ID: 669377
Sample Name: U2ORGDN0Qn
Cookbook: default.jbs
Time: 01:10:50
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

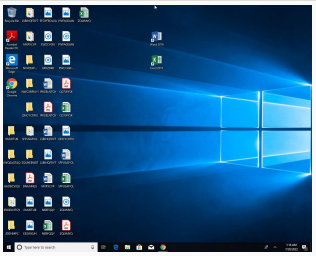
Windows Analysis Report

U2ORGDN0Qn

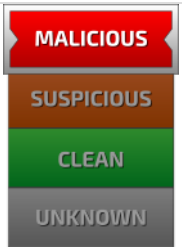
Overview

General Information

Sample Name:	U2ORGDN0Qn (renamed file extension from none to dll)
Analysis ID:	669377
MD5:	d6fd21b5d695c8..
SHA1:	99ecfd834958f29..
SHA256:	d183bbf6549ab1..
Tags:	32 dll exe trojan
Infos:	



Detection



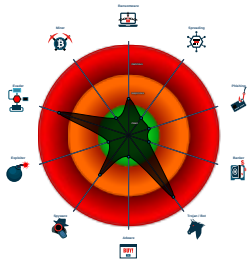
Emotet

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…
- Snort IDS alert for network traffic
- Query firmware table information (lik…
- 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 check if a d…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6428 cmdline: loaddll32.exe "C:\Users\user\Desktop\U2ORGDN0Qn.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6436 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\U2ORGDN0Qn.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6456 cmdline: rundll32.exe "C:\Users\user\Desktop\U2ORGDN0Qn.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - regsvr32.exe (PID: 6560 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Snlvvhp\smhidzyomn.elm" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6444 cmdline: regsvr32.exe /s C:\Users\user\Desktop\U2ORGDN0Qn.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6468 cmdline: rundll32.exe C:\Users\user\Desktop\U2ORGDN0Qn.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 3228 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5312 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2224 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4584 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3492 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7044 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6016 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "144.42.93.111:1",
    "72.67.111.110:3",
    "45.99.0.0:179",
    "255.255.255.255:3",
    "128.191.135.0:2",
    "65.83.89.67:68",
    "40.67.176.0:2",
    "1.255.0.0:65",
    "72.3.180.0:48",
    "168.226.179.0:32",
    "120.5.180.0:48",
    "192.168.2.7:2",
    "196.2.3.0:1408",
    "120.146.177.0:1",
    "156.2.3.0:2076",
    "207.2.3.0:5244",
    "88.147.177.0:1",
    "168.148.177.0:1",
    "224.148.177.0:1",
    "219.2.3.0:5292",
    "48.2.180.0:1",
    "232.254.179.0:1",
    "126.194.0.0:7080",
    "161.94.3.0:3312",
    "222.2.3.0:2076",
    "120.198.184.0:1",
    "120.254.179.0:1"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.407451235.0000000004DD1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.407451235.0000000004DD1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.404108074.0000000000760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.404108074.0000000000760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.402481757.0000000004E10000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 15 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.4e40000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.4e40000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.34c0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.34c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.46b0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 25 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.7 - Destination IP: 51.91.76.89

Timestamp:	192.168.2.751.91.76.894978780802404338 07/20/22-01:13:13.336201
SID:	2404338
Source Port:	49787
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.7 - Destination IP: 119.193.124.41

Timestamp:	192.168.2.7119.193.124.414979070802404304 07/20/22-01:13:15.988655
SID:	2404304
Source Port:	49790
Destination Port:	7080
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

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)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion

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

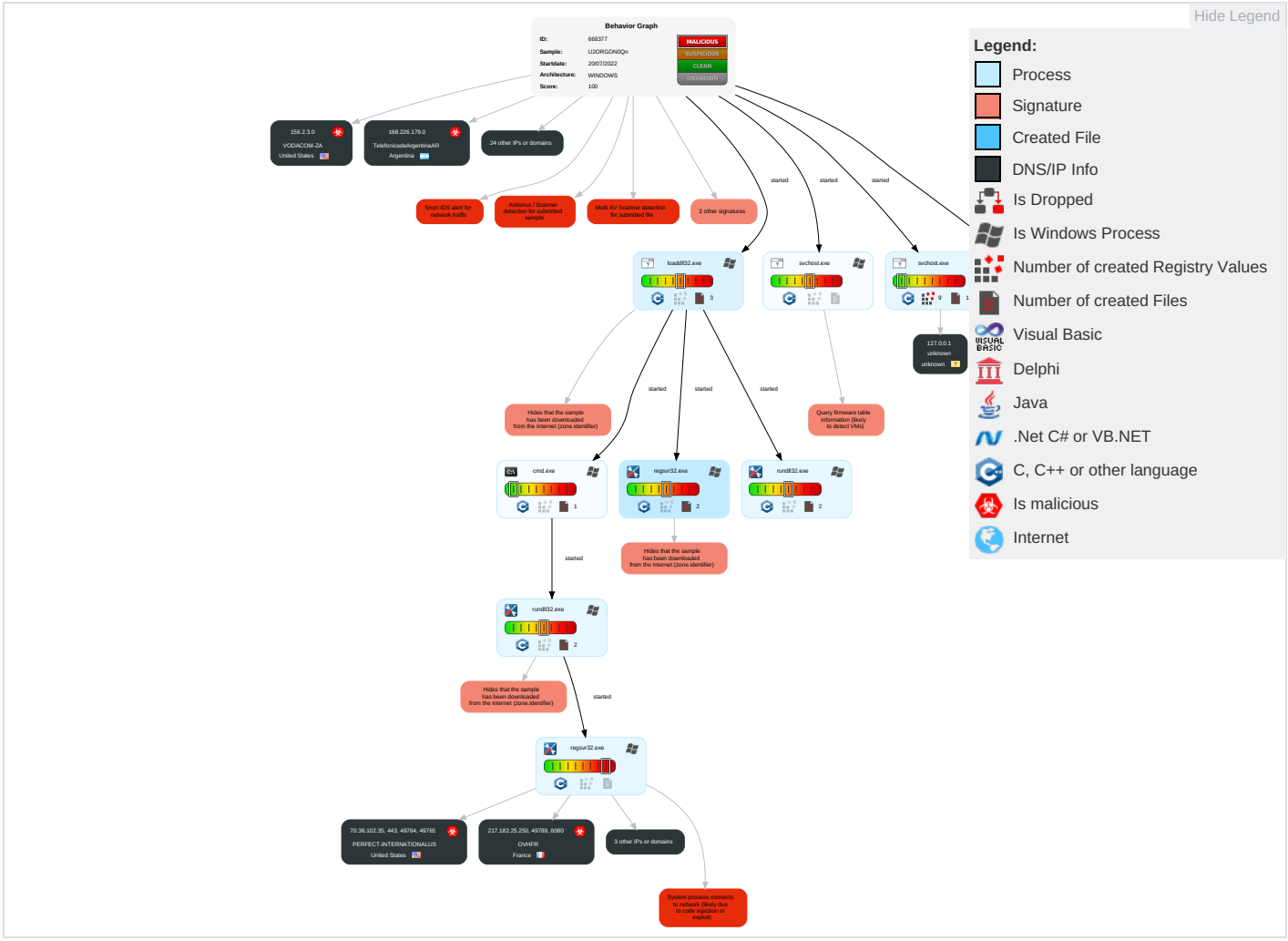
Stealing of Sensitive Information

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	1 2 Virtualization/Sandbox Evasion	LSASS Memory	1 4 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	1 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	1 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	4 5 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

