ID: 669376
Sample Name: 6xfFjxyRXf
Cookbook: default.jbs
Time: 01:10:42
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

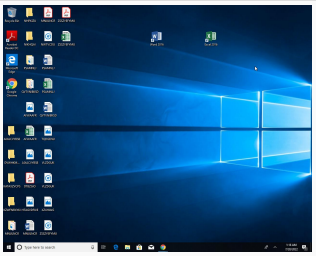
Windows Analysis Report

6xfFjxyRXf

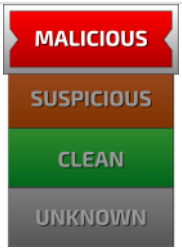
Overview

General Information

Sample Name:	6xfFjxyRXf (renamed file extension from none to dll)
Analysis ID:	669376
MD5:	f63300c5bbb25b..
SHA1:	663b6080201bb8.
SHA256:	9ba940714eb156.
Tags:	32 dll exe trojan
Infos:	



Detection



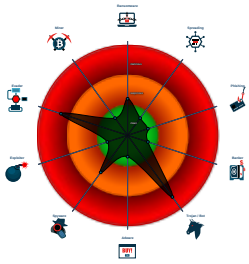
Emotet

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to query local…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6908 cmdline: loaddll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6916 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6944 cmdline: rundll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6932 cmdline: regsvr32.exe /s C:\Users\user\Desktop\6xfFjxyRXf.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 7052 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Nrzawqzutwib\qenu.dlv" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6968 cmdline: rundll32.exe C:\Users\user\Desktop\6xfFjxyRXf.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7068 cmdline: rundll32.exe C:\Users\user\Desktop\6xfFjxyRXf.dll,DllUnregisterServerrrrrrrrrrrr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5776 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7048 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2764 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4348 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5764 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "184.134.163.2:1",
    "192.16.0.0:1472",
    "180.4.0.0:1",
    "148.4.0.0:1",
    "116.4.0.0:1",
    "160.4.0.0:1",
    "128.4.0.0:1",
    "164.4.0.0:1",
    "124.4.0.0:1",
    "176.4.0.0:1",
    "232.22.167.2:48",
    "144.23.167.2:48",
    "195.194.0.0:7080",
    "241.253.2.0:2848",
    "112.135.213.118:5",
    "235.253.2.0:2848",
    "255.255.255.255:3",
    "243.253.2.0:3908",
    "245.253.2.0:5388",
    "192.141.163.2:1",
    "249.253.2.0:2864",
    "28.188.226.4:4597",
    "255.178.3.0:1432",
    "208.146.163.2:1",
    "250.178.3.0:5056",
    "92.179.3.0:808",
    "24.149.166.2:1",
    "94.179.3.0:2448",
    "246.178.3.0:5208",
    "208.60.169.2:1",
    "136.86.171.2:1",
    "32.76.231.4:1"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.406595295.0000000000BF0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.406595295.0000000000BF0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.406684150.0000000000C21000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.406684150.0000000000C21000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.415134102.0000000004F61000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.4f00000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.4f00000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4680000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4680000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.46b0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 19 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.6 - Destination IP: 119.193.124.41	
Timestamp:	192.168.2.6119.193.124.414985970802404304 07/20/22-01:13:31.686515
SID:	2404304
Source Port:	49859
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.6 - Destination IP: 51.91.76.89	
Timestamp:	192.168.2.651.91.76.894984480802404338 07/20/22-01:13:29.114997
SID:	2404338
Source Port:	49844
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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)

