

Virtual Analyzer Report



Submission Context

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

Analysis Overview

Overall risk level	<div>High risk</div> 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	✓		
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	<div>High risk</div> 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	FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E99
MD5	DEE4CFA9FB0A28C29485245440EF3D50
Size	186357 byte(s)

Risk Level	<div>High risk</div>
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	<div></div> Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13

© ATT&CK™ is a trademark of The 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\explore.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	■ ■ ■	0.0.0.0:49169
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 Cloud Applications	No risk	-	Hawb.html
https://iecvlist.microsoft.com/ie11blocklist/1401746408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
https://fonts.gstatic.com/s/ptsans/v12/jizaRExUITo99u79D0KEww.woff	Computers / Internet	No risk	-	Hawb.html
http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab	Software Downloads	No risk	-	Hawb.html
http://ocsp.pki.goog/gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRcRjDCJxnb3nDwj%2Fxz5aZIZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEBcw%2FX18SvRyAwAAAADMD0E%3D	Computers / Internet	No risk	-	Hawb.html
http://www.microsoft.com/pki/certs/MicRocCerAut_2010-06-23.crt	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ocsp.pki.goog/gts1o1core/MFlwUDBOMEwSjAJBgUrDgMCGgUABBRcRjDCJxnb3nDwj%2Fxz5aZIZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEQCw80IEZ3xvQUAAAAh8vC	Computers / Internet	No risk	-	Hawb.html
http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbrv2lBkPpolEVR6gHlCnAQUm%2BIHV2ccHsBqBt5ZlJot39wZhi4CDQHjUqhYqpgSVpULg%3D	Computers / Internet	No risk	-	Hawb.html
http://ie9cvlist.ie.microsoft.com/IE9CompatViewList.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
https://fonts.gstatic.com/s/ptsans/v12/jizfRExUITo99u79B_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-08002739B404}.dat	No risk	-	-	-	4608	BB02092AB0D145352017996CF2F2985D1B47D449
RecoveryStore.{0E12DC2E-BEE1-11EB-B06F-08002739B404}.dat	No risk	-	-	-	4608	8286A21E93E6DF15091AD207CA860B2F129A46CC
{0E12DC2F-BEE1-11EB-B06F-08002739B404}.dat	No risk	-	-	-	4608	66B7AD61E6004EA37F3A9CAF2FACDFB8A6A7D995
RecoveryStore.{38CCAF37-BEE1-11EB-B06F-08002739B404}.dat	No risk	-	-	-	3584	FBBCD6C9EE4AA3DBF515C16D2AD7402E714AF275
~DFC01FA6ADF190A795.TMP	No risk	-	-	-	20480	EA4D9AF1E727D831D32193A96F8BE4029029FEDD
~DF1AAEFA4FE340E9FA.TMP	No risk	-	-	-	16384	BF983F1B7E16997577B6E39F3D5E04692041D210
F0ACCF77CDCBFF39F6191887F6D2D357	No risk	-	-	-	242	B5938F0F54195EC717A65E77409E71B4F1AA5444
jizfRExUITo99u79B_mh0O6tKw[1].woff	No risk	-	-	https://fonts.gstatic.com/s/ptsans/v12/jizfRExUITo99u79B_mh0O6tKw.woff	57524	27DF60E5879AA568876F747F3CFACF28564F9B09
CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B	No risk	-	-	-	394	5CC3EC7C82ABAA05C4DDBF1647D9744D531C8D6A
CC197601BE0898B7B0FCC91FA15D8A69_8A59D0CC8B81246393FAF874672C0BE9	No risk	-	-	-	414	3B7225E3FDF0ADD3C7C1A54D70D4673FFE858687

▼ Suspicious Objects

Type	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\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: (25a2f8, RASMAN, 4) Return: 25a2f58		2432
Call Service API	API Name: OpenServiceW Args: (1ba378, Sens, 4) Return: 1b9ba8		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2432
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2432
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2432
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\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
Write 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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\SecuritySafe Value: 1		2432
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
Call Process API	API Name: CreateProcessW Args: (, "%ProgramFiles%\Internet Explorer\iexplore.exe" SCODEF:2432 CREDAT:79873, , , CREATE_SUSPENDED, , , Process:2504:%ProgramFiles%\Internet Explorer\iexplore.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		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{E7E4BC40-E76A-11CE-A9BB-00AA004AE837} {000214E6-0000-0000-C000-000000000046} 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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2432	2504
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2432	2504
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2432	2504
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2432	2504
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\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: DnsQueryExW Args: (fonts.googleapis.com, 1, 50000000) Return: 0	2432	2504
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, fonts.googleapis.com, 443, , , 3, 8388608, 54933528) Return: cc0008	2432	2504
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /css?family=PT+Sans:400,700, , , 64194584, 12582912, 54933528) Return: cc000c	2432	2504
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-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
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		

Call Network API	API Name: connect Args: (628, 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, !, 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 0.0.0.0:49169		
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, !, 1, 0) Return: 1	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 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, !, 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: 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: None	2432	2504
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
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 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: VSDT_MSCF		
Delete File	Path: %TEMP%\Cab93BE.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%\Cab93BE.tmp Type: VSDT_MSCF		
Delete File	Path: %TEMP%\Cab935D.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%\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
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (37edd7c, 0, 0, 0) Return: 1		2432
Call 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
Detection	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, /IE9CompatViewList.xml, , , 58644848, 4194320, 76528104) Return: cc000c		2432
Call Network API	API Name: socket Args: (2, 2, 0) Return: 674		2432
Call Network API	API Name: socket Args: (23, 2, 0) Return: 674		2432
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 40006000) Return: 9701		2432
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1c, 40006000) Return: 0		2432
Call Network API	API Name: socket Args: (23, 2, 0) Return: 674		2432
Call Network API	API Name: socket Args: (2, 1, 6) Return: 674		2432
Call Network API	API Name: bind Args: (674, 0.0.0.0:49170, 16) Return: 0		2432
Detection	Threat Characteristic: Listens on port 0.0.0.0:49170		
Call Network API	API Name: connect Args: (674, 152.199.19.161:80, 16) Return: ffffffff		2432
Call Network API	API Name: recv Args: (5a4, , 32, 0) Return: ?		2432
Call Network API	API Name: send Args: (5a4, 1, 1, 0) Return: 1		2432
Call Network API	API Name: send Args: (674, GET /IE9CompatViewList.xml HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 [compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0]\r\nHost: ie9cvlist.ie.microsoft.com\r\nConnection: Keep-Alive\r\n\r\n, 219, 0) Return: 219		2432
Call Network API	API Name: recv Args: (674, , 1024, 0) Return: ?		2432
Call Network API	API Name: send Args: (5a4, 1, 1, 0) Return: 1		2432
Call Network API	API Name: recv Args: (5a4, , 32, 0) Return: ?		2432
Call Network API	API Name: recv Args: (674, , 1024, 0) Return: ?		2432
Call Network API	API Name: recv Args: (674, , 8192, 0) Return: ?		2432
Call Network API	API Name: recv Args: (674, , 4969, 0) Return: ?		2432
Call Network API	API Name: recv Args: (674, , 1, 2) Return: ?		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZK\IE9CompatViewList[1].xml Type: VSDT_TEXT_HTML		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZK\IE9CompatViewList[1].xml Type: VSDT_TEXT_HTML		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_EMPTY		2432
Write 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\MXNZOZK\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\VersionHigh Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\VersionLow Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\DXFeatureLevel Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VendorId Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DeviceId Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-SubSysId Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-Revision Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionHigh Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionLow Value: 0		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DXFeatureLevel Value: 0		2432
Call Network API	API Name: socket Args: (2, 2, 0) Return: 8d8	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d8	2432	2504
Call Network API	API Name: socket Args: (2, 2, 0) Return: 8e0	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8e0	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, 1, 40006000) Return: 9701	2432	2504
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 37edd90) Return: 0		2432
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: 8e0	2432	2504
Call Network API	API Name: socket Args: (2, 2, 0) Return: 8e0	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8e0	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: 8e0	2432	2504
Call Network API	API Name: socket Args: (2, 1, 6) Return: 8e0	2432	2504
Call Network API	API Name: bind Args: (8e0, 0.0.0.0:49171, 128) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49171		

