# Virtual Analyzer Report



# Submission Context

Logged	2021-04-24 14:33:35	
Submitter	Manual Submission	
Туре	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		~	<b>~</b>
Hijack, redirection, or data theft		~	~
Malformed, defective, or with known malware traits	~	~	~
Process, service, or memory object change			<b>~</b>
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	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B1 43
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

Туре	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	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B1 43
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



### 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

 $\ensuremath{\text{\fontfamily MITRE}}$  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		0.0.0.049169
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-66x6 6.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	CDDA0CE556B74C07203867D9F32C293A51 A4EAE4
fQzim[1].htm	No risk	-	-	http://bit.do/fQzim	6593	CDDA0CE556B74C07203867D9F32C293A51 A4EAE4
ZCS3PKI.LNK	No risk	-	-	-	893	7B18156379CA78C77FE9C2678B91DF9C9A 62F427
Inquiry Sheet Lists 0240030019.d ocx.LNK	No risk	-	-	-	1145	377694B7C69552463FC5EAC4B6ACF77BB8 EF123A
bit.do.url	No risk	-	-	-	40	2B60CBF31F524A207F512DD9D3A208DC1A BDE286
fQzim.url	No risk	-	-	-	45	0A421BBF9F1827E20B7834B4FE24841D566 01E40
~WRS{EC7C4DC4-74C4-49C4-8 369-3DC352A1C481}.tmp	No risk	-	-	-	9216	F0E0D08BAC4113BD7A965E72AC86F4DAF D63AC3E
~\$quiry Sheet Lists 0240030019.d ocx	No risk	-	-	-	162	FC309EB6C422DD4D8ADFFB627E898A0826 7FEFA5
ExcludeDictionaryEN0409.lex	No risk	-	-	-	2	D62636D8CAEC13F04E28442A0A6FA1AFEB 024BBB
Word12.pip	No risk	-	-	-	1684	F2BBE0704D7495E84F8D755F2F75971E48B F9AA2

