ID: 669371
Sample Name: uVPWqAOMKn
Cookbook: default.jbs
Time: 01:05:11
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

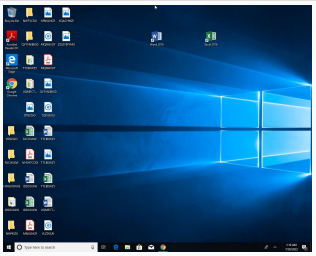
Windows Analysis Report

uVPWqAOMKn

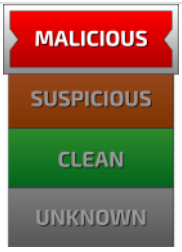
Overview

General Information

Sample Name:	uVPWqAOMKn (renamed file extension from none to dll)
Analysis ID:	669371
MD5:	2e7cff2320794ce..
SHA1:	47c3259798a247..
SHA256:	cc257f8c204386...
Tags:	32 dll exe trojan
Infos:	



Detection



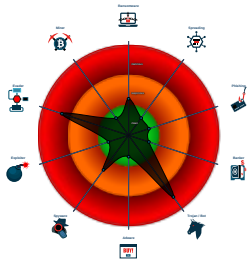
Emotet

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: 6864 cmdline: loaddll32.exe "C:\Users\user\Desktop\uVPWqAOMKn.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6872 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\uVPWqAOMKn.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6900 cmdline: rundll32.exe "C:\Users\user\Desktop\uVPWqAOMKn.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6892 cmdline: regsvr32.exe /s C:\Users\user\Desktop\uVPWqAOMKn.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 7100 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Elutq\fjqpvuhrz.fqb" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6920 cmdline: rundll32.exe C:\Users\user\Desktop\uVPWqAOMKn.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7024 cmdline: rundll32.exe C:\Users\user\Desktop\uVPWqAOMKn.dll,DllUnregisterServerrrrrrrrrrr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6880 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 596 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4464 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5100 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2060 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5116 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "45.142.114.231:8080",
    "209.250.246.206:443",
    "1.234.21.73:7080",
    "134.122.66.193:8080",
    "176.56.128.118:443",
    "195.154.133.20:443",
    "167.99.115.35:8080",
    "189.126.111.200:7080",
    "176.104.106.96:8080",
    "110.232.117.186:8080",
    "1.234.2.232:8080",
    "50.30.40.196:8080",
    "159.65.88.10:8080",
    "45.176.232.124:443",
    "45.118.115.99:8080",
    "206.188.212.92:8080",
    "146.59.226.45:443",
    "46.55.222.11:443",
    "185.157.82.211:8080",
    "129.232.188.93:443",
    "201.94.166.162:443",
    "51.254.140.238:7080",
    "31.24.158.56:8080",
    "178.79.147.66:8080",
    "203.114.109.124:443",
    "216.158.226.206:443",
    "151.106.112.196:8080",
    "167.172.253.162:8080",
    "45.118.135.203:7080",
    "196.218.30.83:443",
    "107.182.225.142:8080",
    "101.50.0.91:8080",
    "79.172.212.216:8080",
    "209.126.98.206:8080",
    "51.91.7.5:8080",
    "72.15.201.15:8080",
    "173.212.193.249:8080",
    "82.165.152.127:8080",
    "103.43.46.182:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.895080994.0000000000E90000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000007.00000002.895080994.0000000000E90000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.417225831.0000000004171000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.417225831.0000000004171000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.895666203.00000000010E1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.regsvr32.exe.4be0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.4be0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.4c10000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.4c10000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.3390000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 31 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.6 - Destination IP: 119.193.124.41

Timestamp:	192.168.2.6119.193.124.414983970802404304 07/20/22-01:08:05.169546
SID:	2404304
Source Port:	49839
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.6 - Destination IP: 51.91.76.89

Timestamp:	192.168.2.651.91.76.894982980802404338 07/20/22-01:08:02.804632
SID:	2404338
Source Port:	49829
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

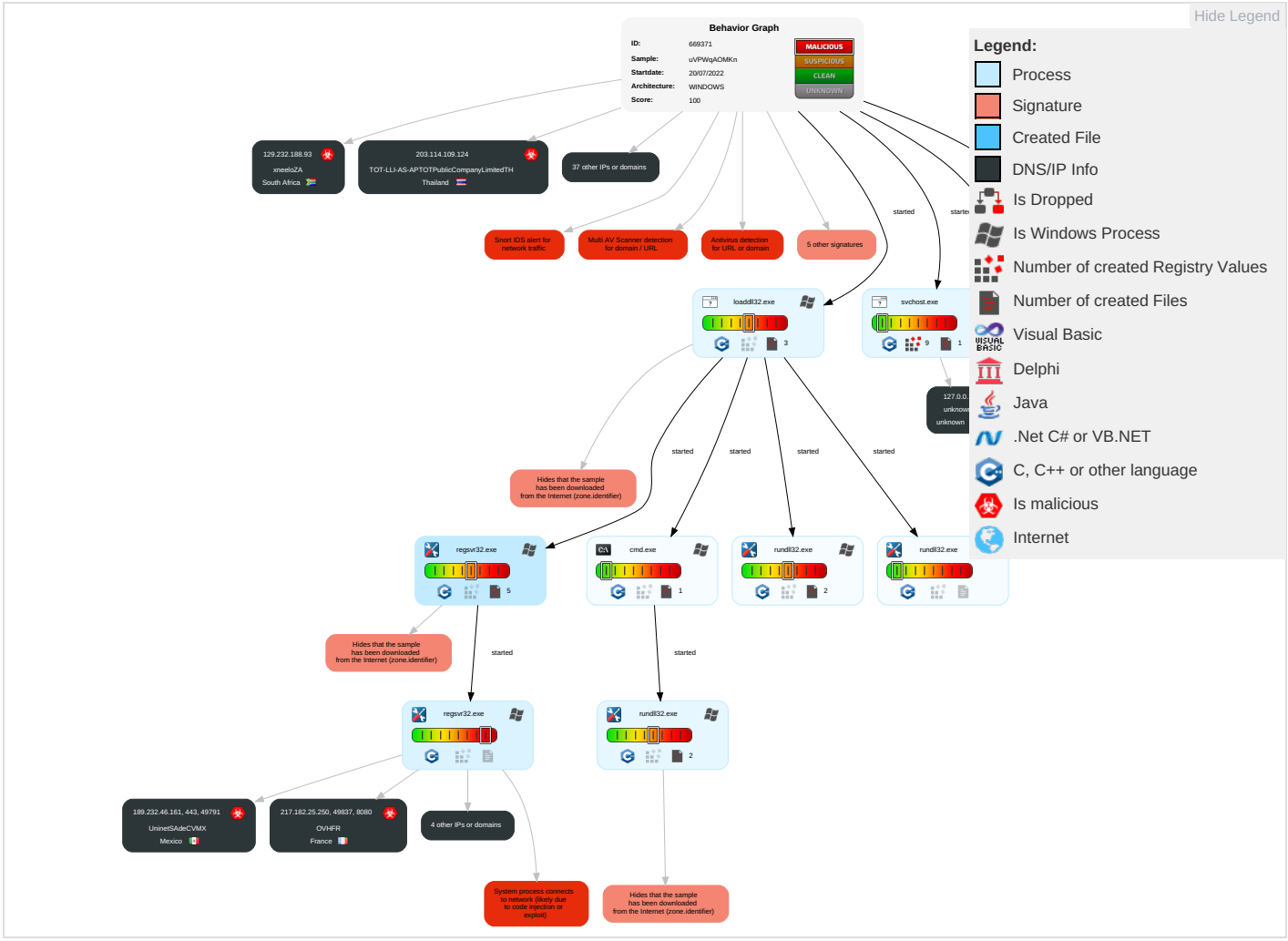
System process connects to network (likely due to code injection or exploit)