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 p-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 12 Sep 2014 18:47:05 GMT\r\nIf-None-Match: *805a83f2b9cecf1:0*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: www.download.windowsupdate.com\r\n\r\n, 1, 303) Return: 0	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, 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, 0.0.0.0:49172, 128) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49172		
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 p-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 12 Sep 2014 18:47:05 GMT\r\nIf-None-Match: *805a83f2b9cecf1:0*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: www.download.windowsupdate.com\r\n\r\n, 1, 303) Return: 0	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (33f4ff0) 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: (4abc80) 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%\CabAB68.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	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, 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%\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
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
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d0	2432	2504
Call System API	API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701	2432	2504
Call System API	API Name: DnsQueryExW Args: (www.microsoft.com, 1c, 40006000) Return: 0	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d4	2432	2504
Call Network API	API Name: socket Args: (2, 2, 0) Return: 8d4	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d4	2432	2504
Call System API	API Name: DnsQueryExW Args: (www.microsoft.com, 1, 40006000) Return: 9701	2432	2504
Call System API	API Name: DnsQueryExW Args: (www.microsoft.com, 1c, 40006000) Return: 0	2432	2504
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8d4	2432	2504
Call Network API	API Name: socket Args: (2, 1, 6) Return: 8d4	2432	2504
Call Network API	API Name: bind Args: (8d4, 0.0.0.0:49175, 128) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call System API	API Name: ConnectEx Args: (8d4, 2.22.42.141:80, 16, 0, 0, 0, 4a119d8) Return: 0	2432	2504
Call Network API	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-CryptoAPI/6.1\r\nHost: www.microsoft.com\r\n\r\n, 1, 154) Return: 0	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: (3442490) Return: 1	2432	2504
Call Network API	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-CryptoAPI/6.1\r\nHost: www.microsoft.com\r\n\r\n, 1, 154) Return: 0	2432	2504
Delete File	Path: %TEMP%\CabE7EE.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%\CabE7EE.tmp Type: VSDT_MSCF		
Call System API	API Name: WinHttpCloseHandle Args: (495ec00) Return: 1	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (3442748) Return: 1	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (3442660) Return: 1	2432	2504
Delete File	Path: %TEMP%\CabE8CA.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%\CabE8CA.tmp Type: VSDT_MSCF		
Call Network API	API Name: send Args: (8e0, GET /msdownload/update/v3/static/trusted/en/authorstsl.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\nHost: 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
Call Network API	API Name: send Args: (8e4, GET /msdownload/update/v3/static/trusted/en/authorstsl.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\nHost: 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
Delete File	Path: %TEMP%\CabEA74.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%\CabEA74.tmp Type: VSDT_MSCF		
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	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 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, 0.0.0.0:49176, 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/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2IBKPoolEVRE6gHICnAQum%2BIHV2ccHsBqBT5ZJot39wZhi4CDQHjUqjhYqpgSVpULg%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.pki.goog\r\n\r\n, 1, 230) Return: 0	2432	2504
Call Network API	API Name: send Args: (914, GET /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2IBKPoolEVRE6gHICnAQum%2BIHV2ccHsBqBT5ZJot39wZhi4CDQHjUqjhYqpgSVpULg%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.pki.goog\r\n\r\n, 1, 230) Return: 0	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: (8d0, GET /gts1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGGUABBRcRjDCJxnb3nDwj%2FxxZfZjgXvAQumNH4bhDrz5vsYJ8YkBu g630J%2FssCEQCw80lEZ3xyQUAAAAh8vC HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ocsp.pki.goog\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
Call System API	API Name: WinHttpCloseHandle Args: (3442578) Return: 1	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (3442748) Return: 1	2432	2504
Delete File	Path: %TEMP%\CabED05.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%\CabED05.tmp Type: VSDT_MSCF		
Call Network API	API Name: send Args: (914, GET /gts1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGGUABBRcRjDCJxb3nDwj%2Fxz5aZIZjgXvAQUMNH4bhDrz5vsYJ8YkBu g630J%2F5sCEQCw80IEZ3xvjQUAAAAh8vC HTTP/1.1\r\nCache-Control: max-age = 86400\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Micros oft-CryptoAPI/6.1\r\nHost: ocsppki.google\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,R..ANA..VtB-z[.e.U3..wU&V.S.,4.....*...<.....].-.-.&\$./N.11.4.Q.0.@...\$....?4.8.89.....i.-W-3[c.7.->@j]ME..sP.-.-.U..M +.O#k.([.Wl....\n..lVr6.T.J....r.5....Lj+....-....z....B...\$.pe....3.F....Q..l.r-....]...u~.....C...c....r.o..Rq7.....Zl...rKXO., 277, 0) Return: 277	2432	2504
Call Network API	API Name: recv Args: (628, , 1500, 0) Return: ?	2432	2504
Call Network API	API Name: send Args: (4c0, l, 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: (4a1cec0, HTTP/1.1 200 OK\r\nContent-Type: text/css; charset=utf-8\r\nAccess-Control-Allow-Origin: *\r\nTiming-Allow-Origi n: *\r\nExpires: Thu, 27 May 2021 11:56:26 GMT\r\nDate: Thu, 27 May 2021 11:56:26 GMT\r\nCache-Control: private, max-age=86400\r\nCross-Origin-Reso urce-Policy: cross-origin\r\nContent-Encoding: gzip\r\nServer: ESF\r\nX-XSS-Protection: 0\r\nX-Frame-Options: SAMEORIGIN\r\nX-Content-Type-Options: no sniff\r\nAlt-Svc: h3-29=":443"; ma=2592000, h3-T051=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="46, 43"\r\nTransfer-Encoding: chunked\r\n\r\n00000001\r\n, 944, 0, , 0, HTTP/1.1 200 OK\r\nContent-Type: text/c ss; charset=utf-8\r\nAccess-Control-Allow-Origin: *\r\nTiming-Allow-Origin: *\r\nExpires: Thu, 27 May 2021 11:56:26 GMT\r\nDate: Thu, 27 May 2021 11:56:26 GMT\r\nCache-Control: private, max-age=86400\r\nCross-Origin-Resource-Policy: cross-origin\r\nContent-Encoding: gzip\r\nServer: ESF\r\nX-XSS-Protection : 0\r\nX-Frame-Options: SAMEORIGIN\r\nX-Content-Type-Options: nosniff\r\nAlt-Svc: h3-29=":443"; ma=2592000, h3-T051=":443"; ma=2592000, h3-Q050=": 443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="46, 43"\r\nTransfer-Encoding: chunked\r\n\r\n 00000001\r\n, 1066, 85325176, 0) Return: 0	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\n\r\nH'Zœ", 32, 0, , 0, 0\r\n\r\n\r\nH'Zœ", 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: ffffffff	2432	2504
Call Network API	API Name: send Args: (4c0, l, 1, 0) Return: 1	2432	2504
Call Network API	API Name: socket Args: (2, 1, 6) Return: 928	2432	2504
Call Network API	API Name: bind Args: (928, 0.0.0.0:49179, 16) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49179		
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, l, 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: (4c0, , 32, 0) Return: ?	2432	2504
Call Network API	API Name: send Args: (8f8, ..., 130, 0) Return: 130	2432	2504
Call Network API	API Name: recv Args: (8f8, , 1024, 0) Return: ?	2432	2504
Call Network API	API Name: send Args: (4c0, l, 1, 0) Return: 1	2432	2504
Call Network API	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, l, 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/jjzifRExUITo99u79B_mh0O6tKw.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
Call Network API	API Name: recv Args: (928, , 92, 0) Return: ?	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, , 1024, 0) Return: ?	2432	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 , l, 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 , l, 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: (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 , 0.0.0.0:49180, 16) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49180		
Call Network API	API Name: connect Args: (960 , 216.58.207.195:443, 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 , l, 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 , l, 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/MFEwTzBNMESwSTAJBgUrDgMCGgUABBRcRjDCJxn3nDwj%2Fxz5aZfZjgXvAQUMNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBcw%2FX18SvRyAwAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: o csp.pki.google\r\n\r\n, 1, 244) Return: 0	2432	2504
Call Network API	API Name: send Args: (914 , GET /gts1o1core/MFEwTzBNMESwSTAJBgUrDgMCGgUABBRcRjDCJxn3nDwj%2Fxz5aZfZjgXvAQUMNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBcw%2FX18SvRyAwAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: o csp.pki.google\r\n\r\n, 1, 244) Return: 0	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (49e79b0) 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: (8f8 , ...,0].....&V.Y3.....'a....V.Ints53lr..'?'b%M..p?'G.mABe...GK..C....'a'U...oL...z..KGIt\rV....., 309, 0) Return: 309	2432	2504
Call Network API	API Name: recv Args: (8f8 , , 1500, 0) Return: ?	2432	2504
Call Network API	API Name: send Args: (4c0 , l, 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: (638 , , 1, 2) Return: ?	2432	2504
Call Network API	API Name: recv Args: (628 , , 1, 2) Return: ?	2432	2504
Call Network API	API Name: recv Args: (8f8 , , 1500, 0) Return: ?	2432	2504
Call System API	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\nContent-Length: 55340\r\n\r\nDate: Tue, 25 May 2021 08:38:03 GMT\r\n\r\nExpires: Wed, 25 May 2022 08:38:03 GMT\r\n\r\nLast-Modified: Tue, 15 Sep 2020 18:09:19 GMT\r\n\r\nX-Content-Type-Options: nosniff\r\n\r\nServer: sffe\r\n\r\nX-XSS-Protection: 0\r\n\r\nAge: 184705\r\n\r\nCache-Control: public, max-age=31536000\r\n\r\nAlt-Svc: h3-29=\":443\"; ma=2592000, h3-T051=\":443\"; ma=2592000, h3-Q050=\":443\"; ma=2592000, h3-Q046=\":443\"; ma=2592000, h3-Q043=\":443\"; ma=2592000, quic=\":443\"; ma=2592000; v=46, 43\"\r\n\r\n\r\nwOFF, 1495, 70775876, 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, ũ'Çx, 1408, 0 , 0, ũ'Çx, 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, «űőűjű, 1408, 0 , 0, «űőűjű, 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, š· ® '%7yJR,đT'ý ~‰†, 1408, 0 , 0, š· ® '%7yJR,đT'ý ~‰†, 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, ŬŠú-itt, 1408, 0 , 0, ŬŠú-itt, 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, «á, Vá5Ā, 1408, 0 , 0, «á, Vá5Ā, 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, ℱ‰, 1408, 0 , 0, ℱ‰, 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, ½, 1408, 0 , 0, ½, 1495, 70770992, 0) Return: 0	2432	2504

