ID: 323572
Sample Name: guy2.exe
Cookbook: default.jbs
Time: 06:34:22
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

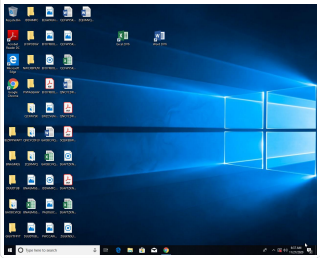
Analysis Report guy2.exe

Overview

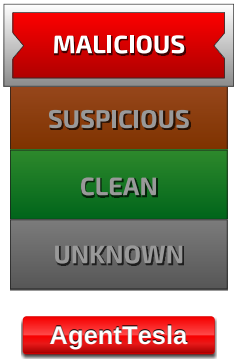
General Information

Sample Name:	guy2.exe
Analysis ID:	323572
MD5:	a0e65c4d3bc5fb5..
SHA1:	ff10833c4ba5793..
SHA256:	d8e273754006eb..
Tags:	AgentTesla PEP

Most interesting Screenshot:



Detection

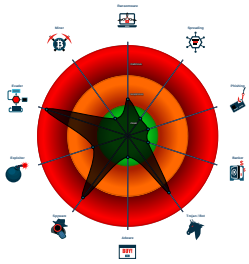


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- May check the online IP address of …
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other

Classification



Startup

- **System is w10x64**
- guy2.exe (PID: 5980 cmdline: 'C:\Users\user\Desktop\guy2.exe' MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - guy2.exe (PID: 3544 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
- xQxAsve.exe (PID: 6628 cmdline: 'C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe' MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 6760 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 6768 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 6776 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 6796 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
- xQxAsve.exe (PID: 6864 cmdline: 'C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe' MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 6928 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
  - xQxAsve.exe (PID: 7020 cmdline: {path} MD5: A0E65C4D3BC5FB564F82FE66AB228044)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.219413063.000000000338F000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000012.00000002.468356599.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.478360103.000000000311000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 22 entries

Source	Rule	Description	Author	Strings

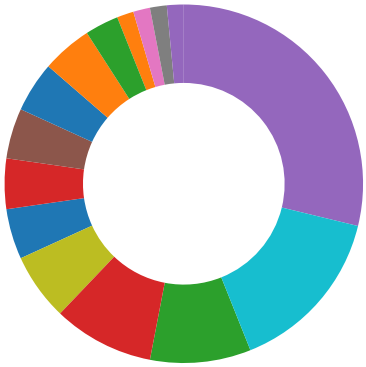
Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.xQxAsve.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.guy2.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
22.2.xQxAsve.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Moves itself to temp 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 Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

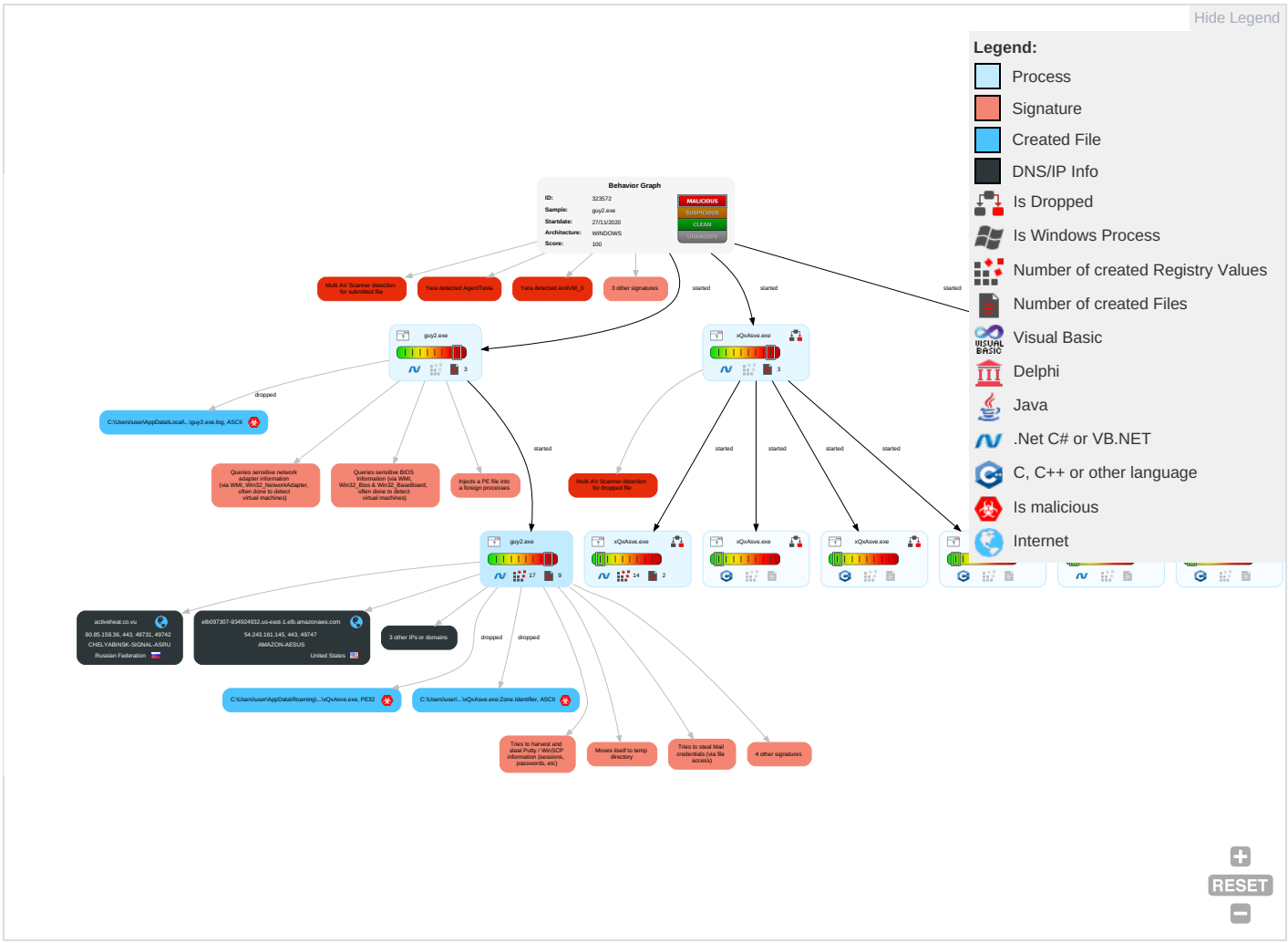
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3	Input Capture 1 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non App Lay Prot
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 3	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	App Lay Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1 1	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Prot Imp
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Con
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Con Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay

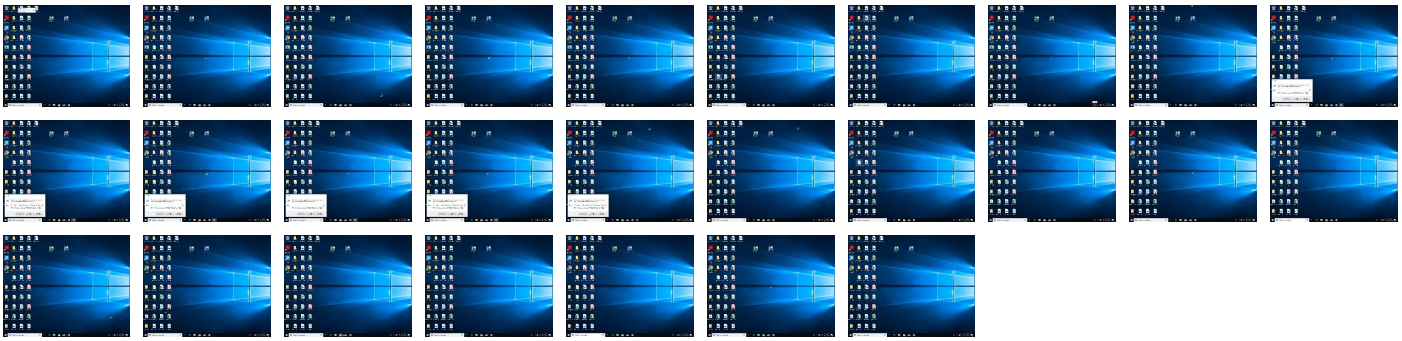
Behavior Graph



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
guy2.exe	59%	Virustotal		Browse
guy2.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe	44%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.xQxAsve.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.guy2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.2.xQxAsve.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://VHlE1Bk1DRzqSW.net853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://https://VHlE1Bk1DRzqSW.net	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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://api.ipify.org4	0%	Avira URL Cloud	safe	
http://https://VHlE1Bk1DRzqSW.net(	0%	Avira URL Cloud	safe	
http://wzhNVX.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://activeheat.co.vuD8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://activeheat.co.vu4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
activeheat.co.vu	80.85.159.36	true	false		high
elb097307-934924932.us-east-1.elb.amazonaws.com	54.243.161.145	true	false		high
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	guy2.exe, 00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.478360103.0000000003141000.00000004.00000001.sdmp, xQxAsve.exe, 00000016.00000002.479682422.0000000003011000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	guy2.exe, 00000000.00000002.224276106.000000000063D0000.00000002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757.00000000054C0000.00000002.00000001.sdmp, xQxAsve.exe, 00000013.00000002.331803714.00000000054E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	guy2.exe, 00000000.00000002.224276106.000000000063D0000.00000002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757.00000000054C0000.00000002.00000001.sdmp, xQxAsve.exe, 00000013.00000002.331803714.00000000054E0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	xQxAsve.exe, 00000013.00000002 .331803714.00000000054E0000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	xQxAsve.exe, 00000013.00000002 .331803714.00000000054E0000.00 000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://activeheat.co.vu	guy2.exe, 00000001.00000002.48 5266825.000000000361B000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.479155669. 0000000003205000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.480320849.00000000 030D5000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	xQxAsve.exe, 00000016.00000002 .479682422.0000000003011000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	guy2.exe, 00000001.00000002.48 0961942.0000000003308000.00000 004.00000001.sdmp	false		high