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	2 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	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	3 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

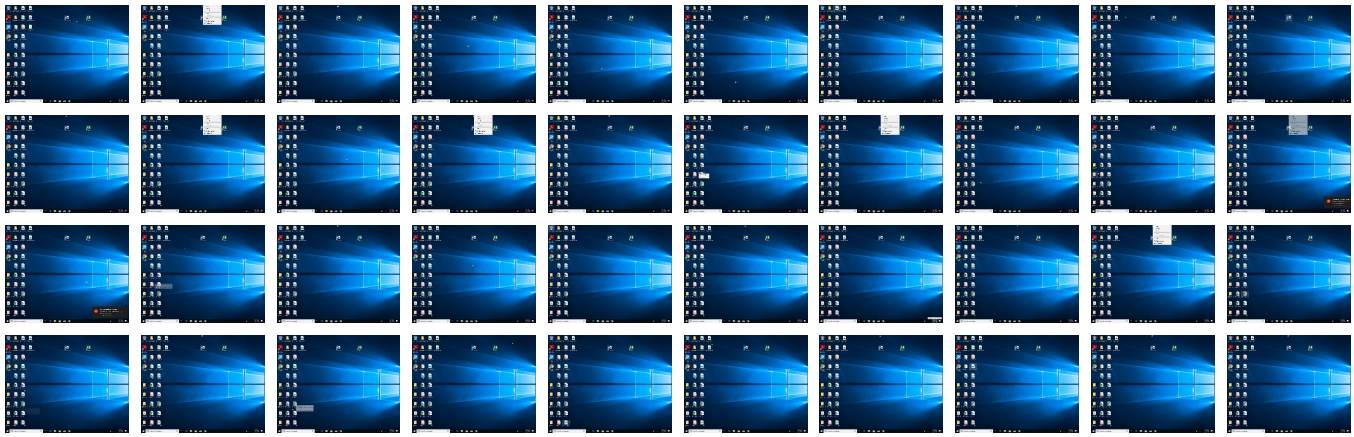
Behavior Graph



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
uVPWqAOMKn.dll	68%	Virustotal		Browse
uVPWqAOMKn.dll	75%	ReversingLabs	Win32.Trojan.Emotet	
uVPWqAOMKn.dll	100%	Avira	TR/AD.Nekark.dwxdl	
uVPWqAOMKn.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.regsvr32.exe.e90000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.4be0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll32.exe.520000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.3010000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4aa0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.3390000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.rundll32.exe.4170000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.regsvr32.exe.10e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.550000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.4140000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.2fe0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.4c10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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://217.182.25.250:8080/BsbzREwLaKqFTTaeHjvPeVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW2	0%	Avira URL Cloud	safe	
http://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkB	0%	Avira URL Cloud	safe	
http://https://189.232.46.161/	14%	Virustotal		Browse
http://https://189.232.46.161/	100%	Avira URL Cloud	malware	
http://https://189.232.46.161/oDKcMsHRRxcdTZdqBLENpsfwBpdNwUtCDsdjXOHPdhyxmepd	100%	Avira URL Cloud	malware	
http://https://216.120.236.62:8080/AriEwZcvJsYjzutuViEY9	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://217.182.25.250:8080/BsbzREwLaKqFTTaeHjvPeVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://217.182.25.250/1.76.89:8080/pdNwUtCDsdjXOHPdhyxmepd	0%	Avira URL Cloud	safe	
http://https://51.91.76.89/4R	100%	Avira URL Cloud	malware	
http://https://51.91.76.89:8080/SErPxnMnZMWCWtStc	100%	Avira URL Cloud	malware	
http://https://217.182.25.250/eVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://189.232.46.161/oDKcMsHRRxcdTZdqBLENpsfwBpdNwUtCDsdjXOHPdhyxmepdV	100%	Avira URL Cloud	malware	
http://https://51.91.76.89:80:8080/	0%	Avira URL Cloud	safe	
http://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkBo	0%	Avira URL Cloud	safe	
http://https://216.120.236.62/o	100%	Avira URL Cloud	malware	
http://https://216.120.236.62/	100%	URL Reputation	malware	
http://https://51.91.76.89/	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://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkB&	0%	Avira URL Cloud	safe	
http://https://119.193.124.41/	0%	Avira URL Cloud	safe	
http://https://189.232.46.161/=R	100%	Avira URL Cloud	malware	
http://https://216.120.236.62:8080/AriEwZcvJsYjzutuViEY	100%	Avira URL Cloud	malware	
http://https://217.182.25.250/	0%	Avira URL Cloud	safe	
http://ctldl.windowsupda	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

