Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-25 09:35:40
Submitter	Manual Submission
Type	XHTML File

Analysis Overview

Overall risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.		
Detections	VAN_DROPPER.UMXX, VAN_BACKDOOR.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	XHTML File	1 - Последнее предупреждение! - P3wQiT54SuP8.xhtml	106BEE5F5E76127310B679819EEEC4619C8DACA1

Analysis Environments

	w2008	CentOS	W10
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	✓		✓

w2008

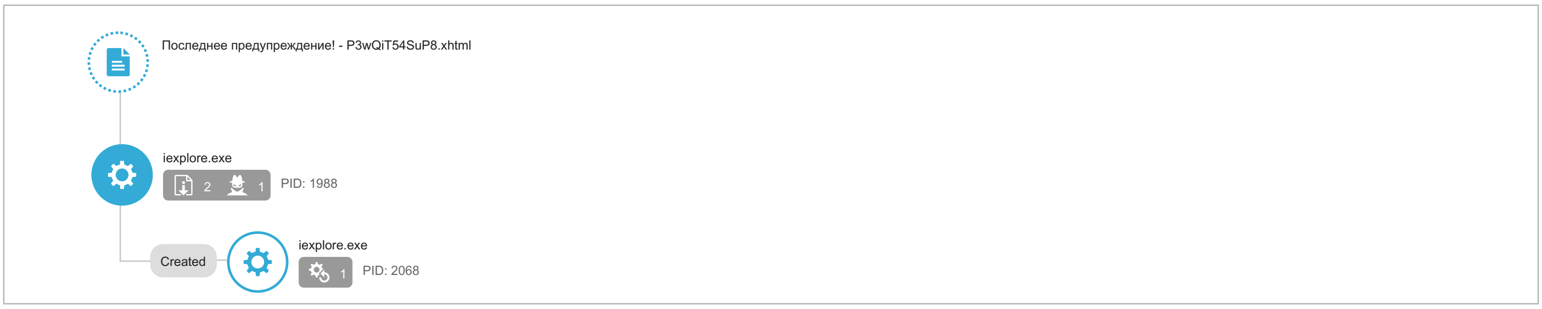
Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Последнее предупреждение! - P3wQiT54SuP8.xhtml (XHTML File)

File name	Последнее предупреждение! - P3wQiT54SuP8.xhtml
File type	XHTML File
SHA-1	106BEE5F5E76127310B679819EEEC4619C8DACA1
SHA-256	392C544E11CB6F9B3DB916B3F042F346ADF65E6EF3FC5D5D0F49CAB34AC065C2
MD5	D3EF37CCCDD95B68B1821D0A3EF0BF80
Size	28821 byte(s)

Risk Level	Low risk
Detection	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (1) File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (3) Suspicious network or messaging activity (2)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Defense Evasion	File Deletion	🟥⬜⬜ Characteristics: 1, 2
Discovery	Network Share Discovery	🟥⬜⬜ Characteristics: 1

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to evade detection and analysis	🟥⬜⬜	Process ID: 2592 Info: Delays execution

Autostart or other system reconfiguration (1)

Characteristic	Significance	Details
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Feeds\FeedsStore.feedsdb-ms

File drop, download, sharing, or replication (2)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Feeds Cache\JLMXRMXX\ieonlinews.microsoft[1] Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms Type: VSDT_WINWORD

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 1988 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Web content contains suspicious URL	🟥⬜⬜	URL: https://manyrub.ru/PTjbrFBk#92115220640823108121770636128401306135502956437546 Threat Name: FRAUD_SCAM.WRS

Process, service, or memory object change (3)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2592 Image Path: %ProgramFiles(x86)%\Microsoft Office\Office12\Wordconv.exe -Embedding
Creates process	🟥⬜⬜	Process ID: 2528 Image Path: %ProgramFiles(x86)%\Microsoft Office\OFFICE11\WINWORD.EXE /n /dde
Creates process	🟥⬜⬜	Process ID: 2068 Image Path: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe SCODEF:1988 CREDAT:79873

Suspicious network or messaging activity (2)

Characteristic	Significance	Details
Listens on port	🟥⬜⬜	0.0.0.0:49177
Listens on port	🟥⬜⬜	127.0.0.1:60392

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ie9cvlist.ie.microsoft.com	152.199.19.161	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ie9cvlist.ie.microsoft.com	152.199.19.161	80	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml

URL	Site Category	Risk Level	Threat	Accessed By
http://ie9cvlist.ie.microsoft.com/IE9CompatViewList.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~DF0426DE8C41032D67.TMP	No risk	-	-	-	36864	9D6A85F0428A16B69274AC4759B20DDF75B45B2A
~DFBB1D80680542C6F3.TMP	No risk	-	-	-	7680	502BE5F60483077B70D409F6B8EFA2CB46C19049
{4AEF97EA-356A-11EC-80F3-080027A1DA7A}.dat	No risk	-	-	-	3584	F96F4F26F83462A81AF970F97885E80202E3EEDB
~DFA7D6C686021BA110.TMP	No risk	-	-	-	7680	2A4AAB3483286B816135893501F314CB27199EAC
~DFB6174CC13ABD0B66.TMP	No risk	-	-	-	7680	6B9B90FBDC73DF90E2DEF9D83276E86D792AA9ED
RecoveryStore.{4AEF97E9-356A-11EC-80F3-080027A1DA7A}.dat	No risk	-	-	-	4608	626A9C45E38764622B5F1ED14903711B69F8B043
~DFA488CED0A84EDB1E.TMP	No risk	-	-	-	7680	664147DBADD7F997FF90790541DCCE1C218520A0
~DF23F0AAC03E16C683.TMP	No risk	-	-	-	36864	9D6A85F0428A16B69274AC4759B20DDF75B45B2A
FeedsStore.feedsdb-ms	No risk	-	-	-	7680	502BE5F60483077B70D409F6B8EFA2CB46C19049
~DF32271C1326387BF0.TMP	No risk	-	-	-	512	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5