# ▼ Suspicious Objects

Туре	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\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2340
Call Filesystem API	API Name: CopyFileExW Args: ( %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.d at, 0, 0, 0, 1) Return: 0		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\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		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
		2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableFileTracing Value: 0	
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\Current\Version\Internet Settings\AutoConfigURL Value: None	2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2340
Call Network 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\Current\Version\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		2340
	API Name: bind Args: ( 634, 0.0.0.49166, 16 ) Return: 0	2340
Detection	Threat Characteristic: Listens on port 0.0.0.049166	
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: Kee	2340
Call Network AFT	p-Alivelrinkin, 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\Intermet\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\Intermet\Server Cache\http://bit.do/\ Value: None	2340
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Intermet\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
		2340 2340
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1	2340
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Cottove Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\ControlFlags Value: 1	2340 2340
Write Registry Key Write Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Value: None	2340 2340 2340
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Cottove Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\ControlFlags Value: 1	2340 2340
Write Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Active Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96	2340 2340 2340 2340
Write Registry Key Write Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Active Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Regular\Guid Value: 7e4b70ee-8296-4	2340 2340 2340
Write Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: Tero Unusu	2340 2340 2340 2340
Write Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  10f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Bit\Names Value: Error Unusu al Noise Entry Exit Probability Cracking CrackingError Debug	2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: Te4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Names Value: Error Unusu  al Noise Entry Exit Probability Cracking CrackingError Debug  API Name: OpenServiceW Args: ( 29668c0, Webclient, 5 ) Return: 29668e8  API Name: WNetAddConnection3W Args: ( a00ee, Remote<\\bit.do\Dav\WWRoot> Local<\\bit.do\Dav\WWRoot>, , , c ) Return: 35	2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Call Service API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  10f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Bit\Names Value: Error Unusu al Noise Entry Exit Probability Cracking CrackingError Debug  API Name: OpenServiceW Args: (29668c0, Webclient, 5 ) Return: 29668e8	2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  10f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: Te4b70ee-8296-4  10f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Nalue: Error Unusu  al Noise Entry Exit Probability Cracking CrackingError Debug  API Name: OpenServiceW Args: ( 29668c0, Webclient, 5 ) Return: 29668e8  API Name: WNetAddConnection3W Args: ( a00ee, Remote<\\bit\do\Dav\WWRoot> Local<\\bit\do\Dav\WWRoot>, , , c ) Return: 35  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\BDEADF00-C265-11D0-BCED-00A0C90AB50F} \{0002	2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API  Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\CottrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: Fror Unusu  al Noise Entry Exit Probability Cracking CrackingError Debug  API Name: OpenServiceW Args: (29668c0, Webclient, 5) Return: 29668e8  API Name: WNetAdConnection3W Args: (a00ee, Remote<\\bit.do\Dav\WWRoot> Local<\\bit.do\Dav\WWRoot>, , , c) Return: 35  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\{BDEADF00-C265-11D0-BCED-00A0C90AB50F} \{0002  14E6-0000-0000-C000-0000000000000000  0xfFFF Value: None  API Name: InternetGetConnectedStateExW Args: (1e132c, 0, 0, 0) Return: 1	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API  Write Registry Key  Call Internet Helper API  Call Internet Helper API  Call Internet Helper API  Call Network API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\CottrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: Fror Unusu al Noise Entry Exit Probability Cracking Error Debug  API Name: OpenServiceW Args: (29668c0, Webclient, 5) Return: 29668e8  API Name: WNetAdConnection3W Args: (a00ee, Remote<\\bit.do\Dav\WWRoot> Local<\\bit.do\Dav\WWRoot>, , , c) Return: 35  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\\BDEADF00-C265-11D0-BCED-00A0C90AB50F} {0002} 14E6-0000-0000-C000-000000000046} 0xFFFF Value: None  API Name: InternetGetConnectedStateExW Args: (1e132c, 0, 0, 0) Return: 1  API Name: socket Args: (2, 2, 17) Return: 668	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API  Write Registry Key  Call Internet Helper API  Call Network API  Call Network API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\CottrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: Fror Unusu al Noise Entry Exit Probability Cracking Error Debug  API Name: OpenServiceW Args: (29668c0, Webclient, 5) Return: 29668e8  API Name: WNetAddConnection3W Args: (a00ee, Remote<\\bit.do\Dav\WWWRoot> Local<\\bit.do\Dav\WWRoot>, , , c) Return: 35  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\\BDEADF00-C265-11D0-BCED-00A0C90AB50F} \{0002  14E6-0000-0000-C000-0000000006} 0xFFFF Value: None  API Name: IntermetGetConnectedStateExW Args: (1e132c, 0, 0, 0) Return: 1  API Name: socket Args: (2, 2, 17) Return: 668  API Name: bind Args: (668, 127.0.0.1:52727, 16) Return: 0	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API  Write Registry Key  Call Internet Helper API  Call Internet Helper API  Call Internet Helper API  Call Network API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\CottrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Cegular\Guid Value: Fror Unusu al Noise Entry Exit Probability Cracking Error Debug  API Name: OpenServiceW Args: (29668c0, Webclient, 5) Return: 29668e8  API Name: WNetAdConnection3W Args: (a00ee, Remote<\\bit.do\Dav\WWRoot> Local<\\bit.do\Dav\WWRoot>, , , c) Return: 35  Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\\BDEADF00-C265-11D0-BCED-00A0C90AB50F} {0002} 14E6-0000-0000-C000-000000000046} 0xFFFF Value: None  API Name: InternetGetConnectedStateExW Args: (1e132c, 0, 0, 0) Return: 1  API Name: socket Args: (2, 2, 17) Return: 668	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Add Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call Service API  Call Internet Helper API  Write Registry Key  Call Internet Helper API  Call Network API  Call Network API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\ControlFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFT	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Write Registry Key  Call Service API Call Internet Helper API Write Registry Key  Call Internet Helper API Call Network API Call Network API Detection  Call Internet Helper API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Micro	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key  Write Registry Key  Call Service API Call Internet Helper API Write Registry Key  Call Internet Helper API Call Network API Call Network API Detection  Call Internet Helper API  Call System API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Micro	2340 2340 2340 2340 2340 2340 2340 2340
Write Registry Key  Write Registry Key  Call Service API Call Internet Helper API Write Registry Key  Call Internet Helper API Call Network API Call Network API Detection  Call Internet Helper API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\CotrolFlags Value: 1  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4  f0f-a3ba-f58ef7bb4e96  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Micro	2340 2340 2340 2340 2340 2340 2340 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: fffffff	2340	
Call Network API	API Name: recv Args: ( 668, , 32, 0 ) Return: ?	2340	
Call Network API	API Name: send Args: ( 668, 1, 1, 0 ) Return: 1	2340	
Call Network API	API Name: send Args: ( 6ac, GET /fQzim HTTP/1.1\r\nAccept: '\"\n\User-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NE T 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, I, 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%iMicrosoftiVMindows\Temporary Internet Files\Content.IE5\MXNZOZKK\fQzim[1].htm, %LOCALAPPDA TA%iMicrosofti\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, #Qzim, HTTP/1.1, , 0, -2143287296, 0 ) Return: cc0010	2340	
Call Network API	API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: acad Args: ( 6ac, HEAD (Corise LTTP)(4 1) In large Acads Microsoft Office Evidence Discovered In the Head ( In the Head ( In the Head) In the Head ( In	2340	
Call Network API	API Name: send Args: ( 6ac, HEAD /fQzim HTTP/1.1\f\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  Detection	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 Call Network API	API Name: recv Args: (6ac, , 1, 2) Return:?  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; Wind ows 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 2340	
	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\v\nAccept: */"\v\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;		
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 Call Network API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\r\nAccept: *\text{UnUser-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  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?	2340	
Call Network API  Call Network API  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; Wind ows 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\r\n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?	2340 2340 2340	
Call Network API Call Network API Call Network API 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; Wind ows 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\r\n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1	2340 2340 2340 2340	
Call Network API Call Network API Call Network API Call Network API Call Filesystem API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\/\nAccept: "/\n\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\/\n\nAccept-Encoding: gzip, deflate\/\n'\nHost: bit.do\/\n'\nConnection: Keep-Alive\/\n'\n'\n'\n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\/\microsoft\)Office\/\nRecent\/\name Qzim.url ) Return: 0	2340 2340 2340 2340 2340	