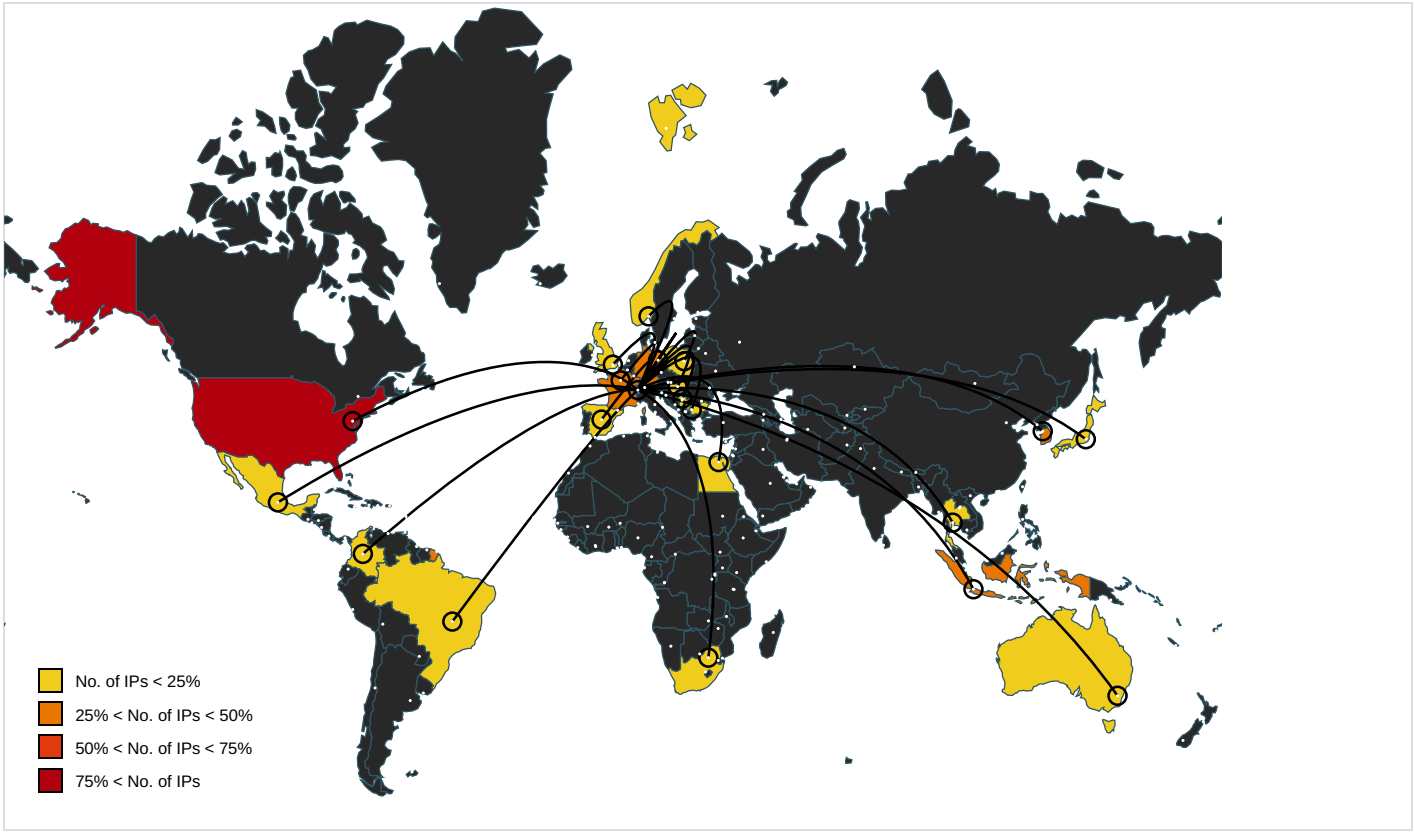
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000017.00000003.588806879.0000022230180000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.585558704.000002223019E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://217.182.25.250:8080/BsbzREwLaKqFTTaeHjvPeVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW2	regsvr32.exe, 00000007.00000002.895366348.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049679.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392382.0000000001006000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkB	regsvr32.exe, 00000007.00000003.594113245.0000000001034000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049679.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.895488066.0000000001034000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://189.232.46.161/	regsvr32.exe, 00000007.00000003.579287319.0000000001006000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.895366348.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049679.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392382.0000000001006000.00000004.00000020.00020000.00000000.sdmp	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://189.232.46.161/oDKcMsHRRxcdTZdqBLENpsfwBpdNwUtCDsdjXOHPdhyxmepd	regsvr32.exe, 00000007.00000002.895293868.0000000000FE6000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://216.120.236.62:8080/AriEwZcvJsYjzutuViEY9	regsvr32.exe, 00000007.00000003.579287319.0000000001006000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.895366348.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049679.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392382.0000000001006000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000002.00000002.896257359.0000029312C00000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://217.182.25.250:8080/BsbzREwLaKqFTTaeHjvPeVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW	regsvr32.exe, 00000007.00000002.895366348.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049679.0000000000FFB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392382.0000000001006000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000017.00000003.589531614.00000222301BC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.589590666.00000222301A6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.589562765.00000222301BC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.589653116.0000022230602000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://217.182.25.250/1.76.89:8080/pdNwUtCDsdjXOHPdhyxmepd	regsvr32.exe, 00000007.00000003.584392382.0000000001006000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://51.91.76.89/4R	regsvr32.exe, 00000007.00000002.89536634 8.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.594049679.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392 382.0000000001006000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://support.hotspotshield.com/	svchost.exe, 00000017.00000003.580472643 .00000222301AD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.580521789.0000022230602000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.580451647 .000002223019C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://51.91.76.89:8080/SErPxnMnZMWCWtStc	regsvr32.exe, 00000007.00000002.89536634 8.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.594049679.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392 382.0000000001006000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000002.895217070.0000000000FAA00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://217.182.25.250/eVlDdCnzQYZNllXagZhyDivNlMzaFBSuCmbSampUWW	regsvr32.exe, 00000007.00000003.58439238 2.0000000001006000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000017.00000003.588806879 .0000022230180000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.585558704.000002223019E000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://189.232.46.161/oDKcMsHRRxcdTZdqBLENpsfwBpdNwUtCDsdjXOHPdhyxmepdV	regsvr32.exe, 00000007.00000003.57928731 9.0000000001006000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://51.91.76.89:80:8080/	regsvr32.exe, 00000007.00000003.58434421 4.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkBo	regsvr32.exe, 00000007.00000002.89536634 8.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.594049679.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://216.120.236.62/o	regsvr32.exe, 00000007.00000003.57928731 9.0000000001006000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.584392382.0000000001006000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://216.120.236.62/	regsvr32.exe, 00000007.00000003.58439238 2.0000000001006000.00000004.00000020.000 20000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://51.91.76.89/	regsvr32.exe, 00000007.00000002.89536634 8.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.594049679.