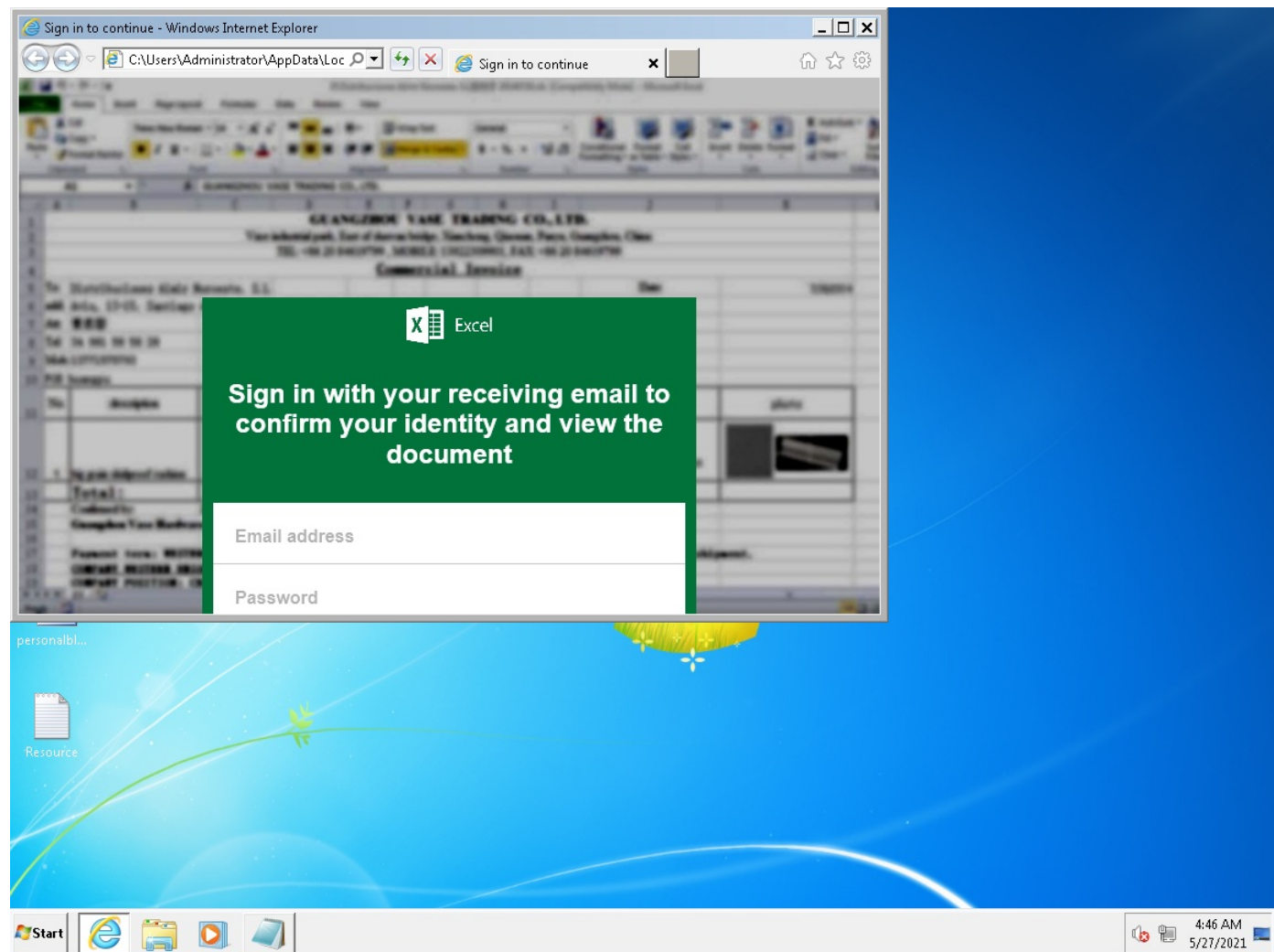
Call Network API	API Name: recv Args: (8f8 , , 1326, 0) Return: ?	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, J6jnXLA, 1408, 0, , 0, J6jnXLA, 1408, 70770992, 0) Return: 0	2432	2504
Call Network API	API Name: recv Args: (8f8 , , 1500, 0) Return: ?	2432	2504
Call System API	API Name: 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"Šă, 1408, 0, , 0, ù@WW"-ý"Šă, 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, èŃ...8jŠYă"‰Y":FI"Œ...ÔD7€, 1408, 0, , 0, èŃ...8jŠYă"‰Y":FI"Œ...ÔD7€, 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, 'TM»ß"b;q'ß"rşdjBbêlÛ@, 1408, 0, , 0, 'TM»ß"b;q'ß"rşdjBbêlÛ@, 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, @¬™ê¬→6M5Mz, 1408, 0, , 0, @¬™ê¬→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, İyİ3]]Y'aŒ, 1408, 0, , 0, İyİ3]]Y'aŒ, 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, ß'ĚĚk"±X\$, 1408, 0, , 0, ß'ĚĚk"±X\$, 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, @ăqSăYôG...¿0cRV,"İ, 320, 0, , 0, @ăqSăYôG...¿0cRV,"İ, 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, ('Z., 1408, 0, , 0, ('Z., 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[>¬ŃQĚ1ĈĖĀĀ', 1408, 0, , 0, YPÚ[>¬ŃQĚ1ĈĖĀĀ', 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, ýpþß", 1408, 0, , 0, ýpþß", 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, þĚĚ(8ŋĚ1¬1Œ"ŒĈ¬d'ê#, 1408, 0, , 0, þĚĚ(8ŋĚ1¬1Œ"ŒĈ¬d'ê#, 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, ŪU^, 1408, 0, , 0, ŪU^, 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, ĬĈepV Ū@;ă?, 1408, 0, , 0, ĬĈepV Ū@;ă?, 1408, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, -^ă, 1408, 0, , 0, -^ă, 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, 1J, 1408, 0, , 0, 1J, 1408, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, aŃ, 1408, 0, , 0, aŃ, 1495, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, Š"JW-«Šjç@ø"Œ"iA"=ŠUeZeĈ-, 1408, 0, , 0, Š"JW-«Šjç@ø"Œ"iA"=ŠUeZeĈ-, 1408, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, ?ùĀêœ:ĀüiĀ, 1408, 0, , 0, ?ùĀêœ:ĀüiĀ, 1495, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, İĚ"Uj[uemQ"r², 1408, 0, , 0, İĚ"Uj[uemQ"r², 1408, 70770992, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (4c03d00, , 1408, 0, , 0, , 1495, 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, ¼, 576, 0, , 0, ¼, 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 /gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRJDCJxbn3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBOW%2FX18SvRyAwAAAADMD0E%3D HTTP/1.1r/nCache-Control: max-age = 86400r/nConnection: Keep-Aliver/nAccept: */*r/nUser-Agent: Microsoft-CryptoAPI/6.1r/nHost: ocs.pki.google/r/nr/n, 1, 276) Return: 0	2432	2504
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4Y3O0HM3\jizaREXUiTo99u79D0KEww[1].woff Type: VSDT_COM_DO S	2432	2504
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4Y3O0HM3\jizaREXUiTo99u79D0KEww[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..ik...U..fM.#.et....aa.8a3.&..... [q.{S...5"...%....r@'E':S...AA.f&...^...rZ.&&...".fy{...M.T.K.\[N.9.v...-lwE...ax.\$~-c.H..ly =K.t.u.....f[6.H3....~2..2.!g...&ui.. N5{.....#.....yU...#..b...}@\$.q[.8..*.b.....T.t....xP...Y..f.y..V.I."Jd....W...~5.D."...;a...AN.Q.....S...M.?G...1S, 309, 0) Return: 30 9	2432	2504
Call Network API	API Name: recv Args: (960 , , 1500, 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: (960 , , 1500, 0) Return: ?	2432	2504