▼ Analysis

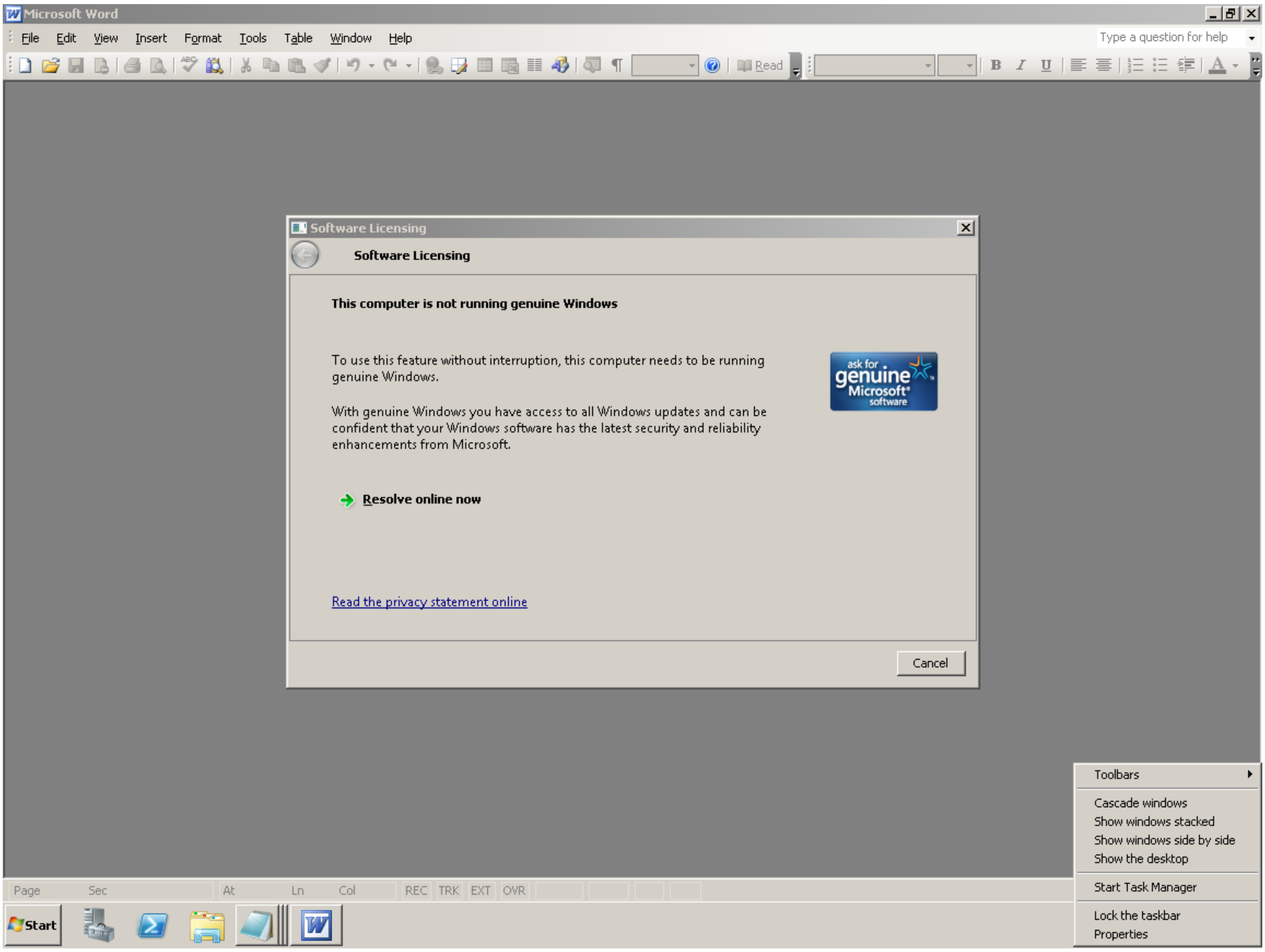
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Web content contains suspicious URL URL: https://manyrub.ru/PTjbrFBk#92115220640823108121770636128401306135502956437546 Threat Name: FRAUD_SCAM.WRS		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags Value: 0		1988
Call Service API	API Name: OpenServiceA Args: (b00220, rasman, 4) Return: affd20		1988
Call Service API	API Name: OpenServiceW Args: (b20698, Sens, 4) Return: b20e18		1988
Call Service API	API Name: OpenServiceA Args: (b00220, RASMAN, 4) Return: afff00		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1988
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		1988
Call Network API	API Name: socket Args: (23, 1, 6) Return: 40c		1988
Call Network API	API Name: socket Args: (23, 1, 6) Return: 40c		1988
Call Network API	API Name: socket Args: (2, 2, 0) Return: 430		1988
Call Network API	API Name: socket Args: (23, 2, 0) Return: 430		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Recovery\AdminActive\{4AEF97E9-356A-11EC-80F3-080027A1DA7A} Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not installed		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\SecuritySafe Value: 1		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FullScreen Value: no		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window_Placement Value: None		1988
Call Process API	API Name: CreateProcessW Args: (, "%ProgramFiles(x86)%\Internet Explorer\iexplore.exe" SCODEF:1988 CREDAT:79873, , , , CREATE_SUSPENDED, , , , Process:2068:%ProgramFiles(x86)%\Internet Explorer\iexplore.exe) Return: 1		1988
Call Thread API	API Name: NtResumeThread Args: (Process:2068,) Return: ?		1988
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2068], ppid[1988) Return: 1		1988
Detection	Threat Characteristic: Creates process Process ID: 2068 Image Path: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe SCODEF:1988 CREDAT:79873		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 420		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None		1988
Call Service API	API Name: OpenServiceW Args: (80a638, FontCache, 14) Return: 80abd8	1988	2068
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2128], ppid[2068) Return: 1	1988	2068
Call Service API	API Name: StartServiceW Args: (80abd8, 0, 0) Return: 1	1988	2068
Call Service API	API Name: StartServiceW Args: (80abd8, 0, 0) Return: 1	1988	2068
Call Mutex API	API Name: CreateMutexW Args: (0, 0, SmartScreen_AppRepSettings_Mutex) Return: 3cc	1988	2068
Call Mutex API	API Name: CreateMutexW Args: (0, 0, SmartScreen_ClientId_Mutex) Return: 234	1988	2068
Call Mutex API	API Name: CreateMutexW Args: (0, 0, CommunicationManager_Mutex) Return: 3e0	1988	2068
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not installed	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3c4f544) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3c4f4d4) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3c4f4d4) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3c4f4d4) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3add3f4) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3add384) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3add384) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3add384) Return: 0	1988	2068
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 3add444) Return: 0	1988	2068
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6ffb0250, -1, 60b198, 60b194, 0) Return: 0		1988
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1988 Info: Enums share folder from API result		

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Suggested Sites\ObjectsCreated Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Suggested Sites\ObjectsCreated_TIMESTAMP Value: None		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Suggested Sites\DeletePending Value: 1		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not installed		1988
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms) Return: 1		1988
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms) Return: 1		1988
Delete File	Path: %LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms Type: VSDT_WINWORD		1988
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\Internet Explorer Suggested Sites~.feed-ms Type: VSDT_WINWORD		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Feeds Cache\JLMXRMXX\ieonlinews.microsoft[1] Type: VSDT_EMPTY		1988
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1988 File: %LOCALAPPDATA%\Microsoft\Feeds Cache\JLMXRMXX\ieonlinews.microsoft[1] Type: VSDT_EMPTY		
Write File	Path: %LOCALAPPDATA%\Microsoft\Feeds\FeedsStore.feedsdb-ms Type: VSDT_WINWORD		1988
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Feeds\FeedsStore.feedsdb-ms		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Suggested Sites\SlicePath Value: None		1988
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (4b3df3c, 0, 0, 0) Return: 1		1988
Call Network API	API Name: socket Args: (2, 2, 17) Return: 684		1988
Call Network API	API Name: bind Args: (684, 127.0.0.1:60392, 16) Return: 0		1988
Detection	Threat Characteristic: Listens on port 127.0.0.1:60392		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0), 0, , , 10000000) Return: cc0004		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72944928) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895920, 4194320, 72944928) Return: cc000c		1988
Call Network API	API Name: socket Args: (2, 2, 0) Return: 6bc		1988
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6bc		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 40006000) Return: 9701		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1c, 40006000) Return: 0		1988
Call Network API	API Name: socket Args: (23, 2, 0) Return: 6bc		1988
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6bc		1988
Call Network API	API Name: bind Args: (6bc, 0.0.0.0:49177, 16) Return: 0		1988
Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (6bc, 152.199.19.161:80, 16) Return: ffffffff		1988
Call Network API	API Name: recv Args: (684, , 32, 0) Return: ?		1988
Call Network API	API Name: send Args: (684, !, 1, 0) Return: 1		1988
Call Network API	API Name: send Args: (6bc, 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; WOW64; Trident/5.0]\r\nHost: ie9cvlist.ie.microsoft.com\r\nConnection: Keep-Alive\r\nCookie: _EDGE_V=1\r\n\r\n, 245, 0) Return: 245		1988
Call Network API	API Name: recv Args: (6bc, , 1024, 0) Return: ?		1988
Call Network API	API Name: send Args: (684, !, 1, 0) Return: 1		1988
Call Network API	API Name: recv Args: (684, , 32, 0) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1024, 0) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 8192, 0) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 4964, 0) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml Type: VSDT_TEXT_HTML		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_EMPTY		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\VersionHigh Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\VersionLow Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\DXFeatureLevel Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VendorId Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DeviceId Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-SubSysId Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-Revision Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionHigh Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-VersionLow Value: 0		1988
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\GPU\Wow64-DXFeatureLevel Value: 0		1988
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 4b3df50) Return: 0		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72944928) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895924, 4194320, 72944928) Return: cc000c		1988

Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72532528) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895924, 4194320, 72532528) Return: cc000c		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72532528) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895924, 4194320, 72532528) Return: cc000c		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72532528) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895924, 4194320, 72532528) Return: cc000c		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Call System API	API Name: DnsQueryExW Args: (ie9cvlist.ie.microsoft.com, 1, 50000000) Return: 0		1988
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ie9cvlist.ie.microsoft.com, 80, , , 3, 0, 72532528) Return: cc0008		1988
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE9CompatViewList.xml, , , 78895924, 4194320, 72532528) Return: cc000c		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		1988
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\IE9CompatViewList[1].xml, %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml, 0, 0, 0, 0) Return: 1		1988
Call Network API	API Name: recv Args: (6bc, , 1, 2) Return: ?		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AEF97E9-356A-11EC-80F3-080027A1DA7A}.dat Type: VSDT_WINWORD		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{4AEF97E9-356A-11EC-80F3-080027A1DA7A}.dat Type: VSDT_WINWORD		1988
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{4AEF97EA-356A-11EC-80F3-080027A1DA7A}.dat Type: VSDT_WINWORD		1988
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{4AEF97EA-356A-11EC-80F3-080027A1DA7A}.dat Type: VSDT_WINWORD		1988
Detection	Threat Characteristic: Creates process Process ID: 2528 Image Path: %ProgramFiles(x86)%\Microsoft Office\OFFICE11\WINWORD.EXE /n /dde		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		2528
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTT Value: None		2528
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		2528
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		2528
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2528
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		2528
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		2528
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.dat, 0, 0, 0, 1) Return: 0		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\{90110409-6000-11D3-8CFE-0150048383C9} Value: None		2528
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		2528
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000630D11C8EF10054038389C\Usage\WORDFiles Value: 5359000b		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\90401109000630D11C8EF10054038389C\Usage\ProductFiles Value: 53590007		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WordConverter12Files Value: 53590001		2528
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%ProgramFiles(x86)%\Microsoft Office\Office12\Wordconv.exe) Return: 1		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WordConverter12Files Value: 53590002		2528
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2528) Return: 1		2528
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\Program) Return: 1		2528
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2528) Return: 1		2528

Detection	Threat Characteristic: Creates process Process ID: 2592 Image Path: %ProgramFiles(x86)%\Microsoft Office\Office12\Wordconv.exe -Embedding		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2528	2592
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2528	2592
Detection	Threat Characteristic: Attempts to evade detection and analysis Process ID: 2592 Info: Delays execution		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WordConverter12Files Value: 53590003	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5359000e	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\TCWP5FilesIntl_1033 Value: 53590001	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\TCWP6FilesIntl_1033 Value: 53590001	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\TCWP5FilesIntl_1033 Value: 53590002	2528	2592
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FEC\Usage\TCWP6FilesIntl_1033 Value: 53590002	2528	2592
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	2528	2592
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	2528	2592
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 44	2528	2592
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 44	2528	2592
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None	2528	2592
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$edsStore.feedsdb-ms.doc) Return: 1		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: 26		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\ProductNonBootFiles Value: 53590002		2528
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\ProductNonBootFiles Value: 53590003		2528
Call Window API	API Name: DialogBoxIndirectParamW Args: (30c90000, 52e320, 201d8, 30e94f68, 1851d0) Return: 6		2528
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		2528
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\BaseSuite\1EBDE4BC9A514630B5412561FA45CCC5 Value: 1		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMSessionCount Value: 2		2528
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Data\Toolbars Value: None		2528

▼ Screenshot



Software Licensing

This computer is not running genuine Windows

To use this feature without interruption, this computer needs to be running genuine Windows.

With genuine Windows you have access to all Windows updates and can be confident that your Windows software has the latest security and reliability enhancements from Microsoft.

Resolve online now

Read the privacy statement online

CentOS

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 - Последнее предупреждение! - P3wQiT54SuP8.xhtml (XHTML File)

File name	Последнее предупреждение! - P3wQiT54SuP8.xhtml
File type	XHTML File
SHA-1	106BEE5F5E76127310B679819EEEC4619C8DACA1
SHA-256	392C544E11CB6F9B3DB916B3F042F346ADF65E6EF3FC5D5D0F49CAB34AC065C2
MD5	D3EF37CCCDD95B68B1821D0A3EF0BF80
Size	28821 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

W10

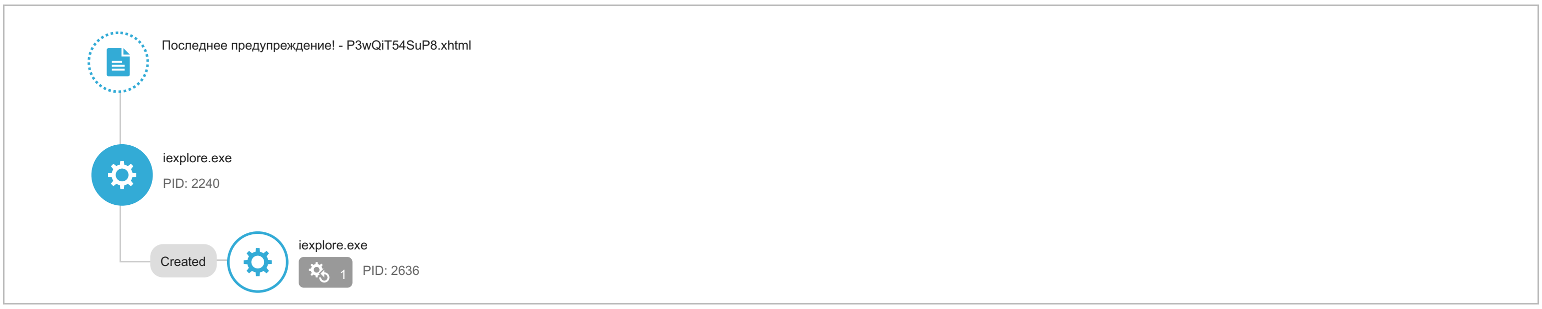
Environment-specific risk level	Low risk The object exhibited mildly suspicious characteristics that are most likely benign.
Detections	VAN_BACKDOOR.UMXX
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Последнее предупреждение! - P3wQiT54SuP8.xhtml (XHTML File)