Call Network API Call Network API Call Network API Call Network API Call Filesystem API Add File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66,png HTTP/1.1\n/nAccept: "/"\n/\u00fcVila/4.0 [compatible; MSIE 7.0; Wind ows 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]\u00fc/nAccept-Encoding: gzip, deflate\u00edrinHost: bit.do\u00edrinConnection: Keep-Alive\u00edrin\u00edrin, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\u00edMicrosoft\u00fcOffice\u00edRecent\u00edQzim.url ) Return: 0  Path: %APPDATA%\u00edMicrosoft\u00fco\u00edFice\u00edRecent\u00edQzim.url Type: VSDT_ASCII	2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66,png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac., 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\n/Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\Office\Recent\n/Qzim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\Office\Recent\n/Qzim.url Type: VSDT_ASCII	2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66,png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\n/Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\Office\Recent\n/Qzim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\Office\Recent\n/Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Network API Call Network API Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac., 1024, 0 ) Return: ?  API Name: send Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\0ffice\Recent\n/Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\0ffice\Recent\n/Qzim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\0ffice\Recent\n/Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac., 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac., 3299, 0 ) Return: ?	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API  Call Network API  Call Network API  Call Network API  Call Filesystem API  Add File  Write File  Call Network API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: send Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\0ffice\Recent\n/Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\0ffice\Recent\n/Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 129, 0 ) Return: ?	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Network API Call Network API Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Add File Add File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66,png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: send Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, 1, 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\0ffice\Recent\f\0z\imu\nurl ) Return: 0  Path: %APPDATA%\Microsoft\0ffice\Recent\f\0z\imu\nurl Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 12, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\\018Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Add File Write File Write File Write File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/nAccept: "/"\n/nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/nAccept-Encoding: gzip, deflate\n/nHost: bit.do\n/nConnection: Keep-Alive\n/n\n/n, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\0ffice\Recent\0ft\Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\0ffice\Recent\0ft\Qzim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\0ffice\Recent\0ft\Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 125, 0 Return: ?  Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\018Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\018Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Network API Call Network API Call Network API Call Filesystem API Add File Write File Call Network API Call File Write File Call Filesystem API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/inAccept: "/"\n/inUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/inAccept-Encoding: gzip, deflate\n/inHost: bit.do\n/inConnection: Keep-Alive\n/in/in, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\0ffice\Recent\0ft\0Zzim.url ) Return: 0  Path: %APPDATA%\Microsoft\0ffice\Recent\0ft\0Zzim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\0ffice\Recent\0ft\0Zzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  Path: %LOCALAPPDATA%\Microsoft\0ffico\0	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Add File Write File Call Filesystem API Add File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/inAccept: "/"\n/inUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/inAccept-Encoding: gzip, deflate\n/inHost: bit.do\n/inConnection: Keep-Alive\n/in/in, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\n/Qzim.url ) Return: 0  Path: %APPDATA%\Microsoft\Office\Recent\n/Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  Path: %LOCALAPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Add File Write File Call Filesystem API Add File Write File	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/inAccept: "/"\n/inUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/inAccept-Encoding: gzip, deflate\n/inHost: bit.do\n/inConnection: Keep-Alive\n/in/in, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\Ozim.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\Office\Recent\Ozim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Call Network API Add File Write File Call Filesystem API Add File Write File Call Filesystem API	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/inAccept: "/"\n/inUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/inAccept-Encoding: gzip, deflate\n/inHost: bit.do\n/inConnection: Keep-Alive\n/in/in, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\Ozim.url Type: VSDT_ASCII  Path: %APPDATA\\Microsoft\Office\Recent\Ozim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  API Name: recv Args: ( 6ac, , 1, 2 ) Return: ?  Path: %LOCALAPDATA\\Microsoft\Microsoft\Mindows\Temporary Internet Files\Content.IE5\Q18Y57L1bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  API Name: DeleteFileW Args: ( %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII  API Name: DeleteFileW Args: ( %APPDATA\\Microsoft\Office\Recent\bit.do.url ) Return: 0  Path: %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII  API Name: DeleteFileW Args: ( %APPDATA\\Microsoft\Office\Recent\bit.do.url ) Return: 0  Path: %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII  Path: %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII  Path: %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII  Path: %APPDATA\\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Add File Write File Call Filesystem API Add File Write File Delete Registry Key Delete Registry Key	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\n/inAccept: "/"\n/inUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows 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]\n/inAccept-Encoding: gzip, deflate\n/inHost: bit.do\n/inConnection: Keep-Alive\n/in/in, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 668, , 32, 0 ) Return: ?  API Name: send Args: ( 668, , 1, 0 ) Return: 1  API Name: beleteFileW Args: ( %APPDATA%!Microsoft!Office\Recent!\Qzim.url ) Return: 0  Path: %APPDATA%!Microsoft!Office\Recent!\Qzim.url Type: VSDT_ASCII  Path: %APPDATA%!Microsoft!Office\Recent!\Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 124, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 129, 0 ) Return: ?  API Name: recv Args: ( 6ac, , 129, 0 ) Return: ?  API Name: recv Args: ( 6ac, ) Return: ?  API Name: recv Args: ( 6ac, ) Return: ?  API Name: recv Args: ( 6ac, ) Return: ?  Path: %LOCALAPDATA%!Microsoft!Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  Path: %LOCALAPDATA%!Microsoft!Windows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  API Name: DeleteFileW Args: ( %APPDATA%!Microsoft!Office\Recentbit.do.url ) Return: 0  Path: %APPDATA%!Microsoft!Office\Recentbit.do.url Type: VSDT_ASCII  Path: %APPDATA%!Microsoft!Office\Recentbit.do.url Type: VSDT_ASCII  Rey: HKEY_CURRENT_USER:Software!Microsoft!Office\12.0!Word\Resiliency\Startupltems\]>& Value: None  Key: HKEY_CURRENT_USER:Software!Microsoft!Office\12.0!Word\File MRUWax Display Value: None	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Call Network API Add File Write File Call Filesystem API Add File Write File Delete Registry Key	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\r/inAccept: "I"\r/inUser-Agent: Mozilia/4.0 [compatible; MSIE 7.0; Wind ows NT 6.1; Triden/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; NET4.0C; MSOffice 12]\r/inAccept.Encoding: gzip, deflate/rinHost: bit.doirinConnection: Keep-Alive\r/inirin, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 668, ., 3, 0 ) Return: ?  API Name: send Args: ( 668, ., 3, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%MicrosofftOffice\RecentlfQzim.url ) Return: 0  Path: %APPDATA%MicrosofftOffice\RecentlfQzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 3299, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 3299, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 12, 2 ) Return: ?  Path: %LOCALAPPDATA%MicrosofftWindows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  Path: %LOCALAPPDATA%MicrosofftWindows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  API Name: DeleteFileW Args: ( %APPDATA%Microsofft\Gffice\Recentlbit.do.url 1 Return: 0  Path: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Reth: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Reth: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.WirdFile MRUMate Display Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 1 Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 3 Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 3 Value: None	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Call Network API Add File Write File Call Filesystem API Add File Urite File Call Filesystem API Call Filesyst	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66,ng HTTP/1.1v/nAccept: "/"vinUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Wind ows NT 6.1; Trident/5.0; SLCO2; .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]/vinAccept-Encoding; gzip, deflate/rinHost: bit.doi/nConnection: Keep-AliveVin/rin, 353, 0 ] Return: 353  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6a6, ., 32, 0 ] Return: ?  API Name: send Args: ( 668, ., 32, 0 ) Return: 1  API Name: send Args: ( 668, ., 1, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%Milcrosoft)Office/Recent/Qzim.url ) Return: 0  Path: %APPDATA%Milcrosoft)Office/Recent/Qzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, ., 1024, 0 ] Return: ?  API Name: Revv Args: ( 6ac, .	2340 2340 2340 2340 2340 2340 2340 2340	
Call Network API Call Filesystem API Add File Write File Call Network API Call Network API Call Network API Call Network API Add File Write File Call Filesystem API Add File Write File Delete Registry Key	API Name: send Args: ( 6ac, GET /images/bit-do-url-shortener-logo-66x66.png HTTP/1.1\r/inAccept: "I"\r/inUser-Agent: Mozilia/4.0 [compatible; MSIE 7.0; Wind ows NT 6.1; Triden/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; NET4.0C; MSOffice 12]\r/inAccept.Encoding: gzip, deflate/rinHost: bit.doirinConnection: Keep-Alive\r/inirin, 353, 0 ) Return: 353  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 668, ., 3, 0 ) Return: ?  API Name: send Args: ( 668, ., 3, 0 ) Return: 1  API Name: DeleteFileW Args: ( %APPDATA%MicrosofftOffice\RecentlfQzim.url ) Return: 0  Path: %APPDATA%MicrosofftOffice\RecentlfQzim.url Type: VSDT_ASCII  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 1024, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 3299, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 3299, 0 ) Return: ?  API Name: recv Args: ( 6ac, ., 12, 2 ) Return: ?  Path: %LOCALAPPDATA%MicrosofftWindows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  Path: %LOCALAPPDATA%MicrosofftWindows\Temporary Internet Files\Content.IE5\Q18Y57L1\bit-do-url-shortener-logo-66x66[1].png Type: VSDT_PNG  API Name: DeleteFileW Args: ( %APPDATA%Microsofft\Gffice\Recentlbit.do.url 1 Return: 0  Path: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Reth: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Reth: %APPDATA%Microsofft\Gffice\Recentlbit.do.url Type: VSDT_ASCII  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.WirdFile MRUMate Display Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 1 Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 3 Value: None  Key: HKEY_CURRENT_USER\Software\Microsofft\Gffice\Recentlbit.do.Word\File MRUMtem 3 Value: None	2340 2340 2340 2340 2340 2340 2340 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\ltem 10 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 11 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 12 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 13 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 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\ltem 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\ltem 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\ltem 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\ltem 38 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 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
		2340
Delete Registry Key  Delete Registry Key	Key: HKEY_CURRENT_USER/Software/Microsoft/Office\12.0\Word\File MRU\Item 45 Value: None	2340
. ,	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	
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\ltem 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\ltem 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\ltem 16 Value: None	2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 17 Value: None	2340
Delete Registry Key  Delete Registry Key		2340
	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	
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
	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		2340
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None	2040
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None	2340
Delete Registry Key Delete Registry Key		