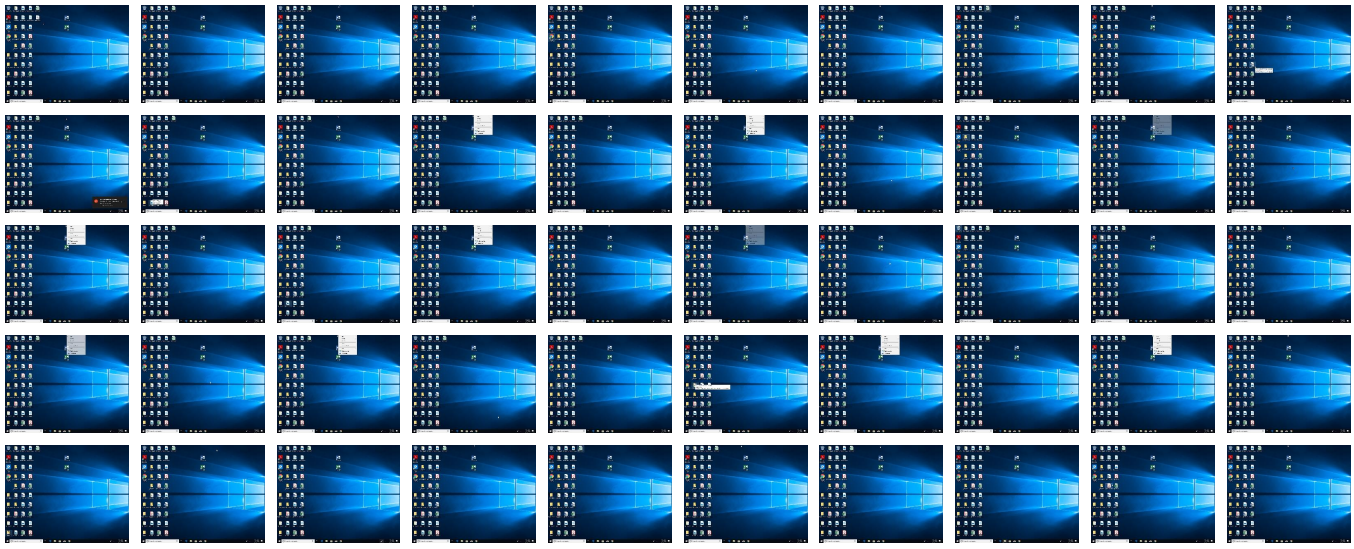
Behavior Graph



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
U2ORGDN0Qn.dll	70%	Virustotal		Browse
U2ORGDN0Qn.dll	73%	ReversingLabs	Win32.Trojan.Emotet	
U2ORGDN0Qn.dll	100%	Avira	TR/Emotet.uwcip	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.46b0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.c70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4e40000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.regsvr32.exe.4680000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.34c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.34f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4e10000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll32.exe.760000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.4dd0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.4da0000.0.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://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	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