File name	Последнее предупреждение! - P3wQiT54SuP8.xhtml
File type	XHTML File
SHA-1	106BEE5F5E76127310B679819EEEC4619C8DACA1
SHA-256	392C544E11CB6F9B3DB916B3F042F346ADF65E6EF3FC5D5D0F49CAB34AC065C2
MD5	D3EF37CCCDD95B68B1821D0A3EF0BF80
Size	28821 byte(s)

Risk Level	Low risk
Detection	VAN_BACKDOOR.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1) Suspicious network or messaging activity (16)

Process Graph



Process Graph Legend

Notable Threat Characteristics

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

Characteristic	Significance	Details
Web content contains suspicious URL	🟥⬜⬜	URL: https://manyrub.ru/PTjbrFBk#92115220640823108121770636128401306135502956437546 Threat Name: FRAUD_SCAM.WRS

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2636 Image Path: %ProgramFiles(x86)%\Internet Explorer\IEXPLORE.EXE SCODEF:2240 CREDAT:148481 /prefetch:2

Suspicious network or messaging activity (16)

Characteristic	Significance	Details
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
Listens on port	🟥⬜⬜	0.0.0.0:49424
Listens on port	🟥⬜⬜	0.0.0.0:49423

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
go.microsoft.com	104.75.59.137	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ctldl.windowsupdate.com	178.79.242.128	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ieonline.microsoft.com	204.79.197.200	53	-	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
go.microsoft.com	104.75.59.137	80	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ocsp.digicert.com	93.184.220.29	80	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ctldl.windowsupdate.com	178.79.242.128	80	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
ieonline.microsoft.com	204.79.197.200	443	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
https://iecvlist.microsoft.com/ie11blocklist/1401746408/versionlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
https://iecvlist.microsoft.com/IE11/1426178821/iecompatviewlist.xml	Business / Economy Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b4d985180751389d	Computers / Internet	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9fd483ab01319dee	Computers / Internet	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?768c120b3b904678	Computers / Internet	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://go.microsoft.com/fwlink/?LinkID=401135	Computers / Internet	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%3D	Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1f3e953389c819c7	Computers / Internet	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml
https://ieonline.microsoft.com/ieflipahead/ie10/rules.xml?mkt=en-US	Business / Economy Computers / Internet Cloud Applications	No risk	-	Последнее предупреждение! - P3wQiT54SuP8.xhtml

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
{5F1B7117-356A-11EC-9BF1-001F3C8C8DBB}.dat	No risk	-	-	-	3584	B19DD777CCF43C5D383D3FE1C754970735D81DB3
RecoveryStore.{5F1B7115-356A-11EC-9BF1-001F3C8C8DBB}.dat	No risk	-	-	-	5632	B88D0B0A7F90C0106040A8D532B4F82798F6B2E0
IEInstrumentation2021[1].htm	No risk	-	-	-	2140	C80654A5A50C561D9B0D04D822481C1DD49C58B6
~DF869CACAEEDF0237D.TMP	No risk	-	-	-	16384	8AA6FF6072117F6B45BE8EA925439A24F308FC97
6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442	No risk	-	-	-	446	EFF53368C1DFA3B2168BB3A72D1DFF3B64DB5C33
7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776	No risk	-	-	-	434	5C047BB20B05F8135D35FDA18FE3D79F4E81A335
~DF0819895C170F0EAE.TMP	No risk	-	-	-	16384	83AE328FE5ADD0C27FC4B84820FE6B07BEA8699B
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	No risk	-	-	-	302	4F5ADDB21035E640FC4F54AFCB06B5449B155EA4
6BADA8974A10C4BD62CC921D13E43B18_1DC6D7385EA816C957BA2B715AC5C442	No risk	-	-	-	1507	6EB05BD724F558C0FFF2413A87F63561089FC810
iecompatviewlist[1].xml	No risk	-	-	https://iecvlist.microsoft.com/IE11/1426178821/iecompatviewlist.xml	230440	7F452881B9846A73F445B0CCDDD997E9DFDF58D6

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Web content contains suspicious URL URL: https://manyrub.ru/PTjbrFBk#92115220640823108121770636128401306135502956437546 Threat Name: FRAUD_SCAM.WRS		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SQM\PIDs\PID_2240 Value: 8c0		2240
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3d4		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\CompatibilityFlags Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2240
Call System API	API Name: WinHttpCloseHandle Args: (9c8df840) Return: 1		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{5F1B7115-356A-11EC-9BF1-001F3C8C8DBB} Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\SecuritySafe Value: 1		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\FullScreen Value: no		2240

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Window_Placement Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\PendingRecovery\AdminActive Value: 0		2240
Call Process API	API Name: CreateProcessW Args: (, "%ProgramFiles(x86)%\Internet Explorer\IEXPLORE.EXE" SCODEF:2240 CREDAT:148481 /prefetch:2, , , , CREATE_SUSPENDED, , , , Process:2636:%ProgramFiles(x86)%\Internet Explorer\iexplore.exe) Return: 1		2240
Call Thread API	API Name: NtResumeThread Args: (Process:2636,) Return: ?		2240
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2636], ppid[2240) Return: 1		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{00000000-0000-0000-0000-000000000000} Value: None		2240
Detection	Threat Characteristic: Creates process Process ID: 2636 Image Path: %ProgramFiles(x86)%\Internet Explorer\IEXPLORE.EXE SCODEF:2240 CREDAT:148481 /prefetch:2		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1	2240	2636
Call Network API	API Name: socket Args: (23, 1, 6) Return: 38c	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2240	2636
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2240	2636
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2240	2636
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2240	2636
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2240	2636
Call Service API	API Name: OpenServiceW Args: (51fbd08, WinHttpAutoProxySvc, 94) Return: 51fc078	2240	2636
Call System API	API Name: WinHttpCloseHandle Args: (525e130) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer) Return: 1	2240	2636
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%SystemRoot%\System32\rundll32.exe shell32.dll, SHCreateLocalServerRunDll {9BA05972-F6A8-11CF-A442-00A0C90A8F39}) Return: 1	2240	2636
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2636) Return: 1	2240	2636
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%windir%\System32\rundll32.exe) Return: 1	2240	2636
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2636) Return: 1	2240	2636
Call Filesystem API	API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\iconcache) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\frameiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\tabiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%USERPROFILE%\AppData\LocalLow\Microsoft\Internet Explorer\tabiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\largeiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\immersiveiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\imdockediconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\imtilelargeiconcache.dat) Return: 0		2240
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Internet Explorer\imtilesmalliconcache.dat) Return: 0		2240
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2240	2636
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2240	2636
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 522c04c) Return: 0	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0	2240	2636
Call Service API	API Name: OpenServiceW Args: (87d9320, WSearch, 1) Return: 87d92f8	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version Value: WS not running	2240	2636
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 522c04c) Return: 0	2240	2636
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (9d44f588, 0, 0, 0) Return: 1		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\SQM\BadProcCount Value: 0		2240
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		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca36e40) Return: 1		2240
Call Network API	API Name: socket Args: (23, 1, 6) Return: 8a4		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: 904		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 904		2240
Call System API	API Name: DnsQueryEx Args: (sqm.telemetry.microsoft.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ieonline.microsoft.com, 1, 50020000) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (sqm.telemetry.microsoft.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 8ec		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 8ec		2240
Call Network API	API Name: bind Args: (8ec, 0.0.0.0:49423, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49423		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, ieonline.microsoft.com, 443, , , 3, 8388608, -1667130240) Return: cc0008		2240
Call System API	API Name: ConnectEx Args: (8ec, 65.55.252.93:443, 16, 0, 0, 0, 9c9c1118) Return: 0		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ieflipahead/ie10/rules.xml?mkt=en-US, , , -1668628128, 12582928, -1667130240) Return: cc000c		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: 920		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 920		2240
Call System API	API Name: DnsQueryEx Args: (ieonline.microsoft.com, 1c, 40026000) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (ieonline.microsoft.com, 1, 40006000) Return: 87		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 92c		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 920		2240
Call Network API	API Name: bind Args: (920, 0.0.0.0:49424, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (920, 204.79.197.200:443, 16, 0, 0, 0, 9ca8c938) Return: 0		2240

