttpOpenRequestW Args: (cc0008, GET, //E9Compat/viewList.xml, , , 58644852, 4194320, 39568160) Return: cc000c  Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/viewList.xml  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Network API Call Network API Call Network API Call Network API Call System API | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%MicrosoftWindows)Temporary Internet FilestContent.IE5MXNZOZKK/IE9CompatViewList[1].xml, %L OCALAPPDATA%MicrosoftWareMicrosoftWinternet Explorer/SearchScopes/DownloadRetries Value: 0  API Name: recv Args: ( 674, 1, 2) Return: ?  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc000s  API Name: HttpOpenRequestW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc000s  API Name: HttpOpenRequestW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%Microsoft/Internet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 1  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0   |      | 2504 2432 2432 2432 2432 2432 2432 2432 24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API Write Registry Key Call Network API Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Network API Call Network API Call Network API Call Network API Call System API | Threat Characteristic: Listens on port 0.0.0.0/49184  API Name: connect Args: (968, 152.199.19.161:443, 16) Return: ffffffff  API Name: DnsQueryExW Args: (ie9cviist.ie.microsoft.com, 1, 50000000) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cviist.ie.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008  API Name: HttpOpenRequestW Args: (cc0008, GET, //E9Compat/viewList.xml, , , 58644852, 4194320, 39568160) Return: cc000c  Path: %LOCALAPPDATA%/Microsoft/Internet Explorer/IECompat/Data/viewList.xml  |      | 2504<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>2432<br>24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Filesystem API  | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%MicrosoftUnternet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%MicrosoftWindows)Temporary Internet FilestContent.IE5MXNZOZKK/IE9CompatViewList[1].xml, %L OCALAPPDATA%MicrosoftWareMicrosoftWinternet Explorer/SearchScopes/DownloadRetries Value: 0  API Name: recv Args: ( 674, 1, 2) Return: ?  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc000s  API Name: HttpOpenRequestW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc000s  API Name: HttpOpenRequestW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%Microsoft/Internet Explorer/IECompatDatalvecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 1  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: CopyFileExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0   |      | 2504 2432 2432 2432 2432 2432 2432 2432 24   |
| Call Network API Call System API Call Internet Helper API Call Internet Helper API Add File Write File Call Network API Call Network API Call Internet Helper API Call System API Call Internet Helper API Call Internet Helper API Call Internet Helper API Call Filesystem API Call Internet Helper API Call System API Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call System API Call Internet Helper API       | Threat Characteristic: Listens on port 0.0.0.0:49184  API Name: connect Args: ( 968, 152.199.19.161:443, 16 ) Return: ffffffff  API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c  Path: %LOCALAPPDATA%IMicrosoftUnternet Explorer/IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%IMicrosoftUnternet Explorer/IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( %LOCALAPPDATA%IMicrosoftWindows)Temporary Internet Files\Content.IE5\MXNZOZKK\IE9Compat\ViewList[1].xml, %L OCALAPPDATA%IMicrosoftUnternet Explorer\IECompatDatal/ecompatdata.xml, 0, 0, 0, 0 ) Return: 1  Key: HKEY_CURRENT_USER\Software\Microsoft\underset Explorer\IECompatDatal/ecompatdata.xml, 0, 0, 0, 0 ) Return: 2  API Name: recv Args: (674, 1, 2) Return: ?  API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008  API Name: HttpOpenRequestW Args: (cc0004, ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: VLOCALAPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( kLOCALAPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( kLOCALAPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml Type: VSDT_TEXT_HTML  API Name: CopyFileExW Args: ( kLOCALAPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml, 0, 0, 0, 0 ) Return: 1  API Name: DnsQueryExW Args: ( kloCalaPPDATA%IMicrosoft\underset Explorer\IECompatDatal/ecompatdata.xml, 0, 0, 0, 0 ) Return: 1  API Name: DnsQueryExW  |      | 2504 2432 2432 2432 2432 2432 2432 2432 24   |

| Call Filesystem API      | API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9Compat\ViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompat\Data\iecom |      | 2432 |
|--------------------------|--|------|------|
| Call Network API         | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |      | 2432 |
| Call Network API         | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |      | 2432 |
| Call System API          | API Name: DnsQueryExW Args: ( ie9cvlist.ie.microsoft.com, 1, 50000000 ) Return: 0  |      | 2432 |
| Call Internet Helper API | API Name: InternetConnectW Args: ( cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 39568160 ) Return: cc0008   |      | 2432 |
| Call Internet Helper API | API Name: HttpOpenRequestW Args: ( cc0008, GET, //E9CompatViewList.xml, , , 58644852, 4194320, 39568160 ) Return: cc000c   |      | 2432 |
| Add File                 | Path: %LOCALAPPDATA%IMicrosoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  |      | 2432 |
| Write File               | Path: %LOCALAPPDATA%IMicrosoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  |      | 2432 |
| Call Filesystem API      | API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Vindows\Temporary Internet Files\Content.IE5\MXNZOZKK\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0 ) Return: 1  |      | 2432 |
| Call Network API         | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |      | 2432 |
| Call Network API         | API Name: recv Args: ( 674, , 1, 2 ) Return: ?   |      | 2432 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFavoritesInitialSelection Value: None   | 2432 | 2504 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFeedsInitialSelection Value: None   | 2432 | 2504 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FullScreen Value: no  |      | 2432 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window_Placement Value: None  |      | 2432 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MINIE\TabBandWidth Value: 1f4  |      | 2432 |
| Add Registry Key         | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\ Value: None   |      | 2432 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\State Value: 0   |      | 2432 |
| Write Registry Key       | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\Schedule Value: 4  |      | 2432 |
| Delete Registry Key      | Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\MFV Value: None  |      | 2432 |
| Add File                 | Path: %LOCALAPPDATA%\\text{Microsoft\text{Internet}} Explorer\\text{Recovery\text{High\Last}} Active\\\\ 38CCAF38-BEE1-11EB-B06F-08002739B404\\\.dat Type: VSDT_WINWO RD   |      | 2432 |
| Write File               | Path: %LOCALAPPDATA%\\text{Microsoft\text{Internet}} Explorer\\text{Recovery\text{High\Last}} Active\\\\ 38CCAF38-BEE1-11EB-B06F-08002739B404\\\.dat Type: VSDT_WINWO RD   |      | 2432 |
| Add File                 | Path: %LOCALAPPDATA%\\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(  |      | 2432 |
| Write File               | Path: %LOCALAPPDATA%\\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(  |      | 2432 |
| Add File                 | Path: %LOCALAPPDATA%iMicrosoft\Internet Explorer\Recovery\High\Active\(0E12DC2F-BEE1-11EB-B06F-08002739B404\).dat Type: VSDT_WINWORD   |      | 2432 |
| Write File               | Path: %LOCALAPPDATA%IMicrosoftInternet Explorer/Recovery/HighlActive\{0E12DC2F-BEE1-11EB-B06F-08002739B404\}.dat Type: VSDT_WINWORD  |      | 2432 |
| Add File                 | Path: %LOCALAPPDATA%\\text{Microsoft\text{\text{Internet Explorer\Recovery\High\Last Active\Recovery\Store.\{38CCAF37-BEE1-11EB-B06F-08002739B404\}.dat Type: VSDT_WINWORD   |      | 2432 |
| Write File               | Path: %LOCALAPPDATA%\\text{Microsoft\Internet} Explorer\\text{Recovery\High\Last} Active\\text{Recovery\Store.}\\ (38CCAF37-BEE1-11EB-B06F-08002739B404\). dat Type: VSDT_WINWORD  |      | 2432 |

#### ▼ Screenshot



### W10

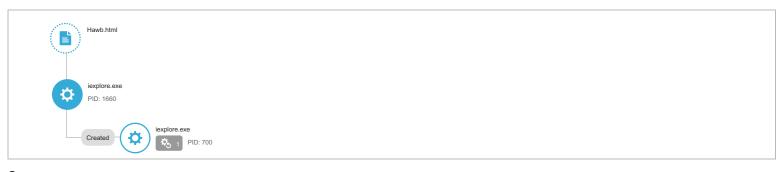
| Environment-specific risk level | High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. |  |  |  |  |
|---------------------------------|---|--|--|--|--|
| Detections                      | VAN_BACKDOOR.UMXX   |  |  |  |  |
| Exploited vulnerabilities       |   |  |  |  |  |
| Network connection              | Custom  |  |  |  |  |

### ▼ Object 1 - Hawb.html (HTML File)

| File name | Hawb.html   |
|-----------|---|
| File type | HTML File   |
| SHA-1     | F7911D858AFCCB9E871595374564EFE2D6449377                        |
| SHA-256   | FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E9 |
| MD5       | DEE4CFA9FB0A28C29485245440EF3D50                                |
| Size      | 186357 byte(s)  |

| Risk Level                | High risk  |
|---------------------------|--|
| Detection                 | VAN_BACKDOOR.UMXX  |
| Exploited vulnerabilities | -  |
| Threat Characteristics    | Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1) Suspicious network or messaging activity (18) |

### Process Graph



#### Process Graph Legend

#### ▼ Notable Threat Characteristics

### ▼ Malformed, defective, or with known malware traits (1)

| Characteristic                     | Significance | Details   |
|------------------------------------|--------------|-----------|
| Web content contains phishing code |              | Hawb.html |

### ▼ Process, service, or memory object change (1)

| Characteristic  | Significance | Details  |
|-----------------|--------------|--|
| Creates process | •==          | Process ID: 700 Image Path: %ProgramFiles(x86)%\Internet Explorer\IEXPLORE.EXE SCODEF:1660 CREDAT:148481 /prefetch:2 |

### ▼ Suspicious network or messaging activity (18)

| Characteristic  | Significance | Details       |
|-----------------|--------------|---------------|
| Listens on port |              | 0.0.0.0:49442 |
| Listens on port |              | 0.0.0.0:49441 |
| Listens on port |              | 0.0.0.0:49440 |
| Listens on port |              | 0.0.0.0:49439 |
| Listens on port |              | 0.0.0.0:49438 |
| Listens on port |              | 0.0.0.0:49437 |
| Listens on port |              | 0.0.0.0:49436 |
| Listens on port |              | 0.0.0.0:49435 |
| Listens on port |              | 0.0.0.0:49434 |
| Listens on port |              | 0.0.0.0:49433 |
| Listens on port |              | 0.0.0.0:49432 |
| Listens on port |              | 0.0.0.0:49431 |
| Listens on port |              | 0.0.0.0:49430 |
| Listens on port |              | 0.0.0.0:49429 |
| Listens on port |              | 0.0.0.0:49428 |
| Listens on port |              | 0.0.0.0:49427 |
| Listens on port |              | 0.0.0.0:49426 |
| Listens on port |              | 0.0.0.0:49425 |

### ▼ Network Destinations

| Domain                      | IP Address     | Port | Location | Risk Level | Threat | Accessed By |
|-----------------------------|----------------|------|----------|------------|--------|-------------|
| ocsp.digicert.com           | 93.184.220.29  | 53   | -        | No risk    | -      | Hawb.html   |
| fonts.googleapis.com        | 142.250.74.10  | 53   | -        | No risk    | -      | Hawb.html   |
| iecvlist.microsoft.com      | 152.199.19.161 | 53   | -        | No risk    | -      | Hawb.html   |
| go.microsoft.com            | 184.86.224.103 | 53   | -        | No risk    | -      | Hawb.html   |
| ocsp.pki.goog               | 216.58.207.227 | 53   | -        | No risk    | -      | Hawb.html   |
| ctldl.windowsupdate.com     | 205.185.216.10 | 53   | -        | No risk    | -      | Hawb.html   |
| sqm.telemetry.microsoft.com | 65.55.252.93   | 53   | -        | No risk    | -      | Hawb.html   |
| fonts.gstatic.com           | 216.58.207.195 | 53   | -        | No risk    | -      | Hawb.html   |
| ieonline.microsoft.com      | 204.79.197.200 | 53   | -        | No risk    | -      | Hawb.html   |
| ocsp.digicert.com           | 93.184.220.29  | 80   | -        | -          | -      | Hawb.html   |
| ocsp.pki.goog               | 216.58.207.227 | 80   | -        | -          | -      | Hawb.html   |
| ctldl.windowsupdate.com     | 205.185.216.10 | 80   | -        | -          | -      | Hawb.html   |
| go.microsoft.com            | 184.86.224.103 | 80   | -        | -          | -      | Hawb.html   |
| fonts.googleapis.com        | 142.250.74.10  | 443  | -        | -          | -      | Hawb.html   |
| sqm.telemetry.microsoft.com | 65.55.252.93   | 443  | -        | -          | -      | Hawb.html   |
| ctldl.windowsupdate.com     | 81.198.165.201 | 80   | -        | -          | -      | Hawb.html   |
| ieonline.microsoft.com      | 204.79.197.200 | 443  | -        | -          | -      | Hawb.html   |
| fonts.gstatic.com           | 216.58.207.195 | 443  | -        | -          | -      | Hawb.html   |
| iecvlist.microsoft.com      | 152.199.19.161 | 443  | -        | -          | -      | Hawb.html   |

| URL Site Category Risk Level Threat Accessed By  http://ocsp.digicert.com/MFEwTzBNMEswSTAJB gUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh% 2FsBYgFV7gQUA95QNVbRTLtm8KF/GxvDl7i90  Site Category Risk Level Threat Accessed By  Hawb.html   |  |
|---|--|
| gUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh% Cloud Applications 2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7l90  |  |
| VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D   |  |
| https://fonts.googleapis.com/css?family=PT+San  |  |
| http://ocsp.pki.goog/gts1o1core/MFlwUDBOMEw   |  |
| https://iecvlist.microsoft.com/ie11blocklist/140174 Business / Economy Computers / Internet Cloud Applications No risk - Hawb.html  |  |
| https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiT Computers / Internet No risk - Hawb.html o99u79D0KEww.woff  |  |
| https://iecvlist.microsoft.com/IE11/1426178821/ie compativiewlist.xml  Business / Economy Computers / Internet Cloud Applications  No risk - Hawb.html  |  |
| http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?e0e 817717432daa8 - Computers / Internet Cloud Applications - |  |
| http://ocsp.digicert.com/MFEwTzBNMEswSTAJB  |  |
| http://ctldl.windowsupdate.com/msdownload/upda telv/3/static/trustedr/en/disallowedcertstl.cab?b46 a730d6789357a  |  |
| http://ocsp.pki.goog/gls1o1core/MFEwTzBNMEs wSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDmj% 2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug63 0J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E %3D  |  |
| http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/pinrulesstl.cab?f15d8c2e5 tb81975 Computers / Internet Cloud Applications Hawb.html   |  |
| http://go.microsoft.com/fwlink/? Computers / Internet No risk - Hawb.html LinkID=401135   |  |
| http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJ Computers / Internet No risk - Hawb.html  BgUrDgMCGgUABBTgXlsxbvr2lBkPpolEVRE6g HICnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CD QHjtJqhjYqpgSVpULg%3D   |  |
| https://ieonline.microsoft.com/ieflipahead/ie10/rul es.xmll?mkt=en-US  Business / Economy Computers / Internet Cloud Applications  No risk - Hawb.html  |  |
| https://fionts.gstatic.com/s/ptsans/v12/jiz/fRExUITo Computers / Internet No risk - Hawb.html 99u79B_mh006tKw.woff  |  |