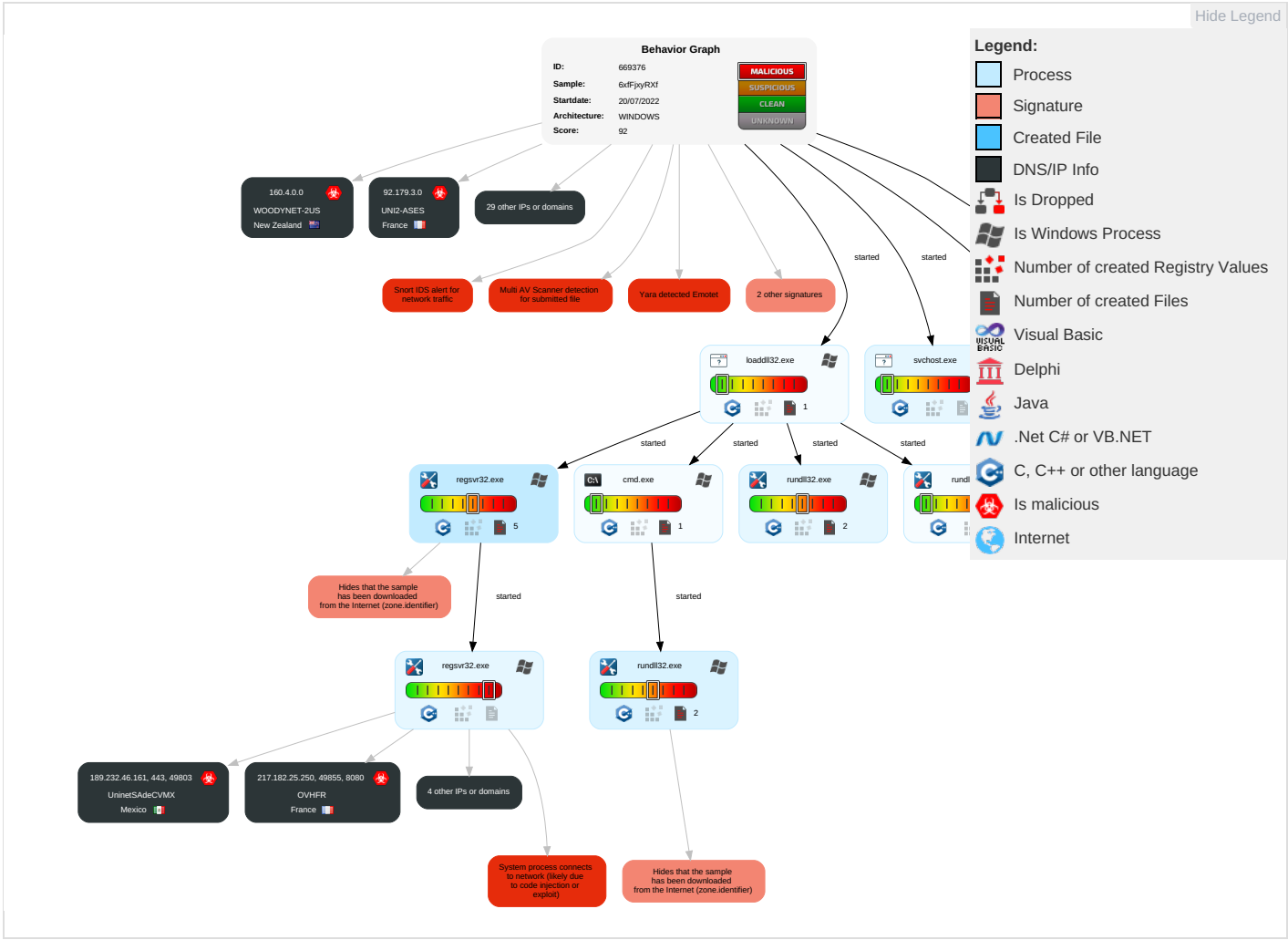
Stealing of Sensitive Information

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	1 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	2 Input Capture	2 System Time Discovery	Remote Services	2 Input Capture	Exfiltration Over Other Network Medium	1 2 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 DLL Side-Loading	2 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	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	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 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	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Application Window 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	1 Remote System 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	2 File and Directory 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	2 6 System Information Discovery	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 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