Call System API	API Name: BCryptDecrypt Args: (49494f0, HTTP/1.1 200 OK\r\nContent-Type: font/woff\r\nAccess-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 Sep 2020 18:10:09 GMT\r\nX-Content-Type-Options: nosniff\r\nServer: sffe\r\nX-XSS-Protection: 0\r\nAge: 155729\r\nCache-Control: public, max-age=31536000\r\nAlt-Svc: h3-29=";443"; ma=2592000, h3-T051=";443"; ma=2592000, h3-Q050=";443"; ma=2592000, h3-Q046=";443"; ma=2592000, h3-Q043=";443"; ma=2592000, quic=";443"; ma=2592000; v=46, 43"\r\n\r\nwOFF, 1408, 0, , 0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nContent-Type: font/woff\r\nAccess-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 Sep 2020 18:10:09 GMT\r\nX-Content-Type-Options: nosniff\r\nServer: sffe\r\nX-XSS-Protection: 0\r\nAge: 155729\r\nCache-Control: public, max-age=31536000\r\nAlt-Svc: h3-29=";443"; ma=2592000, h3-T051=";443"; ma=2592000, h3-Q050=";443"; ma=2592000, h3-Q046=";443"; ma=2592000, h3-Q043=";443"; ma=2592000; v=46, 43"\r\n\r\nwOFF, 1495, 68154652, 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, ρϥρΕηϭ ΕΓ&UΌŦ'<ø<%̣pũÄ §Bðñ, 1408, 0, , 0, ρϥρΕηϭ ΕΓ&UΌŦ'<ø<%̣pũÄ §Bðñ, 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, àÿþİ9@{P@, 1408, 0, , 0, àÿþİ9@{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, ÔÂ&±~"%̣>)lÇİçjı:ĐZĐ`@, 1408, 0, , 0, ÔÂ&±~"%̣>)lÇİçjı: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, ŌđþĴðó^Œ%{, 1408, 0, , 0, ŌđþĴðó^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, Tégı;qÇ, 1408, 0, , 0, Tégı;qÇ, 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, Đ, ĐBĐjúÉát/E8óóp*®âHE^, 1408, 0, , 0, Đ, ĐBĐjúÉát/E8óóp*®âHE^, 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, 'ÔÂô^JLşmqı)lbiè†Â&n"E, 1408, 0, , 0, 'ÔÂô^JLşmqı)lbiè†Â&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, þİn3ÜÊ")ØY'ı¶ ēfz%»_B@gŸ—%"D4âQæ#, 1408, 0, , 0, þİn3ÜÊ")ØY'ı¶ ēfz%»_B@gŸ—%"D4âQæ#, 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, , 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, nvŬ...`â, 1408, 0, , 0, nvŬ...`â, 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, žYŮĂŋ_, 1408, 0, , 0, žYŮĂŋ_, 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, <aÈjVhþCêg, 1408, 0, , 0, <aÈjVhþCêg, 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, ×[âu¶IZÅ], 1408, 0, , 0, ×[âu¶IZÅ], 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, ðõ%;läëÖ_ÿçY"ı,q'è8OG%ıJYfé, 1408, 0, , 0, ðõ%;läëÖ_ÿçY"ı,q'è8OG%ıJYfé, 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, "eW'eß))}fW..., 1408, 0, , 0, "eW'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, (ekböz'ö,+UoiÁCEL_™W, 1408, 0, , 0, (ekböz'ö,+UoiÁCEL_™W, 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, ÚSİþĂ×+_ø™, 1408, 0, , 0, ÚSİþĂ×+_ø™, 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, ZİOó@, 1408, 0, , 0, ZİOó@, 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, , 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, ™üjófYölyGUăĪ, 1408, 0, , 0, ™üjófYölyGUăĪ, 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, i, 1408, 0, , 0, i, 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, vç+5xĂ, 1408, 0, , 0, vç+5xĂ, 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, ™, 320, 0, , 0, ™, 1495, 68149768, 0) Return: 0	2432	2504
Call Network API	API Name: recv Args: (960, , 238, 0) Return: ?	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, "ÉĂ"-A=uFDĂ@sR, 1408, 0, , 0, "ÉĂ"-A=uFDĂ@sR, 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, İđ&0ZŲđŁı!½QÉt:7+, 1408, 0, , 0, İđ&0ZŲđŁı!½QÉt:7+, 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, SP@M, 1408, 0, , 0, SP@M, 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, ±İrFİn6, 1408, 0, , 0, ±İrFİn6, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, "-Q#Ă, 1408, 0, , 0, "-Q#Ă, 1408, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, P, 1408, 0, , 0, P, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, ŁGĪ, 1408, 0, , 0, ŁGĪ, 1408, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, ×¼6™ıŲı×óé<@Łı;:ØŽ^#ſsÇuŲqŲ, 1408, 0, , 0, ×¼6™ıŲı×óé<@Łı;:ØŽ^#ſsÇuŲqŲ, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, , 1408, 0, , 0, , 1408, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (4b8cd20) Return: 1	2432	2504
Call System API	API Name: WinHttpCloseHandle Args: (3442ae8) Return: 1	2432	2504