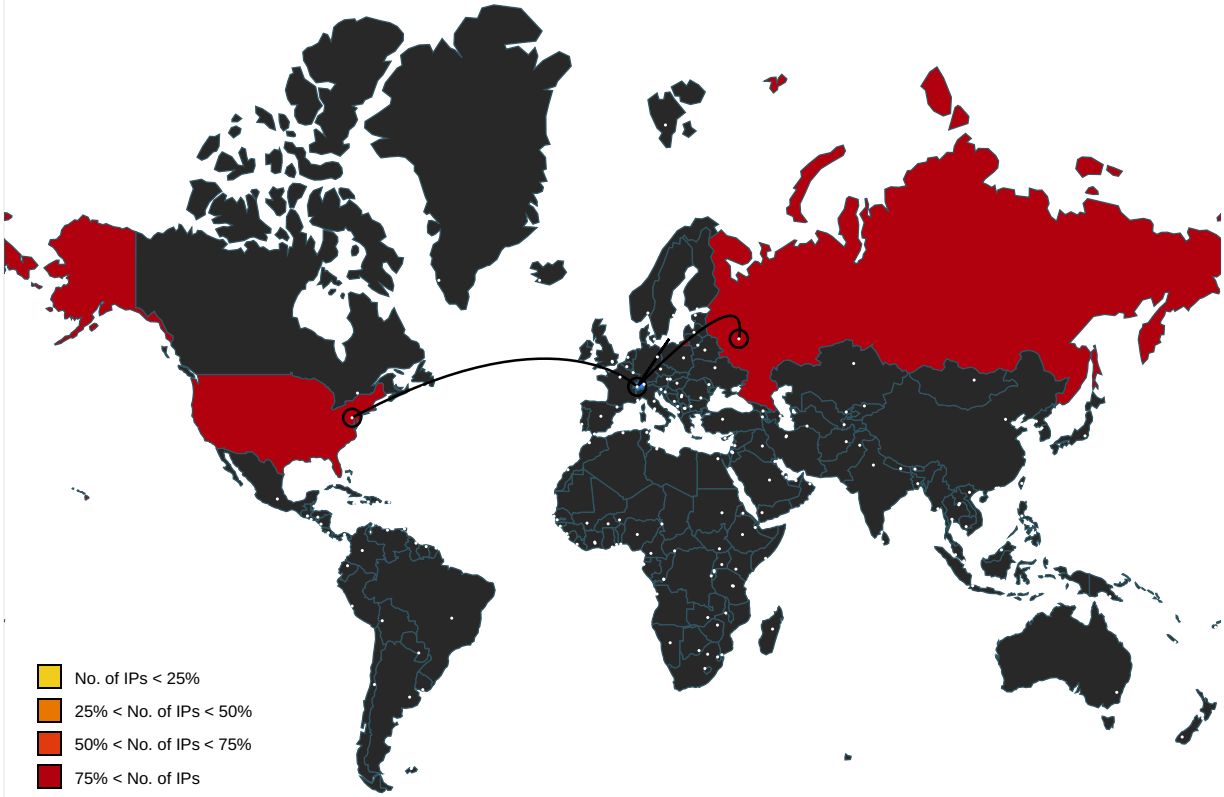
Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://VHlE1Bk1DRzqSW.net853321935-2125563209-4053062332-1002_Classes	guy2.exe, 00000001.00000003.44 3028222.00000000013A4000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://activeheat.co.vu	guy2.exe, 00000001.00000002.48 0411054.00000000032B1000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.479040941. 00000000031E8000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.480129247.00000000 030B8000.00000004.00000001.sdmp	false		high
http://https://VHlE1Bk1DRzqSW.net	guy2.exe, 00000001.00000002.48 4527766.00000000035B9000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	guy2.exe, 00000000.00000002.21 9413063.000000000338F000.00000 004.00000001.sdmp, guy2.exe, 0 0000001.00000002.480411054.000 00000032B1000.00000004.0000000 1.sdmp, xQxAsve.exe, 0000000E. 00000002.301983864.00000000025 51000.00000004.00000001.sdmp, xQxAsve.exe, 00000012.00000002 .479040941.00000000031E8000.00 000004.00000001.sdmp, xQxAsve.exe, 00000013.00000002.3237853 93.0000000002551000.00000004.0 0000001.sdmp, xQxAsve.exe, 000 00016.00000002.480129247.00000 000030B8000.00000004.00000001. sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip	guy2.exe, 00000000.00000002.22 0656712.0000000004351000.00000 004.00000001.sdmp, guy2.exe, 0 0000001.00000002.468399314.000 0000000402000.00000040.0000000 1.sdmp, xQxAsve.exe, 0000000E. 00000002.303356146.00000000035 51000.00000004.00000001.sdmp, xQxAsve.exe, 00000012.00000002 .468356599.0000000000402000.00 000040.00000001.sdmp, xQxAsve.exe, 00000013.00000002.3262359 62.0000000003511000.00000004.0 0000001.sdmp, xQxAsve.exe, 000 00016.00000002.468183567.00000 00000402000.00000040.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org/	guy2.exe, 00000001.00000002.48 0961942.0000000003308000.00000 004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	xQxAsve.exe, 00000016.00000002 .479682422.0000000003011000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	guy2.exe, 00000001.00000002.49 0167943.0000000006DAC000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.487451855. 00000000070B0000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.480320849.00000000 030D5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	guy2.exe, 00000001.00000002.48 0411054.00000000032B1000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.478360103. 0000000003141000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.479682422.00000000 03011000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org4	guy2.exe, 00000001.00000002.48 0961942.0000000003308000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://VHlE1Bk1DRzqSW.net(	guy2.exe, 00000001.00000002.48 4527766.00000000035B9000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://wzhNVX.com	xQxAsve.exe, 00000016.00000002 .479682422.0000000003011000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://activeheat.co.vuD8	guy2.exe, 00000001.00000002.48 5479189.0000000003633000.00000 004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://activeheat.co.vu4	guy2.exe, 00000001.00000002.48 4972239.00000000035F9000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.479040941. 