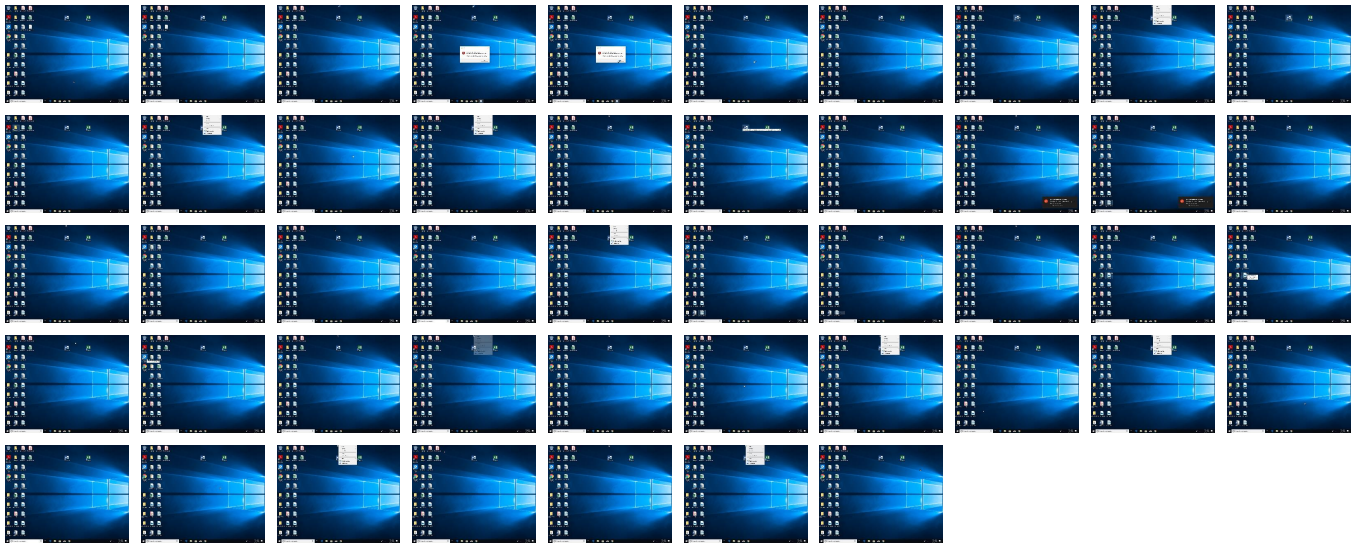
Behavior Graph



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
6xfFjxyRXf.dll	70%	Virustotal		Browse
6xfFjxyRXf.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4680000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.regsvr32.exe.4f00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.c20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.regsvr32.exe.4480000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4f60000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.46b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.2b50000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.bf0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