### ▼ Dropped or Downloaded Files

| File  | Risk Level | Threat | Threat Characteristics | Source URL   | Size (bytes) | SHA-1  |
|---|------------|--------|------------------------|--|--------------|--|
| {0FA7F1DC-BEE1-11EB-9BF2-00<br>1F3C8C8DBB}.dat                            | No risk    | -      | -                      | -  | 3584         | F1CB4BD242B83F0DEBFC20429B180B441E<br>4FA660 |
| RecoveryStore.{0FA7F1DA-BEE1 -11EB-9BF2-001F3C8C8DBB}.dat                 | No risk    | -      | -                      | -  | 5632         | F78A26F659677B888F3038BD396B2649CA2<br>412ED |
| IEInstrumentation2021[1].htm  | No risk    | -      | -                      | -  | 2140         | C80654A5A50C561D9B0D04D822481C1DD4<br>9C58B6 |
| jizaRExUiTo99u79D0KEww[1].wo<br>ff  | No risk    | -      | -                      | https://fonts.gstatic.com/s/ptsans/<br>v12/jizaRExUiTo99u79D0KEww.<br>woff     | 55340        | 0515F781A37C8775C466577EC40AEF136CB<br>CF3CB |
| ~DFAD60AA53D96FDCE3.TMP   | No risk    | -      | -                      | -  | 16384        | A06EAD2C3E32A6F862492EA1CE50BFDE15<br>F465BA |
| CC197601BE0898B7B0FCC91FA<br>15D8A69_D73245CB85BA4F270<br>1FE45752B2B1FC1 | No risk    | -      | -                      | -  | 422          | 7D77058AFC77DD7090CEFE0A4897448D11<br>47CA2D |
| CFE86DBBE02D859DC92F1E17<br>E0574EE8_46766FC45507C0B9<br>E264E4C18BC7288B | No risk    | -      | -                      | -  | 394          | CE840481010320854E95D812BB678E81658<br>ABE29 |
| CC197601BE0898B7B0FCC91FA<br>15D8A69_8A59D0CC8B8124639<br>3FAF874672C0BE9 | No risk    | -      | -                      | -  | 414          | 69626A9B6376FE6DF759417BD509E16EA4B<br>D4F36 |
| jizfRExUiTo99u79B_mh0O6tKw[1] .woff                                       | No risk    | -      | -                      | https://fonts.gstatic.com/s/ptsans/<br>v12/jizfRExUiTo99u79B_mh0O6t<br>Kw.woff | 57524        | 27DF60E5879AA568876F747F3CFACF28564<br>F9B09 |
| ~DF105EE340451AB1B0.TMP   | No risk    | -      | -                      | -  | 16384        | 2DAEA6E53554F7D8D3DD1909E5CB4F48D<br>7395954 |

### ▼ Suspicious Objects

| Туре        | Object                                   | Risk Level |
|-------------|--|------------|
| File (SHA1) | F7911D858AFCCB9E871595374564EFE2D6449377 | High       |

### ▼ Analysis

| Event Type          | Details  | Parent PID | PID  |
|---------------------|--|------------|------|
| Detection           | Threat Characteristic: Web content contains phishing code Hawb.html  |            |      |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SQM\PIDs\PID_1660 Value: 67c   |            | 1660 |
| Call Network API    | API Name: socket Args: ( 23, 1, 6 ) Return: 398  |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\CompatibilityFlags Value: 0   |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0   |            | 1660 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None  |            | 1660 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None  |            | 1660 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None  |            | 1660 |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None   |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None  |            | 1660 |
| Call System API     | API Name: WinHttpCloseHandle Args: ( a1422530 ) Return: 1  |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{0FA7F1DA-BEE1-11EB-9BF2-001F3C8C8DBB} Value: 0   |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running   |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Zones\SecuritySafe Value: 1  |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\FullScreen Value: no  |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Window_Placement Value: None  |            | 1660 |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\PendingRecovery\AdminActive Value: 0  |            | 1660 |
| Call Process API    | API Name: CreateProcessW Args: (, "%ProgramFiles(x86)%\Internet Explorer\IEXPLORE.EXE" SCODEF:1660 CREDAT:148481 /prefetch:2, , , , CREATE_SUSPENDED, , , , Process:700:%ProgramFiles(x86)%\Internet Explorer\iexplore.exe ) Return: 1 |            | 1660 |
| Call Thread API     | API Name: NtResumeThread Args: ( Process:700, ) Return: ?  |            | 1660 |
| Call System API     | API Name: evtchann.SendEvent Args: ( e), pid[700], ppid[1660 ) Return: 1   |            | 1660 |
| Detection           | Threat Characteristic: Creates process Process ID: 700 Image Path: %ProgramFiles(x86)%Internet ExplorerIEXPLORE.EXE SCODEF:1660 CREDAT:148481 /prefetch:2  |            |      |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache ) Return: 1   | 1660       | 700  |
| Call Network API    | API Name: socket Args: ( 23, 1, 6 ) Return: 38c  | 1660       | 700  |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0   | 1660       | 700  |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None  | 1660       | 700  |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None  | 1660       | 700  |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None  | 1660       | 700  |
| Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None  | 1660       | 700  |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None  | 1660       | 700  |
| Call Service API    | API Name: OpenServiceW Args: ( 7e06860, WinHttpAutoProxySvc, 94 ) Return: 7e06158  | 1660       | 700  |
| Call System API     | API Name: WinHttpCloseHandle Args: ( 7e1d810 ) Return: 1   | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1   | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1   | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows\History ) Return: 1   | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1  | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %windir%\SysWOW64\propsys.dll ) Return: 1  | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer ) Return: 1   | 1660       | 700  |
| Call System API     | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%Microsoft\Internet Explorer ) Return: 1  | 1660       | 700  |

| Call System API   | API Name: evtchann.SendEvent Args: ( e), imagepath[%SystemRoot%\System32\rundli32.exe shell32.dll, SHCreateLocalServerRunDll {9BA05972-F6A8-11C   | 1660                         | 700                             |
|---|---|------------------------------|---------------------------------|
|   | F-A442-00A0C90A8F39} ) Return: 1  |                              |                                 |
| Call System API   | API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[700 ) Return: 1   | 1660                         | 700                             |
| Call Internet Helper API  | API Name: InternetOpenW Args: ( Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, 0, , , 10000000 ) Return: cc0004   | 1660                         | 700                             |
| Call System API   | API Name: DnsQueryEx Args: ( fonts.googleapis.com, 1, 50020000 ) Return: 0  | 1660                         | 700                             |
| Call Internet Helper API  | API Name: InternetConnectW Args: ( cc0004, fonts.googleapis.com, 443, , , 3, 8388608, 133094304 ) Return: cc0008  | 1660                         | 700                             |
| Call Internet Helper API  | API Name: HttpOpenRequestW Args: ( cc0008, GET, /css?family=PT+Sans:400,700, , , 136545888, 12582912, 133094304 ) Return: cc000c  | 1660                         | 700                             |
| Call System API   | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1  | 1660                         | 700                             |
| Call System API   | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows ) Return: 1  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 2, 2, 0 ) Return: 6d8  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: 6d8   | 1660                         | 700                             |
| Call System API   | API Name: DnsQueryEx Args: ( fonts.googleapis.com, 1c, 40026000 ) Return: 0   | 1660                         | 700                             |
| Call System API   | API Name: CreateDXGlFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 7e447a4 ) Return: 0   | 1660                         | 700                             |
|   |   | 1660                         | 700                             |
| Call System API   | API Name: CreateDXGIFactory Args: ( {7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 7e447a4 ) Return: 0   |                              |                                 |
| Call System API   | API Name: DnsQueryEx Args: ( fonts.googleapis.com, 1, 40006000 ) Return: 87   | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: 840   | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 844  | 1660                         | 700                             |
| Call Network API  | API Name: bind Args: ( 844, 0.0.0.0:49425, 16 ) Return: 0   | 1660                         | 700                             |
| Detection   | Threat Characteristic: Listens on port 0.0.0.0:49425  |                              |                                 |
| Call System ADI   |   | 1660                         | 700                             |
| Call System API   | API Name: ConnectEx Args: ( 844, 142.250.74.10:443, 16, 0, 0, 0, 7eeba54 ) Return: 0  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 84c  | 1660                         | 700                             |
| Call Network API  | API Name: bind Args: ( 84c, 0.0.0:49426, 16 ) Return: 0   | 1660                         | 700                             |
| Detection   | Threat Characteristic: Listens on port  |                              |                                 |
| Dell Contrar ADI  | 0.0.0.049426  | 4000                         | 700                             |
| Call System API   | API Name: ConnectEx Args: (84c, 142.250.74.10:443, 16, 0, 0, 0, 7eebb54) Return: 0  | 1660                         | 700                             |
| Call Filesystem API   | API Name: RemoveDirectoryW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\(\)iconcache ) Return: 0  |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\frameiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\tabiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %USERPROFILE%\AppData\LocalLow\Microsoft\Internet Explorer\tabiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\largeiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\immersiveiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\imdockediconcache.dat ) Return: 0  |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\imtilelargeiconcache.dat ) Return: 0   |                              | 1660                            |
| Call Filesystem API   | API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Internet Explorer\imtilesmalliconcache.dat ) Return: 0   |                              | 1660                            |
| Call Network API  | API Name: send Args: (84c,, 1, 215) Return: 0   | 1660                         | 700                             |
| Call Network API  | API Name: send Args: ( 844,, 1, 215 ) Return: 0   | 1660                         | 700                             |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0   | 1660                         | 700                             |
| Delete Registry Key   | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N   | 1660                         | 700                             |
| Doloto Nogiota y Noy  | one   | 1000                         |                                 |
| Write Registry Key  | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val   | 1660                         | 700                             |
|   | ue: None  |                              |                                 |
| Call Network API  | API Name: socket Args: ( 23, 1, 6 ) Return: b0c   | 1660                         | 700                             |
| Call Service API  | API Name: OpenServiceW Args: ( 8bb9c78, NetSetupSvc, 4 ) Return: 8bb9cc8  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 1, 6 ) Return: b80   | 1660                         | 700                             |
| Call System API   | API Name: WinHttpCloseHandle Args: ( 9532e28 ) Return: 1  | 1660                         | 700                             |
| Call System API   | API Name: WinHttpCloseHandle Args: ( 951da20 ) Return: 1  | 1660                         | 700                             |
| •   |   |                              |                                 |
| Call Network API  | API Name: socket Args: ( 2, 2, 0 ) Return: bd4  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: bd4   | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 2, 2, 0 ) Return: be4  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: be4   | 1660                         | 700                             |
| Call System API   | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87  | 1660                         | 700                             |
| Call System API   | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1, 40006000 ) Return: 87  | 1660                         | 700                             |
| Call System API   | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: bfc   | 1660                         | 700                             |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: bfc  | 1660                         | 700                             |
| Call Network API  | API Name: bind Args: ( bfc, 0.0.0.949427, 128 ) Return: 0   | 1660                         | 700                             |
| Detection   | Threat Characteristic: Listens on port  |                              |                                 |
| Detection   | 0.0.0.0:49427   |                              |                                 |
|   |   | 1660                         | 700                             |
|   | API Name: ConnectEx Args: ( bfc, 81.198.165.201:80, 16, 0, 0, 0, 8a2c850 ) Return: 0  |                              |                                 |
| Call System API   | API Name: ConnectEx Args: ( bfc, 81.198.165.201:80, 16, 0, 0, 0, 8a2c850 ) Return: 0  API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  | 1660                         | 700                             |
| Call System API<br>Call System API  |   | 1660<br>1660                 | 700<br>700                      |
| Call System API Call System API Call Network API  | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1t/nConnection: Keep-Alivel/n Accept: */"\ninif-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTr/nlf-None-Match: "08f5ab0361ad71:0"\rinuber-Agent: Microsoft-CryptoAPI/10.0\rinuber: ctld   |                              |                                 |
| Call System API Call System API Call Network API Call Network API   | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1\r\nConnection: Keep-Alive\r\n Accept: "\r\n\ntif-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nlf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctld l.windowsupdate.com\r\n\r\n\r\n\n, 1, 287 ) Return: 0   | 1660<br>1660                 | 700                             |
| Call System API Call System API Call Network API Call Network API Call Network API  | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1\r/inConnection: Keep-Alive\r/in Accept: "/minIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTv/nlf-None-Match: "08f5ab0361ad71:0"r/nUser-Agent: Microsoft-CryptoAPI/10.0\r/inHost: ctld Lwindowsupdate.com/vln/r/n, 1, 287 ) Return: 0  API Name: socket Args: ( 2, 1, 6 ) Return: bd0  | 1660<br>1660                 | 700<br>700<br>700               |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API  | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1lvinConnection: Keep-Alive\rin Accept: "/"\rin\nff-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTv\nlf-None-Match: "08f5ab0361ad71:0"\rin\nUser-Agent: Microsoft-CryptoAPI/10.0\rin\nHost: ctld Lwindowsupdate.com\rin\rin\rin\rin\rin\rin\rin\rin\rin\rin  | 1660<br>1660                 | 700                             |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API  | API Name: DnsQueryEx Args: ( ctldl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1\r/inConnection: Keep-Alive\r/in Accept: "/minIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTv/nlf-None-Match: "08f5ab0361ad71:0"r/nUser-Agent: Microsoft-CryptoAPI/10.0\r/inHost: ctld Lwindowsupdate.com/vln/r/n, 1, 287 ) Return: 0  API Name: socket Args: ( 2, 1, 6 ) Return: bd0  | 1660<br>1660                 | 700<br>700<br>700               |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API Detection  | API Name: DnsQueryEx Args: ( ctidl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1\rinConnection: Keep-Alive\rin Accept: /"urnIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\rinIf-None-Match: "08f5ab0361ad71:0"\rinUser-Agent: Microsoft-CryptoAPI/10.0\rinHost: ctid Lwindowsupdate.com\rin\rin\rin, 1, 287 ) Return: 0  API Name: socket Args: ( 2, 1, 6 ) Return: bd0  API Name: bind Args: ( bd0, 0.0.0.0:49428, 128 ) Return: 0  Threat Characteristic: Listens on port   | 1660<br>1660                 | 700<br>700<br>700               |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API Delection Call System API   | API Name: DnsQueryEx Args: ( ctidl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1t/nConnection: Keep-Alive\r/in Accept: "/"r\nfif-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTv\nfif-None-Match: "08f5ab0361ad71:0"\r/inUser-Agent: Microsoft-CryptoAPI/10.0\r/inHost: ctid Lwindowsupdate.com\r/in\r/in, 1, 287 ) Return: 0  API Name: socket Args: ( 2, 1, 6 ) Return: bd0  API Name: bind Args: ( bd0, 0.0.0.049428, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.049428   | 1660<br>1660<br>1660         | 700<br>700<br>700<br>700        |
| Call System API Call System API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call System API Call System API Call System API | API Name: DnsQueryEx Args: ( ctidl.windowsupdate.com, 1c, 40026000 ) Return: 0  API Name: socket Args: ( 23, 2, 0 ) Return: bd0  API Name: send Args: ( bfc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a HTTP/1.1\nConnection: Keep-Alive\n/n Accept: "\n'\nfl-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\nlf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\n'nHost: ctid Lwindowsupdate.com\n'\n\n\n, 1, 287 ) Return: 0  API Name: socket Args: ( 2, 1, 6 ) Return: bd0  API Name: bind Args: ( bd0, 0.0.0.0:49428, 128 ) Return: 0  Threat Characteristic: Listens on port 0.0.0.0:49428  API Name: ConnectEx Args: ( bd0, 81.198.165.201:80, 16, 0, 0, 0, 8a2bf90 ) Return: 0  API Name: send Args: ( bd0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e0e817717432daa8 HTTP/1.1\n'nConnection: Keep-Alive\n'\n\nCoept: "\n'\nlf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\nnlf-None-Match: "08f5ab0361ad71:0"\n'\nUser-Agent: Microsoft-CryptoAPI/10.0\n'\nHost: ct | 1660<br>1660<br>1660<br>1660 | 700<br>700<br>700<br>700<br>700 |

| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bbc888 ) Return: 1  | 1660         | 700               |
|----------------------------------|---|--------------|-------------------|
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 951ee30 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 9513178 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bbea98 ) Return: 1  | 1660         | 700               |
| Call Service API                 | API Name: OpenServiceW Args: ( 8bb9f48, CryptSvc, 5 ) Return: 8bb9c00   | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bbed98 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 951dbd0 ) Return: 1  | 1660         | 700               |
| Delete Registry Key              | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one   | 1660         | 700               |
| Write Registry Key               | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None   | 1660         | 700               |
| Delete Registry Key              | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one   | 1660         | 700               |
| Write Registry Key               | Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None   | 1660         | 700               |
| Call Network API                 | API Name: socket Args: (23, 1, 6) Return: b64   | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 95297a8 ) Return: 1  | 1660         | 700               |
| Call Network API                 | API Name: socket Args: (2, 2, 0) Return: b00  | 1660         | 700               |
| Call Network API                 | API Name: socket Args: (23, 2, 0) Return: b00   | 1660         | 700               |
| Call System API                  | API Name: DnsQueryEx Args: ( ocsp.pki.goog, 1, 40006000 ) Return: 87  | 1660         | 700               |
| Call System API                  | API Name: DnsQueryEx Args: ( ocsp.pki.goog, 1c, 40026000 ) Return: 0  | 1660         | 700               |
| Call Network API                 | API Name: socket Args: (23, 2, 0) Return: b00   | 1660         | 700               |
|                                  |   |              |                   |
| Call Network API                 | API Name: socket Args: (2, 1, 6) Return: b00  | 1660         | 700               |
| Call Network API                 | API Name: bind Args: (b00, 0.0.0.49429, 128 ) Return: 0   | 1660         | 700               |
| Detection                        | Threat Characteristic: Listens on port 0.0.0.0:49429  |              |                   |
| Call System API                  | API Name: ConnectEx Args: ( b00, 216.58.207.227:80, 16, 0, 0, 0, 8a2b6d0 ) Return: 0  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( b00, GET /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXlsxbvr2lBkPpolEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4 CDQHJtJqhjYqpgSVpULg%3D HTTP/1.1lr\nConnection: Keep-Alive\n\nAccept: */"\n\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.pki.goog\r\n\r\n, 1, 2 31 ) Return: 0           | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bbec40 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 953cf38 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bb3b50 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bb3cd8 ) Return: 1  | 1660         | 700               |
| Call Network API                 | API Name: socket Args: ( 23, 1, 6 ) Return: afc   | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 95297e8 ) Return: 1  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( b00, GET /gls1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZlZjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEQCw80IEZ3xvjQUAAAAAh8vC HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.pki. goog\r\nl\r\n, 1, 241) Return: 0 | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 9537490 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 952e318 ) Return: 1  | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bb3b50 ) Return: 1  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 84c,, 1, 126 ) Return: 0   | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 844,, 1, 126 ) Return: 0   | 1660         | 700               |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( 8bb3cd8 ) Return: 1  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 84c,, 1, 87 ) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c8050, , 40, 9daf368, , 0, , 56, 165344348, 0 ) Return: 0   | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c8050, , 9, 9daf3c8, , 0, , 25, 165344444, 0 ) Return: 0  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 844,, 1, 87 ) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c5360, , 40, 9daf368, , 0, , 56, 165344348, 0 ) Return: 0   | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c5360, , 9, 9daf368, , 0, , 25, 165344348, 0 ) Return: 0  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 84c,, 1, 38 ) Return: 0  | 1660         | 700               |
| Call Network API                 | API Name: send Args: ( 84c,, 1, 153 ) Return: 0   | 1660         | 700               |
| Call Network API                 | API Name: send Args: (844,, 1, 38) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c8050, , 377, a6ff248, , 0, , 1239, 175108924, 0 ) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c8050, , 47, aciir44, , 0, , 1239, 17310924, 0 ) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: BCryptDecrypt Args: ( 94c8050, , 441, 8off248, , 0, , 633, 175108924, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 94c8050, , 215, 86ff248, , 0, , 363, 175108924, 0 ) Return: 0  | 1660         | 700               |
| Call System API  Call System API |   | 1660         | 700               |
|                                  | API Name: BCryptDecrypt Args: ( 94c8050, , 103, a6ff248, , 0, , 119, 175108924, 0 ) Return: 0   |              |                   |
| Call Notwork API                 | API Name: BCryptDecrypt Args: ( 94c8050, , 17, a6ff150, , 0, , 33, 175108676, 0 ) Return: 0   | 1660         | 700               |
| Call Network API                 | API Name: send Args: (84c,, 1, 46) Return: 0  | 1660         | 700               |
| Call System API                  | API Name: PathFileExistsW Args: ( %LOCALAPPDATA%Microsoft\Internet Explorer ) Return: 1   | 1660         | 700               |
| Call System API                  | API Name: DnsQueryEx Args: (fonts.gstatic.com, 1, 50020000) Return: 0   | 1660         | 700               |
| Call Internet Helper API         | API Name: InternetConnectW Args: ( cc0004, fonts.gstatic.com, 443, , , 3, 8388608, 144888960 ) Return: cc0008   | 1660         | 700               |
| Call Internet Helper API         | API Name: HttpOpenRequestW Args: ( cc0008, GET, /s/ptsans/v12/jizaRExUiTo99u79D0KEww.woff, , , 136552432, 12582912, 144888960 ) Return: cc000c  | 1660         | 700               |
| Call System API                  | API Name: DnsQueryEx Args: ( fonts.gstatic.com, 1, 50020000 ) Return: 0   | 1660         | 700               |
| Call Internet Helper API         | API Name: InternetConnectW Args: ( cc0004, fonts.gstatic.com, 443, , , 3, 8388608, 156407000 ) Return: cc0010   | 1660         | 700               |
| Call Internet Helper API         | API Name: HttpOpenRequestW Args: ( cc0010, GET, /s/ptsans/v12/jizfRExUiTo99u79B_mh006tKw.woff, , , 136552432, 12582912, 156407000 ) Return: cc0 014   | 1660         | 700               |
| Call Network API                 | API Name: socket Args: ( 2, 2, 0 ) Return: 7e0  | 1660         | 700               |
| Call Network API                 | API Name: socket Args: (23, 2, 0) Return: 7e0   | 1660         | 700               |
|                                  | API Name: DnsQueryEx Args: ( fonts.gstatic.com, 1, 40006000 ) Return: 87  | 1660         | 700               |
|                                  | API Name: DrisQueryEx Args: (fonts.gstatic.com, 1c, 40026000 ) Return: 0  | 1660         | 700               |
| Call System API Call System API  |   | ,000         |                   |
| Call System API                  |   | 1660         | 700               |
| Call System API Call Network API | API Name: socket Args: ( 23, 2, 0 ) Return: 65c   | 1660         | 700               |
| Call System API                  |   | 1660<br>1660 | 700<br>700<br>700 |