00000000031E8000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.480129247.00000000 030B8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http:// https://activeheat.co.vu/dek/inc/f08405615b33f6.php127.0.0.1 POST	xQxAsve.exe, 00000016.00000002 .479682422.0000000003011000.00 000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	guy2.exe, 00000000.00000002.22 0656712.0000000004351000.00000 004.00000001.sdmp, guy2.exe, 0 0000001.00000002.468399314.000 0000000402000.00000040.0000000 1.sdmp, xQxAsve.exe, 0000000E. 00000002.303356146.00000000035 51000.00000004.00000001.sdmp, xQxAsve.exe, 00000012.00000002 .468356599.0000000000402000.00 000040.00000001.sdmp, xQxAsve.exe, 00000013.00000002.3262359 62.0000000003511000.00000004.0 0000001.sdmp, xQxAsve.exe, 000 00016.00000002.468183567.00000 00000402000.00000040.00000001. sdmp	false		high
http://www.jiyu-kobo.co.jp/	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	guy2.exe, 00000000.00000002.22 4276106.00000000063D0000.00000 002.00000001.sdmp, xQxAsve.exe, 0000000E.00000002.305542757. 00000000054C0000.00000002.0000 0001.sdmp, xQxAsve.exe, 000000 13.00000002.331803714.00000000 054E0000.00000002.00000001.sdmp	false		high
http://https://activeheat.co.vu/dek/inc/f08405615b33f6.php	guy2.exe, 00000001.00000002.48 0411054.00000000032B1000.00000 004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.479040941. 00000000031E8000.00000004.0000 0001.sdmp, xQxAsve.exe, 000000 16.00000002.480129247.00000000 030B8000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	guy2.exe, 00000001.00000003.44 5751971.0000000001301000.00000 004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	guy2.exe, 00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp, xQxAsve.exe, 00000012.00000002.478360103.0000000003141000.00000004.00000001.sdmp, xQxAsve.exe, 00000016.00000002.479682422.00000000003011000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.243.161.145	unknown	United States		14618	AMAZON-AESUS	false
80.85.159.36	unknown	Russian Federation		44493	CHELYABINSK-SIGNAL-ASRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323572
Start date:	27.11.2020
Start time:	06:34:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	guy2.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
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.evad.winEXE@17/5@7/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.255.188.83, 168.61.161.212, 51.104.139.180, 2.20.84.85, 20.54.26.129, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 204.79.197.200, 13.107.21.200 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:35:16	API Interceptor	735x Sleep call for process: guy2.exe modified