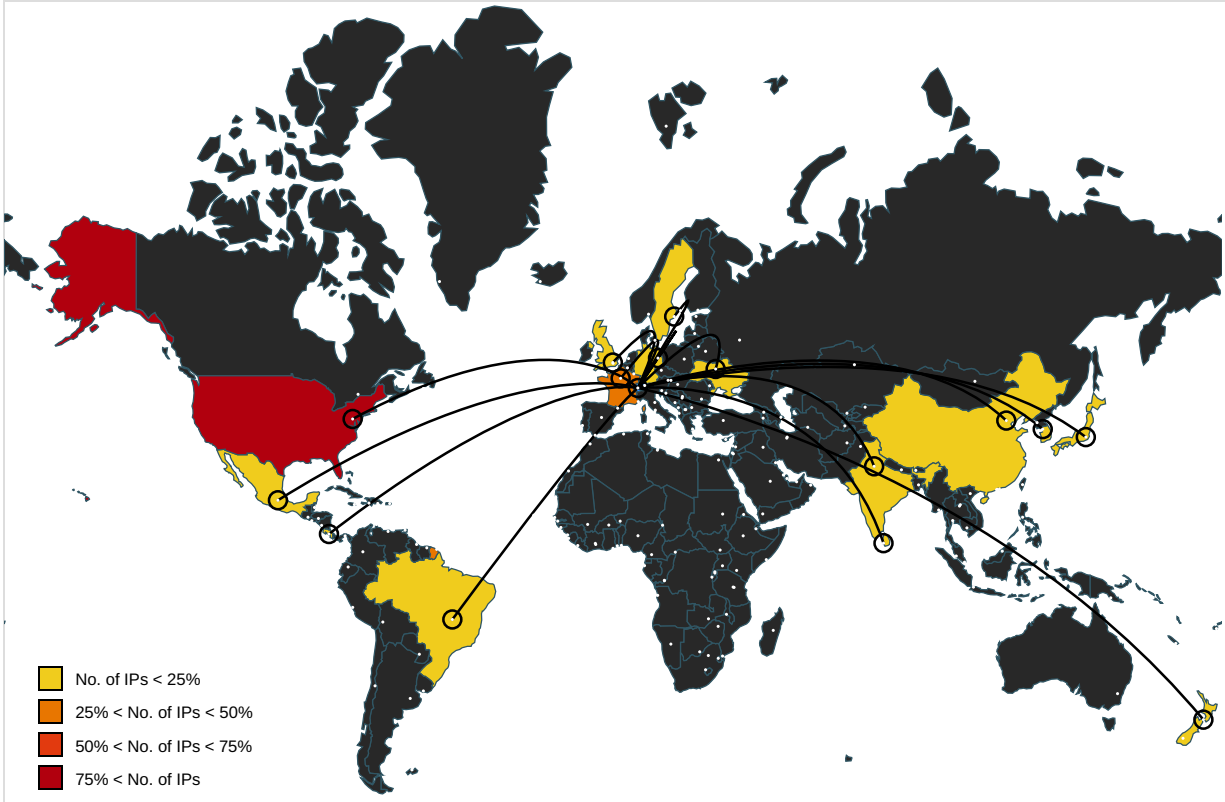
Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000000E.00000003.571353182.0000023F14388000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000000E.00000003.571353182.0000023F14388000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000000E.00000003.571353182.0000023F14388000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 0000000E.00000003.565704127.0000023F14819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564883544.0000023F14388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564185932.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.565394424.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564280175.0000023F14802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564163015.0000023F1439A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564576094.0000023F14803000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000000E.00000003.565704127.0000023F14819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564883544.0000023F14388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564185932.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.565394424.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564280175.0000023F14802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564163015.0000023F1439A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564576094.0000023F14803000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000000E.00000003.565704127.0000023F14819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564883544.0000023F14388000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564185932.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.565394424.0000023F143AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564280175.0000023F14802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564163015.0000023F1439A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.564576094.0000023F14803000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000000E.00000003.571353182.0000023F14388000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.182.25.250	unknown	France		16276	OVHFR	true
160.4.0.0	unknown	New Zealand		715	WOODYNET-2US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.4.0.0	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
235.253.2.0	unknown	Reserved		unknown	unknown	true
249.253.2.0	unknown	Reserved		unknown	unknown	true
32.76.231.4	unknown	United States		2686	ATGS-MMD-ASUS	true
246.178.3.0	unknown	Reserved		unknown	unknown	true
184.134.163.2	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	true
136.86.171.2	unknown	United States		60311	ONEFMCH	true
208.146.163.2	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	true
116.4.0.0	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	true
92.179.3.0	unknown	France		12479	UNI2-ASES	true
189.232.46.161	unknown	Mexico		8151	UninetSAdeCVMX	true
245.253.2.0	unknown	Reserved		unknown	unknown	true
148.4.0.0	unknown	United States		6074	LIUNETUS	true
94.179.3.0	unknown	Ukraine		6849	UKRTELNETUA	true
192.16.0.0	unknown	United States		14153	EDGECAST-IRUS	true
208.60.169.2	unknown	United States		6389	BELLSOUTH-NET-BLKUS	true
176.4.0.0	unknown	Germany		12638	AS12638DuesseldorfDE	true
128.4.0.0	unknown	United States		2	UDEL-DCNUS	true
243.253.2.0	unknown	Reserved		unknown	unknown	true
232.22.167.2	unknown	Reserved		unknown	unknown	true
195.194.0.0	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	true
241.253.2.0	unknown	Reserved		unknown	unknown	true
144.23.167.2	unknown	Costa Rica		64102	OracleCorporationCR	true
255.178.3.0	unknown	Reserved		unknown	unknown	true
51.91.76.89	unknown	France		16276	OVHFR	true
24.149.166.2	unknown	United States		11025	COMCAST-HOUSTONUS	true
28.188.226.4	unknown	United States		7922	COMCAST-7922US	true
124.4.0.0	unknown	India		18302	SKG_NW-AS-KRSKTelecomKR	true
164.4.0.0	unknown	Sweden		44013	SANDVIK-ASSE	true
250.178.3.0	unknown	Reserved		unknown	unknown	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
216.120.236.62	unknown	United States		23535	HOSTROCKETUS	true
112.135.213.118	unknown	Sri Lanka		9329	SLTINT-AS-APSriLankaTelecomInternetLK	true
192.141.163.2	unknown	Brazil		267489	NEOVEXCOMERCIOESERVICOSDETELECOMUNICACOESBR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669376
Start date and time: 20/07/202201:10:42	2022-07-20 01:10:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 37s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	6xfFjxyRXf (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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:	mal92.troj.evad.winDLL@18/2@0/37
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44% (good quality ratio 42.4%) • Quality average: 81.3% • Quality standard deviation: 25.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.40.136.238, 20.223.24.244, 8.241.126.121, 8.248.137.254, 67.26.75.254, 8.238.85.126, 8.248.131.254
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, iris-de-prod-azsc-frc-b.francecentral.cloudapp.azure.com, fg.download.windowsupdate.com.c.footprint.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
01:13:15	API Interceptor	5x Sleep call for process: svchost.exe modified

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\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.127441018847852
Encrypted:	false
SSDEEP:	6:kKk1jku+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:puNkPlE99SNxAhUeE1
MD5:	AF04AB9D40C3B4C211623015BF58DC1B
SHA1:	4089F3384FE9EA0D5236768F1C80DC587BF583B0
SHA-256:	F17D96764E1BAFA37695F143754C0A075AFA0D4950E1DE7FDCB4B260AA47EFA3
SHA-512:	8594DD11B66BDFD68059329F9D453431F4F16EE70C44291CBC7A9463AE7095FDAFD889817556728EDFFA1598CE9D3C2107E31DF73AE541D784695D2D4A96F37
Malicious:	false
Preview:	p..... .....KX.....(..... ....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.926205785552602
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

File name:	6xfFjxyRXf.dll
File size:	421888
MD5:	f63300c5bbb25b90839996a6d1b8daf3
SHA1:	663b6080201bb8258c3a17b552094ae25d0ae9eb
SHA256:	9ba940714eb15665a5e28c43c1e4d1dee3f086d76c197015e0aa4b40b809ded0
SHA512:	79c208f7bd35ee1d6d886184ff1985c78df7acd0282de544e21122ec00e7893bcf1fe6447838679809c7ef8a5da2ef4df4b8b8976db737b41e0cae691661c26d
SSDEEP:	12288:zwn2hR3547jpDMgySAxpuCMS5AhugWarPU:DRJ47xjyXpuCMSqumrP
TLSH:	7094CF0272D0C47AC6EF23785D239B5AA7F9FC208A75C647A751BF8D5E326C1893034A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..... .....2.....j.....Rich.....