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392 382.0000000001006000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000017.00000003.580472643 .00000222301AD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.580521789.0000022230602000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.580451647 .000002223019C000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000017.00000003.580472643 .00000222301AD000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.580521789.0000022230602000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.580451647 .000002223019C000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000017.00000003.588806879 .0000022230180000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.585558704.000002223019E000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://119.193.124.41:7080/VpoQHFAbXxwVXMvalFtvpYGPvlzHFATxmfdXXXqPyAmJeXjvroVHBlPfYCuMPkB&	regsvr32.exe, 00000007.00000002.89548806 6.0000000001034000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://119.193.124.41/	regsvr32.exe, 00000007.00000002.89548806 6.0000000001034000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://189.232.46.161/=R	regsvr32.exe, 00000007.00000003.57928731 9.0000000001006000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.895366348.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049 679.0000000000FFB000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000003.584392382.000000000100600 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://216.120.236.62:8080/AriEwZcvJsYjzutuViEY	regsvr32.exe, 00000007.00000003.57928731 9.0000000001006000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.895366348.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.594049 679.0000000000FFB000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000003.584392382.000000000100600 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://217.182.25.250/	regsvr32.exe, 00000007.00000002.89536634 8.0000000000FFB000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000003.594049679.0000000000FFB000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584392 382.0000000001006000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000003.584335315.000000000103500 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ctldl.windowsupda	regsvr32.exe, 00000007.00000003.59041024 3.0000000001093000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.895607470.0000000001094000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.590332 405.0000000001070000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000017.00000003.588806879 .0000022230180000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.585558704.000002223019E000.00 000004.00000020.00020000.00000000.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
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
103.43.46.182	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
151.106.112.196	unknown	Germany		61157	PLUSSERVER-ASN1DE	true
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
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
206.188.212.92	unknown	United States		55002	DEFENSE-NETUS	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
51.91.7.5	unknown	France		16276	OVHFR	true
209.126.98.206	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
189.232.46.161	unknown	Mexico		8151	UninetSAdeCVMX	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
209.250.246.206	unknown	European Union		20473	AS-CHOOPAUS	true
1.234.21.73	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
82.165.152.127	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
176.56.128.118	unknown	Switzerland		12637	SEEWEBWebhostingcolocationandcloudservicesIT	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
134.122.66.193	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.99.115.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
51.91.76.89	unknown	France		16276	OVHFR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
176.104.106.96	unknown	Serbia		198371	NINETRS	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
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
189.126.111.200	unknown	Brazil		27715	LocawebServicosdeInternetSABR	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
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
146.59.226.45	unknown	Norway		16276	OVHFR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
196.218.30.83	unknown	Egypt		8452	TE-ASTE-ASEG	true
216.120.236.62	unknown	United States		23535	HOSTROCKETUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669371
Start date and time: 20/07/202201:05:11	2022-07-20 01:05:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uVPWqAOMKn (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@19/4@0/46
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 100% (good quality ratio 97.8%) • Quality average: 85.5% • Quality standard deviation: 23.4%
HCA Information:	• Successful, ratio: 95% • 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, conhost.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 8.238.85.126, 8.248.143.254, 67.26.73.254, 8.248.135.254, 8.248.113.254, 20.223.24.244, 8.248.137.254, 8.238.85.254, 8.248.145.254, 8.248.119.254, 8.241.126.121
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.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
01:06:26	API Interceptor	10x 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 user DataBase, version 0x620, checksum 0xe72d5b73, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507321018796131
Encrypted:	false
SSDEEP:	384:M+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:TSB2nSB2RSjlK/+mLesOj1J2
MD5:	234DF96853E1AD63BB182A7E41363F39
SHA1:	5F6DC7CE6E82779213F6390A62B817A6E3A4B100
SHA-256:	F81635A39BA8C0EFCAE9FDFF5DAEE689578707CB89A7191E16F365089AAEFFD0
SHA-512:	F99E7513AE08D26D102FA2E947C09BBB7FE00A50B5E9F9D43E3C4D7675BA617F80DD14B79A918FE6D44E11B1C5D0FD303582DF27668E6DB20E8925B536E105D3
Malicious:	false
Preview:	.-[s... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... .....b.....z.<.....k..Y.....z..... .....