Time	Type	Description
06:35:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run xQxAsve C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
06:35:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run xQxAsve C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
06:35:52	API Interceptor	919x Sleep call for process: xQxAsve.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.243.161.145	1125_56873981.doc	Get hash	malicious	Browse	• api.ipify.org/
	REQUEST FOR QUOTATION-6container.exe	Get hash	malicious	Browse	• api.ipify.org/
	Request for Quote.doc	Get hash	malicious	Browse	• api.ipify.org/
	fw314FjnwM.exe	Get hash	malicious	Browse	• api.ipify.org/
	mT4sVN5EMN.exe	Get hash	malicious	Browse	• api.ipify .orghttp:/ /api.ipify.org/? format=json
	SecuriteInfo.com.ArtemisA49347BCE7B1.exe	Get hash	malicious	Browse	• api.ipify.org/
	JwzZ6mkzIG.exe	Get hash	malicious	Browse	• api.ipify.org/
	scandocuments_pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ_NEW029287652267.exe	Get hash	malicious	Browse	• api.ipify.org/
	Delivery Note - AWD 200038485852- 234920301190.exe	Get hash	malicious	Browse	• api.ipify.org/
	chibuike17.exe	Get hash	malicious	Browse	• api.ipify.org/
	file.exe	Get hash	malicious	Browse	• api.ipify.org/
	5fNtovgDmX.exe	Get hash	malicious	Browse	• api.ipify.org/
	0Cnb8v0C53.exe	Get hash	malicious	Browse	• api.ipify.org/? format=xml
	P9OFS5NEj0.exe	Get hash	malicious	Browse	• api.ipify.org/? format=xml
	VRRh2DUTnA.exe	Get hash	malicious	Browse	• api.ipify.org/? format=xml
	Payment.exe	Get hash	malicious	Browse	• api.ipify.org/
80.85.159.36	Cs8BfAoDKm.exe	Get hash	malicious	Browse	
	GDRw7Y75g7.exe	Get hash	malicious	Browse	
	XyCyrhKd87.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 54.225.169.28
	INVOICE.xlsx	Get hash	malicious	Browse	• 54.204.14.42
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	1125_56873981.doc	Get hash	malicious	Browse	• 54.243.161.145
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.235.142.93
	ER mexico.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 54.243.164.148
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 50.19.252.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7042.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.BackDoor.SpyBotNET.25.30157.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.Trojan.PackedNET.469.31999.exe	Get hash	malicious	Browse	• 54.204.14.42
	Cs8BfAoDKm.exe	Get hash	malicious	Browse	• 54.235.83.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
activeheat.co.vu	Cs8BfAoDKm.exe	Get hash	malicious	Browse	• 80.85.159.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0lnkkq0sM5FeXPK9l7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8l8OtTRdlg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOlU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rl4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2Bl4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 23.20.225.204
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 52.2.188.208
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 52.205.236.122
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	http://searchlf.com	Get hash	malicious	Browse	• 34.196.190.195
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 50.16.119.144
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 3.225.133.96
CHELYABINSK-SIGNAL-ASRU	Cs8BfAoDKm.exe	Get hash	malicious	Browse	• 80.85.159.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GDRw7Y75g7.exe	Get hash	malicious	Browse	• 80.85.159.36
	XyCyrhKd87.exe	Get hash	malicious	Browse	• 80.85.159.36
	order updated Dwg for new order-100920-0086.exe	Get hash	malicious	Browse	• 185.118.165.47
	Invoice No. 26647.exe	Get hash	malicious	Browse	• 185.118.165.47
	file.11.20.doc	Get hash	malicious	Browse	• 185.118.167.118
	file.11.20.doc	Get hash	malicious	Browse	• 185.118.167.118
	require-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	file.11.20.doc	Get hash	malicious	Browse	• 185.118.167.118
	require-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	require-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	dictate-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	decree 11.04.2020.doc	Get hash	malicious	Browse	• 185.118.167.183
	dictate-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	dictate-11.20.doc	Get hash	malicious	Browse	• 185.118.167.183
	decree 11.04.2020.doc	Get hash	malicious	Browse	• 185.118.167.183
	decree 11.04.2020.doc	Get hash	malicious	Browse	• 185.118.167.183
	kDxFrV4k9U.exe	Get hash	malicious	Browse	• 80.85.156.116
	certificate_010.19.2020.doc	Get hash	malicious	Browse	• 80.85.158.53
	certificate_010.19.2020.doc	Get hash	malicious	Browse	• 80.85.158.53