Delete Registry Key		
Delete Registry Rey	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
	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None	2340
Delete Registry Key		
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
		2340
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 44 Value: None	
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\ltem 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
·		2040
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\Startup\tems\`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\Resillency\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\m	2340
	sohtmed.exe	
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlffile\shell\Edit\command\ Value: None	2340
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlffile\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
		2340
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default)\ Value: "%ProgramFiles%\Microsoft\ Office\Office\Office\12\msohtmed.exe" %1	
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 Exploren\Default HTML Editor\shell\edit\deexec\Application\ Value: None	2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Topic\ Value: None	2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\lddeexec\ 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\value\. None	2340
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Value: None	
		2340
Add Registry Key		
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None	2340
		2340 2340
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None	
Delete Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\(\text{leditor\shell\)}\) Value: &Edit	2340
Delete Registry Key Write Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) Value: \"%ProgramFiles\%\Microsoft\"  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default) Value: \"%ProgramFiles\%\Microsoft\"  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default) Value: \"%ProgramFiles\%\Microsoft\"  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default) Value: \"%ProgramFiles\%\Microsoft\"  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\)	2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\) Value: None  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 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Command\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Command\) (Default\) Value: "%ProgramFiles%\Microsoft\ Office\OFFICE11\WINWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Command\) (Default\) Value: "%ProgramFiles%\Microsoft\ Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Command\) (Default\) Value: "%ProgramFiles%\Microsoft\ Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\dit\(Command\) (Default\) (Value: "%ProgramFiles%\Microsoft\)	2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key  Add Registry Key Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Coefault) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Coefault) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Command\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\Command\(Default\) Value: "%ProgramFiles%\Microsoft\ Office\OFFICE11\Win\WinWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Application\ Value: None	2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key Add Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) (Default) Value: "%ProgramFiles%\Microsoft}  Office\OFFICE11\WINWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) (Default) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) (alue: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) (befault) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\text{hedit}\(Command\) (befault) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\(Command\) (befault) Value: WinWord	2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) \(Value\): "%ProgramFiles%\Microsoft\\ Office\OFFICE11\WINWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Value\): None	2340 2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key Add Registry Key Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) Value: "%ProgramFiles%\Microsoft\ Office\OFFICE11\WinNWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) (Default\) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) (Default\) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\) HTML Editor\shell\edit\(Command\) (Default\) (Default\) Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\) HTML Editor\shell\edit\(Command\) (Default\) (Default\) Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\) HTML Editor\shell\edit\(Command\) (Default\) (Default\) (Value: System	2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key Add Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) (Default\) Value: "%ProgramFiles%\Microsoft\ Office\OFFICE11\WiNWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Application\ Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Application\(Default\) Value: WinWord  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\ Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\((Default\) Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\User\Data\S-1-5-18\Products\000002109F100A0C00000000000F01F  E\(\text{Usage\SpellingAndGrammarFiles_3082 Value: 52980004}\)	2340 2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: "%ProgramFiles%\Microsoft\ Office\(OFFiCE11\\WinWORD.EXE" /n /dde\)  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\)  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(Default\)  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microso	2340 2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\) Value: "%ProgramFiles%\Microsoft  Office\OFFICE11\Win\WORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Application\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Application\(Default\) Value: Win\Word  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Application\(Default\) Value: Win\Word  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\(Default\) Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(ddeexec\) Topic\(Default\) Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\User\Data\S-1-5-18\Products\(00002109F100A0C000000000000F01F) EC\Usage\Spelling\And\GrammarFiles_3082\table\S 2value: 52980004  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\(00002109F100A0C000000000000F01F) EC\Usage\Spelling\And\GrammarFiles_3082\table\S 2value: 52980005	2340 2340 2340 2340 2340 2340 2340 2340
Delete Registry Key Write Registry Key Add Registry Key Write Registry Key Add Registry Key Add Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: &Edit  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Command\)\ (Default)\ Value: "%ProgramFiles%\Microsoft\ Office\(OFF\)\(DEfault\)\ Value: "%ProgramFiles%\Microsoft\ Office\(OFF\)\(DEfault\)\(Default\)\ Value: "%ProgramFiles%\Microsoft\ Office\(OFF\)\(DEfault\)\(Default\)\ Value: "%ProgramFiles%\Microsoft\ Office\(OFF\)\(DEfault\)\(Default\)\(Default\)\(Default\)\(Default\)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Value: None\)  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Value: None\)  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Topic\)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Topic\)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Topic\)\ Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default\ HTML Editor\shell\edit\(ddeexec\)\(Topic\)\(Default\)\ Value: System  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\User\Data\S-1-5-18\Products\00002109F100A0C00000000000F01F  EC\Usage\Spelling\AndGrammar\Files_3082\ Value: 52980005  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\User\Data\S-1-5-18\Products\00002109F100A0C00000000000F01F  EC\Usage\Spelling\AndGrammar\Files_3082\ Value: 52980006	2340 2340 2340 2340 2340 2340 2340 2340