Call Network API	API Name: socket Args: (2, 1, 6) Return: 92c		2240
Call Network API	API Name: bind Args: (92c, 0.0.0.0:49425, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (92c, 204.79.197.200:443, 16, 0, 0, 0, 9ca8c778) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1666987584) Return: cc0010		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0010, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1665481840, 12582928, -1666987584) Return: cc0014		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: 998		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1c, 40026000) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 40006000) Return: 87		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a8		2240
Call Network API	API Name: bind Args: (9a8, 0.0.0.0:49426, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49426		
Call System API	API Name: ConnectEx Args: (9a8, 152.199.19.161:443, 16, 0, 0, 0, 9ca8c7e8) Return: 0		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9ac		2240
Call Network API	API Name: bind Args: (9ac, 0.0.0.0:49427, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49427		
Call System API	API Name: ConnectEx Args: (9ac, 152.199.19.161:443, 16, 0, 0, 0, 9ca8ca18) Return: 0		2240
Call Network API	API Name: send Args: (92c, ..., 1, 217) Return: 0		2240
Call Network API	API Name: send Args: (9ac, ..., 1, 217) Return: 0		2240
Call Network API	API Name: send Args: (920, ..., 1, 217) Return: 0		2240
Call Network API	API Name: send Args: (9a8, ..., 1, 217) Return: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0		2240
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2240
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2240
Call Network API	API Name: socket Args: (23, 1, 6) Return: c08		2240
Call System API	API Name: WinHttpCloseHandle Args: (a023ab30) Return: 1		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: ccc		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: ccc		2240
Call System API	API Name: WinHttpCloseHandle Args: (a017b1d0) Return: 1		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2240
Call System API	API Name: WinHttpCloseHandle Args: (a01b2e00) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a01b5520) Return: 1		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: cb8		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cb8		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: cf8		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cf8		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: d00		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: d00		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cd0		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: cd0		2240
Call Network API	API Name: bind Args: (cd0, 0.0.0.0:49428, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49428		
Call System API	API Name: ConnectEx Args: (cd0, 178.79.242.128:80, 16, 0, 0, 0, 9c9988c8) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cdc		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: cdc		2240
Call Network API	API Name: bind Args: (cdc, 0.0.0.0:49429, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49429		
Call System API	API Name: ConnectEx Args: (cdc, 178.79.242.128:80, 16, 0, 0, 0, 9c998ce8) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cec		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: cec		2240
Call Network API	API Name: bind Args: (cec, 0.0.0.0:49430, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49430		
Call System API	API Name: ConnectEx Args: (cec, 178.79.242.128:80, 16, 0, 0, 0, 9c999528) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (ctldl.windowsupdate.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 924		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 924		2240
Call Network API	API Name: bind Args: (924, 0.0.0.0:49431, 128) Return: 0		2240