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Exodus.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	Order 51897.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	98650107.pdf.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	Izezma64.dll	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	fuxenm32.dll	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	ER mexico.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.6057.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.ArtemisTrojan.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7042.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.BackDoor.SpyBotNET.25.30157.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	SecuriteInfo.com.Trojan.PackedNET.469.31999.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36
	Cs8BfAoDKm.exe	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ URGENT NEW ORDER#001_XLS.EXE	Get hash	malicious	Browse	• 54.243.161.145 • 80.85.159.36

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\guy2.exe.log	
Process:	C:\Users\user\Desktop\guy2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xQxAsve.exe.log	
Process:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\guy2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB

C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe	
Process:	C:\Users\user\Desktop\guy2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	510976
Entropy (8bit):	7.72947163728595
Encrypted:	false
SSDEEP:	12288:61b4JO3PrN2iN865O/Tw2dXiQSb8gWT60VDZGht8LF:gb4JO3jN1S55dXib8gV05Zq8
MD5:	A0E65C4D3BC5FB564F82FE66AB228044
SHA1:	FF10833C4BA57938F94C41B75D824AC9E8FE36B4
SHA-256:	D8E273754006EB7118BE058C46EFEF0A1B20AE4929DAD75ECFED1AE1AAE0C0EB
SHA-512:	A73FEA650D5E09338C8792BA22FBC530627C1DCA735630065DB8D1B63DC8B76F69D23DFEC492CA123148BA414464D9FD4EEBDB0DD3B0CDC083E57191C636F0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u._.....0..... .....@.. .....@..... ..@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....r...c.....x...D...@.....0..G.....}.....(.....(.....s...}.....{....o.....(.....{.....{....o....*..0.....(.....{....{.....(....~....vl.....,..{....{....o.....{....{.....o....o.....{....(....}.....o.....3..{....{....o.....+....,@..{....{....o....s.....{.....{....{....o.....{....{....o.....*...{....(...o!.....{....~....o"....*...{....(#...o!.....{....~....o"....*...0..+.....,..{.....+....,...{.

C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\guy2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.72947163728595
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	guy2.exe
File size:	510976

General

MD5:	a0e65c4d3bc5fb564f82fe66ab228044
SHA1:	ff10833c4ba57938f94c41b75d824ac9e8fe36b4
SHA256:	d8e273754006eb7118be058c46efef0a1b20ae4929dad75ecfed1ae1aae0c0eb
SHA512:	a73fea650d5e09338c8792ba22fbc530627c1dca735630065db8d1b63dc8b76f69d23dfec492ca123148ba414464d9fd4eebdb0dd3b0cdc083e57191c636f720
SSDEEP:	12288:61b4JO3PrN2iN865O/Tw2dXiQSb8gWT60VDZGht8LF:gb4JO3jN1S55dXib8gV05Zq8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u._.....0..... ....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47e0d6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBF75EB [Thu Nov 26 09:31:23 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7e084	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x5b8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7c0dc	0x7c200	False	0.837542484894	COM executable for DOS	7.73806831255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5b8	0x600	False	0.429036458333	data	4.09670187577	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x80090	0x328	data		
RT_MANIFEST	0x803c8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

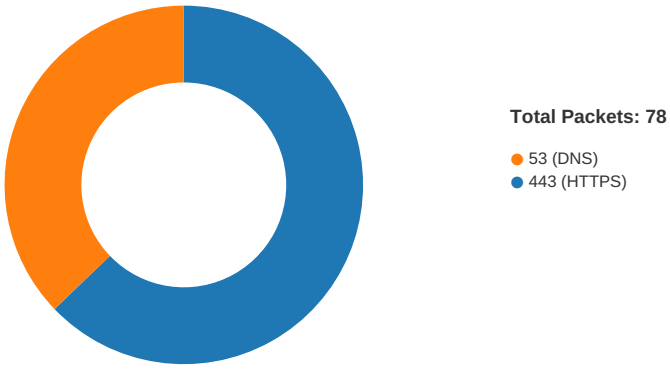
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2020
Assembly Version	1.0.0.0
InternalName	OS.exe
FileVersion	1.0.0.0