File Icon

Icon Hash:	ccccccccd8d2dccc

Static PE Info

General

Entrypoint:	0x100118aa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x623F4EFA [Sat Mar 26 17:35:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	8f8b1cb86c6697dd342b65a36c6ccbb5

Entrypoint Preview

Instruction
push 0000000Ch
push 1002E838h
call 00007F2E98C687AFh
xor eax, eax
inc eax
mov dword ptr [ebp-1Ch], eax
mov esi, dword ptr [ebp+0Ch]
xor edi, edi
cmp esi, edi
jne 00007F2E98C6738Eh
cmp dword ptr [1003A15Ch], edi
je 00007F2E98C67439h
mov dword ptr [ebp-04h], edi
cmp esi, eax
je 00007F2E98C67387h
cmp esi, 02h
jne 00007F2E98C673B3h
mov eax, dword ptr [1003BA54h]
cmp eax, edi
je 00007F2E98C6738Eh

Instruction
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call eax
mov dword ptr [ebp-1Ch], eax
cmp dword ptr [ebp-1Ch], edi
je 00007F2E98C6740Bh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007F2E98C671A7h
mov dword ptr [ebp-1Ch], eax
cmp eax, edi
je 00007F2E98C673F4h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007F2E98C5BA3Ah
mov dword ptr [ebp-1Ch], eax
cmp esi, 01h
jne 00007F2E98C67390h
cmp eax, edi
jne 00007F2E98C6738Ch
push ebx
push edi
push dword ptr [ebp+08h]
call 00007F2E98C6717Dh
cmp esi, edi
je 00007F2E98C67387h
cmp esi, 03h
jne 00007F2E98C673ABh
push ebx
push esi
push dword ptr [ebp+08h]
call 00007F2E98C6716Ah
test eax, eax
jne 00007F2E98C67385h
mov dword ptr [ebp-1Ch], edi
cmp dword ptr [ebp-1Ch], edi
je 00007F2E98C67395h
mov eax, dword ptr [1003BA54h]
cmp eax, edi
je 00007F2E98C6738Ch
push ebx
push esi
push dword ptr [ebp+08h]
call eax
mov dword ptr [ebp-1Ch], eax
or dword ptr [ebp-04h], FFFFFFFFh
mov eax, dword ptr [ebp-1Ch]
jmp 00007F2E98C6739Ch
mov eax, dword ptr [ebp-14h]
mov ecx, dword ptr [eax]

Rich Headers

Programming Language:	• [ASM] VS2003 (.NET) build 3077 • [C] VS2003 (.NET) build 3077 • [C++] VS2003 (.NET) build 3077 • [EXP] VS2003 (.NET) build 3077 • [RES] VS2003 (.NET) build 3077 • [LNK] VS2003 (.NET) build 3077