| Millane   Mill  | Detection           | Threat Characteristic: Listens on port 0.0.0.049430  |      |      |
|---|---------------------|--|------|------|
| Mile  | Call System API     | API Name: ConnectEx Args: ( 7e0, 216.58.207.195:443, 16, 0, 0, 0, 8bb130c ) Return: 0  | 1660 | 700  |
| Procession   Pro  | Call Network API    | API Name: socket Args: ( 2, 1, 6 ) Return: 65c   | 1660 | 700  |
|   | Call Network API    | API Name: bind Args: ( 65c, 0.0.0.0:49431, 16 ) Return: 0  | 1660 | 700  |
| Milliams   | Detection           |  |      |      |
| Personant   Pers  | Call System API     | API Name: ConnectEx Args: ( 65c, 216.58.207.195:443, 16, 0, 0, 0, 8bb178c ) Return: 0  | 1660 | 700  |
|   | Call Network API    | API Name: send Args: ( 7e0,, 1, 212 ) Return: 0  | 1660 | 700  |
| APP Note (Company Company Co  | Call Network API    | API Name: send Args: ( 65c,, 1, 212 ) Return: 0  | 1660 | 700  |
| APPENDENCE   APPENDENCE (CARREST)   APPENDE  | Delete Registry Key | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{00000000-0000-0000-0000-000000000000} Value: None  |      | 1660 |
| Antique and any of the content and professional profess  | Call Network API    | API Name: socket Args: (23, 1, 6) Return: bd4  | 1660 | 700  |
| California Art   Cali  | Call System API     | API Name: WinHttpCloseHandle Args: ( 8a3cb50 ) Return: 1   | 1660 | 700  |
| And Suppose   An  | Call Network API    | g630J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost:   | 1660 | 700  |
| Colfspend Aff   | Call System API     | API Name: WinHttpCloseHandle Args: ( 8a33238 ) Return: 1   | 1660 | 700  |
| An Internation Affile   | Call System API     | API Name: WinHttpCloseHandle Args: ( 94becf8 ) Return: 1   | 1660 | 700  |
| An Internation Affile   | Call System API     | API Nama: WinHttnCloseHandle Arns: ( 8hh3h50 ) Return: 1   | 1660 | 700  |
| March   All Processor (Proc.   150   Reserved   150   |                     |  |      |      |
| March   Marc  |                     |  |      |      |
| Miller   M  |                     |  |      |      |
| An Internation April  |                     |  |      |      |
| Mill Names And Mill Market soot Age (1976) (8.2) Pales in 1 (1976)  |                     |  |      |      |
| APP   |                     |  |      |      |
| 64 Spream ARP   APP Name & Despite Comprise Ang. (1977-06.), 8. a. 2077-05. (1975-06.) A. 2075-05. (1975-06.) A.  |                     |  |      |      |
| APP   American Despite Copyright (1997 166), 200   2  |                     |  |      |      |
| APP   Apr   |                     |  |      |      |
| AP   Passes Dicyplicograph April   SAPPA (1997-1904), 1984, Add 1981, 0. 1, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 1, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 0. 1, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 0. 2, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 0. 2, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 0. 1, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 2015-0, 0. 1, 2025, 1881-1808-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1981-1908-0, 1   Passes Dicyplicograph April   SAPPA (1997-1904), 1980, 198  |                     |  |      |      |
| Cest Systems APP  |                     |  |      |      |
| API Name EPOSPULANDE PAGE (ESTAGO, 1388, ACTIVAL O, 2014, 1881 STORING I) Relation 0   1900   700     |                     |  |      | 700  |
| APA Name: ECrypticropy: April 1 (1985) (1995) (19  |                     |  | 1660 | 700  |
| Cast Systems APP  |                     |  |      |      |
| Cad System AP  AP  Name B CoyptDecrypt Age; (1976) 201, 100 1, 1906, 1901 100 100 1, 1901 100 1, 1901 100 1, 1901 100 1, 1901 100 1, 190  |                     |  | 1660 | 700  |
| Cast System API   | Call System API     |  | 1660 | 700  |
| Cast System API   | Call System API     |  | 1660 | 700  |
| Cast System API   | Call System API     | API Name: BCryptDecrypt Args: ( 95/7a60, ]_, 1389, a05/1d0, , 0, ]_, 22424, 168161988, 0 ) Return: 0   | 1660 | 700  |
| AFT Name  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, Øa, 1389, a05f1d0, , 0, Øa, 21006, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, : PÅ, 1389, a05f1d0, , 0, : PÅ, 19588, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, , ™™Ž¢, 1389, a05f1d0, , 0, , ™™Ž¢, 18170, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, r"¬Ö©Í, 1389, a05f1d0, , 0, r"¬Ö©Í, 16752, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, "Ø9Ú, 1389, a05f1d0, , 0, "Ø9Ú, 15334, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API   API Name: BCyptDecrypt Args: (B577860, E.) 1389, a051140, 0, e.) 1, 1080, 168151988, 0) Return: 0   1660   700  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, àāYÜM£ô, 1389, a05f1d0, , 0, àāYÜM£ô, 13916, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API API Name: BCryptDecrypt Args: (9577a60, s1), 1389, a0511d0, 0, s1), 9662, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x4—h**T, 295*h.n., 1389, a0511d0, 0, x4—h**T, 295*h.n., 2244, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**T, 295*h.n., 1389, a0511d0, 0, x8—h**T, 295*h.n., 2244, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 1389, a0511d0, 0, x8—h**T, 295*h.n., 2244, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 1389, a0511d0, 0, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—x8—h**D, 186161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, x8—x8—x8—x8—x8—x8—x8—x8—x8—x8—x8—x8—x8—x   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, ¿¹Ø, 1389, a05f1d0, , 0, ¿¹Ø, 12498, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Gall System API         API Name: BCypyDecrypt Args: (987/860, xi_m***T_2/g**xi_m, 1389, a05f1d0, 0, xi_m**T_2/g**xi_m, 1389, a05f1d0, 0, xi_m**T_2/g**xi_m, 1389, a05f1d0, 0, xi_m**T_2/g**xi_m, 1389, a05f1d0, 0, xi_m**X                                 | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, Ë, 1389, a05f1d0, , 0, Ë, 11080, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API API Name: BCryptDecrypt Args: (9577a60, All-Vá YEy, 1389, a057td0, 0, All-Vá YEy, 6326, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1389, a057td0, 0, e, 5408, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1389, a057td0, 0, 1, 3909, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1748, a057td0, 0, 1, 1405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1748, a057td0, 0, 1, 1405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1748, a057td0, 0, 0, 1, 1405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1748, a057td0, 0, 0, 31887, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1389, a057td0, 0, 0, 31887, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1389, a057td0, 0, 0, 2, 30469, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1389, a057td0, 0, 0, 2, 30469, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1677) Name: A0574a, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1677) Name: A057460, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1677) Name: A057460, 167046740, 0, 1475, 0, -40574674674047467471 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1479, -40546740474, 1204, 0, 1389, a0571d0, 0, 1475, 0, -40574674674, 0, 1475, 0, -4057467467471 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1479, -4054674674, 1204, 0, 1389, a0571d0, 0, 0, 1476, 148161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (9577a60, 1479, -4054674674, 14861674, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, 1486, | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, s1), 1389, a05f1d0, , 0, s1), 9662, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API API Name: BCryptDeorypt Args: (9577a60, 6, 1389, a0511d0, 0, 6, 5408, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 3890, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, NNe11A, 1389, a0511d0, 0, 1Ne11A, 2572; (168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 11405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 11405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 11405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 11405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1389, a0511d0, 0, 11405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1897a60, 11405, 0, 11405, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1897a60, 11405, 0, 11405, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1897a60, 11405, 0, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 1897a60, 11405, 0, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 21406, 11405, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, 21406, 11405, 11406,  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, ,xL—h*÷T¿g\$"k:\n., 1389, a05f1d0, , 0, ,xL—h*÷T¿g\$"k:\n., 8244, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 3980, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1881d1, 1389, a05f1d0, 0, 0, 1881d, 2572, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 0, 4584,95810.2€, 2839, a05f1d0, 0, 2, 4405, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 3487,95810.2€, 28755, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 3487,95810.2€, 28755, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 2, 30469, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 2, 30469, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 1389, a05f1d0, 0, 0, 2, 30469, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 168710, 1389, a05f1d0, 0, 0, 6, 7, 2383, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 6, 7, 1389, a05f1d0, 0, 0, 6, 7, 22515, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 6, 7, 1389, a05f1d0, 0, 6, 7, 22515, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 7, 2484,654) (7, 7, 7, 7, 7, 7, 7, 7, 7, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (95f7a60, 7, 2484,6546,7, 1389, a05f1d0, 0, 0, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, AšI~V'à ŸEy, 1389, a05f1d0, , 0, AšI~V'à ŸEy, 6826, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API API Name: BCryptDeorypt Args: (9577a60, [Nietli A, 1389, a05f1d0, .0, [Nietli A, 2572, 168161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, u², 1405, 168161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, a½A²/jiNNLOàt, 839, 2555, 168161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, u², 1389, u², 1887, 188161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, u², 2046, 188161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, u², 2046, 188161988, 0] Return: 0 1660 700  Call System API API Name: BCryptDeorypt Args: (9577a60, u², 1389, a05f1d0, .0, u², u², u², u², u², u², u², u², u², u²   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, è, 1389, a05f1d0, , 0, è, 5408, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API         API Name: BCryptDecrypt Args: (9877a60, u², 1389, a05f1d0, 0, u², 1405, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 436A7j8NiO26, 839, a05f1d0, 0, 0, 31887, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 1389, a05f1d0, 0, 0, 23951, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 127, 1389, a05f1d0, 0, 0, 29051, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 162°T)l0, 1389, a05f1d0, 0, 29051, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 62°T), 1389, a05f1d0, 0, 62°T, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 46°T), 1389, a05f1d0, 0, 62°T, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9877a60, 41°Ju, 24)5-360*46*10*10*10*4**e**TEA'A' 12°P, 0, 1389, a05f1d0, 0, 0 *****, 1389, a05f1d0, 0, 0 *******************************  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, , 1389, a05f1d0, , 0, , 3990, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API API Name: BCryptDecrypt Args: (95f7a60, 8½A/jšNuOá£, 839, a05f1d0, , 0, 8½A/jšNuOá£, 22755, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 2, 30469, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 2, 30469, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 627)(0, 27833, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 12710), 1389, a05f1d0, , 0, 62710, 27833, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 18710, 1389, a05f1d0), 0, 6271, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1871, 1389, a05f1d0), 0, 6271, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1871, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1871, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 2±86, 168161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 2±86, 168161988, 0) Return: 0 1660 700  Call System API API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 2*894, 1889, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 0, 19125, 188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 0, 19125, 188161988, 0) Return: 0 1660 700  Call System API API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 0, 19125, 188161988, 0) Return: 0 1660 700  Call System API API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 1887, 2**-188161988, 0) Return: 0 1660 700  Call System API API Name: BCryptDecrypt Args: (95f7a60, 1889, a05f1d0), 0, 1887, 2**-188161988, 0) Return: 0 1660 700  Call System  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60,  INëi11Å, 1389, a05f1d0, , 0,  INëi11Å, 2572, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API   API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, 0, 1389, 408f1d0, 0, 12, 30469, 168161988, 0) Return: 0   1660   700   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, u^, 1389, a05f1d0, , 0, u^, 1405, 168161988, 0 ) Return: 0  | 1660 | 700  |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, 12, 1389, a05f1d0, , 0, 12, 30469, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 168°T)(0, 1389, a05f1d0, , 0, 168°T), 128°T, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 56°*, 1389, a05f1d0, , 0, 65°*, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 5f°*, 1389, a05f1d0, , 0, 2±8i5,loe*1](7¶Oyûq, 1389, a05f1d0, , 0, ½fl.yu_a=6;5-‰0*e£780U¶5åve+TEÅ*A¹¹²         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ½r)GM**½malbald, 1389, a05f1d0, , 0, ½r)GM**½malbald, 2, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ½r)GM**½malbald, 1389, a05f1d0, , 0, ½r)GM**½malbald, 26, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ½r)GM**½malbald, 1389, a05f1d0, , 0, ½r)GM**½malbald, 26, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 1770, 168161988, 0) Return: 0         1660         700 <td< td=""><td>Call System API</td><td><math display="block">API \ Name: \ BCryptDecrypt \ Args: (\ 95f7a60, \ \hat{a}\%\hat{A}/\tilde{j}\\$N\hat{u}O\hat{a}\pounds, \ 839, \ a05f1d0, \ , 0, \ \hat{a}\%\hat{A}/\tilde{j}\\$N\hat{u}O\hat{a}\pounds, \ 32755, \ 168161988, \ 0 \ ) \ Return: 0</math></td><td>1660</td><td>700</td></td<>  | Call System API     | $API \ Name: \ BCryptDecrypt \ Args: (\ 95f7a60, \ \hat{a}\%\hat{A}/\tilde{j}\$N\hat{u}O\hat{a}\pounds, \ 839, \ a05f1d0, \ , 0, \ \hat{a}\%\hat{A}/\tilde{j}\$N\hat{u}O\hat{a}\pounds, \ 32755, \ 168161988, \ 0 \ ) \ Return: 0$ | 1660 | 700  |
| Call System API         API Name: BCryptDecrypt Args: (9577a60, 1389, a05f1d0, 0, 29051, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, [@T])0, 1389, a05f1d0, 0, 6g**, 1389, a05f1d0, 0, 0 fg**, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, ½%*, 1389, a05f1d0, 0, 0 fg**, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, ½%*, 128*, 40*) [0*¶0/yúq, 1389, a05f1d0, 0, 2±i/s, 16x*] [0*¶0/yúq, 23379, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, ½%*, 10*M** = NaUEiá0*G, 1389, a05f1d0, 0, 2±i/s, 16x*] [0*¶0/yúq, 23379, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, ½%*, 10*M** = NaUEiá0*G, 1389, a05f1d0, 0, ½%*, 10*M** = NaUEiá0*G, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (9577a60, ½%*, 10*M**,   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, , 1389, a05f1d0, , 0, , 31887, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, (@T)lO, 1389, a05f1d0, , 0, 6g**, 1389, a05f1d0, , 0, 6g**, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 9g**, 1389, a05f1d0, , 0, 6g**, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 9fl yu_a-ē)5-‰0*6€7i6U¶5Āxe+T£Ā·Ā·1*ZpO_Q, 1389, a05f1d0, , 0, ₹fl yu_a-ē)5-‰0*6€7i6U¶5Āxe+T£Ā·Ā·1*         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ₹fl yo, yu, yu, yu, yu, yu, yu, yu, yu, yu, yu   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, tZ,, 1389, a05f1d0, , 0, tZ,, 30469, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, 65%, 1389, a05f1d0, , 0, 65%, 26215, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ¥fl.yu_a-e)5-‰0*e£7i6U¶5Á×e+T£ÁÁ¹1²pô_Q, 1389, a05f1d0, , 0, ¥fl.yu_a-e)5-‰0*e£7i6U¶5Á×e+T£ÁÁ¹1²         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, z±&ß.loe-½l[O*¶Óyúq, 1389, a05f1d0, , 0, z±&ß.loe-½l[O*¶Óyúq, 23379, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, z±&ß.loe-½l[O*¶Óyúq, 1389, a05f1d0, , 0, v)yGM¹±™aUÉtàú:G, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, v)yGM¹±™aUÉtàú:G, 1389, a05f1d0, , 0, v)yGM¹±™aUÉtàú:G, 21961, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 0, 19125, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 17707, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 0)pSOYNO, 1389, a05f1d0, , 0, 0)pSOYNO, 16289, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 178   | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, , 1389, a05f1d0, , 0, , 29051, 168161988, 0 ) Return: 0   | 1660 | 700  |
| API Name: BCryptDecrypt Args: (95f7a60, ¾fi,ÿu_à-e)5-‰Ö*eÉ?iðU¶5Á×e+T£ÁÁ¹1⁻ZpÒ_Q, 1389, a05f1d0, , 0, ¾fi,ÿu_à-e)5-‰Ö*eÉ?iðU¶5Á×e+T£ÁÁ¹1⁻ZpÒ_Q, 1389, a05f1d0, , 0, ¾fi,ÿu_à-e)5-‰Ö*eÉ?iðU¶5Á×e+T£ÁÁ¹1⁻ZpÒ_Q, 1389, a05f1d0, , 0, ½fi,ÿu_à-e)5-‰Ö*eÉ?iðU¶5Á×e+T£ÁÁ¹1⁻ZpÒ_Q, 1389, a05f1d0, , 0, ½fi,ÿu_à-e)5-‰Ö*iðu, 168161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ½fi,389, a05f1d0, , 0, ½fi,ÿu_à-e)5-‰Ö*iðu, 168161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ½fi,389, a05f1d0, , 0, ½fi,04,18, 14871, 168161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ½fi,389, a05f1d0, , 0, ¼fi,24,4871, 168161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ¼fi,389, a05f1d0, , 0, ¼fi,48,71,68161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ¼fi,389, a05f1d0, , 0, ¼fi,48,71,68161988, 0) Return: 0  Call System API API Name: BCryptDecrypt Args: (95f7a60, ¼fi,48,71,48,71,68161988, 0) Return: 0  API Name: BCryptDecrypt Args: (95f7a60, ¼fi,48,71,48, | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, f@'T)İO, 1389, a05f1d0, , 0, f@'T)İO, 27633, 168161988, 0 ) Return: 0   | 1660 | 700  |
| ŽpÔ_Q, 24797, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, z±š/š,lœ·\¹[Ô¶Ôyúq, 1389, a05f1d0, , 0, z±š/š,lœ·\²[ô¶Öyúq, 23379, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, ½0yGM'±™aUÉtáú:G, 1389, a05f1d0, , 0, ½0yGM'±™aUÉtáú:G, 21961, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, @7 »y¥-4#bBá4p, 1389, a05f1d0, , 0, @7 »y¥-4#bBá4p, 20543, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 0, 19125, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 0, 17707, 168161988, 0 ) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,  | Call System API     | API Name: BCryptDecrypt Args: ( 95f7a60, ō§**, 1389, a05f1d0, , 0, ō§**, 26215, 168161988, 0 ) Return: 0   | 1660 | 700  |
| Call System API       API Name: BCryptDecrypt Args: (95f7a60, ³u)gGM*±™aUÉtàû:G, 1389, a05f1d0, , 0, ³u)gGM*±™aUÉtàû:G, 21961, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, @7 »y¥-4#)Bâ4p, 1389, a05f1d0, , 0, @7 »y¥-4#)Bâ4p, 20543, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 0, 1389, a05f1d0, , 0, 17707, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 17707, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, öjp\$ÖYNÖ, 1389, a05f1d0, , 0, öjp\$ÖYNÖ, 16289, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, Žib, 1389, a05f1d0, , 0, ŽilÖQ*†Lß, 14871, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, N¥ş^*2«**®plz)©¯zj*, 1389, a05f1d0, , 0, N¥ş^*2«**®plz)©¯zj*, 13453, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, 12035, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 12035, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, IWÖ,4%mH., 1389, a05f1d0, , 0,   |                     | ŽpÒ_Q, 24797, 168161988, 0 ) Return: 0   |      |      |
| Call System API       API Name: BCryptIDecrypt Args: (95f7a60, @7 »y¥-4#:Bà4p, 1389, a05f1d0, , 0, @7 »y¥-4#:Bà4p, 20543, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, Ö, 1389, a05f1d0, , 0, 0, 19125, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, 1, 1389, a05f1d0, , 0, 17707, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, ŏ p\$OŶNŌ, 1389, a05f1d0, , 0, ŏ p\$OŶNŌ, 16289, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, ŽilōOʻ†Lß, 1389, a05f1d0, , 0, ŽilōOʻ†Lß, 14871, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, 'N¥§^*2e,**D Z)⊕ Z₁, ', 1389, a05f1d0, , 0, 'N¥§^*2e,**D Z)⊕ Z₁, ', 13453, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 12035, 168161980, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, IWÒ, 4%mH., 1389, a05f1d0, , 0, IWÒ, 4%mH., 10617, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60, IWÒ, 4%mH., 1389, a05f1d0, , 0, IWÒ, 4%mH., 10617, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptIDecrypt Args: (95f7a60,  |                     |  |      |      |
| Call System API       API Name: BCryptDecrypt Args: (95f7a60, Ö, 1389, a05f1d0, , 0, Ö, 19125, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, , 17707, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, ö p\$ÖYNÖ, 1389, a05f1d0, , 0, ö p\$ÖYNÖ, 16289, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, ŽliÖQ'†Lß, 1389, a05f1d0, , 0, ŽliÖQ'†Lß, 14871, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, N¥§^*2e,**D;Z)© Z₁*, 1389, a05f1d0, , 0, N¥§^*2e,**D;Z)© Z₁*, 13453, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, IWÖ, 4%mH., 1389, a05f1d0, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, IWÖ, 4%mH., 1389, a05f1d0, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0       1660       700         Call System API       API Name: BCryptDecrypt Args: (95f7a60, IWÖ, 4%mH., 1389, a05f1d0, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0       1660       700   |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, 0, 17707, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ö p\$ÔYNÔ, 1389, a05f1d0, 0, ö p\$ÔYNÔ, 16289, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, č p\$ÔYLB, 1389, a05f1d0, 0, v, Ž rOQ'tLB, 14871, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 'N¥§^*2ex**D;Z)© Zp*, 1389, a05f1d0, 0, 'N¥§^*2ex**D;Z)© Zp*, 13453, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, 0, 12035, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, IWÔ, 4/mH., 1389, a05f1d0, 0, IWÔ, 4/mH., 10617, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, JuÁ57)wSœ[ī, [@], 366, a05f1d0, 0, IVÔ, 4/mH., 10617, 168161988, 0) Return: 0         1660         700   |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, ölp\$ÓYNŐ, 1389, a05f1d0, , 0, ölp\$ÓYNŐ, 16289, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, ŽliÕQ'†Lß, 1389, a05f1d0, , 0, ŽliÕQ'†Lß, 14871, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 'N¥§^*2e**Pi,Z)© Zip*, 1389, a05f1d0, , 0, 'N¥§^*2e**Pi,Z)© Zip*, 13453, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 12035, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, IWÖ, 4%mH., 1389, a05f1d0, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, JuÅ57\wSce[ī, [@], 366, a05f1d0, , 0, IµÅ57\wSce[ī, [@], 9199, 168161988, 0) Return: 0         1660         700   |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, ŽlfÖQʻ†Lß, 1389, a05f1dQ, , 0, ŽlfÖQʻ†Lß, 14871, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, N¥§^^2q «°P)д'Q° Z₁¸², 1389, a05f1dQ, , 0, N¥§^^2q «°P)д'Q° Z₁¸², 13453, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1dQ, , 0, 12035, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, IWÖ, 4%mH., 1389, a05f1dQ, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, JuÅ57\wSce[ī, [w], 366, a05f1dQ, , 0, IWÖ, 4%mH., 10617, 168161988, 0) Return: 0         1660         700   |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, 'N¥§^^2α**ΦjZ)©¯Zj^*, 1389, a05f1d0, , 0, 'N¥§^^2α**ΦjZ)©¯Zj^*, 13453, 168161988, 0 ) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, , 0, 12035, 168161988, 0 ) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, IWÒ,4%mH., 1389, a05f1d0, , 0, IWÒ,4%mH., 10617, 168161988, 0 ) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, JuÅ57/wSœ[f,@{, 9169, 168161988, 0 ) Return: 0         1660         700  |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, 1389, a05f1d0, 0, 12035, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, IWÖ,4%mH., 1389, a05f1d0, 0, IWÖ,4%mH., 10617, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, JuÅ57/wSœ[j,@(, 366, a05f1d0, 0, 0, JuÅ57/wSœ[j,@(, 9199, 168161988, 0) Return: 0         1660         700  |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: ( 95f7a60, IWÔ,4%mH., 1389, a05f1d0, , 0, IWÔ,4%mH., 10617, 168161988, 0 ) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: ( 95f7a60, ]uÅ57/wSœ[[j,@], 366, a05f1d0, , 0, ]uÅ57/wSœ[[j,@], 9199, 168161988, 0 ) Return: 0         1660         700   |                     |  |      |      |
| Call System API API Name: BCryptDecrypt Args: ( 95f7a60, ]uÅ57\wSœ[î,i®{, 366, a05f1d0, , 0, ]uÅ57\wSœ[î,i®{, 9199, 168161988, 0 } ) Return: 0 1660 700   |                     |  |      |      |
|   |                     |  |      |      |
| Call System ADI ADI Namo: P.Camb Deput Ares: (057760-47-055440-0-0904-45945400-0-) Peturo: 0  |                     |  |      |      |
| Call System API         API Name: BCryptDecrypt Args: (95f7a60, , 17, a05f1d0, , 0, , 8804, 168161988, 0) Return: 0         1660         700           Call System API         API Name: BCryptDecrypt Args: (95f7a60, , 105, a05f1d0, , 0, , 8758, 168161988, 0) Return: 0         1660         700  |                     |  |      |      |
| Call System API API Name: BCryptDecrypt Args: (95f7a60, , 105, a05f1d0, , 0, , 8758, 168161988, 0 ) Return: 0 1660 700  | Oan System AFT      | ли ттенно. Болуниску ун лидь. ( выглави, тио, авытив, т, в, 6736, 100101300, 0 ) Netutit. 0  | 1000 | 700  |

| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, , 1389, a05f1d0, , 0, , 8624, 168161988, 0 ) Return: 0   | 1660 | 700          |
|---|---|------|--------------|
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, §àHNÚ8ý*sžÈ*yžð, 1389, a05f1d0, , 0, §àHNÚ8ý*sžÈ*yžð, 7206, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, «ŠÆÖÖXJ"3, 1389, a05f1d0, , 0, «ŠÆÖÖXJ"3, 5788, 168161988, 0 ) Return: 0   | 1660 | 700          |
| 0.110 / 4.701   | ARIN - PO - IR - IA - (ARIZ 00 10 4000 0774 IO 0 10 4070 40704000 0 IR I - 0  | 4000 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, jG, 1389, a05f1d0, , 0, jG, 4370, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, m, 1389, a05f1d0, , 0, m, 2952, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, "I"^Ä, 1389, a05f1d0, , 0, "I"Ä, 1534, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ‰všÓd, 1389, a05f1d0, , 0, ‰všÓd, 1405, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, Fwô, 1389, a05f1d0, , 0, Fwô, 32755, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, 2úâSÙÎÁ, 1389, a05f1d0, , 0, 2úâSÙÎÁ, 31337, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, Ê, 1389, a05f1d0, , 0, Ê, 29919, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, , 1389, a05f1d0, , 0, , 28501, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ë ×äQ#†Cå, 1389, a05f1d0, , 0, ë ×äQ#†Cå, 27083, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, à@,>ÈŠy~ó8ë, 1389, a05f1d0, , 0, à@,>ÈŠy~ó8ë, 25665, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, őfilSéĕî, 1389, a05f1d0, , 0, őfilSéĕî, 24247, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, k, 1389, a05f1d0, , 0, k, 22829, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, @7, 1389, a05f1d0, , 0, @7, 21411, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ÉþË=el, 1389, a05f1d0, , 0, ÉþË=el, 19993, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: (95f7a60, /Ú_c°Ér′‡;É11Û₁¶×೤qóUnd?e»ÉFĒ, 1389, a05f1d0, , 0, /Ú_c°Ér′‡;É11Û₁¶×೤qóUnd?e»ÉFĒ, 18575, 16816198   | 1660 | 700          |
| Call System Art   | 8, 0 ) Return: 0  | 1000 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, >k, 1389, a05f1d0, , 0, >k, 17157, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, '4, 1389, a05f1d0, , 0, '4, 15739, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 14321, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: (95/7a60, , 1389, a05/1d0, , 0, , 1492), 100/101900, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 9917a60, T. 1889, a05f1d0, , , 0, , 12903, 166161986, 0 ) Return: 0  API Name: BCryptDecrypt Args: ( 95f7a60, Æ, 1389, a05f1d0, , 0, Æ, 11485, 168161988, 0 ) Return: 0                                 | 1660 | 700          |
|   |   |      | 700          |
| Call System API   | API Name: BCryptDecrypt Args: (95/7a60, NcsôÃô3é—ÓP, 839, a05/1d0, , 0, NcsôÃô3é—ÓP, 10067, 168161988, 0) Return: 0   | 1660 |              |
| Call System API   | API Name: BCryptDecrypt Args: (95/7a60, , 1389, a05/1d0, , 0, , 9199, 168/161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ã02¥U¢¿I½QÉt·7+, 1389, a05f1d0, , 0, ã02¥U¢¿I½QÉt·7+, 7781, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, øT³, 1389, a05f1d0, , 0, øT³, 6363, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, A>, 1389, a05f1d0, , 0, A>, 4945, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ¥äÑô%"lyù^, 1389, a05f1d0, , 0, ¥äÑô%"lyù^, 3527, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, t^‰, 1389, a05f1d0, , 0, t^‰, 2109, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | $API \ Name: \ BCryptDecrypt \ Args: (\ 95f7a60, \ Call[G\ddot{y}\ \div) < 3 \\ \&wKîl^a \\ SVØ^*\dot{o}, \ 1389, \ a05f1d0, \ , \ 0, \ Call[G\ddot{y}\ \div) < 3 \\ \&wKîl^a \\ SVØ^*\dot{o}, \ 1405, \ 168161988, \ 0\ ) \ Return: 0$ | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, °F, 1389, a05f1d0, , 0, °F, 15357, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, Æ, 1389, a05f1d0, , 0, Æ, 13939, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, Ö–\r8÷u†däé£kÇ-¤<2¶iişó—/^ 'ū, 1389, a05f1d0, , 0, Ö–\r8÷u†däé£kÇ-¤<2¶iişó—/^ 'ū, 12521, 168161988, 0 ) Re turn: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, "ð=-ðHçQc.féÑZÑ*Ÿā"¥0ĒM4¦PW,"czæ,\rţ", 1389, a05f1d0, , 0, "ð=-ðHçQc.féÑZÑ*Ÿā"¥0ĒM4¦PW,"czæ,\rţ", 11103, 168161988, 0 ) Return: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, 1, 1389, a05f1d0, , 0, 1, 9685, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, tVV,@^, 1389, a05f1d0, , 0, tVV,@^, 8267, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, 3%ñ´eÒNXÍÖ:½ÛJ;¯œi*"], 1389, a05f1d0, , 0, 3%ñ´eÒNXÍÖ:½ÛJ;¯œi*"], 6849, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, Ï0*, 1389, a05f1d0, , 0, Ĭ0*, 5431, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, "j]4Þæ^<Šō, 1389, a05f1d0, , 0, "j]4Þæ^\Šō, 4013, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, ÷1ýÓØÇcÕG, 1389, a05f1d0, , 0, ÷1ýÓØÇcÕG, 2595, 168161988, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 95f7a60, 'PBQmR@SÜTrrU;UEUEVSW=X, 1161, a05f1d0, , 0, 'PBQmR@SÜTrrU;UEUEVSW=X, 1177, 168161988, 0 ) Ret urn: 0  | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 8a34390, , 40, a3af5a8, , 0, , 56, 171636380, 0 ) Return: 0   | 1660 | 700          |
| Call System API   | API Name: BCryptDecrypt Args: ( 8a34390, , 9, a3af4b0, , 0, , 25, 171636132, 0 ) Return: 0  | 1660 | 700          |
| Call Network API  | API Name: send Args: (7e0,, 1, 38) Return: 0  | 1660 | 700          |
| Call Network API  | API Name: send Args: (760,, 1, 46) Return: 0  | 1660 | 700          |
|   |   |      |              |
| Call Network API  | API Name: send Args: (65c,, 1, 38) Return: 0  Key: HKEY CURPENT LISERIS/SETMARE/Classes Local Settings Mui/Cophy/74/52/64R7EN appurage list Value: on LISTophy  | 1660 | 700          |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCachel7d\52C64B7E\LanguageList Value: en-US\0en\0   | 1660 | 700          |
| Call Service API  | API Name: OpenServiceW Args: (94bb838, WSearch, 1) Return: 94bb7c0  | 1660 | 700          |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running  | 1660 | 700          |
| Call System API   | API Name: evtchann.SendEvent Args: ( e), imagepath[%windir% System32\rundli32.exe ) Return: 1   | 1660 | 700          |
| Call System API   | API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[700 ) Return: 1   | 1660 | 700          |
| Call Internet Helper API  | API Name: InternetGetConnectedStateExW Args: ( a346fa38, 0, 0, 0 ) Return: 1  |      | 1660         |
| Write Registry Key  | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SQM\BadProcCount Value: 0   |      | 1660         |
| Call System API   | API Name: WinHttpCloseHandle Args: ( a5758fd0 ) Return: 1   |      | 1660         |
| Call Network API  | API Name: socket Args: ( 23, 1, 6 ) Return: 7d8   |      | 1660         |
| Call Network API  | API Name: socket Args: ( 2, 2, 0 ) Return: 83c  |      | 1660         |
| Call Network API  | API Name: socket Args: ( 23, 2, 0 ) Return: 83c   |      | 1660         |
| Call System API   | API Name: DnsQueryEx Args: ( sqm.telemetry.microsoft.com, 1, 40006000 ) Return: 87  |      | 1660         |
| Call System API   | API Name: DnsQueryEx Args: (sqm.telemetry.microsoft.com, 1c, 40026000 ) Return: 0   |      | 1660         |
| Call Network API  | API Name: socket Args: (23, 2, 0) Return: 7d4   |      | 1660         |
| Call Network API  | API Name: socket Args: (2, 1, 6) Return: 7d4  |      | 1660         |
| Call Network API  | API Name: socket Args: ( 2, 1, 6 ) Return: 704  API Name: bind Args: ( 7d4, 0.0.0:49432, 128 ) Return: 0  |      | 1660         |
| Detection   | Threat Characteristic: Listens on port  0.0.0.049432  |      |              |
| Oall Contact AD'  |   |      | 4000         |
| Call System API   | API Name: ConnectEx Args: (7d4, 65.55.252.93:443, 16, 0, 0, 0, a57254c8 ) Return: 0   |      | 1660         |
|   | API Name: InternetOpenW Args: ( Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko, 0, , , , 10000000 ) Return: cc0004  |      | 1660         |
| Call Internet Helper API  |   |      |              |
| Call System API  Call Internet Helper API  Call Internet Helper API | API Name: DnsQueryEx Args: (ieonline.microsoft.com, 1, 50020000) Return: 0  API Name: InternetConnectW Args: (cc0004, ieonline.microsoft.com, 443, , , 3, 8388608, -1519158432) Return: cc0008  |      | 1660<br>1660 |