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\Spelling\ndGrammarFiles_1033 Value: 52980007	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838			
Write Registry Key	9C\Usage\SpellingAndGrammarFiles_1033 Value: 52980011  Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838	2340		
write registry rey	9C\Usage\SpellingAndGrammarFiles_1033 Value: 52980012			
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 52980005	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01F EC\Usage\Spelling\And\GrammarFiles_1036 Value: 52980006	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAnd\GrammarFiles_1033\Value: 52980013	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\Spelling\nd\GrammarFiles_1033\Value: 52980014	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\Spelling\And\GrammarFiles_1033\Value: 52980015	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 52980016	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 52980017	2340		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\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\Defaultlcon\(Default) Value: "%1"	2340		
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\lconHandler\(Default\) 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\Office 12\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\WINWOR D.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 Exce\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\EXC EL.EXE" /e	2340		
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\shell\edit\deexec\application\(Default) Value: Excel	2340		
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\\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\Office\Office\Office\12\EXCEL.EXE" /e	2340		
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\deexec\application\(Default)\Value: Excel	2340		
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\deexec\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\ledit\command\ Value: None	2340		
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\tedit\iddeexec\Application\ Value: None	2340		
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\tedit\iddeexec\Topic\ Value: None	2340		
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\ 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 Bogistov Kov	Kov: HKEV LOCAL MACHINE/COETWADE/Microsoft/Internet Evaluated Default MUTML Editor/about 3/4 V-1 N			
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\ Value: None			
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\command\(Default) Value: "%ProgramFiles%\Microsoft\Internet Explorer\Default Editor\shell\edit\command\(Default) Value: "%ProgramFiles\(Default) Value\(Default) Value: "%ProgramFiles\(Default) Value\(Default) Va	2340	
Add Registry Key	oft Office\OFFICE11\WINWORD.EXE" /n /dde  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\ Value: None	2340	
Add Registry Key		2340	
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\Application\ Value: None		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\Application\(Default\) Value: WinWord	2340	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\Topic\ Value: None	2340	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default MHTML Editor\shell\edit\deexec\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\mhtmlffile\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\Defaultlcon\(Default\) Value: "%1"	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shellex\lconHandler\(Default\) Value: {42042206-2D85-11D3-8CFF-005004838597}	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtt\OpenWithList\Microsoft Office Word\shell\editt\(Default\) Value: &Open	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\W INWORD.EXE" In Idde	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Application\(Default) Value: WinWord	2340	
		2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\Microsoft Office Word\shell\edit\ddeexec\Topic\(Default\) Value: System		
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\WINWOR D.EXE" /n /dde	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\OpenWithList\WinWord.exe\shell\ledit\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 Excellshell\edit\(Default\) Value: &Open	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT.mhtlOpenWithListlMicrosoft Office Excellshellleditl.commandl(Default) Value: "%ProgramFiles%\Microsoft Office\Office12\text{EXC} EL.EXE" /e	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtt\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\deexec\topic\(Default\) Value: system	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtt\OpenWithList\Excel.exe\shell\editt\(Default\) Value: &Open	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtlOpenWithListlExcel.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office12\EXCEL.EXE" /e	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mht\Open\WithList\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\Offi	2340	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.mhtt\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\Office\Office12\MSPUB.EXE"	2340	
	%1		
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\00002109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52980008	2340	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000002109F10090400000000000F01FE	2340	
Write Registry Key	C\Usage\SpellingAndGrammarFiles_1033 Value: 52980009  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE	2340	
	C\Usage\SpellingAndGrammarFiles_1033 Value: 5298000a		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5298000b	2340	
Add File	Path: %APPDATA%\Microsoft\UProof\ExcludeDictionaryEN0409.lex Type: VSDT_COM_DOS	2340	
Write File	Path: %APPDATA%MicrosoftUProoftExcludeDictionaryEN0409.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	
		2340	
Add Registry Key	Key: HKEY_CURRENT_USER:Software)Microsoft Shared Tools Proofing Tools Grammar\Value: None		
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{EC7C4DC4-74C4-49C4-8369-3DC3 52A1C481}.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-A249-4207-8145-8C5519} 2BAA87}.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-26917 D435B68}.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