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

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

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

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1104327093135997
Encrypted:	false
SSDEEP:	6:kKAo+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:IoNkPlE99SNxAhUeE1
MD5:	BD3023E20A42F6208C626DC69044202A
SHA1:	850B694C0C693B50D651D34C16566E23AF7B3D0A
SHA-256:	2363EF260E13816160B4232B7919FE90FA5EC7265AA07ED363CC412FCE4BF0C8
SHA-512:	565BC3B04ACBFB982E72AFADC9A814E5A88C89BB5B0C575B8671987B4841FB45B415B53C7502F41719177579D5AF9EDB4EF2E203FAE24CD5C70E363DA638578
Malicious:	false
Preview:	p..... .....?/u.....(..... ....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:	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):	6.86612988602313
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 95.51% • InstallShield setup (43055/19) 4.10% • Generic Win/DOS Executable (2004/3) 0.19% • DOS Executable Generic (2002/1) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	uVPWqAOMKn.dll
File size:	667648
MD5:	2e7cff2320794cef37a5a3ac700a11d1
SHA1:	47c3259798a247f00e22f9c2e8e5f6ee7a41ce98
SHA256:	cc257f8c204386f746f457e57c91ab2c93f1d44181fd161eb3a16844700fcd37
SHA512:	a434f5487e86c32d82b3bcf68726c69d92e943f656517c280a6d1a3a672a2f8235b35b63ca4c430b9f16c90316656cff3ba2029a1e00569f83de6633c1b6fe66
SSDEEP:	12288:JSycC8Tu2EEAeClIHRFa7UdUzrAKytI8X0oXYl2N17OP:JSDD7RDhH3dUfOtj0oXYl+OP
TLSH:	69E49E1177D0C072C2BF3630551AA3B566EABC708DB9860B6FD42A7E2E745829D3871F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w..@3.o.3.o.3.o..q..9.o..q..*.o.3.n.w.o.-...*.o.-.....o.-.....o.-...5.o.-...2.o.-...2.o.-...2.o.Rich3.o.....PE..L....!?b...

File Icon

Icon Hash:	00f2cada9a9a4089

Static PE Info

General

Entrypoint:	0x1003dd03
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x623F21F4 [Sat Mar 26 14:23:48 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	923a5ec702466ffd61b422bacc94c6f0

Entrypoint Preview

Instruction
mov edi, edi

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FEC14C1EB67h
call 00007FEC14C26296h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007FEC14C1EA51h
pop ecx
pop ebp
retn 000Ch
push 0000000Ch
push 1006A3C0h
call 00007FEC14C21163h
and dword ptr [ebp-1Ch], 00000000h
mov esi, dword ptr [ebp+08h]
cmp esi, dword ptr [10073C74h]
jnbe 00007FEC14C1EB84h
push 00000004h
call 00007FEC14C26473h
pop ecx
and dword ptr [ebp-04h], 00000000h
push esi
call 00007FEC14C26C7Ah
pop ecx
mov dword ptr [ebp-1Ch], eax
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FEC14C1EB6Eh
mov eax, dword ptr [ebp-1Ch]
call 00007FEC14C2116Fh
ret
push 00000004h
call 00007FEC14C2636Eh
pop ecx
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, dword ptr [ebp+08h]
cmp esi, FFFFFFE0h
ja 00007FEC14C1EC07h
push ebx
push edi
mov edi, dword ptr [100581DCh]
cmp dword ptr [1007353Ch], 00000000h
jne 00007FEC14C1EB7Ah
call 00007FEC14C270C0h
push 0000001Eh
call 00007FEC14C26F0Eh
push 000000FFh
call 00007FEC14C1F206h
pop ecx
pop ecx
mov eax, dword ptr [10073C84h]
cmp eax, 01h
jne 00007FEC14C1EB70h
test esi, esi

Instruction
je 00007FEC14C1EB66h
mov eax, esi
jmp 00007FEC14C1EB65h
xor eax, eax
inc eax
push eax
jmp 00007FEC14C1EB7Eh
cmp eax, 03h

Rich Headers

Programming Language:	• [C] VS2005 build 50727 • [IMP] VS2005 build 50727 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [EXP] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x6d140	0x77	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6aca4	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x75000	0x2a5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa0000	0x638c	.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	0x61d98	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x58000	0x73c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x6abf4	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	0x566c2	0x56800	False	0.5718083905346821	data	6.610517658980479	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x58000	0x151b7	0x15200	False	0.31743481878698226	data	4.865287630812387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6e000	0x6ddc	0x3200	False	0.287421875	data	4.483657430566281	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x75000	0x2a5ec	0x2a600	False	0.8242590800147492	data	7.556606721410915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa0000	0x99de	0x9a00	False	0.4030539772727273	data	5.073570859103221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0x76014	0x20800	data		
RT_CURSOR	0x96814	0x134	data		
RT_CURSOR	0x96948	0xb4	data		
RT_CURSOR	0x969fc	0x134	AmigaOS bitmap font		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x96b30	0x134	data		
RT_CURSOR	0x96c64	0x134	data		
RT_CURSOR	0x96d98	0x134	data		
RT_CURSOR	0x96ecc	0x134	data		
RT_CURSOR	0x97000	0x134	data		
RT_CURSOR	0x97134	0x134	data		
RT_CURSOR	0x97268	0x134	data		
RT_CURSOR	0x9739c	0x134	data		
RT_CURSOR	0x974d0	0x134	data		
RT_CURSOR	0x97604	0x134	AmigaOS bitmap font		
RT_CURSOR	0x97738	0x134	data		
RT_CURSOR	0x9786c	0x134	data		
RT_CURSOR	0x979a0	0x134	data		
RT_BITMAP	0x97ad4	0x4a0	data		
RT_BITMAP	0x97f74	0xb8	data		
RT_BITMAP	0x9802c	0x144	data		
RT_ICON	0x98170	0x10a8	data		
RT_ICON	0x99218	0x10a8	data		
RT_ICON	0x9a2c0	0x10a8	data		
RT_MENU	0x9b368	0x220	data		
RT_DIALOG	0x9b588	0x10c	data		
RT_DIALOG	0x9b694	0x19e	data		
RT_DIALOG	0x9b834	0xfe	data		
RT_DIALOG	0x9b934	0x34	data		
RT_STRING	0x9b968	0x66	data		
RT_STRING	0x9b9d0	0x68	data		
RT_STRING	0x9ba38	0x38	data		
RT_STRING	0x9ba70	0xda	data		
RT_STRING	0x9bb4c	0x280	data		
RT_STRING	0x9bdcc	0x39c	data		
RT_STRING	0x9c168	0x7a	data		
RT_STRING	0x9c1e4	0x12e	data		
RT_STRING	0x9c314	0x104	data		
RT_STRING	0x9c418	0x46	data		
RT_STRING	0x9c460	0x128	data		
RT_STRING	0x9c588	0x188	data		
RT_STRING	0x9c710	0x240	data		
RT_STRING	0x9c950	0x9e	data		
RT_STRING	0x9c9f0	0xb0	Hitachi SH big-endian COFF object file, not stripped, 16640 sections, symbol offset=0x69007200, 201344768 symbols, optional header size 29952		
RT_STRING	0x9caa0	0x30	data		
RT_STRING	0x9cad0	0x1e2	data		
RT_STRING	0x9ccb4	0x5be	data		
RT_STRING	0x9d274	0x2e4	data		
RT_STRING	0x9d558	0x366	data		
RT_STRING	0x9d8c0	0xa6	data		
RT_STRING	0x9d968	0xee	data		
RT_STRING	0x9da58	0x11e	data		
RT_STRING	0x9db78	0x4fe	data		
RT_STRING	0x9e078	0x270	data		
RT_STRING	0x9e2e8	0x2e	data		
RT_STRING	0x9e318	0x73a	data		
RT_STRING	0x9ea54	0x530	data		
RT_STRING	0x9ef84	0x2d2	data		
RT_STRING	0x9f258	0x4c	data		
RT_ACCELERATOR	0x9f2a4	0x50	data		
RT_GROUP_CURSOR	0x9f2f4	0x22	Lotus unknown worksheet or configuration, revision 0x2		

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x9f318	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f32c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f340	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f354	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f368	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f37c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f390	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f3a4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f3b8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f3cc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f3e0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f3f4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f408	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x9f41c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x9f430	0x14	data		
RT_GROUP_ICON	0x9f444	0x14	data		
RT_GROUP_ICON	0x9f458	0x14	data		
RT_MANIFEST	0x9f46c	0x15a	ASCII text, with CRLF line terminators	English	United States
None	0x9f5c8	0x22	data		

Imports

DLL	Import
KERNEL32.dll	RtlUnwind, Sleep, RaiseException, HeapReAlloc, HeapSize, VirtualProtect, VirtualAlloc, GetSystemInfo, VirtualQuery, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LCMapStringW, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, HeapFree, GetEnvironmentStringsW, HeapCreate, HeapDestroy, VirtualFree, QueryPerformanceCounter, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount, GetTimeZoneInformation, LCMapStringA, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, GetConsoleCP, GetConsoleMode, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, CreateFileA, SetEnvironmentVariableA, HeapAlloc, GetCommandLineA, GetTickCount, GetFileSizeEx, SystemTimeToFileTime, LocalFileTimeToFileTime, FileTimeToLocalFileTime, FileTimeToSystemTime, CreateFileW, GetShortPathNameW, GetVolumeInformationW, FindFirstFileW, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, lstrcmpiW, GetThreadLocale, GetStringTypeExW, DeleteFileW, MoveFileW, InterlockedIncrement, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, GetModuleHandleA, InterlockedDecrement, GetCurrentDirectoryW, GlobalGetAtomNameW, FormatMessageW, LocalFree, MulDiv, lstrcpyA, lstrcpyW, lstrlenA, GlobalReAlloc, GetDiskFreeSpaceW, GetFullPathNameW, GetTempFileNameW, GetFileTime, SetFileTime, GetFileAttributesW, GlobalFindAtomW, GetVersionExW, CompareStringW, LoadLibraryA, GetVersionExA, GlobalUnlock, CloseHandle, FreeResource, GlobalFree, GetPrivateProfileStringW, lstrlenW, WritePrivateProfileStringW, GetPrivateProfileIntW, GlobalAddAtomW, GetCurrentProcessId, GetLastError, SetLastError, GlobalDeleteAtom, GetCurrentThread, GetCurrentThreadId, ConvertDefaultLocale, EnumResourceLanguagesW, GetModuleFileNameW, lstrcmpA, GetLocaleInfoW, LoadLibraryW, WideCharToMultiByte, CompareStringA, MultiByteToWideChar, InterlockedExchange, GlobalLock, lstrcmpW, GlobalAlloc, FreeLibrary, GetModuleHandleW, GetProcAddress, ExitProcess, LockResource, SizeofResource, LoadResource, FreeEnvironmentStringsW, FindResourceW