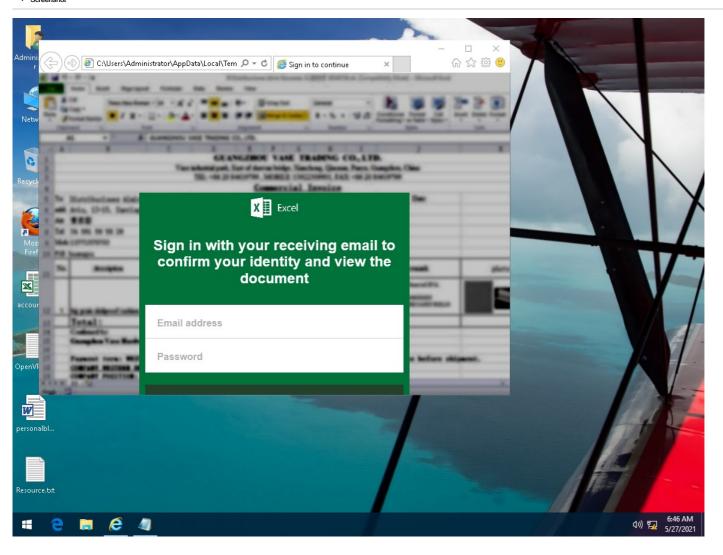
| Call Internet Helper API  Call Network API   |  |              |
|--|--|--------------|
| Call Network API   | API Name: HttpOpenRequestW Args: ( cc0008, GET, /ieflipahead/ie10/rules.xml?mkt=en-US, , , -1558919568, 12582928, -1519158432 ) Return: cc000c   | 1660         |
|  | API Name: socket Args: ( 2, 2, 0 ) Return: 8c4   | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8c4  | 1660         |
| Call System API  | API Name: DnsQueryEx Args: ( ieonline.microsoft.com, 1c, 40026000 ) Return: 0  | 1660         |
| Call System API  | API Name: DnsQueryEx Args: ( ieonline.microsoft.com, 1, 40006000 ) Return: 87  | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 8d8  | 1660         |
| Call Network API   | API Name: socket Args: ( 2, 1, 6 ) Return: 8c4   | 1660         |
| Call Network API   | API Name: bind Args; ( 8c4, 0.0.0.49433, 16 ) Return: 0  | 1660         |
| Detection  | Threat Characteristic: Listens on port   | 1000         |
| Detection  | 0.0.0.94433  |              |
| Call System API  | API Name: ConnectEx Args: ( 8c4, 204.79.197.200:443, 16, 0, 0, 0, a57a3eb8 ) Return: 0   | 1660         |
| Call Network API   | API Name: socket Args: ( 2, 1, 6 ) Return: 8d8   | 1660         |
| Call Network API   | API Name: bind Args: ( 8d8, 0.0.0.49434, 16 ) Return: 0  | 1660         |
|  |  | 1000         |
| Detection  | Threat Characteristic: Listens on port 0.0.0.0:49434   |              |
| Call System API  | API Name: ConnectEx Args: ( 8d8, 204.79.197.200:443, 16, 0, 0, 0, a57a3c88 ) Return: 0   | 1660         |
| Call System API  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0   | 1660         |
|  |  |              |
| Call Network API   | API Name: send Args: (8c4,, 1, 217 ) Return: 0   | 1660         |
| Call Network API   | API Name: send Args: ( 8d8,, 1, 217 ) Return: 0  | 1660         |
| Call Internet Helper API   | API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1519566688 ) Return: cc0010   | 1660         |
| Call Internet Helper API   | API Name: HttpOpenRequestW Args: ( cc0010, GET, //E11/1426178821/iecompatviewlist.xml, , , -1554595984, 12582928, -1519566688 ) Return: cc0014   | 1660         |
| Write Registry Key   | Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\rd\152C64B7E\LanguageList Value: en-US\0en\0   | 1660         |
| Call Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: b60   | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: b60  | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 1, 6 ) Return: b88  | 1660         |
| Call System API  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1c, 40026000 ) Return: 0  | 1660         |
| Call System API  | API Name: DnsQueryEx Args: (iecviist.microsoft.com, 1, 4006000) Return: 87   | 1660         |
|  |  |              |
| Call Network API   | API Name: socket Args: (23, 2, 0) Return: bf0  | 1660         |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: bf4   | 1660         |
| Call Network API   | API Name: bind Args: ( bf4, 0.0.0.0:49435, 16 ) Return: 0  | 1660         |
| Detection  | Threat Characteristic: Listens on port 0.0.0.0:49435   |              |
| Call System API  | API Name: ConnectEx Args: ( bf4, 152.199.19.161:443, 16, 0, 0, 0, a581fcf8 ) Return: 0   | 1660         |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: c14   | 1660         |
| Call Network API   | API Name: bind Args: ( c14, 0.0.0.0:49436, 16 ) Return: 0  | 1660         |
| Detection  | Threat Characteristic: Listens on port   |              |
|  | 0.0.0.0:49436  |              |
| Call System API  | API Name: ConnectEx Args: ( c14, 152.199.19.161:443, 16, 0, 0, 0, a581f438 ) Return: 0   | 1660         |
| Call Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: c18   | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: c18  | 1660         |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a5847a40 ) Return: 1  | 1660         |
| Call Network API   | API Name: send Args: ( c14,, 1, 217 ) Return: 0  | 1660         |
| Call System API  | API Name: DnsQueryEx Args: ( ocsp.digicert.com, 1, 40006000 ) Return: 87   | 1660         |
| Call Network API   |  | 1660         |
|  | API Name: send Args: ( bf4,, 1, 217 ) Return: 0  |              |
| Call System API  | API Name: DnsQueryEx Args: ( ocsp.digicert.com, 1c, 40026000 ) Return: 0   | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: be0  | 1660         |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: be0   | 1660         |
| Call Network API   | API Name: bind Args: ( be0, 0.0.0.0:49437, 128 ) Return: 0   | 1660         |
| Detection  | Threat Characteristic: Listens on port   |              |
|  | 0.0.0.49437  |              |
| Call System API  | API Name: ConnectEx Args: ( be0, 93.184.220.29:80, 16, 0, 0, 0, a5725e68 ) Return: 0   | 1660         |
| Call Network API   | $API \ Name: send \ Args: (\ be0,\ GET/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom\%2FnYB45SPUEwQU5Z1ZMIJHWMys\%2BghUNoZ7000000000000000000000000000000000000$   | 1660         |
|  | OrUETfACEA8Ull8gIGmZT9XHrHiJQel%3D HTTP/1.1\n\nConnection: Keep-Alive\n\nAccept: */"\n\nUser-Agent: Microsoft-CryptoAPI/10.0\n\nHost: ocsp.digicert .com\n\n\n\n, 1, 236 ) Return: 0   |              |
| Call System ADI  |  | 1660         |
| Call System API  | API Name: WinHttpCloseHandle Args: (a583/300 ) Return: 1   | 1660         |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a57d30f0 ) Return: 1  | 1660         |
| Call Network API   | API Name: socket Args: ( 23, 1, 6 ) Return: c18  | 1660         |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a5834380 ) Return: 1  | 1660         |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a58325c0 ) Return: 1  | 1660         |
| Call Network API   | API Name: send Args: ( 8c4,, 1, 158 ) Return: 0  | 1660         |
| Call Network API   | API Name: send Args: ( 8d8,, 1, 158 ) Return: 0  | 1660         |
| Call Network API   | API Name: send Args: ( 8d8,, 1, 87 ) Return: 0   | 1660         |
| Call System API  | API Name: BCryptDecrypt Args: ( a57d3e60, , 40, a6ade8a0, , 0, , 56, -1498551868, 0 ) Return: 0  | 1660         |
| Call Network API   | API Name: send Args: ( 8c4,, 1, 87 ) Return: 0   | 1660         |
| Call System API  | API Name: BCryptDecrypt Args: ( a57d3e60, , 9, a6ade8a0, , 0, , 25, -1498551868, 0 ) Return: 0   | 1660         |
|  | API Name: BCryptDecrypt Args. ( a57dd0e0, , 40, a6ade6f0, , 0, , 56, -1498552300, 0 ) Return: 0  | 1660         |
| Call System API  |  |              |
| Call System API  | API Name: send Args: ( 8c4,, 1, 38 ) Return: 0   | 1660         |
| Call Network API   |  | 1660         |
| Call Network API Call Network API  | API Name: send Args: ( 8d8,, 1, 291 ) Return: 0  |              |
| Call Network API   | API Name: send Args: ( 8d8,, 1, 291 ) Return: 0  API Name: send Args: ( 8d8,, 1, 38 ) Return: 0  | 1660         |
| Call Network API Call Network API  |  | 1660<br>1660 |
| Call Network API Call Network API Call Network API                                 | API Name: send Args: ( 8d8,, 1, 38 ) Return: 0   |              |
| Call Network API Call Network API Call Network API Call System API                 | API Name: send Args: (8d8,, 1, 38) Return: 0  API Name: BCryptDecrypt Args: (a57cd0e0, , 9, a346ef00, , 0, , 25, -1555632092, 0) Return: 0  API Name: WinHttpCloseHandle Args: (a57c8610) Return: 1  API Name: send Args: (be0, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7l90  VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\nConnection: Keep-Alive\nAccept: */"\nDuser-Agent: Microsoft-CryptoAPl/10.0\nInhost: ocsp.digicert. | 1660         |
| Call Network API Call Network API Call Network API Call System API Call System API | API Name: send Args: (8d8,, 1, 38) Return: 0  API Name: BCryptDecrypt Args: (a57dd0e0, , 9, a346ef00, , 0, , 25, -1555632092, 0) Return: 0  API Name: WinHttpCloseHandle Args: (a57c8610) Return: 1  API Name: send Args: (be0, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7l90   | 1660<br>1660 |

| Call System API                  | API Name: WinHttpCloseHandle Args: ( a57d1e30 ) Return: 1   | 1660         |
|----------------------------------|---|--------------|
| Call System API                  | API Name: WinHttpCloseHandle Args: ( a57d1e30 ) Return: 1  API Name: WinHttpCloseHandle Args: ( a58d45a0 ) Return: 1  | 1660         |
| Call Network API                 | API Name: send Args: ( c14,, 1, 126 ) Return: 0   | 1660         |
| Call Network API                 | API Name: send Args: ( bf4,, 1, 126 ) Return: 0   | 1660         |
| Call System API                  | API Name: WinHttpCloseHandle Args: ( a58349e0 ) Return: 1   | 1660         |
| Call Network API                 | API Name: send Args: ( c14,, 1, 87 ) Return: 0  | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5876c90, , 39, a6bde950, , 0, , 97, -1497503116, 0 ) Return: 0   | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5876c90, , 13, a6bde950, , 0, , 29, -1497503116, 0 ) Return: 0   | 1660         |
| Call Network API                 | API Name: send Args: (bf4,, 1, 87 ) Return: 0   | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5878bc0, , 39, a6bdeb00, , 0, , 97, -1497502684, 0 ) Return: 0   | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5878bc0, , 13, a6bdeb00, , 0, , 29, -1497502684, 0 ) Return: 0   | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5876c90, , 9, a6bdeb00, , 0 , 25, -1497502684, 0 ) Return: 0   | 1660         |
| Call Network API                 | API Name: send Args: (c14,, 1, 305 ) Return: 0  | 1660         |
| Call Network API                 | API Name: send Args: ( br4,, 1, 38 ) Return: 0  | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5878bc0, , 9, a6bdeb00, , 0, , 25, -1497502684, 0 ) Return: 0  | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a5876c90, , 231, a6bdeb00, , 0, , 247, -1497502684, 0 ) Return: 0   | 1660         |
| Call Network API                 | API Name: send Args: ( c14,, 1, 38 ) Return: 0  | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a57d3e60, , 697, a67de900, , 0, , 713, -1501697500, 0 ) Return: 0   | 1660         |
| Add File                         | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_EMPTY   | 1660         |
| Write File                       | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   | 1660         |
| Call System API                  | API Name: DnsQueryEx Args: ( go.microsoft.com, 1, 50020000 ) Return: 0  | 1660         |
| Call Internet Helper API         | API Name: InternetConnectW Args: ( cc0004, go.microsoft.com, 80, , , 3, 0, -1519566688 ) Return: cc0008   | 1660         |
| Call Internet Helper API         | API Name: HttpOpenRequestW Args: ( cc0004, gs.microsoft.com, 60, , , 5, 0, 151556668, 4194320, -1519566688 ) Return: cc000c   | 1660         |
| Call Network API                 | API Name: socket Args: (2, 2, 0) Return: 778  | 1660         |
| Call Network API                 | API Name: socket Args: (23, 2, 0) Return: 778   | 1660         |
| Call System API                  | API Name: DnsQueryEx Args: ( go.microsoft.com, 1, 40006000 ) Return: 87   | 1660         |
| Call System API                  | API Name: DisQueryEx Args. (go.microsoft.com, 1c, 40006000) Return: 0   | 1660         |
| Call Network API                 | API Name: socket Args: (23, 2, 0) Return: 310   | 1660         |
| Call Network API                 | API Name: socket Args: (2, 1, 6) Return: 778  | 1660         |
| Call Network API                 | API Name: bind Args: (778, 0.0.0.0:49438, 16 ) Return: 0  | 1660         |
| Detection                        | Threat Characteristic: Listens on port  | 1000         |
| Decement                         | 0.0.0.49438   |              |
| Call System API                  | API Name: ConnectEx Args: ( 778, 184.86.224.103:80, 16, 0, 0, 0, a57a3c88 ) Return: 0   | 1660         |
| Call Network API                 | API Name: socket Args: ( 2, 1, 6 ) Return: 310  | 1660         |
| Call Network API                 | API Name: bind Args: ( 310, 0.0.0.0:49439, 16 ) Return: 0   | 1660         |
| Detection                        | Threat Characteristic: Listens on port  |              |
|                                  | 0.0.0.0:49439   |              |
| Call System API                  | API Name: ConnectEx Args: ( 310, 184.86.224.103:80, 16, 0, 0, 0, a57a3dd8 ) Return: 0   | 1660         |
| Call Network API                 | API Name: send Args: (778, GET //wiink/)2LinklD=401135 HTTP/1.1\r\nAccept: "/"\r\nUA-CPU: AMD64\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozill a/5.0 [Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0] like Geckot\r\nHost: go.microsoft.com\r\nConnection: Keep-Alive\r\nCookie: SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=3A2A988979454AA08EBDB710B96ADCC2&dmnchg=1; SRCHUSR=D0B=20191114; _ga=GA1.2.1718225526.1573749281; _EDGE _S=F=14SID=2229018C53806F7F237511C852A86E0B&mkt=en-us; _EDGE_V=1; SRCHUPGUSR=SRCHLANGV2=en; _SS=SID=2229018C53806F7F2375 _11C852A86E0B\r\n, 1, 514 ) Return: 0 | 1660         |
| Call Network API                 | API Name: recv Args: ( 310, , 1, 2 ) Return: ?  | 1660         |
| Call Network API                 | API Name: recv Args: ( 778, , 1, 2 ) Return: ?  | 1660         |
| Call Network API                 | API Name: send Args: ( 8d8,S, 1, 344 ) Return: 0  | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a57d3e60, , 1765, a356e8e0, , 0, , 1781, -1554585084, 0 ) Return: 0   | 1660         |
| Call System API                  | API Name: BCryptDecrypt Args: ( a57d3e60, , 9, a356e630, , 0, , 25, -1554585772, 0 ) Return: 0  | 1660         |
| Delete Registry Key              | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\11CE4E0A4FD3CD25F064BE57BB2A9DE723823 1CC\ Value: None   | 1660         |
| Delete Registry Key              | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE998873 9F Value: None  | 1660         |
| Add Registry Key                 | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE998873 9F\ Value: None   | 1660         |
| Write Registry Key               | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournalt\Certificates\4EEF7FAF0062D34ABEE6137E774438AE998873<br>9F\Blob Value: None   | 1660         |
| Write Registry Key               | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\HistoryJournalCertificate\NextUpdateDate Value: 139b10a9  | 1660         |
| Call System API                  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  | 1660         |
| Call Internet Helper API         | API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1519566688 ) Return: cc0008  | 1660         |
| Call Internet Helper API         | API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1558919760, 12582928, -1519566688 ) Return: cc000c  | 1660         |
| Add File                         | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   | 1660         |
| Write File                       | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML   | 1660         |
| Call Internet Helper API         | API Name: InternetOpenW Args: ( , 0, , , 0 ) Return: cc0008   | 1660         |
| Call System API                  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  | 1660         |
| Call Internet Helper API         | API Name: InternetConnectW Args: ( cc0008, iecvlist.microsoft.com, 443, , , 3, 0, 0 ) Return: cc000c  | 1660         |
| Call Internet Helper API         | API Name: HttpOpenRequestW Args: ( cc000c, GET, /ie11blocklist/1401746408/versionlist.xml, , , -1554583064, 79692288, 0 ) Return: cc0010  | 1660         |
| Call Network API                 | API Name: socket Args: ( 2, 1, 6 ) Return: 2d4  | 1660         |
| Call Network API                 | API Name: bind Args: ( 2d4, 0.0.0.0:49440, 16 ) Return: 0   | 1660         |
| Detection                        | Threat Characteristic: Listens on port 0.0.0.0'49440  |              |
|                                  | API Name: ConnectEx Args: ( 2d4, 152.199.19.161:443, 16, 0, 0, 0, a581f4a8 ) Return: 0  | 1660         |
| Call System API                  |   |              |
| Call System API Call Network API | API Name: send Args: ( 2d4,b., 1, 359 ) Return: 0   | 1660         |
|                                  | API Name: send Args: ( 2d4,b., 1, 359 ) Return: 0  API Name: send Args: ( 2d4,, 1, 126 ) Return: 0  | 1660<br>1660 |

| College AS   | API Name: BCryptDecrypt Args: ( a57377e0, HTTP/1.1 304 Not Modifiedi\nAccept-Ranges: bytes\nAge: 675\nCache-Control: max-age=3600\nDate: Thu , 27 May 2021 11:56:29 GMT\nEtag: 0x8D8BD7E4D55BBE4\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\nServer: ECAcc (ska/F6AB)\n\nX-Cache: HIT\n\nx-ms-blob-type: BlockBlob\n\nx-ms-lease-status: unlocked\n\nx-ms-request-id: bf9c4e70-801e-00de-03ed-52bdab000000\n\nx-ms-version: 2009-09-19\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n  |              | 1660   |
|--|--|--------------|--|
| Call Network API   | API Name: recv Args: ( 2d4, , 1, 2 ) Return: ?   |              | 1660   |
| Write Registry Key   | Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e40adb5b   |              | 1660   |
| Write Registry Key   | Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed   |              | 1660   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a1413fc0 ) Return: 1  |              | 1660   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a5756850 ) Return: 1  |              | 1660   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a141f0c0 ) Return: 1  |              | 1660   |
| Call System API  | API Name: WinHttpCloseHandle Args: ( a58254f0 ) Return: 1  |              | 1660   |
| •  |  |              |  |
| Call Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: 7b0   |              | 1660   |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 7b0  |              | 1660   |
| Call System API  | API Name: DnsQueryEx Args: ( sqm.telemetry.microsoft.com, 1, 40006000 ) Return: 87   |              | 1660   |
| Call System API  | API Name: DnsQueryEx Args: ( sqm.telemetry.microsoft.com, 1c, 40026000 ) Return: 0   |              | 1660   |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: 7b0  |              | 1660   |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: 7b0   |              | 1660   |
| Call Network API   | API Name: bind Args: ( 7b0, 0.0.0.49441, 128 ) Return: 0   |              | 1660   |
|  |  |              | 1000   |
| Detection  | Threat Characteristic: Listens on port 0.0.0:49441   |              |  |
| Call System API  |  |              | 1660   |
| Call System API  | API Name: ConnectEx Args: (7b0, 65.55.252.93:443, 16, 0, 0, 0, a56d0a88 ) Return: 0  | 4000         |  |
| Call Internet Helper API   | API Name: InternetOpenW Args: (, 0, , , 0) Return: cc0008  | 1660         | 700  |
| Call System API  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0   | 1660         | 700  |
| Call Internet Helper API   | API Name: InternetConnectW Args: ( cc0008, iecvlist.microsoft.com, 443, , , 3, 0, 0 ) Return: cc000c   | 1660         | 700  |
| Call Internet Helper API   | API Name: HttpOpenRequestW Args: ( cc000c, GET, /ie11blocklist/1401746408/versionlist.xml, , , 171636996, 79692288, 0 ) Return: cc0010   | 1660         | 700  |
| Call Network API   | API Name: socket Args: ( 2, 2, 0 ) Return: c28   | 1660         | 700  |
| Call Network API   | API Name: socket Args: (23, 2, 0) Return: c28  | 1660         | 700  |
|  |  |              |  |
| Call System API  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 40006000 ) Return: 87  | 1660         | 700  |
| Call System API  | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1c, 40026000 ) Return: 0  | 1660         | 700  |
| Call Network API   | API Name: socket Args: ( 23, 2, 0 ) Return: c40  | 1660         | 700  |
| Call Network API   | API Name: socket Args: (2, 1, 6) Return: c40   | 1660         | 700  |
| Call Network API   | API Name: bind Args: ( c40, 0.0.0.0:49442, 16 ) Return: 0  | 1660         | 700  |
| Detection  | Threat Characteristic: Listens on port   |              |  |
|  | 0.0.0.049442   |              |  |
| Call System API  | API Name: ConnectEx Args: ( c40, 152.199.19.161:443, 16, 0, 0, 0, 8a3231c ) Return: 0  | 1660         | 700  |
| Call Network API   | API Name: send Args: ( c40,, 1, 199 ) Return: 0  | 1660         | 700  |
| Call Network API   | API Name: send Args: ( c40,, 1, 126 ) Return: 0  | 1660         | 700  |
| Call Network API   | API Name: send Args: ( c40,!, 1, 550 ) Return: 0   | 1660         | 700  |
| Call System API  | API Name: BCryptDecrypt Args: ( 8a86d00, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu  | 1660         | 700  |
|  | , 27 May 2021 11:56:33 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache:  |              |  |
|  | HITVinx-ms-blob-type: BlockBlobivinx-ms-lease-status: unlocked/vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/vinx-ms-version: 2009-09-19/ vinvinx, 376, a6ff248, v, 0, HTTP/1.1 304 Not Modified/vinAccept-Ranges: bytes/vinAge: 3184/vinCache-Control: max-age=3600/vinDate: Thu, 27 May 2021 11:5 6:33 GMTvinEtag: 0x8D8BD7E4D558BE4/vinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTvinServer: ECAcc (ska/F771)/vinX-Cache: HITvinx-ms-blob-typ e: BlockBlobivinx-ms-lease-status: unlocked/vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/vinx-ms-version: 2009-09-19/vin/vin, 392, 1751089 24, 0 ) Return: 0  |              |  |
| Call Network API   | rinkrin, 376, a6if(248, , 0, HTTP/1.1 304 Not ModifiedkrinAccept-Ranges: byteskrinAge: 3184krinCache-Control: max-age=3600krinDate: Thu, 27 May 2021 11:5 6:33 GMTkrinEtag: 0x8D8BD7E4D55BBE4krinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTkrinServer: ECAcc (ska/F771)krinX-Cache: HITkrinx-ms-blob-typ e: BlockBlobkrinx-ms-lease-status: unlockedkrinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000krinx-ms-version: 2009-09-19krinkrin, 392, 1751089  | 1660         | 700  |
| Call Network API Write Registry Key  | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nx-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\r\n, 392, 1751089 24, 0 ) Return: 0   | 1660<br>1660 | 700<br>700   |
| Write Registry Key   | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\nternet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  |              |  |
| Write Registry Key Write Registry Key  | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\VersionManager\LastCheckForUpdate\LowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\VersionManager\LastCheckForUpdate\HighDateTime Value: 1d752ed   | 1660         | 700<br>700   |
| Write Registry Key Write Registry Key Call System API  | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\sOFTWARE\mathbb{Microsoft\l\nternet} Explorer\versionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\sOFTWARE\mathbb{Microsoft\l\nternet} Explorer\versionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\(\text{ist.microsoft.com}\), 1, 50020000 ) Return: 0   | 1660         | 700<br>700<br>1660                                 |
| Write Registry Key Write Registry Key Call System API Call Internet Helper API   | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-yp e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\sOFTWARE\microsoft\l\ntermet Explorer\version\manager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\sOFTWARE\microsoft\l\ntermet Explorer\version\manager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\iist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\iist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  | 1660         | 700<br>700<br>1660<br>1660                         |
| Write Registry Key Write Registry Key Call System API  | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\sOFTWARE\mathbb{Microsoft\l\nternet} Explorer\versionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\sOFTWARE\mathbb{Microsoft\l\nternet} Explorer\versionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\(\text{ist.microsoft.com}\), 1, 50020000 ) Return: 0   | 1660         | 700<br>700<br>1660                                 |
| Write Registry Key Write Registry Key Call System API Call Internet Helper API   | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nX-ms-blob-yp e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n\n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\sOFTWARE\microsoft\l\ntermet Explorer\version\manager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\sOFTWARE\microsoft\l\ntermet Explorer\version\manager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\iist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\iist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  | 1660         | 700<br>700<br>1660<br>1660                         |
| Write Registry Key Write Registry Key Call System API Call Internet Helper API Call Internet Helper API  | r/nivn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/vinAccept-Ranges: bytesivinAge: 3184\vinCache-Control: max-age=3600\vinDate: Thu, 27 May 2021 11:5 6:33 GMTVinEtag: 0x8D8BDTE4D55BBE4\vinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTVinServer: ECAcc (ska/F771)\vinX-Cache: HITVinX-ms-blob-typ e: BlockBloblvinx-ms-lease-status: unlocked\vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\vinx-ms-version: 2009-09-19\vin\vin, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\lnternet Explorer\versionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\lnternet Explorer\versionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\vist.microsoft.com, 1, 50020000 ) Return: 0  API Name: Internet\ConnectW Args: ( cc0004, iecv\vist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompatview\vist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c   | 1660         | 700<br>700<br>1660<br>1660                         |
| Write Registry Key Write Registry Key Call System API Call Internet Helper API Add File  | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nx-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER:SOFTWARE\microsoft\nternet Explorer\version\manager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER:SOFTWARE\microsoft\nternet Explorer\version\manager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\ist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\ist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompat/viewlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  | 1660         | 700<br>700<br>1660<br>1660<br>1660                 |
| Write Registry Key Write Registry Key Call System API Call Internet Helper API Call Internet Helper API Add File Write File Write Registry Key   | r\n\r\n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3184\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:5 6:33 GMT\r\nEtag: 0x8D8BDTE4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nx-ms-blob-typ e: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\r\nx-ms-version: 2009-09-19\r\n\r\n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\sOFTWARE\Microsoft\l\nternet Explorer\versionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\sOFTWARE\Microsoft\l\nternet Explorer\versionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\versionSt.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\versionSt.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompat/versionst.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: \( \text{LOCALAPPDATA}\text{Microsoft\l\nternet Explorer\versionpatdata\text{Lecompatdata.xml Type: VSDT_TEXT_HTML} \)  Key: HKEY_CURRENT_USER\sOFTWARE\Microsoft\l\nternet Explorer\lEcompatData\versionpatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\sOFTWARE\Microsoft\l\nternet Explorer\lEcompatData\versionpatdata.xml Type: VSDT_TEXT_HTML   | 1660         | 700<br>700<br>1660<br>1660<br>1660<br>1660<br>1660 |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  | r/n/n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified in Accept-Ranges: bytesivinAge: 3184/rinCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11:5 6:33 GMT/rinEtag: 0x8D8BD7E4D55BBE4/rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT/rinServer: ECAcc (ska/F771)/rinX-Cache: HITr/rinX-ms-blob-typ e: BlockBlobl/rinx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rinx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0000  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Delete Registry Key   | r/ni/n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified in Accept-Ranges: bytesivinAge: 3184/rinCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11:5 6:33 GMT/rinEtag: 0x8D8BD7E4D55BBE4/rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT/rinServer: ECAcc (ska/F771)/rinX-Cache: HITr/rinX-ms-blob-typ e: BlockBlobl/rinx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rinx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompat/viewlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  | r/n/n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified in Accept-Ranges: bytesivinAge: 3184/rinCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11:5 6:33 GMT/rinEtag: 0x8D8BD7E4D55BBE4/rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT/rinServer: ECAcc (ska/F771)/rinX-Cache: HITr/rinX-ms-blob-typ e: BlockBlobl/rinx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rinx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0000  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Delete Registry Key   | r/ni/n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified in Accept-Ranges: bytesivinAge: 3184/rinCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11:5 6:33 GMT/rinEtag: 0x8D8BD7E4D55BBE4/rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT/rinServer: ECAcc (ska/F771)/rinX-Cache: HITr/rinX-ms-blob-typ e: BlockBlobl/rinx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rinx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompat/viewlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\vecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  | r/ni/n, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/n/nAccept-Ranges: bytes/n/nAge: 3184/n/Cache-Control: max-age=3600/n/nDate: Thu, 27 May 2021 11:5 6:33 GMTh/nEtag: 0x8D8BD7E4D55BBE4/n/nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTh/nServer: ECAcc (ska/F771)/n/nX-Cache: HITn/nx-ms-blob-typ e: BlockBlobl/nx-ms-lease-status: unlocked/nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/nx-ms-version: 2009-09-19/n/n/n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8386608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E11/1426178821/iecompat/veivlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\ntermet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\ntermet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\ntermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None   | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  | r/ni/nn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/nnAccept-Ranges: bytes/nnAge: 3184/nnCache-Control: max-age=3600/nnDate: Thu, 27 May 2021 11:5 6:33 GMTh/inEtag: 0x8D8BD7E4D55BBE4/nnLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTh/inServer: ECAcc (ska/F771)/rinX-Cache: HITn/inx-ms-blob-typ e: BlockBlobl/nnx-ms-lease-status: unlocked/nnx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/nnx-ms-version: 2009-09-19/nn/nn, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E11/1426178821/iecompat/viewlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompat/data.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompat/data.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\MFV Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  | 1660         | 700 700 1660 1660 1660 1660 1660 1660 16           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API   | r/ni/nn, 376, a6ff248, . 0, HTTP/1.1 304 Not Modified/nnAccept-Ranges: bytes/nnAge: 3184/nnCache-Control: max-age=3600/nnDate: Thu, 27 May 2021 11:5 6:33 GMTh/inEtag: 0x8D88D7E4D558BE4/nnLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTh/inServer: ECAcc (ska/F771)hr/inX-Cache: HITn/inx-ms-blob-typ e: BlockBlobl/nnx-ms-lease-status: unlocked/nnx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/nnx-ms-version: 2009-09-19lv/nn/n, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, , 1, 2 ) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, /iE11/1426178821/iecompat/viewlist.xml, , , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None   | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API   | r/n/rn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/rnAccept-Ranges: bytes/rnAge: 3184/rnCache-Control: max-age=3600/rnDate: Thu, 27 May 2021 11:5 6:33 GMTVrinEtag: 0x8D88D7E4D558BE4/rnLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTVrinServer: ECAcc (ska/F771)/rinX-Cache: HITVrinx-ms-blob-typ e: BlockBlobl/rnx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rnx-ms-version: 2009-09-19/rnin/n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: e10b8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: e10b8d4  API Name: InternetConnectW Args: ( iecv\ist.microsoft\com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( c00004, iecv\ist.microsoft\com, 443, , , 3, 8388608, -1518497984 ) Return: c00008  API Name: HttpOpenRequestW Args: ( c00008, GET, /iE11/1426178821/iecompat/view\ist.xml, , , -1554595984, 12582928, -1518497984 ) Return: c0000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\verompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\verompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  API Name: InternetConnectW Args: ( iccv\iist.microsoft\Lom,  | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Call Internet Helper API   | r/nivn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modifiedt/vhAccept-Ranges: bytesivinAge: 3184\vinCache-Control: max-age=3600\vinDate: Thu, 27 May 2021 11:5 6:33 GMT\vinEtag: 0x8D8BDTE4D558BE4\vinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\vinServer: ECAcc (ska/F771)\vinX-Cache: HITv\vinx-ms-blob-type e: BlockBlobivinx-ms-lease-status: unlocked\vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\vinx-ms-version: 2009-09-19\vin\vin, 392, 1751089 24, 0.) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\vist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\vist.microsoft.com, 443, , , 3, 838608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecv\vist.microsoft.compat/Data\viscompatdiedta.xml Type: VSDT_TEXT_HTML  Path: \( \) LOCALAPPDATA\( \) Microsoft\lintermet Explorer\Viscompatdiedta.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Intermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  API Name: InternetConnectW Args: ( iecv\vist.microsoft\Loom, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( iecv\vist.microsoft\Loom, 443, , , 3, 8388608, -1518497984 ) R | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Add File   | r/n/rn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/rnAccept-Ranges: bytes/rnAge: 3184/rnCache-Control: max-age=3600/rnDate: Thu, 27 May 2021 11:5 6:33 GMTVrinEtag: 0x8D88D7E4D558BE4/rnLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTVrinServer: ECAcc (ska/F771)/rinX-Cache: HITVrinx-ms-blob-typ e: BlockBlobl/rnx-ms-lease-status: unlocked/rinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rnx-ms-version: 2009-09-19/rnin/n, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: e10b8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: e10b8d4  API Name: InternetConnectW Args: ( iecv\ist.microsoft\com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( c00004, iecv\ist.microsoft\com, 443, , , 3, 8388608, -1518497984 ) Return: c00008  API Name: HttpOpenRequestW Args: ( c00008, GET, /iE11/1426178821/iecompat/view\ist.xml, , , -1554595984, 12582928, -1518497984 ) Return: c0000c  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\verompatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\verompatdata.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None  API Name: InternetConnectW Args: ( iccv\iist.microsoft\Lom,  | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Call Internet Helper API   | r/nivn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modifiedt/vhAccept-Ranges: bytesivinAge: 3184\vinCache-Control: max-age=3600\vinDate: Thu, 27 May 2021 11:5 6:33 GMT\vinEtag: 0x8D8BDTE4D558BE4\vinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\vinServer: ECAcc (ska/F771)\vinX-Cache: HITv\vinx-ms-blob-type e: BlockBlobivinx-ms-lease-status: unlocked\vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000\vinx-ms-version: 2009-09-19\vin\vin, 392, 1751089 24, 0.) Return: 0  API Name: recv Args: ( c40, , 1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\vist.microsoft.com, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecv\vist.microsoft.com, 443, , , 3, 838608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0004, iecv\vist.microsoft.compat/Data\viscompatdiedta.xml Type: VSDT_TEXT_HTML  Path: \( \) LOCALAPPDATA\( \) Microsoft\lintermet Explorer\Viscompatdiedta.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\lintermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Intermet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  API Name: InternetConnectW Args: ( iecv\vist.microsoft\Loom, 1, 50020000 ) Return: 0  API Name: InternetConnectW Args: ( iecv\vist.microsoft\Loom, 443, , , 3, 8388608, -1518497984 ) R | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Add File   | rnivin, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/inAccept-Ranges: bytesivinAge: 3184/rinCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11:5 6:33 GMTTvinEtag: 0x8D8BD7E4D55BBE4/rinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTTvinServer: ECAcc (skalF771)/rinX-Cache: HITvinx-ms-blob-byp e: BlockBlobivinx-ms-lease-status: unlocked/vinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000/rinx-ms-version: 2009-09-19/rinVrin, 392, 1751089 24, 0, 1 Return: 0  API Name: recv Args: (c40, .1, 2) Return: ?  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed  API Name: DnsQueryEx Args: (iecviist.microsoft.com, 1, 5002000) Return: 0  API Name: Internet\ConnectW Args: (c0004, iecviist.microsoft.com, 443, , , 3, 8388608, -1518497984) Return: c00008  API Name: HttpOpenRequestW Args: (c00008, GET, /iE11/1426178821/iecompat/veiwlist.xml, , , -1554595984, 12582928, -1518497984) Return: c0000c  Path: %LOCALAPPDATA\Microsoft\Internet Explorer\IECompatData\Wicrosoft\Internet Explorer\IECompa | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  | trinin, 376, a6ff248, , 0, HTTP/1.1 304 Not Modified/inAccept-Ranges: bytesirinAge: 3184irinCache-Control: max-age=3600irinDate: Thu, 27 May 2021 11:5 6:33 GMTVinEtag: 0x8D8BD7z4D558BEAirinLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTVinServer: ECAcc (ska/F771)vinX-Cache: HTTVinX-ms-blob-byp e: BlockBlöb/inX-ms-lease-status: unlockedivinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000vinx-ms-version: 2009-09-19vinivin, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, . 1, 2 ) Return: ?  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 1d752ed  API Name: DnsQueryEx Args: ( iecv\stamicrosoft\com, 1, 50020000 ) Return: 0  API Name: InternetConnect\Wargs: ( cc0004, iecv\stamicrosoft\com, 443, , , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HttpOpenRequest\Wargs: ( cc0008, GET, /iE11/1426178821/iecompatdieta.xml Type: VSDT_TEXT_HTML  Path: \%LOCALAPPDATA\%\Microsoft\Internet Explorer\Stamicrosoft\Internet Explorer\Stamicrosoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None  API Name: InternetConnectify Arg | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  | nnivîn, 376, a6ff248, , 0, HTTP/1.1 304 Not Modifiedt/inAccept-Ranges: bytesivînAge: 3184ivînCache-Control: max-age=3600vînDate: Thu, 27 May 2021 11:5 6:33 GMTvinElag: 0x80B8D7E4D558BE4ivînLast-Modified: Wed, 20 Jan 2021 20:02:23 GMTvinServer: ECAcc (skaF771)vinX-Cache: HITrinx-ms-blob-byte e BlockBlobin/mx-ms-lease-status: unlockedrivinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000vinx-ms-version: 2009-99-19ivînivîn, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40., 1, 2 ) Return: ?  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftInternet ExploreriVersionManager/LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftInternet ExploreriVersionManager/LastCheckForUpdateHighDateTime Value: e1d752ed  API Name: InstrumetConnectW Args: ( iceviist-microsoft.com, 1, 5002000)   | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  | Innivin, 376, a6ff248, , 0, HTTP/1.1 304 Not ModifiedrivinAccept-Ranges: bytesivinAge: 3184ivinCache-Control: max-age=3600ivinDate: Thu, 27 May 2021 11:5 6.33 GMTvinEtag: 0x80B8D7E4D558B8E4ivinLast-Modified: Wed., 20 Jan 2021 20:02:23 GMTvinServer: ECAcc (ska/F771)vinX-Cache: HTTvinx-ms-blob-type e: BlockBlobNinx-ms-lease-status: unlockedrinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000vinx-ms-version: 2009-09-19ivinvin, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, . 1, 2 ) Return: ?  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Internet}\) Explorer\(\text{VersionManager\}\) Last\(\text{CheckForUpdateLowDateTime}\) Value: e61bb8d4  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Internet}\) Explorer\(\text{VersionManager\}\) Last\(\text{CheckForUpdateHighDateTime}\) Value: e61bb8d4  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Cor000}\), 1.50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iccvilist.microsoft.com, 443, , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HitpOpenRequestW Args: ( cc0008, GET, //E11/1426178821/lecompat/viewlist.xml, . , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA\(\text{Microsoft\) internet Explorer\(\text{IECOmpatData\) exompatibative compatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA\(\text{Microsoft\) internet Explorer\(\text{Text}\) Exp     | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call System API   | Inhin, 376, a6ft248, 0, 0 HTTP/1.1 304 Not ModifiedrivinAccept-Ranges: bytesivinAge: 3184/rnCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11.5 6.33 GMTvinEtag: 0x80B8D7E4D558BEAfvinLast-Modifiedr: Wed., 20 Jan 2021 20:02:23 GMTvinServer: EcAcc (ska/F771)/rinX-Cache: HTTvinx-ms-biob-typ e. BlockBlob/mx-ms-lease-status: unlockedr/nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a30000001/nx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, 1, 2) Return: 7  Key: HKEY_CURRENT_USER:SOFTWARE!Microsoftlinternet Explorer/VersionManager/LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER:SOFTWARE!Microsoftlinternet Explorer/VersionManager/LastCheckForUpdateHighDateTime Value: e61bb8d4  API Name: DnsQueryEx Args: ( iecvilst.microsoft.com, 1, 50020000) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoft.com, 43, ., ., 3, 838608, -1518497984) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E111/1426178821/fecompat/data.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%/MicrosoftInternet Explorer/IECompat/Dataliecompat/data.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Decay/DateQueue Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage/LastProcessed Value: None  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoftInternet Explorer/TabbedBrowsing/NewTabPage/LastProcessed Value: None  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoftInternet Explorer/NewTa | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API   | Innivin, 376, a6ff248, , 0, HTTP/1.1 304 Not ModifiedrivinAccept-Ranges: bytesivinAge: 3184ivinCache-Control: max-age=3600ivinDate: Thu, 27 May 2021 11:5 6.33 GMTvinEtag: 0x80B8D7E4D558B8E4ivinLast-Modified: Wed., 20 Jan 2021 20:02:23 GMTvinServer: ECAcc (ska/F771)vinX-Cache: HTTvinx-ms-blob-type e: BlockBlobNinx-ms-lease-status: unlockedrinx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a3000000vinx-ms-version: 2009-09-19ivinvin, 392, 1751089 24, 0 ) Return: 0  API Name: recv Args: ( c40, . 1, 2 ) Return: ?  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Internet}\) Explorer\(\text{VersionManager\}\) Last\(\text{CheckForUpdateLowDateTime}\) Value: e61bb8d4  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Internet}\) Explorer\(\text{VersionManager\}\) Last\(\text{CheckForUpdateHighDateTime}\) Value: e61bb8d4  Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft\(\text{Cor000}\), 1.50020000 ) Return: 0  API Name: InternetConnectW Args: ( cc0004, iccvilist.microsoft.com, 443, , 3, 8388608, -1518497984 ) Return: cc0008  API Name: HitpOpenRequestW Args: ( cc0008, GET, //E11/1426178821/lecompat/viewlist.xml, . , -1554595984, 12582928, -1518497984 ) Return: cc000c  Path: %LOCALAPPDATA\(\text{Microsoft\) internet Explorer\(\text{IECOmpatData\) exompatibative compatdata.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA\(\text{Microsoft\) internet Explorer\(\text{Text}\) Exp     | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write Registry Key  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API   | Inhin, 376, a6ft248, 0, 0 HTTP/1.1 304 Not ModifiedrivinAccept-Ranges: bytesivinAge: 3184/rnCache-Control: max-age=3600/rinDate: Thu, 27 May 2021 11.5 6.33 GMTvinEtag: 0x80B8D7E4D558BEAfvinLast-Modifiedr: Wed., 20 Jan 2021 20:02:23 GMTvinServer: EcAcc (ska/F771)/rinX-Cache: HTTvinx-ms-biob-typ e. BlockBlob/mx-ms-lease-status: unlockedr/nx-ms-request-id: 77a83b40-901e-008e-73e7-52a2a30000001/nx-ms-version: 2009-09-19/rin/rin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: ( c40, 1, 2) Return: 7  Key: HKEY_CURRENT_USER:SOFTWARE!Microsoftlinternet Explorer/VersionManager/LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USER:SOFTWARE!Microsoftlinternet Explorer/VersionManager/LastCheckForUpdateHighDateTime Value: e61bb8d4  API Name: DnsQueryEx Args: ( iecvilst.microsoft.com, 1, 50020000) Return: 0  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoft.com, 43, ., ., 3, 838608, -1518497984) Return: cc0008  API Name: HttpOpenRequestW Args: ( cc0008, GET, //E1171426178821/fecompat/data.xml Type: VSDT_TEXT_HTML  Path: %LOCALAPPDATA%/MicrosoftInternet Explorer/IECompat/Dataliecompat/data.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Decay/DateQueue Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage!Losa/Processed Value: None  Key: HKEY_CURRENT_USER:SOFTWARE!MicrosoftInternet Explorer/TabbedBrowsing/NewTabPage/LastProcessed Value: None  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoftInternet Explorer/TabbedBrowsing/NewTabPage/LastProcessed Value: None  API Name: InternetConnectW Args: ( cc0004, iecvilst.microsoftInternet Explorer/NewTab | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write Registry Key  Call System API  Call Internet Helper API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API  Call System API   | Inhivin, 376, a8ft248, 0, HTTP/1.1 304 Not ModifiedrivnAccept-Ranges: bytesivinAge: 3184/vinCache-Control: max-age=3600vinDate: Thu, 27 May 2021 11:5 633 GMTVinEtag. 0x808B07E4058B8E4vinLast-Modified: Wed, 20 Jan 2021 2002:23 GMTVinServer: ECAc. (skaF771)vinX-Cache: HTVinx-ms-blob-byc e: BlockBlob/twinx-ms-lease-status: unlockedvinx-ms-request-ld: 77a83b40-901e-008e-73e7-52a2a3000000vinx-ms-version: 2009-09-19vinvin, 392, 1751089 24, 0) Return: 0  API Name: recv Args: (c40, .1, 2) Return: 7  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftInternet ExploreriVersionManager/LastCheckForUpdateLowDateTime Value: e61bb8d4  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftUnternet ExploreriVersionManager/LastCheckForUpdateHighDateTime Value: e10b8d4  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftUnternet ExploreriVersionManager/LastCheckForUpdateHighDateTime Value: e10b8d4  API Name: DnsQueryEx Args: (iecviist.microsoft.com, 1, 50020000) Return: 0  API Name: HttpOpenRequestW Args: (c00008, GET, /fE11/1428178821/lecompativiewilst.ml, ., 1554959894, 12582928, -1518497984) Return: c0000c  Path: %LOCALAPPDATA%:MicrosoftUnternet Exploreri/ECompat/Datalecompat/data.xml Type: VSDT_TEXT_HTML  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftUnternet Exploreri/Eboren/TabbedBrowsingNewTabPagelDecayDateQueue Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftUnternet Exploreri/TabbedBrowsingNewTabPagelDecayDateQueue Value: None  Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftUnternet Explorer/TabbedBrowsingNewTabPagelDecayDateQueue Value: None  API Name: InternetConnectW Args: (iecviist.microsoftCom, 1, 50020000) Return: 0  API Name: httpOpenRequestW Args: (iecviist.microsoftCom, 1, 50020000) Return: 0  API Name: WinHttpCloseHand | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |
| Write Registry Key  Call System API  Call Internet Helper API  Call Internet Helper API  Add File  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call Internet Helper API  Add File  Write Registry Key  Call System API  Call Internet Helper API | API Name: InternetConnectW Args: ( co0004, iecvilst.microsoftInternet Explorer\TabbetBrownstata, 3, 8388608, -1518497984 ) Return: co0006  Path: %LOCALAPPDATA%\MicrosoftInternet Explorer\TabbetBrowning\text{internet} Explorer\TabbetBrowningintern       | 1660         | 700 700 700 1660 1660 1660 1660 1660 166           |