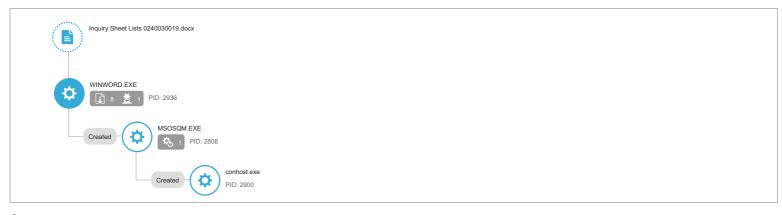
Environment-specific risk level	High risk  The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Trojan.W97M.FORMBOOK.AM		
Exploited vulnerabilities			
Network connection	Custom		

# ▼ 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	24DC6F5183A801C1E50F0142EAB5A4CE13CFAB3779D71B4FC1D3A86816E2B1 43
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

 $\ensuremath{\mathbb{C}}$  ATT&CKTM 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%UETE3DF.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%UETE239.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-66x6 6.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	CDDA0CE556B74C07203867D9F32C293A51 A4EAE4
fQzim[1].htm	No risk	-	-	http://bit.do/fQzim	6593	CDDA0CE556B74C07203867D9F32C293A51 A4EAE4
fQzim.url	No risk	-	-	-	45	0A421BBF9F1827E20B7834B4FE24841D566 01E40
bit.do.url	No risk	-	-	-	40	2B60CBF31F524A207F512DD9D3A208DC1A BDE286
msosqmcached.dat	No risk	-	-	-	788	12222B0001861514D0F76ACA9EB4B7CA287 E9BD3
~WRS{0614E162-C183-4D98-99 A4-7F938DBC8556}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12 B46E6
FSF-{0E1EEE64-E8C6-4E2A-975 9-63CF07FD8988}.FSF	No risk	-	-	-	114	B42E8477A968B6E644EBC3A67217B891BB A64EA6
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8 B09665
~WRS{6EBF22BE-3A68-4B32-89 E7-238C7FD9BB8F}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
~\$quiry Sheet Lists 0240030019.d ocx	No risk	-	-	-	162	645F6D91474FB3BDE3AA8BCCF411B388E0 F80263