Call System API	API Name: WinHttpCloseHandle Args: (3442660) Return: 1	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, ySVİİv²dDPT~Äĵ<, 1408, 0, , 0, ySVİİv²dDPT~Äĵ<, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, /+Ã*ĖJN-k?İn, 1408, 0, , 0, /+Ã*ĖJN-k?İn, 1408, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, İ%Ė*İİİY*âĵİ]]M×RU^İy)ĖŠp`ÙQ, 1408, 0, , 0, İ%Ė*İİİY*âĵİ]]M×RU^İy)ĖŠp`ÙQ, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, Ûİİİ`Â¹, 1408, 0, , 0, Ûİİİ`Â¹, 1408, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, ĳ[C", 1408, 0, , 0, ĳ[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
Call System API	API Name: BCryptDecrypt Args: (49494f0, 6, 1408, 0, , 0, 6, 1495, 68149768, 0) Return: 0	2432	2504
Call System API	API Name: BCryptDecrypt Args: (49494f0, N±Öİ (Û`»çqušĥ, 1408, 0, , 0, N±Öİ (Û`»çqušĥ, 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\IEY6ZFZU4\jizfRExUiTo99u79B_mh0O6İKw[1].woff Type: VSDT_COM_DOS	2432	2504
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\IEY6ZFZU4\jizfRExUiTo99u79B_mh0O6İKw[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, /İe11blockİst/1401746408/versionİst.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: 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
Call Network API	API Name: bind Args: (968, 0.0.0.0:49182, 16) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49182		
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
Call Network API	API Name: bind Args: (968, 0.0.0.0:49183, 16) Return: 0	2432	2504
Detection	Threat Characteristic: Listens on port 0.0.0.0:49183		
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, .., 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 0.0.0.0:49184		
Call Network API	API Name: connect Args: (968, 152.199.19.161:443, 16) Return: fffffff	2432	2504
Call System API	API Name: DnsQueryExW Args: (İe9cvİstİe.microsoft.com, 1, 50000000) Return: 0		2432
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, İe9cvİstİe.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008		2432
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /İE9CompatViewİst.xml, , , 58644852, 4194320, 39568160) Return: cc000c		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\İMXNZOZKK\İE9CompatViewİst[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml, 0, 0, 0, 0) Return: 1		2432
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes\DownloadRetİes Value: 0		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: (İe9cvİstİe.microsoft.com, 1, 50000000) Return: 0		2432
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, İe9cvİstİe.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008		2432
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /İE9CompatViewİst.xml, , , 58644852, 4194320, 39568160) Return: cc000c		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\İMXNZOZKK\İE9CompatViewİst[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.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
Call System API	API Name: DnsQueryExW Args: (İe9cvİstİe.microsoft.com, 1, 50000000) Return: 0		2432
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, İe9cvİstİe.microsoft.com, 80, , , 3, 0, 39568160) Return: cc0008		2432
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /İE9CompatViewİst.xml, , , 58644852, 4194320, 39568160) Return: cc000c		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\İecompatdata.xml Type: VSDT_TEXT_HTML		2432

Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOKK\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
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, /IE9CompatViewList.xml, , , 58644852, 4194320, 39568160) Return: cc000c		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2432
Write 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\MXNZOKK\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\AddToFavorites\InitialSelection Value: None	2432	2504
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\AddToFeeds\InitialSelection 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%\Microsoft\Internet Explorer\Recovery\High\Last Active\{38CCAF38-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Last Active\{38CCAF38-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0E12DC2E-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0E12DC2E-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{0E12DC2F-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{0E12DC2F-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Last Active\RecoveryStore.{38CCAF37-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Last Active\RecoveryStore.{38CCAF37-BEE1-11EB-B06F-08002739B404}.dat Type: VSDT_WINWORD		2432

▼ Screenshot



Environment-specific risk level	<div>High risk</div> 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	FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E99
MD5	DEE4CFA9FB0A28C29485245440EF3D50
Size	186357 byte(s)

Risk Level	<div>High risk</div>
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/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJLQoXyo4hxex7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	Hawb.html
https://fonts.googleapis.com/css?family=PT+Sans:400,700	Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ocsp.pki.goog/gts1o1core/MFwUDBOMEwWSJAJBgUrDgMCGgUABBRcRjDCJxnb3nDwj%2Fxz5aZTZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEQCow80IEZ3xvQUAAAAh8vC	Computers / Internet	No risk	-	Hawb.html
https://iecvlist.microsoft.com/ie11blocklist/1401746408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
https://fonts.gstatic.com/s/ptsans/v12/jizaRExUITo99u79D0KEww.woff	Computers / Internet	No risk	-	Hawb.html
https://iecvlist.microsoft.com/IE11/1426178821/iecompatviewlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e0e817717432daa8	Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIUJHWMys%2BgghUNoZ70rUETFACEA8UllBgGmZT9XHrHIJQel%3D	Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b46a730d6789357a	Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://ocsp.pki.goog/gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRcRjDCJxnb3nDwj%2Fxz5aZTZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEBcw%2FX18SvRyAwAAAAADMD0E%3D	Computers / Internet	No risk	-	Hawb.html
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?f15d8c2e51b81975	Computers / Internet Cloud Applications	No risk	-	Hawb.html
http://go.microsoft.com/fwlink/?LinkID=401135	Computers / Internet	No risk	-	Hawb.html
http://ocsp.pki.goog/gsr2ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXisxbvr2IBkPpoiEVRE6gHiCnAQUm%2BIHVZccHsBqBt5ZJot39wZhi4CDQHjUqhYqpGSPvULg%3D	Computers / Internet	No risk	-	Hawb.html
https://ieonline.microsoft.com/iefflipahead/ie10/rules.xml?mkt=en-US	Business / Economy Computers / Internet Cloud Applications	No risk	-	Hawb.html
https://fonts.gstatic.com/s/ptsans/v12/jizfRExUITo99u79B_mh0O6IKw.woff	Computers / Internet	No risk	-	Hawb.html

▼ **Dropped or Downloaded Files**

--

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
{0FA7F1DC-BEE1-11EB-9BF2-001F3C8C8DBB}.dat	No risk	-	-	-	3584	F1CB4BD242B83F0DEBFC20429B180B441E4FA660
RecoveryStore.{0FA7F1DA-BEE1-11EB-9BF2-001F3C8C8DBB}.dat	No risk	-	-	-	5632	F78A26F659677B888F3038BD396B2649CA2412ED
IEInstrumentation2021{1}.htm	No risk	-	-	-	2140	C80654A5A50C561D9B0D04D822481C1DD49C58B6
jizaRExUiTo99u79D0KEww{1}.woff	No risk	-	-	https://fonts.gstatic.com/s/ptsans/v12/jizaRExUiTo99u79D0KEww.woff	55340	0515F781A37C8775C466577EC40AEF136CB CF3CB
~DFAD60AA53D96FDCE3.TMP	No risk	-	-	-	16384	A06EAD2C3E32A6F862492EA1CE50BFDE15F465BA
CC197601BE0898B7B0FCC91FA15D8A69_D73245CB85BA4F2701FE45752B2B1FC1	No risk	-	-	-	422	7D77058AFC77DD7090CEFE0A4897448D1147CA2D
CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B	No risk	-	-	-	394	CE840481010320854E95D812BB678E81658ABE29
CC197601BE0898B7B0FCC91FA15D8A69_8A59DOCC8B81246393FAF874672C0BE9	No risk	-	-	-	414	69626A9B6376FE6DF759417BD509E16EA4BD4F36
jizIRExUiTo99u79B_mh0O6tKw{1}.woff	No risk	-	-	https://fonts.gstatic.com/s/ptsans/v12/jizIRExUiTo99u79B_mh0O6tKw.woff	57524	27DF60E5879AA568876F747F3CFACF28564F9B09
~DF105EE340451AB1B0.TMP	No risk	-	-	-	16384	2DAEA6E53554F7D8D3DD1909E5CB4F48D7395954