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x354d0	0x80	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x338dc	0xf0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c000	0x24b90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x61000	0x385c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x302d0	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2b000	0x54c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x33854	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x29ffe	0x2a000	False	0.6064278738839286	COM executable for DOS	6.692976248573253	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2b000	0xa550	0xb000	False	0.3276589133522727	data	4.950983780735592	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x36000	0x5a58	0x3000	False	0.24137369791666666	data	3.613770783713054	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c000	0x24b90	0x25000	False	0.9165368982263513	data	7.7821351881075715	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x61000	0x83bc	0x9000	False	0.2816840277777778	data	3.490541222086245	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0x3cf40	0x20800	data	English	United States
RT_CURSOR	0x5dd30	0x134	data	English	United States
RT_CURSOR	0x5de68	0xb4	data	English	United States
RT_CURSOR	0x5df48	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x5e098	0x134	data	English	United States
RT_CURSOR	0x5e1e8	0x134	data	English	United States
RT_CURSOR	0x5e338	0x134	data	English	United States
RT_CURSOR	0x5e488	0x134	data	English	United States
RT_CURSOR	0x5e5d8	0x134	data	English	United States
RT_CURSOR	0x5e728	0x134	data	English	United States
RT_CURSOR	0x5e878	0x134	data	English	United States
RT_CURSOR	0x5e9c8	0x134	data	English	United States
RT_CURSOR	0x5eb18	0x134	data	English	United States
RT_CURSOR	0x5ec68	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x5edb8	0x134	data	English	United States
RT_CURSOR	0x5ef08	0x134	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x5f058	0x134	data	English	United States
RT_BITMAP	0x5f290	0xb8	data	English	United States
RT_BITMAP	0x5f348	0x144	data	English	United States
RT_ICON	0x3cac0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x5d740	0x264	data	English	United States
RT_DIALOG	0x5f1a8	0xe8	data	English	United States
RT_STRING	0x5f490	0x82	data	English	United States
RT_STRING	0x5f518	0x2a	data	English	United States
RT_STRING	0x5f548	0x192	data	English	United States
RT_STRING	0x5f6e0	0x4e2	data	English	United States
RT_STRING	0x5ff58	0x31a	data	English	United States
RT_STRING	0x5fc78	0x2dc	data	English	United States
RT_STRING	0x60ab8	0x8a	data	English	United States
RT_STRING	0x5fbc8	0xac	data	English	United States
RT_STRING	0x609a8	0xde	data	English	United States
RT_STRING	0x60278	0x4c4	data	English	United States
RT_STRING	0x60740	0x264	data	English	United States
RT_STRING	0x60a88	0x2c	data	English	United States
RT_STRING	0x60b48	0x42	data	English	United States
RT_GROUP_CURSOR	0x5df20	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x5e710	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e080	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e5c0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e470	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5eda0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e320	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e9b0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e1d0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5e860	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5eb00	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5ec50	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5eef0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5f040	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x5f190	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x3cf28	0x14	data	English	United States
RT_VERSION	0x5d9a8	0x388	data	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	RtlUnwind, HeapFree, HeapAlloc, VirtualProtect, VirtualAlloc, GetSystemInfo, VirtualQuery, GetCommandLineA, HeapReAlloc, HeapSize, LCMapStringA, LCMapStringW, HeapDestroy, HeapCreate, VirtualFree, IsBadWritePtr, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, UnhandledExceptionFilter, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, SetUnhandledExceptionFilter, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, SetStdHandle, SetEnvironmentVariableA, GetTickCount, GetFileTime, GetFileAttributesA, FileTimeToLocalFileTime, FileTimeToSystemTime, GetOEMCP, GetCPInfo, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, DeleteCriticalSection, InitializeCriticalSection, RaiseException, GlobalFlags, InterlockedIncrement, WritePrivateProfileStringA, FormatMessageA, LocalFree, MulDiv, SetLastError, GlobalGetAtomNameA, GlobalFindAtomA, lstrcatA, lstrcmpW, lstrcpynA, InterlockedDecrement, GlobalUnlock, GlobalFree, FreeResource, GlobalAddAtomA, FindResourceA, LoadResource, LockResource, SizeofResource, GetCurrentThread, GetCurrentThreadId, GlobalLock, GlobalAlloc, FreeLibrary, GlobalDeleteAtom, lstrcmpA, GetModuleFileNameA, GetModuleHandleA, GetProcAddress, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, LoadLibraryA, CompareStringW, CompareStringA, lstrlenA, lstrcmpiA, GetVersion, GetLastError, WideCharToMultiByte, MultiByteToWideChar, GetVersionExA, GetThreadLocale, GetLocaleInfoA, GetACP, InterlockedExchange, OpenProcess, TerminateProcess, Sleep, CreateToolhelp32Snapshot, Process32First, Process32Next, CloseHandle, FreeEnvironmentStringsA, ExitProcess
USER32.dll	RegisterClipboardFormatA, PostThreadMessageA, MessageBeep, GetNextDlgGroupItem, InvalidateRgn, InvalidateRect, CopyAcceleratorTableA, SetRect, IsRectEmpty, CharNextA, GetSysColorBrush, ReleaseCapture, LoadCursorA, SetCapture, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, wsprintfA, MoveWindow, SetWindowTextA, IsDialogMessageA, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, GetClassLongA, GetClassInfoExA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, SetFocus, IsChild, GetForegroundWindow, GetTopWindow, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSubMenu, GetMenuItemID, GetMenuItemCount, GetSysColor, AdjustWindowRectEx, EqualRect, GetClassInfoA, RegisterClassA, UnregisterClassA, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, SetWindowLongA, OffsetRect, DrawIcon, SendMessageA, IsIconic, GetClientRect, EnableWindow, LoadIconA, GetSystemMetrics, GetWindowTextLengthA, IsWindowVisible, GetWindowRect, GetWindowTextA, GetClassNameA, EnumWindows, IntersectRect, SystemParametersInfoA, GetWindowPlacement, PtInRect, UnhookWindowsHookEx, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, ReleaseDC, GetDC, CopyRect, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamA, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, SetMenuItemBitmaps, GetFocus, ModifyMenuA, GetMenuState, EnableMenuItem, GetMessageTime, DestroyMenu, ShowWindow, PostMessageA, CharUpperA, PostQuitMessage, SetCursor, IsWindowEnabled, GetLastActivePopup, GetWindowLongA, GetParent, MessageBoxA, ValidateRect, GetCursorPos, PeekMessageA, GetKeyState, GetActiveWindow, DispatchMessageA, TranslateMessage, GetMessageA, CallNextHookEx, SetWindowsHookExA, LoadBitmapA, GetMenuCheckMarkDimensions, CheckMenuItem
GDI32.dll	GetMapMode, GetTextColor, GetRgnBox, GetDeviceCaps, GetStockObject, DeleteDC, ExtSelectClipRgn, ScaleWindowExtEx, SetWindowExtEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, GetBkColor, CreateBitmap, Escape, ExtTextOutA, TextOutA, RectVisible, PtVisible, GetWindowExtEx, GetViewportExtEx, DeleteObject, SetMapMode, RestoreDC, SaveDC, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateRectRgnIndirect, SelectObject
comdlg32.dll	GetFileTitleA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter
ADVAPI32.dll	RegQueryValueExA, RegOpenKeyExA, RegDeleteKeyA, RegEnumKeyA, RegOpenKeyA, RegQueryValueA, RegCreateKeyExA, RegSetValueExA, RegCloseKey
COMCTL32.dll	ImageList_Destroy
SHLWAPI.dll	PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
oledlg.dll	
ole32.dll	CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, CLSIDFromProgID, OleUninitialize, CoFreeUnusedLibraries, CoRegisterMessageFilter, OleFlushClipboard, OleIsCurrentClipboard, CoRevokeClassObject, OleInitialize
OLEAUT32.dll	SysFreeString, SysAllocStringLen, VariantClear, VariantChangeType, VariantInit, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, SystemTimeToVariantTime, SafeArrayDestroy, SysAllocString, VariantCopy