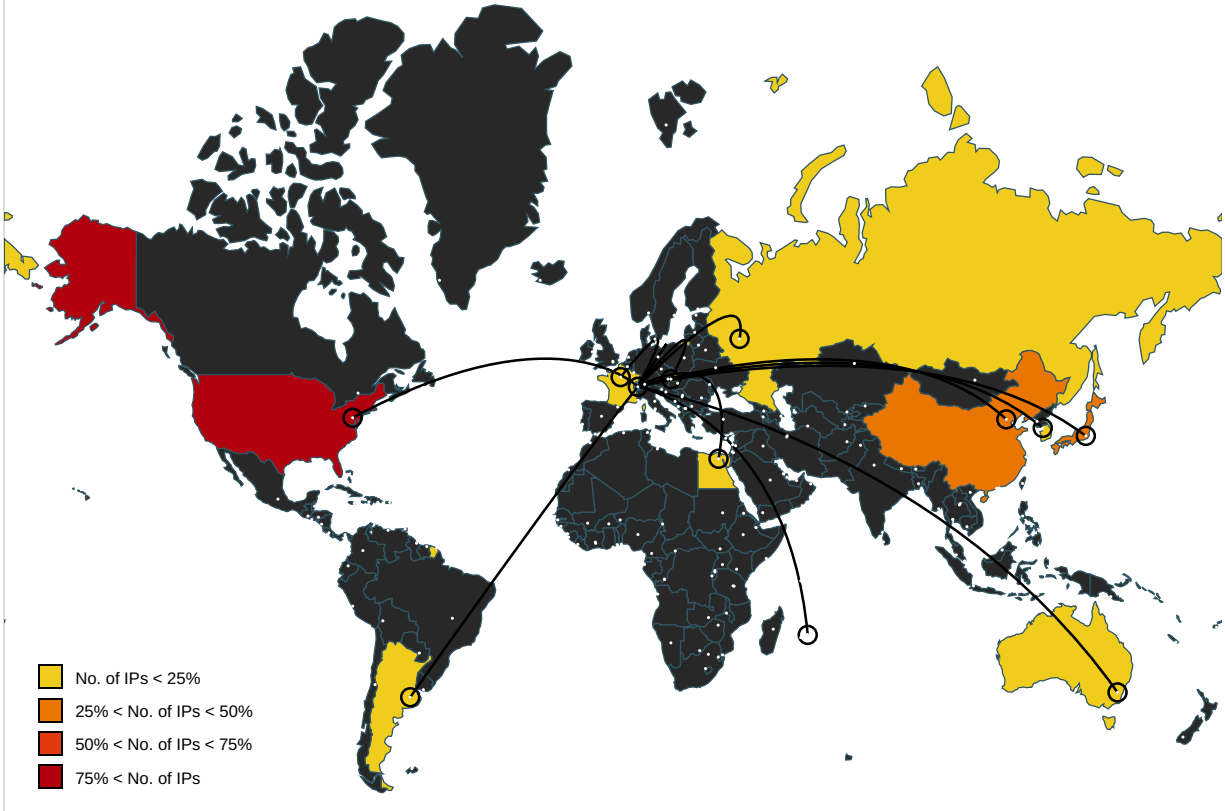
Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001A.00000003.751770239.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.750524881.0000026ACDD98000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 00000010.00000002.911823382.0000022053814000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.784059543.0000026ACD2E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001A.00000003.751770239.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.750524881.0000026ACDD98000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001A.00000003.757137213.0000026ACDD9D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.758965380.0000026ACDDA9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.757153416.0000026ACDDA9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000001A.00000003.751770239.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.750524881.0000026ACDD98000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001A.00000003.746061424.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746140948.0000026ACDDA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746120290.0000026ACDD96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746230097.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.747380316.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001A.00000003.746061424.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746140948.0000026ACDDA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746120290.0000026ACDD96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746230097.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.747380316.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001A.00000003.746061424.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746140948.0000026ACDDA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746120290.0000026ACDD96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.746230097.0000026ACE202000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.747380316.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001A.00000003.751770239.0000026ACDD75000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.750524881.0000026ACDD98000.00000004.00000020.00020000.00000000.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
156.2.3.0	unknown	United States		29975	VODACOM-ZA	true
70.36.102.35	unknown	United States		22439	PERFECT-INTERNATIONALUS	true
88.147.177.0	unknown	Russian Federation		12389	ROSTELECOM-ASRU	true
144.42.93.111	unknown	United States		27402	IBC-N1US	true
161.94.3.0	unknown	Japan		14298	EPA-NETUS	true
224.148.177.0	unknown	Reserved		unknown	unknown	true
45.99.0.0	unknown	Egypt		37069	MOBINILEG	true
40.67.176.0	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
120.146.177.0	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
168.226.179.0	unknown	Argentina		22927	TelefonicadeArgentinaAR	true
222.2.3.0	unknown	Japan		2516	KDDIKDDICORPORATIONJP	true
72.3.180.0	unknown	United States		33070	RMH-14US	true
48.2.180.0	unknown	United States		2686	ATGS-MMD-ASUS	true
168.148.177.0	unknown	United States		27435	OPSOURCE-INCUS	true
126.194.0.0	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
120.254.179.0	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	true
1.255.0.0	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
65.83.89.67	unknown	United States		6389	BELLSOUTH-NET-BLKUS	true
207.2.3.0	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	true
219.2.3.0	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
51.91.76.89	unknown	France		16276	OVHFR	true
120.5.180.0	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
120.198.184.0	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	true
128.191.135.0	unknown	United States		1503	DNIC-AS-01503US	true
72.67.111.110	unknown	United States		5650	FRONTIER-FRTRUS	true
196.2.3.0	unknown	Mauritius		33764	AFRINIC-ZA-JNB-ASMU	true
232.254.179.0	unknown	Reserved		unknown	unknown	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
92.240.254.110	unknown	Slovakia (SLOVAK Republic)		42005	LIGHTSTORM-COMMUNICATIONS-SRO-SK-ASPeeringsSK	true

Private

IP
192.168.2.7
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669377
Start date and time: 20/07/202201:10:50	2022-07-20 01:10:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	U2ORGDN0Qn (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:	28
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.winDLL@18/4@0/32
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.6%) • Quality average: 78.6% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 98% • 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, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 8.248.131.254, 67.26.81.254, 8.253.207.120, 67.26.139.254, 8.238.85.254, 23.211.4.86, 20.72.205.209, 40.74.108.123, 20.223.24.244
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, settings-prod-wus2-2.westus2.cloudapp.azure.com, settings-prod-wjp-1.japanwest.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, b-ring.msedge.net, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, fp-as.azureedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, wu-bg-shim.trafficmanager.net, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, displaycatalog-rp.md.mp.microsoft.co
- 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
01:13:44	API Interceptor	11x 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:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x4b058f10, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25070476958191645
Encrypted:	false
SSDEEP:	384:E+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:7SB2nSB2RSjlK/+mLesOj1J2
MD5:	2A1D97ECE7A09694DCDC3DBEBF8E6C03
SHA1:	F836D4C60C4A7CCAE077AB03A7CF377E23C11E0E
SHA-256:	2C5C9D67A6A7B625AEAC76F9DF5812B6BFB1574DF10240683DFD51768E16581D
SHA-512:	5DCCE94BB5C161D22469080B33D8C07A6FC08A67EE8B77A20DA6820063987E1EF296582FCA2840F35683AE75C2D0B05185031963F98711C3CFF249A67AC927FE
Malicious:	false
Preview:	K..... .....e.f.3...w.....&.....w..-....z#.h.(.....3...w.....B.....@..... ....3...w..... .....-....zy.....s.-....zy..... .....

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.....ul.....}.....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):	3.1274410188478514
Encrypted:	false

SSDEEP:	6:kKhtB+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:BNkPlE99SNxAhUeE1
MD5:	2AC1CECFB474F66BAB5079C5371A3C36
SHA1:	153FC7D9E8E63C1B0461A02F3AA43C3650A1F702
SHA-256:	A7E579ABF654DCDFED18DFD6D89E44F927A8DA2ACA22880F44B48A32FC7D7F38
SHA-512:	36FA521463F46F4462CD55C51143C33C43385070E70D310F4EC2F3DA62DA743CA1B6C69E18CDF0580F9FAACB580B3B6E75B499CCC1510CC63489DD8600758B
Malicious:	false
Preview:	p..... .....(..... .....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."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.416846331718697
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:	U2ORGDN0Qn.dll
File size:	626688
MD5:	d6fd21b5d695c8bd6148491de24c02e5
SHA1:	99ecfd834958f2950d3c54caa085db3183061421
SHA256:	d183bbf6549ab1ee108898e48b16d14dfdc50da7131eb8b2c71d4a18ae439d72
SHA512:	870d3c741af9c800e9d17c7e8ac15aca0c4bc972b85e3ab9fae43251ef62d64824eabe9ae8c0095d34a72931531df97e5ce9b337e1f576d4eebe3ee7909753b5
SSDEEP:	6144:XvRov7wREVy3B6yu4YXep2v5uYxl8msgrR8drCSi78SLUYeDrQ0Ax+xSEN:ZsVyXu4YupcuYEmxrSsmD8fx+xJ
TLSH:	38D46C117691C832FC995F34359392BD1FF87F64AAA48227EF903A4D6BB35008E146D7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7...d...d...d+..d...d+..d...d...d...d.!.d...d.!.d`..d.!.dv..d.!.d...d.!.d...d.!.d...dRich...d.....PE..L...p.<b...

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x100209c7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x623C8770 [Thu Mar 24 15:00:00 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:	196752bd65f33bc6f5dd0426f39259ae

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007FC23CAFBD17h
call 00007FC23CB0321Ah
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007FC23CAFBC02h
pop ecx
retn 000Ch
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 100397B4h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
test eax, eax
pop edi
mov dword ptr [ebp-04h], eax
pop esi
je 00007FC23CAFBD1Eh
test byte ptr [eax], 00000008h
je 00007FC23CAFBD19h
mov dword ptr [ebp-0Ch], 01994000h
lea eax, dword ptr [ebp-0Ch]
push eax
push dword ptr [ebp-10h]
push dword ptr [ebp-1Ch]
push dword ptr [ebp-20h]
call dword ptr [100360E0h]
leave
retn 0008h
push 00000000h
push dword ptr [esp+14h]
push dword ptr [esp+14h]
push dword ptr [esp+14h]
push dword ptr [esp+14h]
call 00007FC23CB032E9h
add esp, 14h

Instruction
ret
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007FC23CAFBD36h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007FC23CAFBD60h
test ecx, 00000003h
jne 00007FC23CAFBD01h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx

Rich Headers

Programming Language:	• [ASM] VS2005 build 50727 • [C] VS2005 build 50727 • [C++] VS2005 build 50727 • [EXP] VS2005 build 50727 • [RES] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x434c0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x41914	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4b000	0x480b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x94000	0x3fe8	.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	0x3b9a0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x36000	0x53c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x4188c	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	0x340f7	0x35000	False	0.5665859006485849	data	6.63826832292909	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x36000	0xd514	0xe000	False	0.3163539341517857	data	4.885899483264565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x44000	0x6598	0x3000	False	0.2610677083333333	data	4.030187754909099	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x4b000	0x480b4	0x49000	False	0.5451626712328768	data	6.348672990248238	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	0x8660	0x9000	False	0.3055284288194444	data	3.8230472463394145	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0x4c074	0x20800	data	Spanish	Mexico
RT_CURSOR	0x6c874	0x134	data		
RT_CURSOR	0x6c9a8	0xb4	data		
RT_CURSOR	0x6ca5c	0x134	AmigaOS bitmap font		
RT_CURSOR	0x6cb90	0x134	data		
RT_CURSOR	0x6ccc4	0x134	data		
RT_CURSOR	0x6cdf8	0x134	data		
RT_CURSOR	0x6cf2c	0x134	data		
RT_CURSOR	0x6d060	0x134	data		
RT_CURSOR	0x6d194	0x134	data		
RT_CURSOR	0x6d2c8	0x134	data		
RT_CURSOR	0x6d3fc	0x134	data		
RT_CURSOR	0x6d530	0x134	data		
RT_CURSOR	0x6d664	0x134	AmigaOS bitmap font		
RT_CURSOR	0x6d798	0x134	data		
RT_CURSOR	0x6d8cc	0x134	data		
RT_CURSOR	0x6da00	0x134	data		
RT_BITMAP	0x6db34	0xb8	data		
RT_BITMAP	0x6dbec	0x144	data		
RT_ICON	0x6dd30	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6e018	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6e140	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6e428	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6e550	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6e838	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6e960	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6ec48	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6ed70	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6f058	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6f180	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6f468	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6f590	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6f878	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6f9a0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	Spanish	Mexico
RT_ICON	0x6fc88	0x128	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_ICON	0x6fdb0	0x10828	dBase III DBT, version number 0, next free block index 40	Spanish	Mexico
RT_ICON	0x805d8	0x10828	dBase III DBT, version number 0, next free block index 40	Spanish	Mexico
RT_DIALOG	0x90e00	0x12c	data		

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x90f2c	0x134	data		
RT_DIALOG	0x91060	0xfe	data		
RT_DIALOG	0x91160	0x34	data		
RT_STRING	0x91194	0x52	data		
RT_STRING	0x911e8	0xb0	Hitachi SH big-endian COFF object file, not stripped, 16640 sections, symbol offset=0x69007200, 201344768 symbols, optional header size 29952		
RT_STRING	0x91298	0x30	data		
RT_STRING	0x912c8	0x1d0	data		
RT_STRING	0x91498	0x5bc	data		
RT_STRING	0x91a54	0x31c	data		
RT_STRING	0x91d70	0x300	data		
RT_STRING	0x92070	0xb0	data		
RT_STRING	0x92120	0xee	data		
RT_STRING	0x92210	0x11e	data		
RT_STRING	0x92330	0x4d0	data		
RT_STRING	0x92800	0x248	data		
RT_STRING	0x92a48	0x2e	data		
RT_STRING	0x92a78	0x4c	data		
RT_GROUP_CURSOR	0x92ac4	0x22	Lotus unknown worksheet or configuration, revision 0x2		
RT_GROUP_CURSOR	0x92ae8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92afc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b10	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b24	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b38	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b4c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b60	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b74	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b88	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92b9c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92bb0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92bc4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92bd8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x92bec	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x92c00	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92c24	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92c48	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92c6c	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92c90	0x14	data	Spanish	Mexico
RT_GROUP_ICON	0x92ca4	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92cc8	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92cec	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92d10	0x22	data	Spanish	Mexico
RT_GROUP_ICON	0x92d34	0x14	data	Spanish	Mexico
RT_VERSION	0x92d48	0x314	data		
RT_MANIFEST	0x9305c	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

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

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x1000373c

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

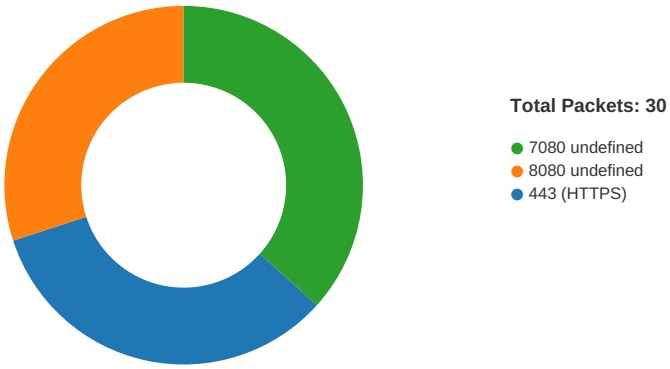
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.751.91.76.8949 78780802404338 07/20/22-01:13:13.336201	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49787	8080	192.168.2.7	51.91.76.89
192.168.2.7119.193.124.4 14979070802404304 07/20/22-01:13:15.988655	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49790	7080	192.168.2.7	119.193.124.41

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:12:51.423614025 CEST	49764	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.423677921 CEST	443	49764	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.423819065 CEST	49764	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.476835012 CEST	49764	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.476869106 CEST	443	49764	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.659399986 CEST	443	49764	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.769865990 CEST	49765	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.769902945 CEST	443	49765	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.770019054 CEST	49765	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.771061897 CEST	49765	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.771079063 CEST	443	49765	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.950787067 CEST	443	49765	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.954233885 CEST	49766	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.954286098 CEST	443	49766	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.954395056 CEST	49766	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.954909086 CEST	49766	443	192.168.2.7	70.36.102.35
Jul 20, 2022 01:12:51.954955101 CEST	443	49766	70.36.102.35	192.168.2.7
Jul 20, 2022 01:12:51.955027103 CEST	49766	443	192.168.2.7	70.36.102.35

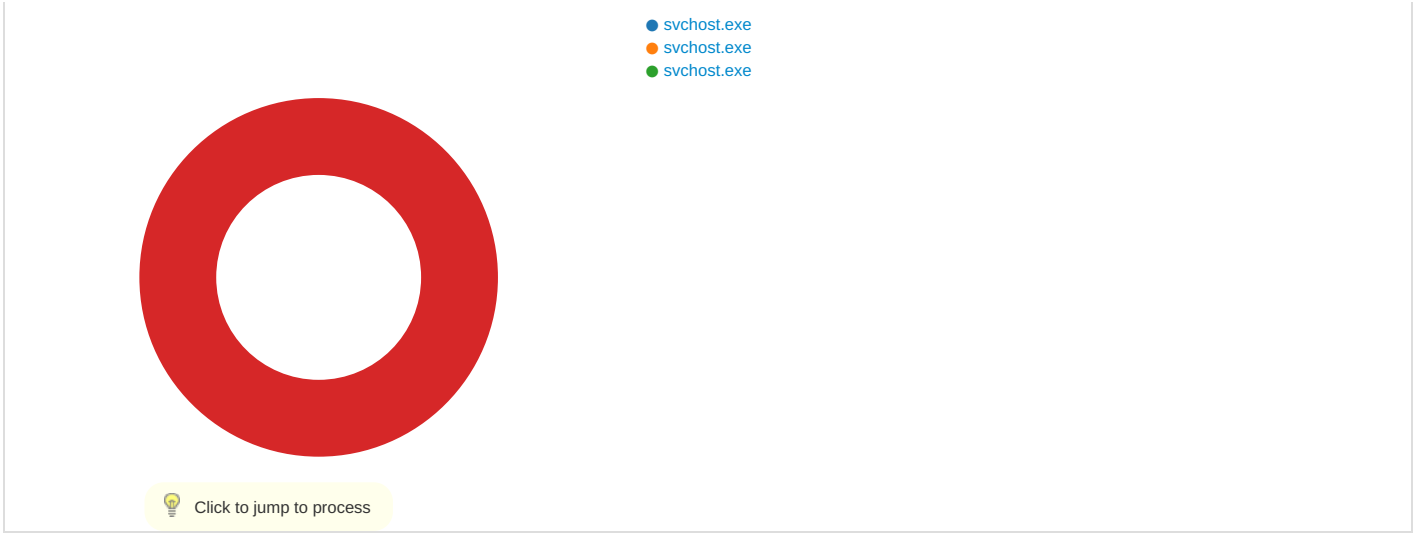
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:12:52.040544033 CEST	49767	8080	192.168.2.7	92.240.254.110
Jul 20, 2022 01:12:55.081345081 CEST	49767	8080	192.168.2.7	92.240.254.110
Jul 20, 2022 01:13:01.084445953 CEST	49767	8080	192.168.2.7	92.240.254.110
Jul 20, 2022 01:13:13.336200953 CEST	49787	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:13:13.358731031 CEST	8080	49787	51.91.76.89	192.168.2.7
Jul 20, 2022 01:13:13.894943953 CEST	49787	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:13:13.917062998 CEST	8080	49787	51.91.76.89	192.168.2.7
Jul 20, 2022 01:13:14.582453966 CEST	49787	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:13:14.608050108 CEST	8080	49787	51.91.76.89	192.168.2.7
Jul 20, 2022 01:13:14.650358915 CEST	49789	8080	192.168.2.7	217.182.25.250
Jul 20, 2022 01:13:14.681106091 CEST	8080	49789	217.182.25.250	192.168.2.7
Jul 20, 2022 01:13:15.285722017 CEST	49789	8080	192.168.2.7	217.182.25.250
Jul 20, 2022 01:13:15.315843105 CEST	8080	49789	217.182.25.250	192.168.2.7
Jul 20, 2022 01:13:15.951112032 CEST	49789	8080	192.168.2.7	217.182.25.250
Jul 20, 2022 01:13:15.980804920 CEST	8080	49789	217.182.25.250	192.168.2.7
Jul 20, 2022 01:13:15.988655090 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:16.251542091 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:16.251754045 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:16.265714884 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:16.528732061 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:16.543241024 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:16.543298006 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:16.543468952 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:20.245265961 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:20.505635023 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:20.505755901 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:20.511050940 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:20.822393894 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:21.662751913 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:21.662872076 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:13:24.663368940 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:24.663414955 CEST	7080	49790	119.193.124.41	192.168.2.7
Jul 20, 2022 01:13:24.663590908 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:14:41.336133957 CEST	49790	7080	192.168.2.7	119.193.124.41
Jul 20, 2022 01:14:41.336183071 CEST	49790	7080	192.168.2.7	119.193.124.41

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2022 01:13:00.850657940 CEST	8.8.8.8	192.168.2.7	0xa2ed	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2022 01:13:00.850657940 CEST	8.8.8.8	192.168.2.7	0xa2ed	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: 6428, Parent PID: 1820

General

Target ID:	0
Start time:	01:12:19
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\U2ORGDN0Qn.dll"
Imagebase:	0xd70000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000000.00000002.404108074.0000000000760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.404108074.0000000000760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.405167814.0000000000C71000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.405167814.0000000000C71000.00000020.00001000.00020000.00000000.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: cmd.exe PID: 6436, Parent PID: 6428

General

Target ID:	1
Start time:	01:12:19
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\U2ORGDN0Qn.dll",#1
Imagebase:	0xdd0000
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: 6444, Parent PID: 6428

General

Target ID:	2
Start time:	01:12:20
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\U2ORGDN0Qn.dll
Imagebase:	0xcc0000
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: 00000002.00000002.402481757.0000000004E10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.402481757.0000000004E10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.402503054.0000000004E41000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.402503054.0000000004E41000.00000020.00001000.00020000.00000000.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: 6456, Parent PID: 6436

General

Target ID:	3
Start time:	01:12:20
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\U2ORGDN0Qn.dll",#1
Imagebase:	0x1d0000
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: 00000003.00000002.407451235.0000000004DD1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.407451235.0000000004DD1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.407424342.0000000004DA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.407424342.0000000004DA0000.00000040.00001000.00020000.00000000.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\Snlvvhp\smhidzyomn.elm:Zone.Identifier	success or wait	1	4DE594F	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: **6468**, Parent PID: **6428**

General

Target ID:	4
Start time:	01:12:21
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\U2ORGDN0Qn.dll,DllRegisterServer
Imagebase:	0x1d0000
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: 00000004.00000002.403789419.00000000034F1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.403789419.00000000034F1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.403716182.00000000034C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.403716182.00000000034C0000.00000040.00001000.00020000.00000000.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: **6560**, Parent PID: **6456**

General

Target ID:	5
Start time:	01:12:26

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\Snlvvhp\smhidzyomn.elm"
Imagebase:	0xcc0000
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: 00000005.00000002.910976307.0000000004680000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.910976307.0000000004680000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.911072354.00000000046B1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.911072354.00000000046B1000.00000020.00001000.00020000.00000000.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: svchost.exe PID: **3228**, Parent PID: **604**

General

Target ID:	10
Start time:	01:12:59
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:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **5312**, Parent PID: **604**

General

Target ID:	12
Start time:	01:13:19
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:	0x7ff7e8070000
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: **2224**, Parent PID: **604**

General

Target ID:	16
Start time:	01:13:44
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7e8070000
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4584**, Parent PID: **604**

General

Target ID:	19
Start time:	01:14:03
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:	0x7ff7e8070000
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: **3492**, Parent PID: **604**

General

Target ID:	20
Start time:	01:14:30
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:	0x7ff7e8070000
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: **7044**, Parent PID: **604**

General

Target ID:	24
Start time:	01:14:32
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff7e8070000
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6016**, Parent PID: **604**

General

Target ID:	26

Start time:	01:14:52
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:	0x7ff7e8070000
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

Disassembly

No disassembly