▼ Suspicious Objects

Type	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\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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\CurrentVersion\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\EXPLORE.EXE" SCODEF:1660 CREDAT:148481 /prefetch:2 , , , CREATE_SUSPENDED , , , Process:700:%ProgramFiles(x86)%\Internet Explorer\explore.exe) Return: 1		1660
Call Thread API	API Name: NiResumeThread 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 Explorer\EXPLORE.EXE SCODEF:1660 CREDAT:148481 /prefetch:2		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache) 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\CurrentVersion\Internet Settings\ProxyEnable Value: 0	1660	700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	1660	700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	1660	700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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\CurrentVersion\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\rundll32.exe shell32.dll, SHCreateLocalServerRunDll (9BA05972-F6A8-11C F-A442-00A0C90A8F39)] 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: 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: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 7e447a4) Return: 0	1660	700
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 7e447a4) Return: 0	1660	700
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 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, 0.0.0.0:49426, 16) Return: 0	1660	700
Detection	Threat Characteristic: Listens on port 0.0.0.0:49426		
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\tableiconcache.dat) Return: 0		1660
Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\AppData\Local\Low\Microsoft\Internet Explorer\tableiconcache.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\lmmersiveiconcache.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\7d152c64b7e\LanguageList Value: en-US\0en0	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 Val ue: None	1660	700
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, 0.0.0.0:49427, 128) Return: 0	1660	700
Detection	Threat Characteristic: Listens on port 0.0.0.0:49427		
Call System API	API Name: ConnectEx Args: (bfc, 81.198.165.201:80, 16, 0, 0, 0, 8a2c850) Return: 0	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: bd0	1660	700
Call Network API	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\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctld l.windowsupdate.com\r\n\r\n, 1, 287) Return: 0	1660	700
Call Network API	API Name: socket Args: (2, 1, 6) Return: bd0	1660	700
Call Network API	API Name: bind Args: (bd0, 0.0.0.0:49428, 128) Return: 0	1660	700
Detection	Threat Characteristic: Listens on port 0.0.0.0:49428		
Call System API	API Name: ConnectEx Args: (bd0, 81.198.165.201:80, 16, 0, 0, 0, 8a2bf90) Return: 0	1660	700
Call Network API	API Name: send Args: (bd0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e0e817717432daa8 HTTP/1.1\r\nConnection: Keep-Alive\r\n nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ct ldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (9520e10) Return: 1	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (951f290) Return: 1	1660	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: None	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: None	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, 0.0.0.0:49429, 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/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2lBkPpolEVRE6gHicnAQUM%2BIHV2ccHsBqBt5ZJot39wZhi4CDQHjLqjhYqpgSVpULg%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.pki.goog\r\n\r\n, 1, 231) 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 /gts1o1core/MFlwUDBOMEwwSjAJBgUrDgMCGGUABBRcRjDCJxbn3nDwj%2Fxz5aZTzgXvAQUMNH4bhDrz5vsYJ8YkBug630J%2FSsCEQCw80IEZ3xvjQUAAAAAh8vC HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.pki.goog\r\n\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, , 441, a6ff248, , 0, , 833, 175108924, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (94c8050, , 215, a6ff248, , 0, , 363, 175108924, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (94c8050, , 103, a6ff248, , 0, , 119, 175108924, 0) Return: 0	1660	700
Call System 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_mh0O6tKw.woff, , , 136552432, 12582912, 156407000) Return: cc0014	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
Call System API	API Name: DnsQueryEx Args: (fonts.gstatic.com, 1, 40006000) Return: 87	1660	700
Call System API	API Name: DnsQueryEx Args: (fonts.gstatic.com, 1c, 40026000) Return: 0	1660	700
Call Network API	API Name: socket Args: (23, 2, 0) Return: 65c	1660	700
Call Network API	API Name: socket Args: (2, 1, 6) Return: 7e0	1660	700
Call Network API	API Name: bind Args: (7e0, 0.0.0.0:49430, 16) Return: 0	1660	700