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x100048a0
DllUnregisterServerrrrrrrrrrrr	2	0x100048d0

Possible Origin

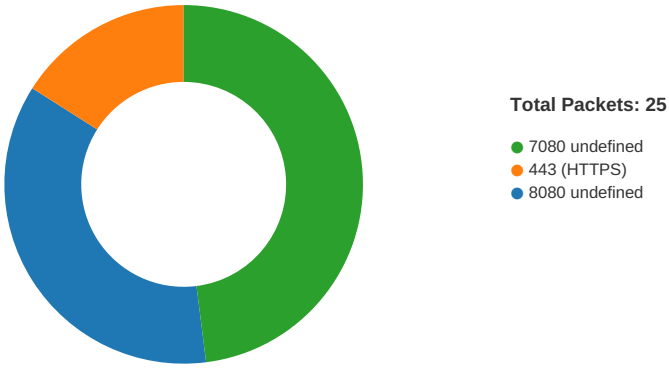
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6119.193.124.4 14985970802404304 07/20/22-01:13:31.686515	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49859	7080	192.168.2.6	119.193.124.41
192.168.2.651.91.76.8949 84480802404338 07/20/22-01:13:29.114997	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49844	8080	192.168.2.6	51.91.76.89

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:12:37.545278072 CEST	49773	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:12:40.626862049 CEST	49773	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:12:46.650408030 CEST	49773	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:12:58.788846016 CEST	49803	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:12:58.788919926 CEST	443	49803	189.232.46.161	192.168.2.6
Jul 20, 2022 01:12:58.789094925 CEST	49803	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:12:58.832343102 CEST	49803	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:12:58.832392931 CEST	443	49803	189.232.46.161	192.168.2.6
Jul 20, 2022 01:13:29.083200932 CEST	49803	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:13:29.114996910 CEST	49844	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:13:29.136509895 CEST	8080	49844	51.91.76.89	192.168.2.6
Jul 20, 2022 01:13:29.722778082 CEST	49844	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:13:29.745616913 CEST	8080	49844	51.91.76.89	192.168.2.6
Jul 20, 2022 01:13:30.323734999 CEST	49844	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:13:30.349111080 CEST	8080	49844	51.91.76.89	192.168.2.6
Jul 20, 2022 01:13:30.386081934 CEST	49855	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:13:30.417004108 CEST	8080	49855	217.182.25.250	192.168.2.6
Jul 20, 2022 01:13:30.952959061 CEST	49855	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:13:30.982132912 CEST	8080	49855	217.182.25.250	192.168.2.6
Jul 20, 2022 01:13:31.526103020 CEST	49855	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:13:31.560188055 CEST	8080	49855	217.182.25.250	192.168.2.6
Jul 20, 2022 01:13:31.686515093 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:31.950680971 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:31.955549002 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:31.956378937 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:32.217185974 CEST	7080	49859	119.193.124.41	192.168.2.6