Description	Data
CompanyName	Vendetta Inc.
LegalTrademarks	
Comments	
ProductName	Aku Form
ProductVersion	1.0.0.0
FileDescription	Aku Form
OriginalFilename	OS.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 06:35:42.780715942 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:42.869282961 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:42.869483948 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:42.940324068 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.032150984 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032182932 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032196999 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032208920 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032222033 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032232046 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.032341957 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.090656042 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.178728104 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.218417883 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.430408001 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.520558119 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.562222004 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.674767971 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:43.783885956 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.788064957 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:43.788158894 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:35:48.789292097 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:48.789359093 CET	443	49731	80.85.159.36	192.168.2.3
Nov 27, 2020 06:35:48.792985916 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.561378956 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.646553040 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.646697044 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.738228083 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.822659969 CET	443	49742	80.85.159.36	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 06:36:25.823120117 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.823177099 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.823220968 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.823236942 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.823250055 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.823308945 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.826543093 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.831581116 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:25.916596889 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:25.956355095 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.043056011 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.130143881 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.131346941 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.162440062 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.227655888 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.231195927 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.231350899 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.250801086 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.251027107 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.308250904 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.396351099 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.397814035 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.397836924 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.397854090 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.397866964 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.398065090 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.398099899 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.402324915 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.408324957 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.497232914 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.550127029 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.596128941 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.687160015 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.690042973 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:26.788806915 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.794173956 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:26.794421911 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:31.236711025 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:31.236762047 CET	443	49742	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:31.236824989 CET	49742	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:31.800113916 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:31.800463915 CET	443	49743	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:31.800681114 CET	49743	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:43.995280027 CET	49731	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:43.996757984 CET	49745	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:44.082891941 CET	443	49745	80.85.159.36	192.168.2.3
Nov 27, 2020 06:36:44.082979918 CET	49745	443	192.168.2.3	80.85.159.36
Nov 27, 2020 06:36:56.603790998 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.706784964 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.706906080 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.707495928 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.810539007 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.810589075 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.810622931 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.810655117 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.810683012 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.810708046 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.810766935 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.811727047 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.835602045 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.938765049 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:36:56.990135908 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:56.994956017 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:36:57.100821972 CET	443	49747	54.243.161.145	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 06:36:57.146384954 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:37:05.639552116 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:37:05.743084908 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:37:05.743105888 CET	443	49747	54.243.161.145	192.168.2.3
Nov 27, 2020 06:37:05.743189096 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:37:05.743263960 CET	49747	443	192.168.2.3	54.243.161.145
Nov 27, 2020 06:37:06.021018982 CET	49748	443	192.168.2.3	80.85.159.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 06:35:05.527204990 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:05.562722921 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:06.547791004 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:06.583292961 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:07.221653938 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:07.248811960 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:08.337989092 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:08.365093946 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:09.374047041 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:09.401307106 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:10.498193026 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:10.527770996 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:11.553212881 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:11.580805063 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:12.569529057 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:12.604892969 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:13.611418962 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:13.638717890 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:14.659322977 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:14.704514027 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:15.532130957 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:15.559286118 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:16.628631115 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:16.655605078 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:19.816878080 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:19.852576017 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:32.030726910 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:32.057739973 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:39.688111067 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:39.730329037 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:42.558103085 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:42.695727110 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:51.592988014 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:51.643186092 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 06:35:55.280731916 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:35:55.320084095 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:07.437165022 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:07.464298010 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:11.865447044 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:11.902117014 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:25.307754040 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:25.433378935 CET	53	60633	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:26.097640991 CET	61292	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:26.133351088 CET	53	61292	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:42.998397112 CET	63619	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:43.026184082 CET	53	63619	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:44.377599955 CET	64938	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:44.412810087 CET	53	64938	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:44.945775032 CET	61946	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:44.991517067 CET	53	61946	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:56.531215906 CET	64910	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:36:56.558594942 CET	53	64910	8.8.8.8	192.168.2.3
Nov 27, 2020 06:36:56.575598001 CET	52123	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 06:36:56.602844954 CET	53	52123	8.8.8.8	192.168.2.3
Nov 27, 2020 06:37:05.984216928 CET	56130	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:37:06.019807100 CET	53	56130	8.8.8.8	192.168.2.3
Nov 27, 2020 06:37:17.993158102 CET	56338	53	192.168.2.3	8.8.8.8
Nov 27, 2020 06:37:18.020297050 CET	53	56338	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 06:35:42.558103085 CET	192.168.2.3	8.8.8.8	0x9aee	Standard query (0)	activeheat.co.vu	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:25.307754040 CET	192.168.2.3	8.8.8.8	0x54c6	Standard query (0)	activeheat.co.vu	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:26.097640991 CET	192.168.2.3	8.8.8.8	0x4b05	Standard query (0)	activeheat.co.vu	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:44.377599955 CET	192.168.2.3	8.8.8.8	0xf9d5	Standard query (0)	activeheat.co.vu	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.531215906 CET	192.168.2.3	8.8.8.8	0x4a37	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.575598001 CET	192.168.2.3	8.8.8.8	0x11b6	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 06:37:05.984216928 CET	192.168.2.3	8.8.8.8	0xf43f	Standard query (0)	activeheat.co.vu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 06:35:42.695727110 CET	8.8.8.8	192.168.2.3	0x9aee	No error (0)	activeheat.co.vu		80.85.159.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:25.433378935 CET	8.8.8.8	192.168.2.3	0x54c6	No error (0)	activeheat.co.vu		80.85.159.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:26.133351088 CET	8.8.8.8	192.168.2.3	0x4b05	No error (0)	activeheat.co.vu		80.85.159.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:44.412810087 CET	8.8.8.8	192.168.2.3	0xf9d5	No error (0)	activeheat.co.vu		80.85.159.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.558594942 CET	8.8.8.8	192.168.2.3	0x4a37	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 27, 2020 06:36:56.602844954 CET	8.8.8.8	192.168.2.3	0x11b6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 27, 2020 06:37:06.019807100 CET	8.8.8.8	192.168.2.3	0xf43f	No error (0)	activeheat.co.vu		80.85.159.36	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