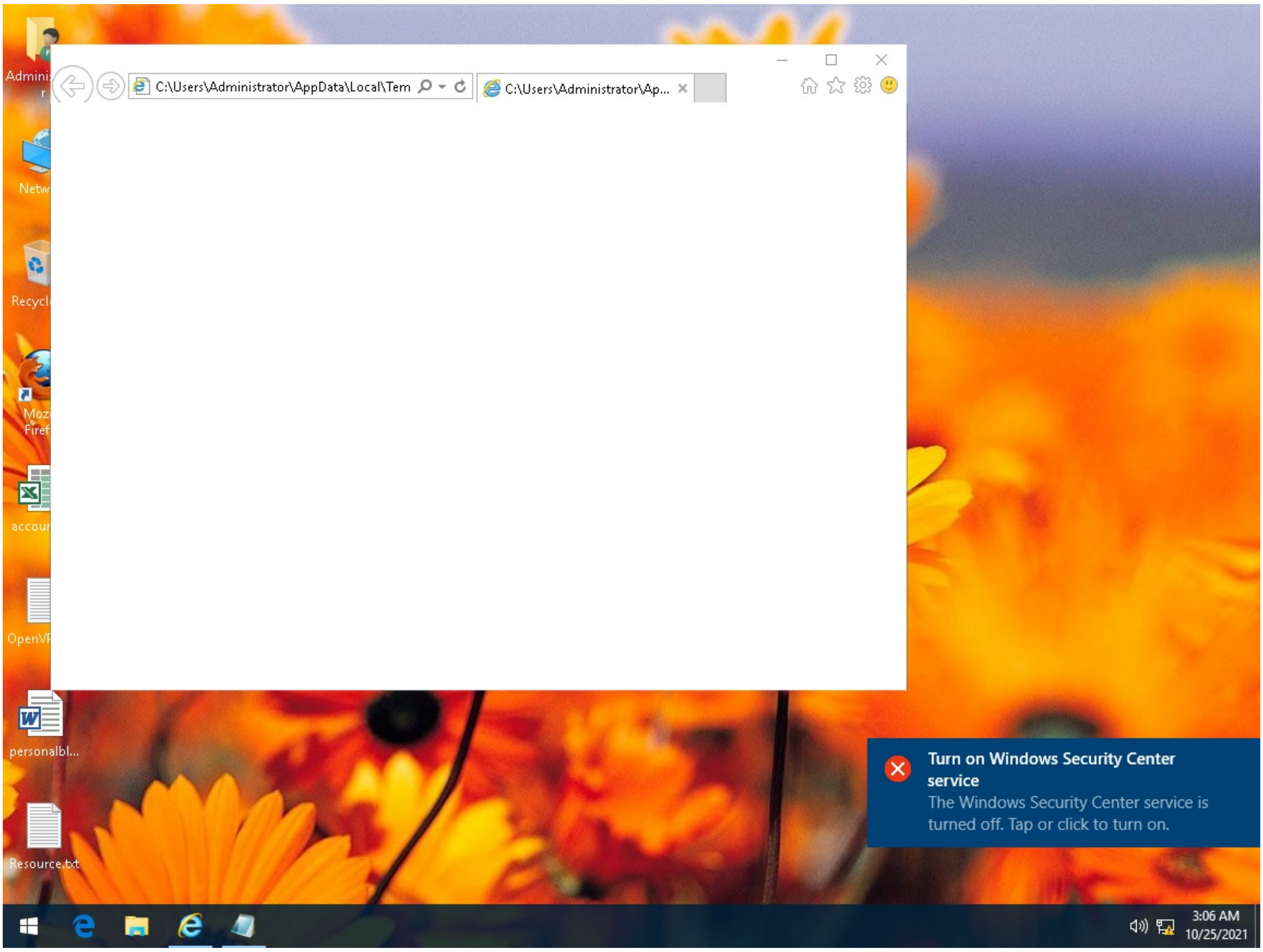
Detection	Threat Characteristic: Listens on port 0.0.0.0:49431		
Call System API	API Name: ConnectEx Args: (924, 178.79.242.128:80, 16, 0, 0, 0, 9c999d68) Return: 0		2240
Call Network API	API Name: send Args: (cd0, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?768c120b3b904678 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 05 Apr 2019 05:33:13 GMT\r\nIf-None-Match: "8072d4f71ebd41:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0		2240
Call Network API	API Name: send Args: (cdc, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1f3e953389c819c7 HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 05 Apr 2019 05:33:13 GMT\r\nIf-None-Match: "8072d4f71ebd41:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0		2240
Call Network API	API Name: send Args: (cec, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b4d985180751389d HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 05 Apr 2019 05:33:13 GMT\r\nIf-None-Match: "8072d4f71ebd41:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0		2240
Call Network API	API Name: send Args: (924, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9fd483ab01319dee HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Fri, 05 Apr 2019 05:33:13 GMT\r\nIf-None-Match: "8072d4f71ebd41:0"\r\nUser-Agent: Microsoft-CryptoAPI/10.0\r\nHost: ctldl.windowsupdate.com\r\n\r\n, 1, 287) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a01b5160) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014d250) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca497d0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0209300) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a01b2a40) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014d700) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca4a270) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca4bbf0) Return: 1		2240
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2240
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2240
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2240
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2240
Call System API	API Name: WinHttpCloseHandle Args: (a024aad0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a02388f0) Return: 1		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: bf8		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: bf8		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: d20		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: d20		2240
Call System API	API Name: DnsQueryEx Args: (ocsp.digicert.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ocsp.digicert.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (ocsp.digicert.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: d1c		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: d1c		2240
Call Network API	API Name: bind Args: (d1c, 0.0.0.0:49432, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49432		
Call System API	API Name: ConnectEx Args: (d1c, 93.184.220.29:80, 16, 0, 0, 0, 9c998ce8) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (ocsp.digicert.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: ccc		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: ccc		2240
Call Network API	API Name: bind Args: (ccc, 0.0.0.0:49433, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49433		
Call System API	API Name: ConnectEx Args: (ccc, 93.184.220.29:80, 16, 0, 0, 0, 9c9988c8) Return: 0		2240
Call Network API	API Name: send Args: (d1c, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%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, 1, 236) Return: 0		2240
Call Network API	API Name: send Args: (ccc, GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2BnRyLFPYjID1ie%2Bx%2BdSjo%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, 1, 242) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a021cbc0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014c440) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0206ee0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0208420) Return: 1		2240
Call Network API	API Name: send Args: (9ac, ..., 1, 126) Return: 0		2240
Call Network API	API Name: send Args: (9ac, ..., 1, 87) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 39, a002ed50, , 0, , 97, -1610420620, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 13, a002ed50, , 0, , 29, -1610420620, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 9, a012ea40, , 0, , 25, -1609372828, 0) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0242f30) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014cf30) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0207fe0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0206cc0) Return: 1		2240
Call Network API	API Name: send Args: (920, ..., 1, 158) Return: 0		2240
Call Network API	API Name: send Args: (920, ..., 1, 87) Return: 0		2240
Call Network API	API Name: send Args: (9ac, ..., 1, 38) Return: 0		2240
Call Network API	API Name: send Args: (9ac, ...0, 1, 309) Return: 0		2240
Call Network API	API Name: send Args: (920, ..., 1, 291) Return: 0		2240

Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 281, a002ef00, , 0, , 1407, -1610420188, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 9, a002ef00, , 0, , 1097, -1610420188, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 16383, a002ec50, , 0, , 16399, -1610420876, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0,)+QáË^ìG9, 1, a002ec50, , 0,)+QáË^ìG9, 9350, -1610420876, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, , 9, a002ec50, , 0, , 9320, -1610420876, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015cdd0, Ð)Ï¨), 9266, a002ec50, , 0, Ð)Ï¨), 9282, -1610420876, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a021bfe0, , 40, a0d2ed20, , 0, , 94, -1596789180, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a021bfe0, , 9, a0d2ed20, , 0, , 25, -1596789180, 0) Return: 0		2240
Call Network API	API Name: send Args: (920, ..., 1, 38) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a021bfe0, , 882, a002ef00, , 0, , 898, -1610420188, 0) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a022e2e0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014ded0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca4af30) Return: 1		2240
Call Network API	API Name: send Args: (92c, ..., 1, 158) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0206220) Return: 1		2240
Call Network API	API Name: send Args: (92c, ..., 1, 87) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015c060, , 40, a002ed50, , 0, , 56, -1610420620, 0) Return: 0		2240
Call Network API	API Name: send Args: (92c, ..., 1, 38) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a015c060, , 9, a012ea40, , 0, , 25, -1609372828, 0) Return: 0		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_EMPTY		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\VersionHigh Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\VersionLow Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\DXFeatureLevel Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-VendorId Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-DeviceId Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-SubSysId Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-Revision Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-VersionHigh Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-VersionLow Value: 0		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\GPU\Wow64-DXFeatureLevel Value: 0		2240
Call System API	API Name: CreateDXGIFactory Args: ({7B7166EC-21C7-44AE-B21A-C9AE321AE369}, 9cbaaf60) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0230a60) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014c120) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca4b150) Return: 1		2240
Call Network API	API Name: send Args: (9a8, ..., 1, 126) Return: 0		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0208200) Return: 1		2240
Call Network API	API Name: send Args: (9a8, ..., 1, 87) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a01600c0, , 39, a002ef00, , 0, , 97, -1610420188, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a01600c0, , 13, a002ef00, , 0, , 29, -1610420188, 0) Return: 0		2240
Call Network API	API Name: send Args: (9a8, ..., 1, 38) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a01600c0, , 9, a002ec50, , 0, , 25, -1610420876, 0) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (go.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, go.microsoft.com, 80, , , 3, 0, -1608853360) Return: cc0008		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /fwlink/?LinkID=401135, , , -1668628128, 4194320, -1608853360) Return: cc000c		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: cbc		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: cbc		2240
Call System API	API Name: DnsQueryEx Args: (go.microsoft.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (go.microsoft.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 91c		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: cbc		2240
Call Network API	API Name: bind Args: (cbc, 0.0.0.0:49434, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49434		
Call System API	API Name: ConnectEx Args: (cbc, 104.75.59.137:80, 16, 0, 0, 0, 9ca8c388) Return: 0		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 91c		2240
Call Network API	API Name: bind Args: (91c, 0.0.0.0:49435, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49435		
Call System API	API Name: ConnectEx Args: (91c, 104.75.59.137:80, 16, 0, 0, 0, 9ca8c9a8) Return: 0		2240
Call Network API	API Name: send Args: (cbc, 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; SUID=M; _EDGE_S=F=1&SID=1434DE52BAE3644C0EAACE89BBCB65DE&mkt=en-us; _EDGE_V=1; SRCHHPGUSR=SRCHLANG=en; _SS=SID=1434DE52BAE3644C0EAACE89BBCB, 1, 520) Return: 0		2240
Call Network API	API Name: recv Args: (91c, , 1, 2) Return: ?		2240
Call Network API	API Name: recv Args: (cbc, , 1, 2) Return: ?		2240
Call Network API	API Name: send Args: (920, ...^, 1, 355) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a021bfe0, , 1767, 9cbaed00, , 0, , 1783, -1665470940, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a021bfe0, , 9, 9cbaea50, , 0, , 25, -1665471628, 0) Return: 0		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\11CE4E0A4FD3CD25F064BE57BB2A9DE7238231CC\ Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739F Value: None		2240

Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739F\ Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates\MSIEHistoryJournal\Certificates\4EEF7FAF0062D34ABEE6137E774438AE9988739F\Blob Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\HistoryJournalCertificate\NextUpdateDate Value: 1461efaa		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1608853360) Return: cc0008		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1668628320, 12582928, -1608853360) Return: cc000c		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 0) Return: cc0008		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, iecvlist.microsoft.com, 443, , , 3, 0, 0) Return: cc000c		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, GET, /ie11blocklist/1401746408/versionlist.xml, , , -1676478696, 79692288, 0) Return: cc0010		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 238		2240
Call Network API	API Name: bind Args: (238, 0.0.0.0:49436, 16) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49436		
Call System API	API Name: ConnectEx Args: (238, 152.199.19.161:443, 16, 0, 0, 0, a01a3c78) Return: 0		2240
Call Network API	API Name: send Args: (238, ...b., 1, 359) Return: 0		2240
Call Network API	API Name: send Args: (238, ..., 1, 126) Return: 0		2240
Call Network API	API Name: send Args: (238, ...', 1, 556) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a0210ce0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 3297\r\nCache-Control: max-age=3600\r\nContent-MD5: GlRdAFK1gfuyq0xSEzhGvA==\r\nContent-Type: text/xml\r\nDate: Mon, 25 Oct 2021 08:06:23 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F6BA)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: dbcc67be-301e-0029-7a6f-c99b40000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16278\r\n\r\n#48Õ?ý, 452, 9cbaed00, , 0, HTTP/1.1 200 OK\r\nAccept-Ranges: bytes\r\nAge: 3297\r\nCache-Control: max-age=3600\r\nContent-MD5: GlRdAFK1gfuyq0xSEzhGvA==\r\nContent-Type: text/xml\r\nDate: Mon, 25 Oct 2021 08:06:23 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F6BA)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: dbcc67be-301e-0029-7a6f-c99b40000000\r\nx-ms-version: 2009-09-19\r\nContent-Length: 16278\r\n\r\n#48Õ?ý, 1407, -1665470940, 0) Return: 0		2240
Call System API	API Name: BCryptDecrypt Args: (a0210ce0, ï»¿<?xml version="1.0" encoding="utf-8"?>\r\n<blocklist version="28" ttlHigh="50" ttlLow="1251635200">\r\n <blocklistentries>\r\n <blocklistentry key="{dbc80044-a445-435b-bc74-9c25c1c588a9}" entrytype="2" />\r\n <blocklistentry key="{e19f9331-3110-11d4-991c-005004d3b3db}" entrytype="2" />\r\n <blocklistentry key="{8ad9c840-044e-11d1-b3e9-00805f499d93}" entrytype="2" />\r\n <blocklistentry key="{761497bb-d6f0-462c-b6eb-d4daf1d92d43}" entrytype="2" />\r\n <blocklistentry key="{5852f5ed-8bf4-11d4-a245-0080c6f74284}" entrytype="2" />\r\n <blocklistentry key="{CAFEEFAC-*}" entrytype="2" />\r\n <blocklistentry key="javaws.exe" entrytype="1" />\r\n <blocklistentry key="jp2launcher.exe" entrytype="1" />\r\n <blocklistentry key="ssvagent.exe" entrytype="1" />\r\n <blocklistentry key="unpack200.exe" entrytype="1" />\r\n <blocklistentry key="{dfeaf541-f3e1-4c24-acac-99c30715084a}" entrytype="2" />\r\n <blocklistentry key="agcp.exe" entrytype="1" />\r\n <blocklistentry key="Silverlight.Configuration.exe" entrytype="1" />\r\n <blocklistentry key="{d27cdb6e-ae6d-11cf-96b8-444553540000}" entrytype="2" />\r\n </blocklistentries>\r\n <groupentries>\r\n <groupentry groupname="Java(TM)" fwdlink="https://go.microsoft.com/fwlink/?LinkID=401352" />\r\n <groupentry groupname="Java(TM) 1.4" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Java(TM) 1.5" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Java(TM) 1.6" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Java(TM) 1.7" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Java(TM) 1.8" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Java(TM) 9" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Silverlight 5" fwdlink="http://" latestgroup="1" />\r\n <groupentry groupname="Silverlight" fwdlink="https://go.microsoft.com/fwlink/?LinkID=513071" />\r\n <groupentry groupname="AdobeFlash" fwdlink="https://aka.ms/FlashEOLUpdate" silentblock="1"/>\r\n </groupentries>\r\n <blocklistfullentries>\r\n <blocklistentry key="{dbc80044-a445-435b-bc74-9c25c1c588a9}" entrytype="2">\r\n <versionentries numberofelements="5">\r\n <versionentry groupname="Java(TM) 9" filename="jp2ssv.dll" productversion="9.0.1-65535.65535.65535.65535" fileversion="12.0.1.0-65535.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.8" filename="jp2ssv.dll" productversion="8.0.1510.0-8.65535.65535.65535" fileversion="11.151.0.0-11.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.7" filename="jp2ssv.dll" productversion="7.0.1610.0-7.65535.65535.65535" fileversion="10.161.0.0-10.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.6" filename="jp2ssv.dll" productversion="6.0.1710.0-6.65535.65535.65535" fileversion="6.0.1710.0-6.65535.65535.65535" />\r\n <versionentry groupname="Java(TM)" filename="*" productversion="*" fileversion="*" />\r\n </versionentries>\r\n </blocklistentry>\r\n <blocklistentry key="{e19f9331-3110-11d4-991c-005004d3b3db}" entrytype="2">\r\n <versionentries numberofelements="8">\r\n <versionentry groupname="Java(TM) 9" filename="jp2iexp.dll" productversion="9.0.1-65535.65535.65535.65535" fileversion="12.0.1.0-65535.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.8" filename="jp2iexp.dll" productversion="8.0.1510.0-8.65535.65535.65535" fileversion="11.151.0.0-11.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.7" filename="jp2iexp.dll" productversion="7.0.1610.0-7.65535.65535.65535" fileversion="10.161.0.0-10.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.7" filename="ssv.dll" productversion="7.0.1610.0-7.65535.65535.65535" fileversion="10.161.0.0-10.65535.65535.65535" />\r\n <versionentry groupname="Java(TM) 1.6" filename="jp2iexp.dll" productversion="6.0.1710.0-6.65535.65535.65535" fileversion="6.0.1710.0-6.65535.65535.65535" />\r\n <versionentry groupname="Java(T) Return: 0		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\VersionManager\verA1BF.tmp Type: VSDT_EMPTY		2240
Call Network API	API Name: recv Args: (238, , 1, 2) Return: ?		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\VersionManager\verA1BF.tmp Type: VSDT_TEXT_HTML		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\VersionManager\verA1BF.tmp Type: VSDT_TEXT_HTML		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\VersionManager\versionlist.xml Type: VSDT_TEXT_HTML		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastUpdateLowDateTime Value: 33d36e96		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastUpdateHighDateTime Value: 1d7c977		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 33d36e96		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d7c977		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca4cad0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9ca346c0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9c8d8550) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a02119b0) Return: 1		2240
Call Network API	API Name: socket Args: (2, 2, 0) Return: c54		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: c54		2240
Call System API	API Name: DnsQueryEx Args: (sqm.telemetry.microsoft.com, 1, 40006000) Return: 87		2240
Call System API	API Name: DnsQueryEx Args: (sqm.telemetry.microsoft.com, 1c, 40026000) Return: 0		2240
Call Network API	API Name: socket Args: (23, 2, 0) Return: 830		2240
Call Network API	API Name: socket Args: (2, 1, 6) Return: 830		2240
Call Network API	API Name: bind Args: (830, 0.0.0.0:49437, 128) Return: 0		2240
Detection	Threat Characteristic: Listens on port 0.0.0.0:49437		
Call System API	API Name: ConnectEx Args: (830, 65.55.252.93:443, 16, 0, 0, 0, 9caa1ef8) Return: 0		2240
Call Internet Helper API	API Name: InternetOpenW Args: (, 0, , , 0) Return: cc0004	2240	2636
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0	2240	2636
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 0, 0) Return: cc0008	2240	2636

Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /ie11blocklist/1401746408/versionlist.xml, , , 131527372, 79692288, 0) Return: cc000c	2240	2636
Call System API	API Name: WinHttpCloseHandle Args: (523c040) Return: 1	2240	2636
Call Network API	API Name: socket Args: (2, 2, 0) Return: 854	2240	2636
Call Network API	API Name: socket Args: (23, 2, 0) Return: 854	2240	2636
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 40006000) Return: 87	2240	2636
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1c, 40026000) Return: 0	2240	2636
Call Network API	API Name: socket Args: (23, 2, 0) Return: 864	2240	2636
Call Network API	API Name: socket Args: (2, 1, 6) Return: 854	2240	2636
Call Network API	API Name: bind Args: (854, 0.0.0.0:49438, 16) Return: 0	2240	2636
Detection	Threat Characteristic: Listens on port 0.0.0.0:49438		
Call System API	API Name: ConnectEx Args: (854, 152.199.19.161:443, 16, 0, 0, 0, 880249c) Return: 0	2240	2636
Call Network API	API Name: send Args: (854, ..., 1, 199) Return: 0	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\7d\52C64B7E\LanguageList Value: en-US\0en\0	2240	2636
Call Service API	API Name: OpenServiceW Args: (989e1f8, CryptSvc, 5) Return: 989e4f0	2240	2636
Call Network API	API Name: send Args: (854, ..., 1, 126) Return: 0	2240	2636
Call Network API	API Name: send Args: (854, ...', 1, 556) Return: 0	2240	2636
Call System API	API Name: BCryptDecrypt Args: (986d750, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3306\r\nCache-Control: max-age=3600\r\nDate: Mon, 25 Oct 2021 08:06:32 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F696)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: dbcc67be-301e-0029-7a6f-c99b40000000\r\nx-ms-version: 2009-09-19\r\n\r\nÎøfð,ˆá=šg0Pµ¥þ5, 376, 919f308, , 0, HTTP/1.1 304 Not Modified\r\nAccept-Ranges: bytes\r\nAge: 3306\r\nCache-Control: max-age=3600\r\nDate: Mon, 25 Oct 2021 08:06:32 GMT\r\nEtag: 0x8D8BD7E4D55BBE4\r\nLast-Modified: Wed, 20 Jan 2021 20:02:23 GMT\r\nServer: ECAcc (ska/F696)\r\nX-Cache: HIT\r\nx-ms-blob-type: BlockBlob\r\nx-ms-lease-status: unlocked\r\nx-ms-request-id: dbcc67be-301e-0029-7a6f-c99b40000000\r\nx-ms-version: 2009-09-19\r\n\r\nÎøfð,ˆá=šg0Pµ¥þ5, 392, 152695804, 0) Return: 0	2240	2636
Call Network API	API Name: recv Args: (854, , 1, 2) Return: ?	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime Value: 39152234	2240	2636
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime Value: 1d7c977	2240	2636
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1608853360) Return: cc0008		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1676491616, 12582928, -1608853360) Return: cc000c		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\MFV Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue Value: None		2240
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed Value: None		2240
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\MFV Value: None		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1608853360) Return: cc0008		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1665481840, 12582928, -1608853360) Return: cc000c		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Call System API	API Name: WinHttpCloseHandle Args: (a0207980) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (9caa0ed0) Return: 1		2240
Call System API	API Name: WinHttpCloseHandle Args: (a014d250) Return: 1		2240
Call Filesystem API	API Name: DeleteFileW Args: ( ) Return: 0		2240
Call System API	API Name: DnsQueryEx Args: (iecvlist.microsoft.com, 1, 50020000) Return: 0		2240
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, iecvlist.microsoft.com, 443, , , 3, 8388608, -1608853360) Return: cc0008		2240
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /IE11/1426178821/iecompatviewlist.xml, , , -1676491616, 12582928, -1608853360) Return: cc000c		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\IECompatData\iecompatdata.xml Type: VSDT_TEXT_HTML		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{5F1B7117-356A-11EC-9BF1-001F3C8C8DBB}.dat Type: VSDT_WINWORD		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\{5F1B7117-356A-11EC-9BF1-001F3C8C8DBB}.dat Type: VSDT_WINWORD		2240
Add File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5F1B7115-356A-11EC-9BF1-001F3C8C8DBB}.dat Type: VSDT_WINWORD		2240
Write File	Path: %LOCALAPPDATA%\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5F1B7115-356A-11EC-9BF1-001F3C8C8DBB}.dat Type: VSDT_WINWORD		2240

▼ Screenshot



Turn on Windows Security Center service
The Windows Security Center service is turned off. Tap or click to turn on.

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