| Call System API          | API Name: DnsQueryEx Args: ( iecvlist.microsoft.com, 1, 50020000 ) Return: 0   | 1660 |
|--------------------------|--|------|
| Call Internet Helper API | API Name: InternetConnectW Args: ( cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1518770160 ) Return: cc0008                               | 1660 |
| Call Internet Helper API | API Name: HttpOpenRequestW Args: ( cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1554595984, 12582928, -1518770160 ) Return: cc000c     | 1660 |
| Add File                 | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  | 1660 |
| Write File               | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML  | 1660 |
| Add File                 | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0FA7F1DA-BEE1-11EB-9BF2-001F3C8C8DBB}.dat Type: VSD T_WINWORD | 1660 |
| Write File               | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0FA7F1DA-BEE1-11EB-9BF2-001F3C8C8DBB}.dat Type: VSD T_WINWORD | 1660 |
| Add File                 | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\(0FA7F1DC-BEE1-11EB-9BF2-001F3C8C8DBB)\.dat Type: VSDT_WINWORD               | 1660 |
| Write File               | Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\(0FA7F1DC-BEE1-11EB-9BF2-001F3C8C8DBB\).dat Type: VSDT_WINWORD               | 1660 |

#### ▼ Screenshot



## 

### ▼ Object 1 - Hawb.html (HTML File)

Network connection

| File name | Hawb.html   |
|-----------|---|
| File type | HTML File   |
| SHA-1     | F7911D858AFCCB9E871595374564EFE2D6449377                        |
| SHA-256   | FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E9 |
| MD5       | DEE4CFA9FB0A28C29485245440EF3D50                                |
| Size      | 186357 byte(s)  |

Custom

| Risk Level                | Unrated |
|---------------------------|---------|
| Detection                 | -       |
| Exploited vulnerabilities | -       |

### Node Notable Threat Characteristics Anti-security, self-preservation Submitted sample Malformed, defective, or with known malware traits Autostart or other system reconfiguration Process, service, or memory object change Root process Deception, social engineering Rootkit, cloaking Child process File drop, download, sharing, or replication Suspicious network or messaging activity \_\_\_\_ Direct event Hijack, redirection, or data theft ----- Indirect event Created Event actions