### ▼ Suspicious Objects

Туре	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\Startup\tems\ 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\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	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\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	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\Resillency\StartupItems\+v' Value: None	2936
Add File	Path: %APPDATA%\Microsoft\Templates\-\$Normal.dotm Type: VSDT_COM_DOS	2936
Write File	Path: %APPDATA%\Microsoff\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\Current\Version\\Installer\UserData\\S-1-5-18\\Products\\00005119110000000000000000000000000000	2936
Call System API	API Name: DeviceloControl 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\FS D-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%\(2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D\)	
Call Filocyctom API	Type: VSDT_COM_DOS  ADI Namo: Deleta EliaM Arce: / %/TEMP%/1/2679E2E4_E0C7_4CCA_9CA0_279A9CEE602D) \ Patura: 1	2026
Call Filesystem API Call Filesystem API	API Name: DeleteFileW Args: ( %TEMP%\(2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D\) ) Return: 1  API Name: DeleteFileW Args: ( %TEMP%\(2578F2E4-F0C7-4CCA-9CA0-378A9CFE592D\) ) Return: 0	2936
Write File	Path: %LOCALAPPDATA%IMicrosoft(Office)15.0(OfficeFileCache)FSD-CNRY.FSD Type: VSDT COM DOS	2936
	Path: %LOCALAPPDATA%/Microsoft/Office/15.0/OfficeFileCache/FSD-CNRY.FSD Type: VSDT_COM_DOS  Path: %LOCALAPPDATA%/Microsoft/Office/15.0/OfficeFileCache/FSD-CNRY.FSD Type: VSDT_COM_DOS	2936
Write File	,	
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\000051191100000000000000000000000000000	2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\AceFiles\ntl_1033\tValue: 52980001	2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\AceFiles\ntl_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\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109E60090400000000000F01FE C\Usage\AceFiles\nt_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%UETE239.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\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	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\(15.0\)\Office\(FileCache\)\Loc alCacheFileEditManager\(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: \text{ 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\Current\Version\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\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	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%MicrosoftWindows ) Return: 1	2936	
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\History) Return: 1	2936	
Call Network API	API Name: PathrileExistsW Args: (%LOCALAPPDATA%Microsoftwindowstristory) Return: 1  API Name: socket Args: (23, 1, 6) Return: c0c	2936	
Call Network API  Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: cuc  API Name: socket Args: ( 2, 2, 0 ) Return: c68	2936	
Call Network API			
	API Name: Socket Args: ( 23, 2, 0 ) Return: c68  API Name: DesQuantity Args: ( bit do. 1, 40006000 ) Peturn: 67	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  Detection	API Name: bind Args: ( c68, 0.0.0.049423, 128 ) Return: 0  Threat Characteristic: Listens on port	2936	
Call System API	0.0.0.0/49423  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\nConnection: Keep-Alive\nUser-Agent: Microsoft Office Word 2013\n\nX-MSGETWEBURL: t\n\nX-IDCR L_ACCEPTED: t\n\nHost: bit.do\n\n\n\n\n, 1, 139 ) Return: 0	2936	
	API Name: WinHttpCloseHandle Args: ( c3f1360 ) Return: 1	2936	
Call System API		2936	
Call System API Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1	2930	
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\internet\Server Cache\Count Value: 1  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\internet\Server Cache\http://bit.do/\ Value: None	2936	
Write Registry Key			
Write Registry Key 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 Add Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\ Value: None  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Type Value: 0	2936 2936	