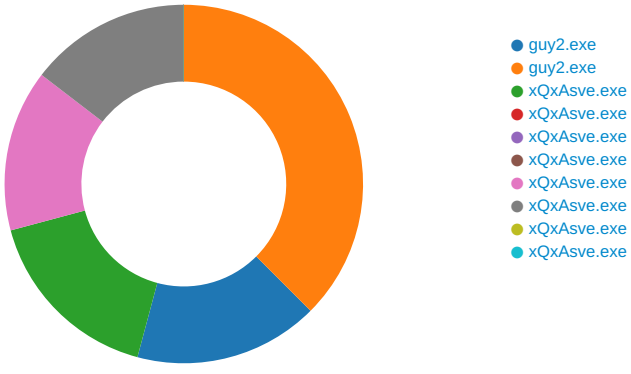
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 06:35:43.032232046 CET	80.85.159.36	443	192.168.2.3	49731	CN=activeheat.co.vu CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 25 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Feb 24 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 27, 2020 06:36:25.826543093 CET	80.85.159.36	443	192.168.2.3	49742	CN=activeheat.co.vu CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 25 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Feb 24 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 27, 2020 06:36:26.402324915 CET	80.85.159.36	443	192.168.2.3	49743	CN=activeheat.co.vu CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Nov 25 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Feb 24 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 27, 2020 06:36:56.811727047 CET	54.243.161.145	443	192.168.2.3	49747	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: guy2.exe PID: 5980 Parent PID: 5696

General

Start time:	06:35:09
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\guy2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\guy2.exe'
Imagebase:	0xec0000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 00000000.00000002.219413063.000000000338F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.220656712.0000000004351000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\guy2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\guy2.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1FC907	WriteFile

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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: guy2.exe PID: 3544 Parent PID: 5980

General

Start time:	06:35:17
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\guy2.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd90000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.480411054.00000000032B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.468399314.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming\xQxAsve	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\th3yaotv.tsz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CD3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe:Zone.Identifier	success or wait	1	65CBC9A	DeleteFileW
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	success or wait	1	6CD36A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\guy2.exe	C:\Users\user\AppData\Local\Temp\tmpG946.tmp	success or wait	1	65CC2B2	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 eb 75 bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 c2 07 00 00 08 00 00 00 00 00 00 d6 e0 07 00 00 20 00 00 00 00 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 08 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....u._......... ....0................. ....@.. ....@ ....@................	success or wait	4	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD3DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD3DD66	CopyFileW

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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\e0c6bd35-64dc-4753-a898-548701c1c4ef	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\th3yaotv.tsz\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	xQxAsve	unicode	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe	success or wait	1	6CD3646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	xQxAsve	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CD3DE2E	RegSetValueExW

Analysis Process: xQxAsve.exe PID: 6628 Parent PID: 3388

General

Start time:	06:35:50
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe'
Imagebase:	0xc0000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 0000000E.00000002.303356146.0000000003551000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.302094753.0000000002593000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 44%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xQxAsve.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\xQxAsve.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1FC907	WriteFile

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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: xQxAsve.exe PID: 6760 Parent PID: 6628

General

Start time:	06:35:53
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1f0000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xQxAsve.exe PID: 6768 Parent PID: 6628

General

Start time:	06:35:54
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2c0000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xQxAsve.exe PID: 6776 Parent PID: 6628

General

Start time:	06:35:54
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x130000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xQxAsve.exe PID: 6796 Parent PID: 6628

General

Start time:	06:35:55
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xce0000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 00000012.00000002.468356599.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.478360103.0000000003141000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.478360103.0000000003141000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown

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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: xQxAsve.exe PID: 6864 Parent PID: 3388

General

Start time:	06:35:58
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe'
Imagebase:	0x10000

File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 00000013.00000002.326235962.0000000003511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.323785393.0000000002551000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown

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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: xQxAsve.exe PID: 6928 Parent PID: 6864

General

Start time:	06:36:03
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x320000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: xQxAsve.exe PID: 7020 Parent PID: 6864

General

Start time:	06:36:04
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\xQxAsve\xQxAsve.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc80000
File size:	510976 bytes
MD5 hash:	A0E65C4D3BC5FB564F82FE66AB228044
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: 00000016.00000002.479682422.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.479682422.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.468183567.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis