ID: 669370
Sample Name: 9818t9ks1s
Cookbook: default.jbs
Time: 01:05:10
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

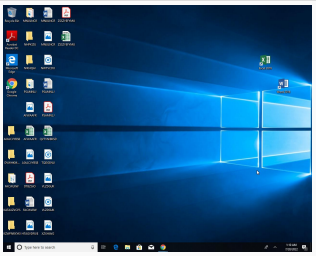
Windows Analysis Report

9818t9ks1s

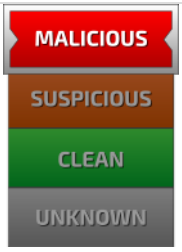
Overview

General Information

Sample Name:	9818t9ks1s (renamed file extension from none to dll)
Analysis ID:	669370
MD5:	83418a9af56db9..
SHA1:	0ea68aab3721e5.
SHA256:	4a688f571024b0..
Tags:	32 dll exe trojan
Infos:	



Detection



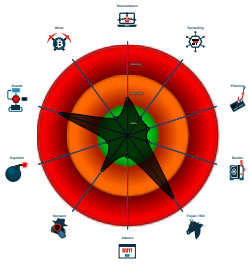
Emotet

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…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6888 cmdline: loaddll32.exe "C:\Users\user\Desktop\9818t9ks1s.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6896 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\9818t9ks1s.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6924 cmdline: rundll32.exe "C:\Users\user\Desktop\9818t9ks1s.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6912 cmdline: regsvr32.exe /s C:\Users\user\Desktop\9818t9ks1s.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 7020 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Bvqee\qeggfkimakwygr.che" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6932 cmdline: rundll32.exe C:\Users\user\Desktop\9818t9ks1s.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7040 cmdline: rundll32.exe C:\Users\user\Desktop\9818t9ks1s.dll,DllUnregisterServerr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5084 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6324 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6576 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3952 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7028 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5748 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "51.91.7.5:8080",
    "197.242.150.244:8080",
    "1.234.2.232:8080",
    "173.212.193.249:8080",
    "51.91.76.89:8080",
    "151.106.112.196:8080",
    "107.182.225.142:8080",
    "103.43.46.182:443",
    "195.201.151.129:8080",
    "51.254.140.238:7080",
    "153.126.146.25:7080",
    "176.56.128.118:443",
    "188.44.20.25:443",
    "119.193.124.41:7080",
    "70.36.102.35:443",
    "45.142.114.231:8080",
    "46.55.222.11:443",
    "82.165.152.127:8080",
    "212.237.17.99:8080",
    "92.240.254.110:8080",
    "217.182.25.250:8080",
    "189.126.111.200:7080",
    "212.24.98.99:8080",
    "45.176.232.124:443",
    "192.99.251.50:443",
    "216.158.226.206:443",
    "206.188.212.92:8080",
    "176.104.106.96:8080",
    "159.65.88.10:8080",
    "138.185.72.26:8080",
    "203.114.109.124:443",
    "103.75.201.2:443",
    "1.234.21.73:7080",
    "209.126.98.206:8080",
    "50.30.40.196:8080",
    "209.250.246.206:443",
    "178.79.147.66:8080",
    "50.116.54.215:443",
    "185.8.212.130:7080",
    "31.24.158.56:8080",
    "146.59.226.45:443",
    "72.15.201.15:8080",
    "110.232.117.186:8080",
    "5.9.116.246:8080",
    "185.157.82.211:8080",
    "129.232.188.93:443",
    "158.69.222.101:443",
    "164.68.99.3:8080",
    "45.118.135.203:7080",
    "101.50.0.91:8080",
    "195.154.133.20:443",
    "196.218.30.83:443",
    "45.118.115.99:8080",
    "167.99.115.35:8080",
    "79.172.212.216:8080",
    "159.8.59.82:8080"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.440856153.00000000049E1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000002.440856153.00000000049E1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.438019180.00000000049F1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.438019180.00000000049F1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.440822056.00000000049B0000.00000040.00001000.00020000.00000000.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.49b0000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.49b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4290000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4290000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.4c70000.0.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: 192.168.2.5 - Destination IP: 119.193.124.41

Timestamp:	192.168.2.5119.193.124.414982270802404304 07/20/22-01:07:10.809694
SID:	2404304
Source Port:	49822
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.5 - Destination IP: 51.91.76.89

Timestamp:	192.168.2.551.91.76.894981180802404338 07/20/22-01:07:08.508000
SID:	2404338
Source Port:	49811
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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

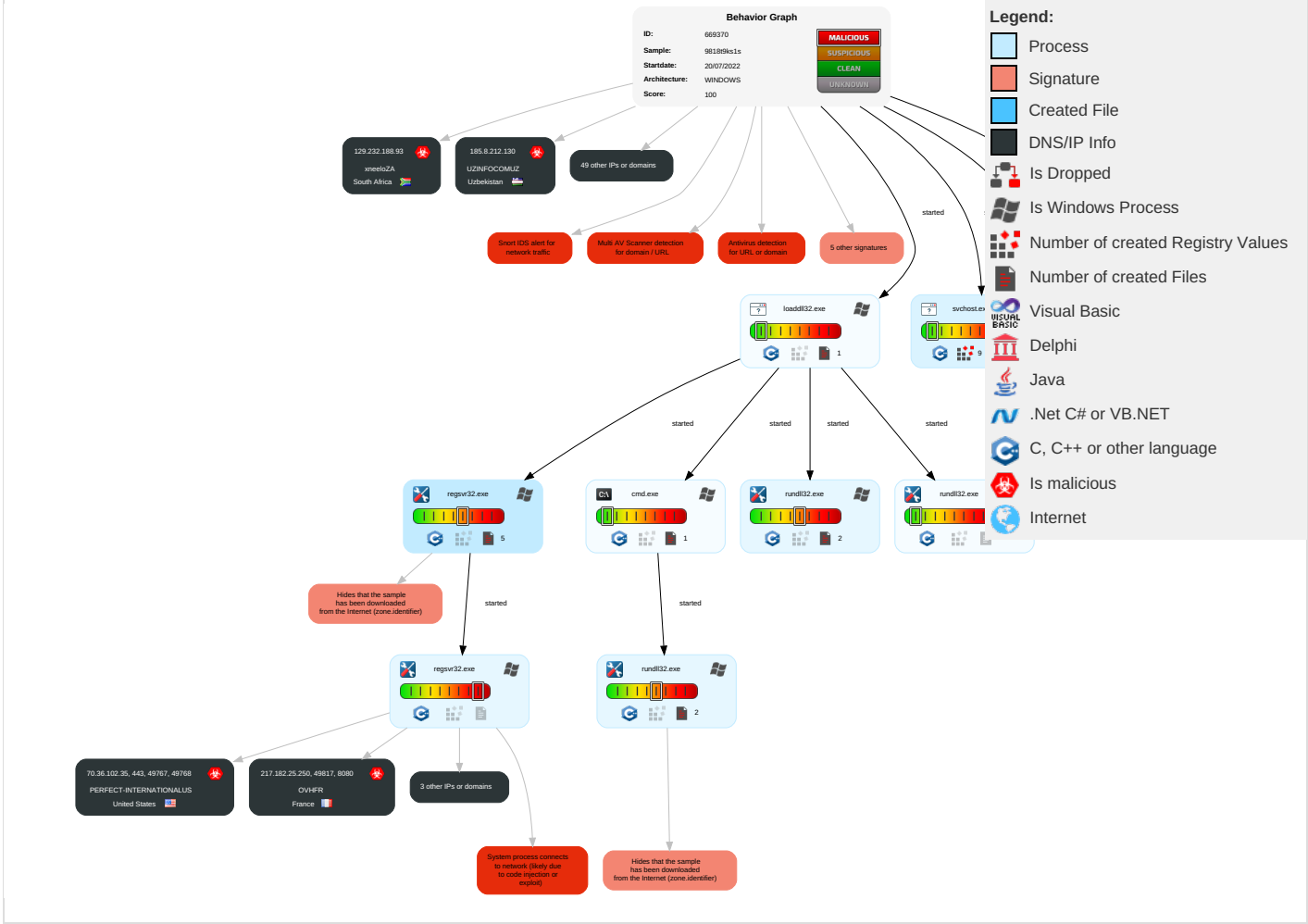
Yara detected Emotet

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	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	1 Input Capture	2 System Time Discovery	Remote Services	1 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	3 Virtualization/Sandbox Evasion	LSASS Memory	3 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	3 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	3 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

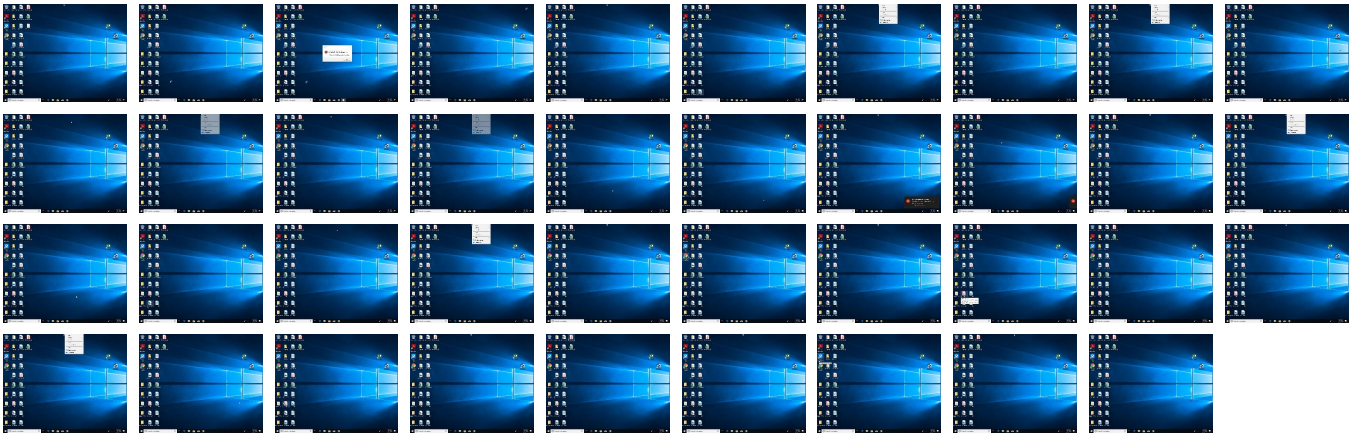
Hide Legend



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
9818t9ks1s.dll	70%	Virustotal		Browse
9818t9ks1s.dll	100%	Avira	TR/AD.Nekark.bnwrm	
9818t9ks1s.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.49b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.4290000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.4c70000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.4d70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.49e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.42c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.49f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.3110000.0.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://70.36.102.35/v	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQdF	100%	Avira URL Cloud	malware	
http://https://70.36.102.35/	14%	Virustotal		Browse
http://https://70.36.102.35/	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQdT	100%	Avira URL Cloud	malware	
http://schemas.dmtf.o	0%	Avira URL Cloud	safe	
http://https://92.240.254.110:8080/gECMlLDhVoiKFtzKjjRUPjlZHZhhxfpHLqiKeXIlMdFcRqaPxeg	0%	Avira URL Cloud	safe	
http://https://92.240.254.110/6.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQd	0%	Avira URL Cloud	safe	
http://https://92.240.254.110/	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQd	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

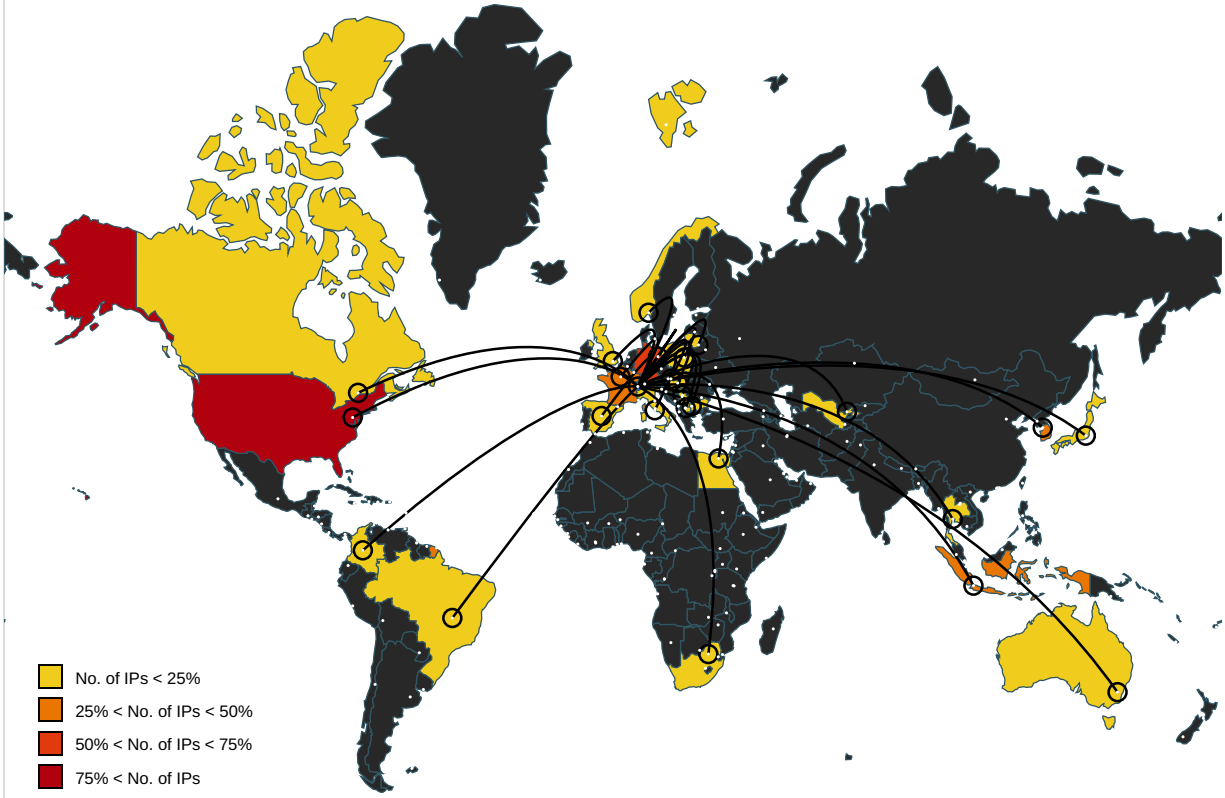
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/	svchost.exe, 0000000D.00000002.836571481.00000195808AF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000018.00000003.654122875.000002554B9B3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654040928.000002554B991000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654068801.000002554B9A2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://70.36.102.35/v	regsvr32.exe, 00000005.00000003.481253554.000000000331E000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.526452741.000000000331E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000018.00000003.654122875.000002554B9B3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654040928.000002554B991000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654068801.000002554B9A2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQdF	regsvr32.exe, 00000005.00000003.48125355 4.000000000331E000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.526452741.000000000331E000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://70.36.102.35/	regsvr32.exe, 00000005.00000003.52645274 1.000000000331E000.00000004.00000020.000 20000.00000000.sdmp	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000018.00000003.650938728 .000002554BE1A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.650909580.000002554B9B1000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.651038741 .000002554B98F000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.650818268.000002554B98F000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650841411 .000002554B9A0000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.651011860.000002554BE02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650968671 .000002554BE1A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000018.00000003.650938728 .000002554BE1A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.650909580.000002554B9B1000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.651038741 .000002554B98F000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.650818268.000002554B98F000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650841411 .000002554B9A0000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.651011860.000002554BE02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650968671 .000002554BE1A000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000018.00000003.654122875 .000002554B9B3000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.654040928.000002554B991000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654068801 .000002554B9A2000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 0000000D.00000002.836929466 .0000019586090000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000002.684378033.000002554AEEB000.00 000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000018.00000003.659846928 .000002554B991000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.659413155.000002554BE18000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.659476166 .000002554B9A6000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 8.00000003.659437692.000002554BE02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.659235634 .000002554B9A6000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQdT	regsvr32.exe, 00000005.00000003.48125355 4.000000000331E000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.526452741.000000000331E000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.dmtf.o	svchost.exe, 0000000D.00000002.836571481 .00000195808AF000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://92.240.254.110:8080/gECMlLDhVoiKFtzKjjRUPjlZHZhhxfpHLqiKeXIlMdFcRqaPxeg	regsvr32.exe, 00000005.00000002.95397921 5.000000003347000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.538622366.000000003347000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://92.240.254.110/6.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQd	regsvr32.exe, 00000005.00000003.52645274.000000000331E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://92.240.254.110/	regsvr32.exe, 00000005.00000003.52645274.000000000331E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000018.00000003.654122875.000002554B9B3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654040928.000002554B991000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.654068801.000002554B9A2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/enumeratio	svchost.exe, 0000000D.00000002.836571481.00000195808AF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000018.00000003.650938728.000002554BE1A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650909580.000002554B9B1000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.651038741.000002554B98F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650818268.000002554B98F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650841411.000002554B9A0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.651011860.000002554BE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000018.00000003.650968671.000002554BE1A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://70.36.102.35/gVsYreJaRCTZGAqrRgMzhhpqBeNQd	regsvr32.exe, 00000005.00000003.48125355.400000000331E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.182.25.250	unknown	France		16276	OVHFR	true
151.106.112.196	unknown	Germany		61157	PLUSSERVER-ASN1DE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.172.212.216	unknown	Hungary		61998	SZERVERPLEXHU	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
51.254.140.238	unknown	France		16276	OVHFR	true
195.201.151.129	unknown	Germany		24940	HETZNER-ASDE	true
206.188.212.92	unknown	United States		55002	DEFENSE-NETUS	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
209.126.98.206	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
1.234.21.73	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
176.56.128.118	unknown	Switzerland		12637	SEEWEBWebhostingcolocationandcloudservicesIT	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
167.99.115.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
185.8.212.130	unknown	Uzbekistan		48979	UZINFOCOMUZ	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
51.91.76.89	unknown	France		16276	OVHFR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASAS CABLETELCOC	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
31.24.158.56	unknown	Spain		50926	INFORTELECOM-ASES	true
50.30.40.196	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
189.126.111.200	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
146.59.226.45	unknown	Norway		16276	OVHFR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
196.218.30.83	unknown	Egypt		8452	TE-ASTE-ASEG	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
101.50.0.91	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
195.154.133.20	unknown	France		12876	OnlineSASFR	true
185.157.82.211	unknown	Poland		42927	S-NET-ASPL	true
70.36.102.35	unknown	United States		22439	PERFECT-INTERNATIONALUS	true
103.43.46.182	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
51.91.7.5	unknown	France		16276	OVHFR	true
5.9.116.246	unknown	Germany		24940	HETZNER-ASDE	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
209.250.246.206	unknown	European Union		20473	AS-CHOOPAUS	true
82.165.152.127	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
176.104.106.96	unknown	Serbia		198371	NINETRS	true
192.99.251.50	unknown	Canada		16276	OVHFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
92.240.254.110	unknown	Slovakia (SLOVAK Republic)		42005	LIGHTSTORM-COMMUNICATIONS-SRO-SK-ASPeeringsSK	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669370
Start date and time: 20/07/202201:05:10	2022-07-20 01:05:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9818t9ks1s (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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@19/5@0/58
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 97.2%) • Quality average: 84.5% • Quality standard deviation: 23.7%
HCA Information:	• Successful, ratio: 94% • 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, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.106.86.13, 23.205.181.161, 13.71.55.58, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, settings-prod-cin-2.centralindia.cloudapp.azure.com, sls.update.microsoft.com, 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, settings-prod-wus3-1.westus3.cloudapp.azure.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, e1723.g.akamaiedge.net, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, store-images.s-microsoft.com, go.microsoft.com.edgekey.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
01:06:51	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\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false

Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24943716309551126
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU49:BJiRdwfu2SRU49
MD5:	00654427E58616B58C62FC50C2B52CAE
SHA1:	FAE33CDA4A87AE87F8C54F629D947A73C0F3D752
SHA-256:	03367E7F1FBA65E7384C510DBEF162E503A7499F98E712C23D2A4990677EBACD
SHA-512:	50B9C51F0154E0AC12BFE61392E0295E5B70A93338AE526C115E018FE46A93596226C4B2A0BD74C2B254883E93F1CC2A7BFF900D505722DC7CB765E1B5EF9A2D
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x31ef495f, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25054036977537886
Encrypted:	false
SSDEEP:	384:7jM+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:7jTSB2nSB2RSjlK/+mLesOj1J2
MD5:	F449C6D8DF10E7E1F61BDD97A6494F87
SHA1:	CE664D962FF28C7AD92580FEAB4E450998815495
SHA-256:	5928D3F1531BDD70D74FF76EEF2344721E7398CC22D3F203F09CBEDD149DE78A
SHA-512:	5B77117B0644DAB36AC90631921320E6B5978D08E4D7B852E212F6E89335E7021068E8570BF8E777941328E3B4E1511AF61F99DD07D633BB8195149C484955B9
Malicious:	false
Preview:	1.I_... .....e.f.3...w.....).....z..3....z9.h.(.....z....).....3...w.....B.....@..... ....(.0.....z.....z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07303587911152667
Encrypted:	false
SSDEEP:	3:R4HR7vWMoximlll/tksjibD1tHlllall3VkttlmlnI:grW/iWMwibD1tfA3
MD5:	F2E666170C5999D5002A645DC8634D6E
SHA1:	20FFA1FAF1479110694542B7972C3F5155A9BED6
SHA-256:	57FB4BC8D3FFC4201342D81B07349EA6BC5728AFB0C4213E52AC91FB781D2E1E
SHA-512:	331576024162E4BBD3517803D81CEC60A8A12D1DED59E31B50FCA8DCC2D0721EE075955591EF0116383F3188729105F45E65CE4F376610963ECDA11978181B6B
Malicious:	false
Preview:	=.....3...w..3....z9.....z.....z.....z..yM.I....z}i.....z..... ....

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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
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):	6.352826845434315
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 98.32% • Windows Screen Saver (13104/52) 1.29% • 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:	9818t9ks1s.dll
File size:	655360
MD5:	83418a9af56db91ff2c78c4b2b9d62f8
SHA1:	0ea68aab3721e509ce0b1bff7e574eda037798be
SHA256:	4a688f571024b08f9793559427d8692471f5aa715882899c631c3052eac7c6a1
SHA512:	dadfeea6c52deda79860158036b60c54e907483b3f317e270d44e5949db169f4a26e748956654d914a3c9dda52c264e2c79bc0073254d9e58c62d9b5e69205a2
SSDEEP:	6144:/6ZMFXzqfoSHr/mvcQYbi2HN8C8BgifO7y7TcuVqrWLWN7Ypsi6Ih9vH0/oUHahE:/8MFX47ivcQMNsrD4KJjO69cI
TLSH:	06D47C0EFFD1C1B2D36B123019D5C64823ADBF2CEAA1C5B777A8BE1D69326C14512B16
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)..0m..cm..cm..c...cg..c...ck..c~..co..c...c|..cm..c@..ch..cq..ch..c...cF..cd..ch..c...ch..cl..c...cl..ch..cl..cRichm..c.....

File Icon

Icon Hash:	c0cc4c687ccccc78

Static PE Info

General

Entrypoint:	0x1001131c
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:	0x623CFB7E [Thu Mar 24 23:15:10 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:	d63ab94f4bb6b5d2f0f6092bf07e00ac

Entrypoint Preview
Instruction
push 0000000Ch
push 10041D40h
call 00007FB05074AA61h
xor eax, eax
inc eax
mov dword ptr [ebp-1Ch], eax
mov esi, dword ptr [ebp+0Ch]
xor edi, edi
cmp esi, edi
jne 00007FB05074987Eh
cmp dword ptr [1004F3C8h], edi
je 00007FB050749929h
mov dword ptr [ebp-04h], edi
cmp esi, eax
je 00007FB050749877h
cmp esi, 02h
jne 00007FB0507498A3h
mov eax, dword ptr [10050CB4h]
cmp eax, edi
je 00007FB05074987Eh
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 00007FB0507498FBh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007FB050749697h
mov dword ptr [ebp-1Ch], eax
cmp eax, edi
je 00007FB0507498E4h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007FB05073E608h
mov dword ptr [ebp-1Ch], eax
cmp esi, 01h
jne 00007FB050749880h
cmp eax, edi
jne 00007FB05074987Ch
push ebx
push edi
push dword ptr [ebp+08h]
call 00007FB05074966Dh
cmp esi, edi
je 00007FB050749877h
cmp esi, 03h
jne 00007FB05074989Bh
push ebx
push esi
push dword ptr [ebp+08h]

Instruction
call 00007FB05074965Ah
test eax, eax
jne 00007FB050749875h
mov dword ptr [ebp-1Ch], edi
cmp dword ptr [ebp-1Ch], edi
je 00007FB050749885h
mov eax, dword ptr [10050CB4h]
cmp eax, edi
je 00007FB05074987Ch
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 00007FB05074988Ch
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	0x4aa40	0x6e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x48844	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x51000	0x480a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	0x4e40	.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	0x43830	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3c000	0x668	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x487bc	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	0x3a49e	0x3b000	False	0.6009418034957628	data	6.6116392367886405	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x3c000	0xeaae	0xf000	False	0.32220052083333334	data	5.046533656475497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4b000	0x5cb8	0x3000	False	0.2513834635416667	data	3.8346109495878085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x51000	0x480a0	0x49000	False	0.5524534460616438	data	6.0777904674160155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x9a000	0x8810	0x9000	False	0.3506673177083333	data	4.48951519417909	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0x747c0	0x20800	data		
RT_CURSOR	0x95028	0x134	data		
RT_CURSOR	0x95160	0xb4	data		
RT_CURSOR	0x95240	0x134	AmigaOS bitmap font		
RT_CURSOR	0x95390	0x134	data		
RT_CURSOR	0x954e0	0x134	data		
RT_CURSOR	0x95630	0x134	data		
RT_CURSOR	0x95780	0x134	data		
RT_CURSOR	0x958d0	0x134	data		
RT_CURSOR	0x95a20	0x134	data		
RT_CURSOR	0x95b70	0x134	data		
RT_CURSOR	0x95cc0	0x134	data		
RT_CURSOR	0x95e10	0x134	data		
RT_CURSOR	0x95f60	0x134	AmigaOS bitmap font		
RT_CURSOR	0x960b0	0x134	data		
RT_CURSOR	0x96200	0x134	data		
RT_CURSOR	0x96350	0x134	data		
RT_BITMAP	0x522e0	0x428	data		
RT_BITMAP	0x520c0	0xe0	GLS_BINARY_LSB_FIRST	Spanish	Mexico
RT_BITMAP	0x965a0	0xb8	data		
RT_BITMAP	0x96658	0x144	data		
RT_ICON	0x52a98	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x632d8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x73b18	0x2e8	data		
RT_ICON	0x73e00	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x73f50	0x2e8	data		
RT_ICON	0x74238	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x74388	0x2e8	data		
RT_ICON	0x74670	0x128	GLS_BINARY_LSB_FIRST		
RT_MENU	0x52728	0x23a	data		
RT_MENU	0x521b0	0x46	data	Spanish	Mexico
RT_DIALOG	0x52968	0x12c	data		
RT_DIALOG	0x521f8	0xe2	data	Spanish	Mexico
RT_DIALOG	0x964a0	0xfe	data		
RT_STRING	0x96810	0x92	data		
RT_STRING	0x967a0	0x6a	data	Spanish	Mexico
RT_STRING	0x968a8	0x48	data		
RT_STRING	0x96938	0x19e	data		
RT_STRING	0x96c08	0x280	data		
RT_STRING	0x97010	0x39c	data		
RT_STRING	0x96f90	0x7a	data		
RT_STRING	0x96ad8	0x12e	data		
RT_STRING	0x96e88	0x104	data		
RT_STRING	0x968f0	0x46	data		
RT_STRING	0x973b0	0x128	data		
RT_STRING	0x974d8	0x240	data		
RT_STRING	0x97718	0x9e	data		
RT_STRING	0x977b8	0xb0	Hitachi SH big-endian COFF object file, not stripped, 16640 sections, symbol offset=0x69007200, 201344768 symbols, optional header size 29952		
RT_STRING	0x97868	0x30	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0x97898	0x1d0	data		
RT_STRING	0x97a68	0x5bc	data		
RT_STRING	0x98418	0x31c	data		
RT_STRING	0x98118	0x300	data		
RT_STRING	0x98fa0	0xb0	data		
RT_STRING	0x98028	0xee	data		
RT_STRING	0x98e50	0x11e	data		
RT_STRING	0x98738	0x4d0	data		
RT_STRING	0x98c08	0x248	data		
RT_STRING	0x98f70	0x2e	data		
RT_STRING	0x99050	0x4c	data		
RT_ACCELERATOR	0x94fc0	0x68	data		
RT_GROUP_CURSOR	0x95218	0x22	Lotus unknown worksheet or configuration, revision 0x2		
RT_GROUP_CURSOR	0x95a08	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95378	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x958b8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95768	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x96098	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95618	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95ca8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x954c8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95b58	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95df8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x95f48	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x961e8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x96338	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x96488	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x632c0	0x14	data		
RT_GROUP_ICON	0x73f28	0x22	data		
RT_GROUP_ICON	0x73b00	0x14	data		
RT_GROUP_ICON	0x74360	0x22	data		
RT_GROUP_ICON	0x74798	0x22	data		
None	0x52708	0x1e	data		
None	0x521a0	0xa	data	Spanish	Mexico

Imports

DLL	Import

DLL	Import
KERNEL32.dll	RtlUnwind, GetSystemTimeAsFileTime, GetCommandLineA, TerminateProcess, HeapReAlloc, HeapSize, HeapDestroy, HeapCreate, VirtualFree, IsBadWritePtr, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, VirtualQuery, QueryPerformanceCounter, GetCurrentProcessId, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, SetStdHandle, SetEnvironmentVariableA, GetSystemInfo, VirtualAlloc, VirtualProtect, HeapFree, HeapAlloc, GetTickCount, SystemTimeToFileTime, LocalFileTimeToFileTime, FileTimeToLocalFileTime, FileTimeToSystemTime, GetOEMCP, GetCPInfo, GetShortPathNameA, CreateFileA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, DeleteFileA, MoveFileA, GetCurrentDirectoryA, GlobalFlags, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, InterlockedIncrement, InterlockedDecrement, DeleteCriticalSection, InitializeCriticalSection, RaiseException, GetDiskFreeSpaceA, GetFullPathNameA, GetTempFileNameA, GetFileTime, SetFileTime, GetFileAttributesA, GlobalGetAtomNameA, GlobalFindAtomA, lstrcatA, lstrcmpW, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, CloseHandle, GlobalAddAtomA, GetCurrentThread, GetCurrentThreadId, FreeLibrary, GlobalDeleteAtom, lstrcmpA, GetModuleFileNameA, GetModuleHandleA, GetProcAddress, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, LoadLibraryA, FreeResource, SetLastError, GlobalFree, FindResourceA, LoadResource, LockResource, SizeofResource, MulDiv, GlobalAlloc, GlobalLock, GlobalUnlock, FormatMessageA, lstrcpynA, LocalFree, ExitProcess, GetStringTypeExA, CompareStringW, CompareStringA, lstrlenA, lstrcmpiA, GetVersion, GetLastError, WideCharToMultiByte, MultiByteToWideChar, GetVersionExA, GetThreadLocale, GetLocaleInfoA, GetACP, UnhandledExceptionFilter, InterlockedExchange
USER32.dll	KillTimer, WindowFromPoint, GetDCEx, LockWindowUpdate, RegisterClipboardFormatA, PostThreadMessageA, SetRect, CharNextA, DestroyIcon, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, FillRect, LoadCursorA, GetSysColorBrush, SetParent, GetSystemMenu, DeleteMenu, IsRectEmpty, IsZoomed, GetDC, ReleaseDC, LoadMenuA, DestroyMenu, UnpackDDElParam, ReuseDDElParam, ReleaseCapture, LoadAcceleratorsA, InsertMenuItemA, CreatePopupMenu, SetRectEmpty, BringWindowToTop, SetMenu, TranslateAcceleratorA, InvalidateRect, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, GetClassLongA, GetClassNameA, SetPropA, GetPropA, RemovePropA, IsChild, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, LoadIconA, MapWindowPoints, TrackPopupMenu, SetForegroundWindow, SetTimer, GetClientRect, GetMenu, GetSysColor, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, GetClassInfoA, RegisterClassA, UnregisterClassA, DefWindowProcA, CallWindowProcA, OffsetRect, IntersectRect, SystemParametersInfoA, IsIconic, GetWindowPlacement, GetWindowRect, CopyRect, PtInRect, GetWindow, SetWindowContextHelpId, MapDialogRect, wsprintfA, GetWindowTextLengthA, GetWindowTextA, SetWindowPos, CharUpperA, UpdateWindow, EnableWindow, SendMessageA, GetClassInfoExA, GetSubMenu, GetMenuItemCount, InsertMenuA, GetMenuItemID, AppendMenuA, SetFocus, ShowWindow, MoveWindow, SetWindowLongA, GetDlgCtrlID, SetWindowTextA, IsDialogMessageA, SendDlgItemMessageA, GetMenuItemInfoA, InflateRect, SetMenuItemBitmaps, GetFocus, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, SetWindowsHookExA, CallNextHookEx, GetMessageA, TranslateMessage, MessageBeep, GetNextDlgGroupItem, SetCapture, InvalidateRgn, CopyAcceleratorTableA, GetMenuStringA, GetMenuState, EndDialog, GetNextDlgTabItem, GetParent, IsWindowEnabled, GetDlgItem, GetWindowLongA, IsWindow, DestroyWindow, CreateDialogIndirectParamA, GetSystemMetrics, SetActiveWindow, GetActiveWindow, GetDesktopWindow, PostQuitMessage, PostMessageA, SetCursor, ShowOwnedPopups, GetLastActivePopup, MessageBoxA, ValidateRect, GetCursorPos, PeekMessageA, GetKeyState, IsWindowVisible, DispatchMessageA
GDI32.dll	CreateSolidBrush, CreateFontIndirectA, GetBkColor, GetTextColor, GetStockObject, GetRgnBox, PatBlt, SetRectRgn, CombineRgn, GetMapMode, CreatePatternBrush, ExtSelectClipRgn, ScaleWindowExtEx, SetWindowExtEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, Escape, ExtTextOutA, TextOutA, RectVisible, PtVisible, GetPixel, BitBlt, GetWindowExtEx, CreateRectRgnIndirect, GetDeviceCaps, CreateRectRgn, SelectClipRgn, IntersectClipRect, ExcludeClipRect, SetMapMode, SetBkMode, RestoreDC, SaveDC, GetTextExtentPoint32A, GetTextMetricsA, CreateFontA, GetCharWidthA, DeleteObject, SelectObject, StretchDIBits, DeleteDC, CreateCompatibleDC, CreateCompatibleBitmap, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateBitmap, GetViewportExtEx
comdlg32.dll	GetSaveFileNameA, GetFileTitleA, GetOpenFileNameA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter
ADVAPI32.dll	GetFileSecurityA, RegSetValueA, RegOpenKeyA, RegQueryValueExA, RegOpenKeyExA, RegDeleteKeyA, RegEnumKeyA, RegQueryValueA, RegCreateKeyExA, RegSetValueExA, RegDeleteValueA, RegCreateKeyA, RegCloseKey, SetFileSecurityA
SHELL32.dll	DragQueryFileA, ExtractIconA, SHGetFileInfoA, DragFinish
COMCTL32.dll	ImageList_Draw, ImageList_GetImageInfo, ImageList_Destroy
SHLWAPI.dll	PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
oledlg.dll	
ole32.dll	CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CLSIDFromString, CLSIDFromProgID, CoTaskMemFree, OleUninitialize, CoFreeUnusedLibraries, CoRegisterMessageFilter, OleFlushClipboard, OleIsCurrentClipboard, CoRevokeClassObject, CoTaskMemAlloc, OleInitialize
OLEAUT32.dll	SysAllocStringLen, VariantClear, VariantChangeType, VariantInit, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, SystemTimeToVariantTime, SafeArrayDestroy, SysAllocString, VariantCopy, SysFreeString

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10005090
DllUnregisterServerr	2	0x100050c0

Possible Origin

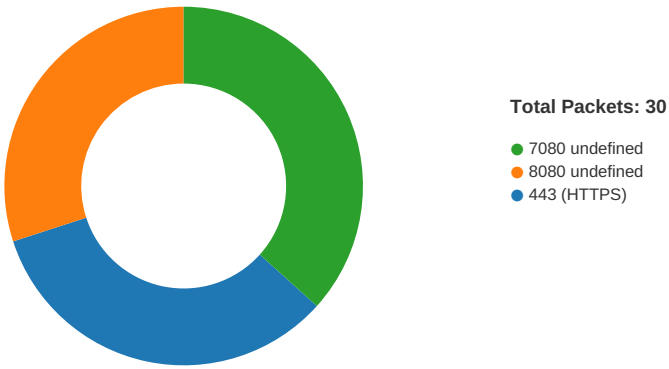
Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5119.193.124.4 14982270802404304 07/20/22-01:07:10.809694	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49822	7080	192.168.2.5	119.193.124.41
192.168.2.551.91.76.8949 81180802404338 07/20/22-01:07:08.508000	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49811	8080	192.168.2.5	51.91.76.89

Network Port Distribution



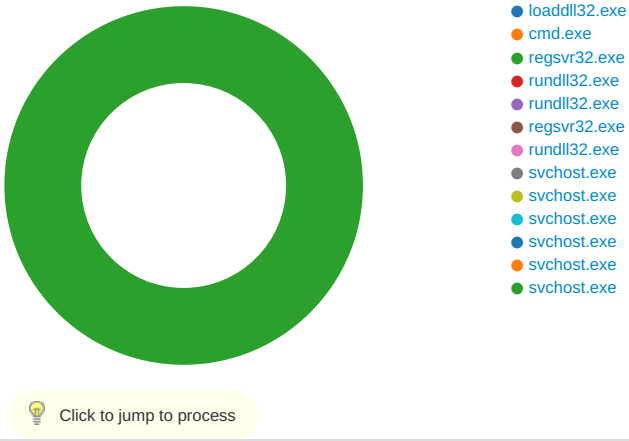
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:06:46.936866999 CEST	49767	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:46.936918020 CEST	443	49767	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:46.937026024 CEST	49767	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:46.988656998 CEST	49767	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:46.988699913 CEST	443	49767	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.166369915 CEST	443	49767	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.175667048 CEST	49768	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.175726891 CEST	443	49768	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.175817966 CEST	49768	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.176795959 CEST	49768	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.176825047 CEST	443	49768	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.348900080 CEST	443	49768	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.356182098 CEST	49769	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.356241941 CEST	443	49769	70.36.102.35	192.168.2.5
Jul 20, 2022 01:06:47.356360912 CEST	49769	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.356899023 CEST	49769	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.356967926 CEST	443	49769	70.36.102.35	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:06:47.357043982 CEST	49769	443	192.168.2.5	70.36.102.35
Jul 20, 2022 01:06:47.450864077 CEST	49770	8080	192.168.2.5	92.240.254.110
Jul 20, 2022 01:06:50.456844091 CEST	49770	8080	192.168.2.5	92.240.254.110
Jul 20, 2022 01:06:56.457360983 CEST	49770	8080	192.168.2.5	92.240.254.110
Jul 20, 2022 01:07:08.507999897 CEST	49811	8080	192.168.2.5	51.91.76.89
Jul 20, 2022 01:07:08.528073072 CEST	8080	49811	51.91.76.89	192.168.2.5
Jul 20, 2022 01:07:09.036581039 CEST	49811	8080	192.168.2.5	51.91.76.89
Jul 20, 2022 01:07:09.056623936 CEST	8080	49811	51.91.76.89	192.168.2.5
Jul 20, 2022 01:07:09.567893982 CEST	49811	8080	192.168.2.5	51.91.76.89
Jul 20, 2022 01:07:09.589181900 CEST	8080	49811	51.91.76.89	192.168.2.5
Jul 20, 2022 01:07:09.615654945 CEST	49817	8080	192.168.2.5	217.182.25.250
Jul 20, 2022 01:07:09.643641949 CEST	8080	49817	217.182.25.250	192.168.2.5
Jul 20, 2022 01:07:10.146051884 CEST	49817	8080	192.168.2.5	217.182.25.250
Jul 20, 2022 01:07:10.174648046 CEST	8080	49817	217.182.25.250	192.168.2.5
Jul 20, 2022 01:07:10.771107912 CEST	49817	8080	192.168.2.5	217.182.25.250
Jul 20, 2022 01:07:10.799603939 CEST	8080	49817	217.182.25.250	192.168.2.5
Jul 20, 2022 01:07:10.809694052 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:11.079042912 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:11.079195976 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:11.082602024 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:11.353307962 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:11.369446039 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:11.369509935 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:11.369604111 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:12.626746893 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:12.898112059 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:12.898277998 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:12.903048992 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:13.218106985 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:14.065052986 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:14.065643072 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:07:17.064517021 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:17.064565897 CEST	7080	49822	119.193.124.41	192.168.2.5
Jul 20, 2022 01:07:17.064661980 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:08:36.268321991 CEST	49822	7080	192.168.2.5	119.193.124.41
Jul 20, 2022 01:08:36.268376112 CEST	49822	7080	192.168.2.5	119.193.124.41

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6888**, Parent PID: **3552**

General

Target ID:	0
Start time:	01:06:21
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\9818t9ks1s.dll"
Imagebase:	0xff0000
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: **6896**, Parent PID: **6888**

General

Target ID:	1
Start time:	01:06:22
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\9818t9ks1s.dll",#1
Imagebase:	0x1100000
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: **6912**, Parent PID: **6888**

General

Target ID:	2
Start time:	01:06:22
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\9818t9ks1s.dll

Imagebase:	0x8f0000
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: 00000002.00000002.440856153.00000000049E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.440856153.00000000049E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.440822056.00000000049B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.440822056.00000000049B0000.00000040.00001000.00020000.00000000.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\Bvqee\qeggfkimakwygr.che:Zone.Identifier	success or wait	1	49F594F	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: **6924**, Parent PID: **6896**

General

Target ID:	3
Start time:	01:06:22
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\9818t9ks1s.dll",#1
Imagebase:	0xc60000
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: 00000003.00000002.438019180.00000000049F1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.438019180.00000000049F1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.437810837.0000000003110000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.437810837.0000000003110000.00000040.00001000.00020000.00000000.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: rundll32.exe PID: **6932**, Parent PID: **6888**

General	
Target ID:	4
Start time:	01:06:23
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9818t9ks1s.dll,DllRegisterServer
Imagebase:	0xc60000
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: 00000004.00000002.438281451.0000000004290000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.438281451.0000000004290000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.438313364.00000000042C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.438313364.00000000042C1000.00000020.00001000.00020000.00000000.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: regsvr32.exe PID: **7020**, Parent PID: **6912**

General	
Target ID:	5
Start time:	01:06:26
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\Bvqee\qeggfkimakwygr.che"
Imagebase:	0x8f0000
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: 00000005.00000002.954167693.0000000004C70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.954167693.0000000004C70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.954213063.0000000004D71000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.954213063.0000000004D71000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7040**, Parent PID: **6888**

General	
Target ID:	6
Start time:	01:06:27
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\9818t9ks1s.dll,DllUnregisterServerr
Imagebase:	0xc60000
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: **5084**, Parent PID: **580**

General

Target ID:	12
Start time:	01:06:47
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:	0x7ff78ca80000
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: **6324**, Parent PID: **580**

General

Target ID:	13
Start time:	01:06:51
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:	0x7ff78ca80000
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	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: **6576**, Parent PID: **580**

General	
Target ID:	14
Start time:	01:07:04
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:	0x7ff78ca80000
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: **3952**, Parent PID: **580**

General	
Target ID:	16
Start time:	01:07:10
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:	0x7ff78ca80000
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: **7028**, Parent PID: **580**

General	
Target ID:	22
Start time:	01:07:41
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:	0x7ff78ca80000
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: **5748**, Parent PID: **580**

General

Target ID:	24
Start time:	01:07:51
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:	0x7ff78ca80000
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