Write Registry Key	Key: HKFY CURRENT USER/SOFTWAREMicrosoft/Office\15.0/Common\nternet/Server Cache\htm://hit.do/AEaballMakier/dersion Value: 0	2936
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\Delgat\Maigar\Dersion\Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do/\CobaltMinor\Version\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, 0.0.0:49424, 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	2936
Call Network API	: bit.dol/nh/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	2936
	_ACCEPTED: tlrlnHost: bit.dolrlnlrln, 1, 139 ) Return: 0	
Call System API	API Name: WinHttpCloseHandle Args: ( c4ab470 ) Return: 1	2936
Write Registry Key	Key: HKEY CURRENT USER/SOFTWARE/Microsoft/Office\15.0\Common\Intermet\Server Cache\Count Value: 2	2936
	,	2936
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://bit.do\Value: None	
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; .NE T 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	
0.110.1471	0.0.0.49425	0000
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: (rd8, GET /f0zim HTTPf/1.1\n\nAccept: \name{\text{"\n'\n\u00ddlser.}} Net CLR 3.0.30729; NSOffice: MSOffice:	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\lNetCache\Content.MSO\E72166BA.htm Type: VSDT_TEXT_HTML	2936
Write File	Path: %LOCALAPPDATA%IMicrosoft\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\nConnec	2936
	tion: Keep-Alive\r\n\r\n, 1, 133) Return: 0	
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\NetCache\Content.MSO\13CA5373.wmf	
	File: %LOCALAPPDATA%initicrosofttvvindowstinetcachetcontent.inso/13caos73.wmi  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 2936
Call Internet Helper API Detection	API Name: Http:OpenRequestW Args: ( cc0008, GET, /images/bit-do-url-shortener-logo-66x66.png, , , 16344008, 4261904, 206270480 ) Return: cc000c  Threat Characteristic: Connects to remote URL or IP address	2930
retection	http://bit.do/images/bit-do-url-shortener-logo-66x66.png	
all Network API	API Name: recv Args: ( cf8, , 1, 2 ) Return: ?	2936
all 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; Wind	2936
	ows 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]\(n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	
all Network API	API Name: recv Args: ( cf8, , 1, 2 ) Return: ?	2936
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\::' Value: None	2936
/rite Registry Key	Key; HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000005119110000000000000000000000000000	2936
	C\Usage\WORDFiles Value: 52980135	
all Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\fQzim.url ) Return: 0	2936
dd File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII	2936
/rite File	Path: %APPDATA%\Microsoft\Office\Recent\fQzim.url Type: VSDT_ASCII	2936
all Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\bit.do.url ) Return: 0	2936
dd File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII	2936
/rite File	Path: %APPDATA%\Microsoft\Office\Recent\bit.do.url Type: VSDT_ASCII	2936
all Internet Helper API	API Name: NetShareEnum Args: ( , 503, 72599b90, -1, 12427ea4, 12427ea0, 0 ) Return: 0	2936
etection	Threat Characteristic: Executes commands or uses API to obtain system information  Process ID: 2936	
	Info: Enums share folder from API result	
all Service API	API Name: OpenServiceW Args: ( c4b8900, Webclient, 5 ) Return: c4b8770	2936
all System API	API Name: PathFileExistsW Args: ( %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms ) Return:	2936
olate DesistanK	1  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From #10#Forks (OWenDon From Active Name) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN From MINISTER (OWENDON FROM ACTIVE NAME) value Name  Ken HKEV CHEDENT HEEDIGGETHADEN FROM FROM ACTIVE NAME  KEN HKEV CHEDENT HEEDIGGETHADEN FROM ACTIVE NAME (OWENDON FROM ACTIVE NAM	2000
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startupltems\az\ Value: None	2936
all Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft\Schemas\MS Word_restart.xml) Return: 0	2936
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startupltems\"m' Value: None	2936 2936
elete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startupltems\Value: None	2936
elete Registry Key all System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Value: None	2936
rite Registry Key	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%Microsoft Office\Of	2936
rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F0F	2936
vitte registry recy	ECIUsagel Spelling And Grammar Files_3082 Value: 5298002e	2000
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00005109F100C040000000000F01F	2936
	ECiUsage\SpellingAndGrammarFiles_1036 Value: 5298002e	
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usaqe\Spelling\AndGrammarFiles 1033 \Value: 5298005f	2936
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F	2936
The registry rey	ECIUsagel Spelling And Grammar Files_3082 Value: 5298002f	2000
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\linstaller\UserData\S-1-5-18\Products\00005109F100A0C00000000000F0FF	2936
	ECiUsage\SpellingAndGrammarFiles_3082 Value: 52980030	
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036\Value: 5298002f	2936
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100C040000000000F01F	2936
	EClUsage\SpellingAndGrammarFiles_1036 Value: 52980030	
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE	2936
=	C\Usage\SpellingAndGrammarFiles_1033 Value: 52980060	
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usaqe\Spelling\AndGrammarFiles 1033 \Value: 52980061	2936
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Persion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE	2936
	C\Usage\SpellingAndGrammarFiles_1033 Value: 52980062	
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE	2936
	C\Usage\SpellingAndGrammarFiles_1033 Value: 52980063	0000
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FE  C\Usage\SpellingAndGrammarFiles_1033 Value: 52980064	2936
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE	2936
	C\Usage\SpellingAndGrammarFiles_1033 Value: 52980065	
all Service API	API Name: OpenServiceW Args: ( c6a48e8, Webclient, 5 ) Return: c6a4aa0	2936
all System API	API Name: PathFileExistsW Args: ( %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms ) Return: 1	2936
all System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office\Office\Office\Delta(\text{WINWORD.EXE}) Return: 1	2936
all Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%/Microsoft/Windows\\)NetCache\Content.\\ API Name: DeleteFileW Args: ( %LOCALAPPDATA%\\)Microsoft\\ Microsoft\\ Microsoft\ Microsoft\\ Microsoft\\ Microsoft\\ Microsoft\ Microsoft\ Microsoft\ Microsoft\ Microsoft\ Microsoft\ Microsoft\ Microsoft\ Mic	2936
	p) Return: 1	
all Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\E72166BA.htm ) Return: 1	2936
all System API	API Name: WinHttpCloseHandle Args: ( c3efee8 ) Return: 1	2936
all System API	API Name: WinHttpCloseHandle Args: ( 12ed5b8 ) Return: 1	2936
all System API	API Name: WinHttpCloseHandle Args: ( c345038 ) Return: 1	2936
rite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None	2936
all Filesystem API	API Name: DeleteFileW Args: ( %WorkingDir%\~\$quiry Sheet Lists 0240030019.docx ) Return: 1	2936
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	2936
rall Filosystom ABI	C\Usage\WORDFiles Value: 52980136  ADI Name: DelahaFile\W Ares: \( %\ OCAL APPDATA\\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\	2026
all Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Windows\INetCache\Content.Word\~WRS{0614E162-C183-4D98-99A4-7F938DBC8556}.tmp ) Return: 1	2936
elete File	Path: %LOCALAPPDATA%IMicrosoftWindowsIINetCachelContent.MSO\E72166BA.htm Type: VSDT_TEXT_HTML	2936
etection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection	
	Process ID: 2936  Fig. (CLOCAL ADDDATA) Microsoff Mindoun INAC cohol Contant MCONT73165DA htm.	
	File: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\E72166BA.htm	

Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\\NetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		2936
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\C4C10ED8.png Type: VSDT_PNG		2936
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\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%IMicrosoft\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\NetCache\Content.Word\~WRS{6EBF22BE-3A68-4B32-89E7-238C7FD9BB8F}.tm p ) 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\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		2936
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		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)%IMicrosoft Shared(Office15/msosqm.exe		
Call Mutex API	API Name: CreateMutexA Args: ( 0, 0, LocalMsoSqmExeMutex ) 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