DLL	Import
USER32.dll	SystemParametersInfoW, InvalidateRect, GetMenuStringW, AppendMenuW, InsertMenuW, ShowWindow, MoveWindow, SetWindowTextW, IsDialogMessageW, RegisterWindowMessageW, LoadIconW, SendDlgItemMessageW, SendDlgItemMessageA, WinHelpW, IsChild, GetCapture, GetClassLongW, GetClassNameW, SetPropW, GetPropW, RemovePropW, SetFocus, GetWindowTextLengthW, GetWindowTextW, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, ScrollWindow, TrackPopupMenu, SetMenu, SetScrollRange, GetScrollRange, SetScrollPos, IsRectEmpty, SetForegroundWindow, ShowScrollBar, GetClientRect, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreateWindowExW, GetClassInfoExW, GetClassInfoW, RegisterClassW, GetSysColor, AdjustWindowRectEx, ScreenToClient, SetParent, DeferWindowPos, GetScrollInfo, SetScrollInfo, CopyRect, PtInRect, GetDlgCtrlID, DefWindowProcW, CallWindowProcW, GetMenu, SetWindowLongW, OffsetRect, IntersectRect, SystemParametersInfoA, IsIconic, EnableWindow, UpdateWindow, PostQuitMessage, PostMessageW, GetWindowPlacement, GetWindowRect, GetSystemMetrics, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamW, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, SetWindowsHookExW, CallNextHookEx, GetMessageW, TranslateMessage, FillRect, SetWindowRgn, ClientToScreen, SetTimer, KillTimer, SetCapture, LoadCursorW, ReleaseCapture, SetRectEmpty, DeleteMenu, GetScrollPos, GetSystemMenu, CheckMenuItem, EnableMenuItem, GetMenuState, ModifyMenuW, SendMessageW, GetParent, GetFocus, LoadBitmapW, GetMenuCheckMarkDimensions, SetMenuItemBitmaps, SetCursor, ShowOwnedPopups, MessageBoxW, IsWindowEnabled, GetLastActivePopup, GetWindowLongW, GetWindowThreadProcessId, SetWindowPos, MapDialogRect, SetWindowContextHelpId, GetWindow, ValidateRect, GetCursorPos, PeekMessageW, GetKeyState, IsWindowVisible, GetActiveWindow, DispatchMessageW, IsZoomed, ReleaseDC, GetDC, TranslateAcceleratorW, BringWindowToTop, PostThreadMessageW, RegisterClipboardFormatW, LockWindowUpdate, GetDCEx, WindowFromPoint, GetMenuItemInfoW, InflateRect, MessageBeep, GetNextDlgGroupItem, InvalidateRgn, SetRect, CopyAcceleratorTableW, CharNextW, CharUpperW, DestroyIcon, GetSysColorBrush, EndPaint, BeginPaint, GetWindowDC, GrayStringW, DrawTextExW, DrawTextW, TabbedTextOutW, UnpackDDElParam, ReuseDDElParam, LoadMenuW, DestroyMenu, LoadAcceleratorsW, InsertMenuItemW, EqualRect, CreatePopupMenu, DrawIcon
GDI32.dll	BitBlt, GetPixel, PtVisible, RectVisible, TextOutW, ExtTextOutW, Escape, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowExtEx, ScaleWindowExtEx, GetWindowExtEx, CreatePatternBrush, GetStockObject, CreateSolidBrush, GetBkColor, GetTextColor, CreateRectRgnIndirect, GetRgnBox, CreateFontIndirectW, PatBlt, SetRectRgn, CombineRgn, GetMapMode, GetViewportExtEx, CreateRectRgn, SelectClipRgn, IntersectClipRect, ExtSelectClipRgn, CreateBitmap, SetMapMode, SetBkMode, RestoreDC, SaveDC, CreateCompatibleBitmap, CreateCompatibleDC, StretchDIBits, DeleteDC, CreateFontW, GetCharWidthW, DeleteObject, GetTextExtentPoint32W, GetTextMetricsW, SelectObject, Ellipse, LPtoDP, CreateEllipticRgn, GetDeviceCaps, GetObjectW, SetBkColor, SetTextColor, GetClipBox, ExcludeClipRect
COMDLG32.dll	GetFileTitleW
WINSPOOL.DRV	DocumentPropertiesW, ClosePrinter, OpenPrinterW
ADVAPI32.dll	RegSetValueW, GetFileSecurityW, SetFileSecurityW, RegDeleteValueW, RegSetValueExW, RegCreateKeyExW, RegQueryValueW, RegOpenKeyW, RegEnumKeyW, RegDeleteKeyW, RegOpenKeyExW, RegQueryValueExW, RegCloseKey, RegCreateKeyW
SHELL32.dll	DragFinish, ExtractIconW, SHGetFileInfoW, DragQueryFileW
SHLWAPI.dll	PathFindFileNameW, PathStripToRootW, PathIsUNCW, PathFindExtensionW, PathRemoveFileSpecW
oledlg.dll	OleUIBusyW
ole32.dll	CoRevokeClassObject, OleInitialize, CoFreeUnusedLibraries, OleUninitialize, CoInitializeEx, CoUninitialize, CoCreateInstance, CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, OleIsCurrentClipboard, CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, CLSIDFromProgID, OleFlushClipboard, CoRegisterMessageFilter, CoGetClassObject
OLEAUT32.dll	VariantCopy, SysAllocString, SafeArrayDestroy, OleCreateFontIndirect, SystemTimeToVariantTime, VariantTimeToSystemTime, SysStringLen, VariantInit, VariantChangeType, VariantClear, SysAllocStringLen, SysFreeString
ODBC32.dll	

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x100059a6
DllUnregisterServerrrrrrrrrr	2	0x100059c1

Possible Origin

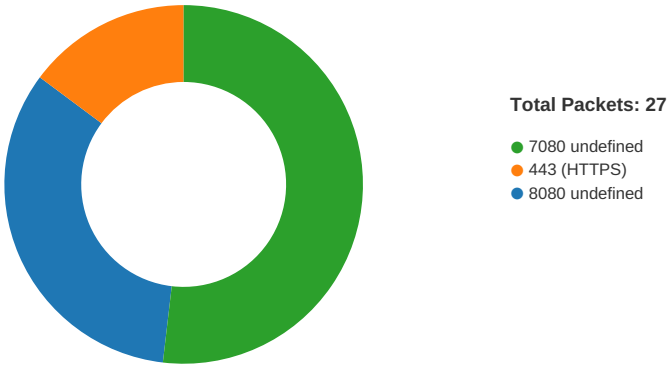
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6119.193.124.4 14983970802404304 07/20/22-01:08:05.169546	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49839	7080	192.168.2.6	119.193.124.41
192.168.2.651.91.76.89 49829802404338 07/20/22-01:08:02.804632	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49829	8080	192.168.2.6	51.91.76.89