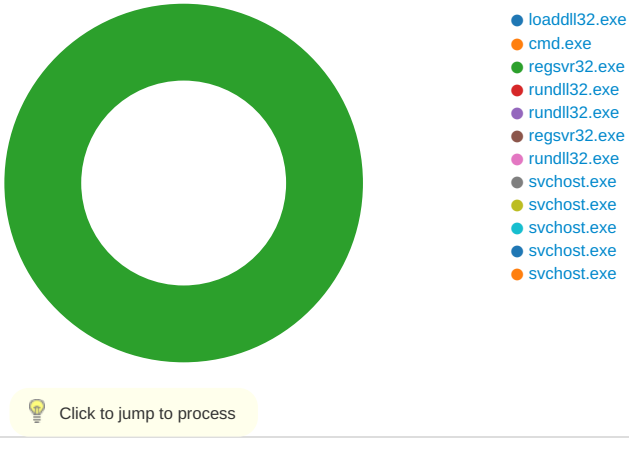
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:13:32.231532097 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:32.231570959 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:32.243074894 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:37.208336115 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:37.470942020 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:37.474697113 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:37.478393078 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:37.783706903 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:38.629363060 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:38.629446983 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:13:41.630054951 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:41.630089045 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:13:41.630225897 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:14:27.472696066 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:14:27.472757101 CEST	49859	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:14:27.734839916 CEST	7080	49859	119.193.124.41	192.168.2.6
Jul 20, 2022 01:14:27.735079050 CEST	49859	7080	192.168.2.6	119.193.124.41

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2022 01:12:48.819976091 CEST	8.8.8.8	192.168.2.6	0xdbb6	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2022 01:12:48.819976091 CEST	8.8.8.8	192.168.2.6	0xdbb6	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6908**, Parent PID: **792**

General

Target ID:	0
Start time:	01:12:04
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll"
Imagebase:	0x70000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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

Analysis Process: cmd.exe PID: 6916, Parent PID: 6908

General

Target ID:	1
Start time:	01:12:05
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll",#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:	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

Analysis Process: regsvr32.exe PID: 6932, Parent PID: 6908

General

Target ID:	2
Start time:	01:12:06
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\6xfFjxyRXf.dll
Imagebase:	0x1d0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.415134102.0000000004F61000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.415134102.0000000004F61000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.414918130.0000000004F00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.414918130.0000000004F00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Nrzawqzutwib\qenu.dlv:Zone.Identifier	success or wait	1	4F7594F	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: **6944**, Parent PID: **6916**

General

Target ID:	3
Start time:	01:12:06
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\6xfFjxyRXf.dll",#1
Imagebase:	0x1210000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.406595295.0000000000BF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.406595295.0000000000BF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.406684150.0000000000C21000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.406684150.0000000000C21000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
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

Analysis Process: rundll32.exe PID: **6968**, Parent PID: **6908**

General

Target ID:	4
Start time:	01:12:07
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6xfFjxyRXf.dll,DllRegisterServer

Imagebase:	0x1210000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.406621589.00000000046B1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.406621589.00000000046B1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.406594585.0000000004680000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.406594585.0000000004680000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
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

Analysis Process: regsvr32.exe PID: **7052**, Parent PID: **6932**

General

Target ID:	5
Start time:	01:12:12
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Nrzawqzutwib\qenu.dlv"
Imagebase:	0x1d0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.917544011.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.917544011.0000000002B50000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.917618972.0000000004481000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.917618972.0000000004481000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7068**, Parent PID: **6908**

General

Target ID:	6
Start time:	01:12:12
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\6xfFjxyRXf.dll,DllUnregisterServerrrrrrrrrrr
Imagebase:	0x1210000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5776, Parent PID: 588

General

Target ID:	9
Start time:	01:12:26
Start date:	20/07/2022
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:	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

Analysis Process: svchost.exe PID: 7048, Parent PID: 588

General

Target ID:	11
Start time:	01:12:43
Start date:	20/07/2022
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

Analysis Process: svchost.exe PID: 2764, Parent PID: 588

General

Target ID:	12
Start time:	01:12:49
Start date:	20/07/2022
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

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: **4348**, Parent PID: **588**

General

Target ID:	14
Start time:	01:13:08
Start date:	20/07/2022
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

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

Analysis Process: svchost.exe PID: **5764**, Parent PID: **588**

General

Target ID:	21
Start time:	01:14:07
Start date:	20/07/2022
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

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