Detection	Threat Characteristic: Listens on port 0.0.0.0:49430		
Call System API	API Name: ConnectEx Args: (7e0, 216.58.207.195:443, 16, 0, 0, 0, 8bb130c) Return: 0	1660	700
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
Detection	Threat Characteristic: Listens on port 0.0.0.0:49431		
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
Call Network API	API Name: send Args: (65c, ..., 1, 212) Return: 0	1660	700
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{00000000-0000-0000-0000-000000000000} Value: None		1660
Call Network API	API Name: socket Args: (23, 1, 6) Return: bd4	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (8a3cb50) Return: 1	1660	700
Call Network API	API Name: send Args: (b00, GET /gls/1o1core/MFEwTzBNMEswStAJBgUrDgMCGgUABBRcRjDCJxbn3nDwj%2Fxz5aZlZjgXvAQUmNH4bhDrz5vsYJ8YkBu g630J%2FSsCEBOW%2FX18SvRyAwAAAAADMD0E%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocs.pki.google/r/n/r/n, 1, 245) Return: 0	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (8a33238) Return: 1	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (94becf8) Return: 1	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (8bb3b50) Return: 1	1660	700
Call Network API	API Name: send Args: (7e0, ..., 1, 126) Return: 0	1660	700
Call Network API	API Name: send Args: (65c, ..., 1, 126) Return: 0	1660	700
Call System API	API Name: WinHttpCloseHandle Args: (8bb3e60) Return: 1	1660	700
Call Network API	API Name: send Args: (7e0, ..., 1, 87) Return: 0	1660	700
Call Network API	API Name: send Args: (7e0, ..., 1, 166) Return: 0	1660	700
Call Network API	API Name: send Args: (7e0, ..., 1, 82) Return: 0	1660	700
Call Network API	API Name: send Args: (65c, ..., 1, 87) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 40, a05f1d0, , 0, , 56, 168162236, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 9, a05f1d0, , 0, , 32755, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 338, a05f1d0, , 0, , 32717, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 32350, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ¶mÛ, 1389, a05f1d0, , 0, ¶mÛ, 30932, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 29514, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ±H, 1389, a05f1d0, , 0, ±H, 28096, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, cÄL, 1389, a05f1d0, , 0, cÄL, 26678, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, >ù...¿Úv¶)×¼â, 1389, a05f1d0, , 0, >ù...¿Úv¶)×¼â, 25260, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, úxÔÛÉ, 1389, a05f1d0, , 0, úxÔÛÉ, 23842, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ¯, 1389, a05f1d0, , 0, ¯, 22424, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, Øa, 1389, a05f1d0, , 0, Øa, 21006, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, : PÄ, 1389, a05f1d0, , 0, : PÄ, 19588, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , ™™Žġ, 1389, a05f1d0, , 0, , ™™Žġ, 18170, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, r~ÖĖĭ, 1389, a05f1d0, , 0, r~ÖĖĭ, 16752, 168161988, 0) Return: 0	1660	700
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: BCryptDecrypt Args: (95f7a60, ääYÜMEò, 1389, a05f1d0, , 0, ääYÜMEò, 13916, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ¿'Ø, 1389, a05f1d0, , 0, ¿'Ø, 12498, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, Ê, 1389, a05f1d0, , 0, Ê, 11080, 168161988, 0) Return: 0	1660	700
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: BCryptDecrypt Args: (95f7a60, xL—h*+T¿gŠ'k;·n, 1389, a05f1d0, , 0, xL—h*+T¿gŠ'k;·n, , 8244, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, AšI~Vâ ÝEy, 1389, a05f1d0, , 0, AšI~Vâ ÝEy, 6826, 168161988, 0) Return: 0	1660	700
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: (95f7a60, , 1389, a05f1d0, , 0, , 3990, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, Nè11Ä, 1389, a05f1d0, , 0, Nè11Ä, 2572, 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, ä¼Ä/ġšNüOâE, 839, a05f1d0, , 0, ä¼Ä/ġšNüOâE, 32755, 168161988, 0) Return: 0	1660	700
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, tZ,, 1389, a05f1d0, , 0, tZ,, 30469, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 29051, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, f@'T)lO, 1389, a05f1d0, , 0, f@'T)lO, 27633, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, öŠ™, 1389, a05f1d0, , 0, öŠ™, 26215, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ¶ĭĭ.yu_â-èj5-%ö*Ö*âÉ?iöU¶ĭ5Ä×e+TEÁ'Á'1'ŽpÖ_Q, 1389, a05f1d0, , 0, ¶ĭĭ.yu_â-èj5-%ö*Ö*âÉ?iöU¶ĭ5Ä×e+TEÁ'Á'1'ŽpÖ_Q, 24797, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, z±š/š.ĭæ~\ĭ Ô ¶ĭÖyúq, 1389, a05f1d0, , 0, z±š/š.ĭæ~\ĭ Ô ¶ĭÖyúq, 23379, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ºÿyGM'±™äUÉtäü:G, 1389, a05f1d0, , 0, ºÿyGM'±™äUÉtäü:G, 21961, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, @7 »y¼-4#·Bâ4p, 1389, a05f1d0, , 0, @7 »y¼-4#·Bâ4p, 20543, 168161988, 0) Return: 0	1660	700
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, öĭp\$ÖYÑÖ, 1389, a05f1d0, , 0, öĭp\$ÖYÑÖ, 16289, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ŽĭlÖQ'±Lš, 1389, a05f1d0, , 0, ŽĭlÖQ'±Lš, 14871, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, 'Nš\$^*2«*DjZ)©~Zĭ; , 1389, a05f1d0, , 0, 'Nš\$^*2«*DjZ)©~Zĭ; , 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, JuÄ57wSœĭ, ®, 366, a05f1d0, , 0, JuÄ57wSœĭ, ®, 9199, 168161988, 0) Return: 0	1660	700
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, , 1389, a05f1d0, , 0, , 8624, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, \$àHNÜ8ÿ^sZÊ^y2ð, 1389, a05f1d0, , 0, \$àHNÜ8ÿ^sZÊ^y2ð, 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
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, .L^Ä, 1389, a05f1d0, , 0, .L^Ä, 1534, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, %všÖd, 1389, a05f1d0, , 0, %všÖd, 1405, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, Fwð, 1389, a05f1d0, , 0, Fwð, 32755, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, 2úàSÚÍÄ, 1389, a05f1d0, , 0, 2úàSÚÍÄ, 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, è ×àQ#†Cà, 1389, a05f1d0, , 0, è ×àQ#†Cà, 27083, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, à@.>ÊŠÿ~ò8è, 1389, a05f1d0, , 0, à@.>ÊŠÿ~ò8è, 25665, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ôjîlSëèi, 1389, a05f1d0, , 0, ôjîlSëèi, 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, ÊpÊ=el, 1389, a05f1d0, , 0, ÊpÊ=el, 19993, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, /Ü_c°Ê^´†jÊ1Ü:¶×àªqðUnd?ewÊFÊ, 1389, a05f1d0, , 0, /Ü_c°Ê^´†jÊ1Ü:¶×àªqðUnd?ewÊFÊ, 18575, 168161988, 0) Return: 0	1660	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: (95f7a60, , 1389, a05f1d0, , 0, , 12903, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, /Æ, 1389, a05f1d0, , 0, /Æ, 11485, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, NcsðÄð3é—ÖP, 839, a05f1d0, , 0, NcsðÄð3é—ÖP, 10067, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, , 1389, a05f1d0, , 0, , 9199, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, ä0žYUğ¿l¼QÊt7+, 1389, a05f1d0, , 0, ä0žYUğ¿l¼QÊt7+, 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, ¥ãÑð%°"ÿyù", 1389, a05f1d0, , 0, ¥ãÑð%°"ÿyù", 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, ÇalıGÿ +)<3¿@wKıf^jSVØªð, 1389, a05f1d0, , 0, ÇalıGÿ +)<3¿@wKıf^jSVØªð, 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-lr8-u†däèEkÇ-ø<ž¶îlšó—/°"ü, 1389, a05f1d0, , 0, Ö-lr8-u†däèEkÇ-ø<ž¶îlšó—/°"ü, 12521, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, "ð=ðHçQc.fèÑZNªYã¥0ÊM4jPW,"czæ,...l†", 1389, a05f1d0, , 0, "ð=ðHçQc.fèÑZNªYã¥0ÊM4jPW,"czæ,...l†", 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"eÖNXİÖ:½ÜJ]"œi"m", 1389, a05f1d0, , 0, 3%ñ"eÖNXİÖ:½ÜJ]"œi"m", 6849, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, İÖ", 1389, a05f1d0, , 0, İÖ", 5431, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, "j4bæ^¿šð, 1389, a05f1d0, , 0, "j4bæ^¿šð, 4013, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, +ÿÖØÇ:ÖG, 1389, a05f1d0, , 0, +ÿÖØÇ:ÖG, 2595, 168161988, 0) Return: 0	1660	700
Call System API	API Name: BCryptDecrypt Args: (95f7a60, -PBQmRøSÛTrU:UÊUÊVSW=X, 1161, a05f1d0, , 0, -PBQmRøSÛTrU:UÊUÊVSW=X, 1177, 168161988, 0) Return: 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: (7e0, ..., 1, 46) Return: 0	1660	700
Call Network API	API Name: send Args: (65c, ..., 1, 38) Return: 0	1660	700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en10	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\rundll32.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\SQL\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: bind Args: (7d4, 0.0.0.0:49432, 128) Return: 0		1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49432		
Call System API	API Name: ConnectEx Args: (7d4, 65.55.252.93:443, 16, 0, 0, 0, a57254c8) Return: 0		1660
Call Internet Helper API	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 System API	API Name: DnsQueryEx Args: (ieonline.microsoft.com, 1, 50020000) Return: 0		1660
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ieonline.microsoft.com, 443, , , 3, 8388608, -1519158432) Return: cc0008		1660

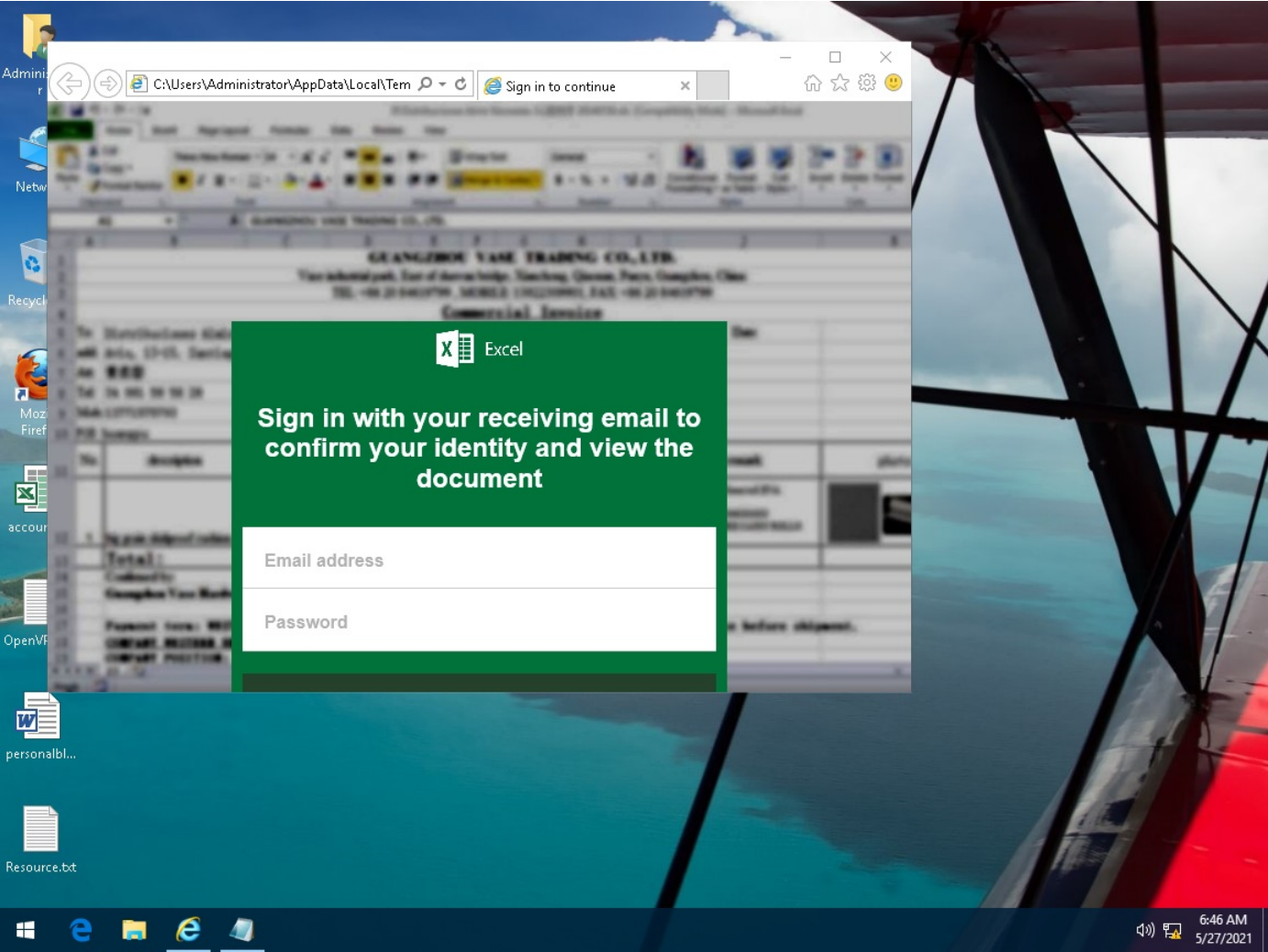
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ieflipahead/ie10/rules.xml?mkt=en-US, , , -1558919568, 12582928, -1519158432) Return: cc000c		1660
Call Network API	API Name: socket Args: (2, 2, 0) Return: 8c4		1660
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8c4		1660
Call System API	API Name: DnsQueryEx Args: (leonline.microsoft.com, 1c, 40026000) Return: 0		1660
Call System API	API Name: DnsQueryEx Args: (leonline.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, 0.0.0.0:49433, 16) Return: 0		1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49433		
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, 0.0.0.0:49434, 16) Return: 0		1660
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, /IE11/1426178821/iecompatviewlist.xml, , , -1554595984, 12582928, -1519566688) Return: cc0014		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\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: (iecvlist.microsoft.com, 1, 40006000) 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	API Name: send Args: (bf4, ..., 1, 217) Return: 0		1660
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 0.0.0.0:49437		
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%2FnYB45SPUEwQU5Z1ZMJJHW/Mys%2BghUNoZ7OrUETfACEA8Ull8glGmZT9XhRrHlJQel%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.digicert.com\r\n\r\n\r\n, 1, 236) Return: 0		1660
Call System API	API Name: WinHttpCloseHandle Args: (a583f300) 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
Call System API	API Name: BCryptDecrypt Args: (a57dd0e0, , 40, a6ade6f0, , 0, , 56, -1498552300, 0) Return: 0		1660
Call Network API	API Name: send Args: (8c4, ..., 1, 38) Return: 0		1660
Call Network API	API Name: send Args: (8d8,, 1, 291) Return: 0		1660
Call Network API	API Name: send Args: (8d8, ..., 1, 38) Return: 0		1660
Call System API	API Name: BCryptDecrypt Args: (a57dd0e0, , 9, a346ef00, , 0, , 25, -1555632092, 0) Return: 0		1660
Call System API	API Name: WinHttpCloseHandle Args: (a57c8610) Return: 1		1660
Call Network API	API Name: send Args: (be0, GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn1Rh6Doh%2FsBygFv7gQUA95QNVbRTLtm8KPIGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ocsp.digicert.com\r\n\r\n\r\n, 1, 236) Return: 0		1660
Call System API	API Name: WinHttpCloseHandle Args: (a5854a50) Return: 1		1660

Call System API	API Name: WinHttpCloseHandle Args: (a57d1e30) Return: 1		1660
Call System API	API Name: WinHttpCloseHandle Args: (a58345a0) 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: (bf4, ..., 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: (cc0008, GET, /fwlink?LinkId=401135, , , -1558919568, 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: DnsQueryEx Args: (go.microsoft.com, 1c, 40026000) 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 0.0.0.0:49438		
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 /fwlink?LinkId=401135 HTTP/1.1\r\nAccept: */*\r\nUA-CPU: AMD64\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 [Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0] like Gecko\r\nHost: go.microsoft.com\r\nConnection: Keep-Alive\r\nCookie: SRCHD=AF=NOFORM; SRCHUID=V=2&GUID=3A2A988979454AA08EBDB710B96ADCC2&dmnchg=1; SRCHUSR=DOB=20191114; _ga=GA1.2.1718225526.1573749281; _EDGE_S=F=1&SID=2229018C53806F7F237511C852A86E0B&mkt=en-us; _EDGE_V=1; SRCHHPGUSR=SRCHLANGV2=en; _SS=SID=2229018C53806F7F237511C852A86E0B\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\11CE4E0A4FD3CD25F064BE57BB2A9DE7238231CC Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739F Value: None		1660
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739F Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739FBlob Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\HistoryJournal\Certificate\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		
Call System API	API Name: ConnectEx Args: (2d4, 152.199.19.161:443, 16, 0, 0, 0, a581f4a8) Return: 0		1660
Call Network API	API Name: send Args: (2d4,b., 1, 359) Return: 0		1660
Call Network API	API Name: send Args: (2d4, ..., 1, 126) Return: 0		1660
Call Network API	API Name: send Args: (2d4, ...,1, 1, 550) Return: 0		1660

Call System API	API Name: BcryptDecrypt Args: (a57377e0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 675\r\nCache-Control: max-age=3600\r\nDate: Thu , 27 May 2021 11:56:29 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F6AB)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: bf9c4e70-801e-00de-03ed-52bdab000000\r\nx-ms-version: 2009-09-19\r\n\r\nJ\r\nuøæ, 375, a314ef20, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 675\r\nCache-Control: max-age=3600\r\nDate: Thu, 27 May 2021 11:56:29 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F6AB)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: bf9c4e70-801e-00de-03ed-52bdab000000\r\nx-ms-version: 2009-09-19\r\n\r\nJ\r\nruøæ, 391, -1558908860, 0) Return: 0		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, 0.0.0.0:49441, 128) Return: 0		1660
Detection	Threat Characteristic: Listens on port 0.0.0.0:49441		
Call System API	API Name: ConnectEx Args: (7b0, 65.55.252.93:443, 16, 0, 0, 0, a56d0a88) Return: 0		1660
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 0.0.0.0:49442		
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 , 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: HIT\r\nx-ms-blob-type: 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\nJ\r\nr\r\n\r\nJ\r\n376, 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 11:56:33 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F771)\r\nX-Cache: HIT\r\nx-ms-blob-type: 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\nJ\r\nr\r\n\r\nJ\r\n392, 175108924, 0) Return: 0	1660	700
Call Network API	API Name: recv Args: (c40, , 1, 2) Return: ?	1660	700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: e61bb8d4	1660	700
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d752ed	1660	700
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, -1518497984) Return: cc0008		1660
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1554595984, 12582928, -1518497984) 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
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\IMFV Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None		1660
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None		1660
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\IMFV Value: None		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, -1518497984) Return: cc0008		1660
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1558919760, 12582928, -1518497984) 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 System API	API Name: WinHttpCloseHandle Args: (a58314c0) Return: 1		1660
Call System API	API Name: WinHttpCloseHandle Args: (a57c8a50) Return: 1		1660
Call System API	API Name: WinHttpCloseHandle Args: (a57d3280) Return: 1		1660
Call Filesystem API	API Name: DeleteFileW Args: () Return: 0		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, -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

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: VSDT_WINWORD	1660
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0FA7F1DA-BEE1-11EB-9BF2-001F3C8C8DBB}.dat Type: VSDT_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



CentOS w Docker

▼

Environment-specific risk level	Unrated	Virtual Analyzer does not support the file format, or the file is empty.
Detections	-	
Exploited vulnerabilities	-	
Network connection	Custom	


▼ Object 1 - Hawb.html (HTML File)


File name	Hawb.html
File type	HTML File
SHA-1	F7911D858AFCCB9E871595374564EFE2D6449377
SHA-256	FEAD8882737862D95646BBF95620D9D46F29995FECB6A65ADE671F9761B42E99
MD5	DEE4CFA9FB0A28C29485245440EF3D50
Size	186357 byte(s)


Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-


Process Graph Legend


Node

Submitted sample

Root process

Child process


Direct event


Indirect event


Created

Event actions


Notable Threat Characteristics


Anti-security, self-preservation


Autostart or other system reconfiguration


Deception, social engineering


File drop, download, sharing, or replication

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