Network Port Distribution



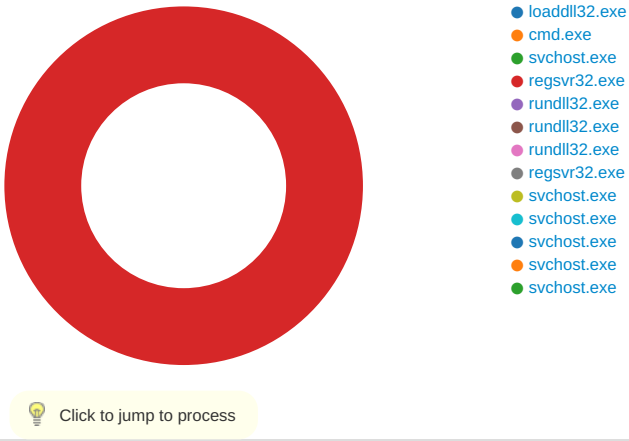
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:07:08.966242075 CEST	49778	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:07:11.958714962 CEST	49778	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:07:18.037332058 CEST	49778	8080	192.168.2.6	216.120.236.62
Jul 20, 2022 01:07:30.051042080 CEST	49791	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:07:30.051096916 CEST	443	49791	189.232.46.161	192.168.2.6
Jul 20, 2022 01:07:30.051228046 CEST	49791	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:07:30.083218098 CEST	49791	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:07:30.083266020 CEST	443	49791	189.232.46.161	192.168.2.6
Jul 20, 2022 01:08:02.734313011 CEST	49791	443	192.168.2.6	189.232.46.161
Jul 20, 2022 01:08:02.804631948 CEST	49829	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:08:02.824671984 CEST	8080	49829	51.91.76.89	192.168.2.6
Jul 20, 2022 01:08:03.451442957 CEST	49829	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:08:03.474623919 CEST	8080	49829	51.91.76.89	192.168.2.6
Jul 20, 2022 01:08:03.982745886 CEST	49829	8080	192.168.2.6	51.91.76.89
Jul 20, 2022 01:08:04.002677917 CEST	8080	49829	51.91.76.89	192.168.2.6
Jul 20, 2022 01:08:04.011221886 CEST	49837	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:08:04.039258957 CEST	8080	49837	217.182.25.250	192.168.2.6
Jul 20, 2022 01:08:04.545238018 CEST	49837	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:08:04.573170900 CEST	8080	49837	217.182.25.250	192.168.2.6
Jul 20, 2022 01:08:05.076992035 CEST	49837	8080	192.168.2.6	217.182.25.250
Jul 20, 2022 01:08:05.104994059 CEST	8080	49837	217.182.25.250	192.168.2.6
Jul 20, 2022 01:08:05.169545889 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:05.428386927 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:05.428514957 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:05.429109097 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:05.687645912 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:05.702069044 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:05.702131033 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:05.702181101 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:05.702214003 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:08.176017046 CEST	49839	7080	192.168.2.6	119.193.124.41

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:08:08.436299086 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:08.436445951 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:08.441541910 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:08.743889093 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:09.619560003 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:09.621532917 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:12.618496895 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:12.618542910 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:12.618627071 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:12.620954037 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:58.926661968 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:58.926764965 CEST	49839	7080	192.168.2.6	119.193.124.41
Jul 20, 2022 01:08:59.187184095 CEST	7080	49839	119.193.124.41	192.168.2.6
Jul 20, 2022 01:08:59.187335014 CEST	49839	7080	192.168.2.6	119.193.124.41

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6864**, Parent PID: **5076**

General

Target ID:	0
Start time:	01:06:25
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\uVPWqAOMKn.dll"
Imagebase:	0x10c0000
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: 00000000.00000002.418860992.0000000000520000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.418860992.0000000000520000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.418887391.0000000000551000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.418887391.0000000000551000.00000020.00001000.00020000.00000000.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: **6872**, Parent PID: **6864**

General

Target ID:	1
Start time:	01:06:25
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\uVPWqAOMKn.dll",#1
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6880**, Parent PID: **588**

General

Target ID:	2
Start time:	01:06:25
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:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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: regsvr32.exe PID: **6892**, Parent PID: **6864**

General

Target ID:	3
Start time:	01:06:26
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\uVPWqAOMKn.dll
Imagebase:	0x11b0000
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: 00000003.00000002.398365713.0000000004BE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.398365713.0000000004BE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.398389005.0000000004C11000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.398389005.0000000004C11000.00000020.00001000.00020000.00000000.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\Elutq\fjqpvuhrz.fqb:Zone.Identifier	success or wait	1	4C2594F	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: **6900**, Parent PID: **6872**

General

Target ID:	4
Start time:	01:06:26
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\uVPWqAOMKn.dll",#1
Imagebase:	0x110000
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: 00000004.00000002.396892983.0000000004AA1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.396892983.0000000004AA1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.396801505.0000000003390000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.396801505.0000000003390000.00000040.00001000.00020000.00000000.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: **6920**, Parent PID: **6864**

General

Target ID:	5
Start time:	01:06:26
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\uVPWqAOMKn.dll,DllRegisterServer
Imagebase:	0x110000
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: 00000005.00000002.404579825.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.404579825.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.410822400.0000000003011000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.410822400.0000000003011000.00000020.00001000.00020000.00000000.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: **7024**, Parent PID: **6864**

General

Target ID:	6
Start time:	01:06:31
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\uVPWqAOMKn.dll,DllUnregisterServerrrrrrrrrrr

Imagebase:	0x110000
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: 00000006.00000002.417225831.0000000004171000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.417225831.0000000004171000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.417170755.0000000004140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.417170755.0000000004140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: regsvr32.exe PID: **7100**, Parent PID: **6892**

General

Target ID:	7
Start time:	01:06:36
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\Elutq\fjqpvuhrz.fqb"
Imagebase:	0x11b0000
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: 00000007.00000002.895080994.0000000000E90000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.895080994.0000000000E90000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.895666203.00000000010E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.895666203.00000000010E1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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: **596**, Parent PID: **588**

General

Target ID:	13
Start time:	01:07:02
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4464**, Parent PID: **588**

General	
Target ID:	14
Start time:	01:07:03
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:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5100**, Parent PID: **588**

General	
Target ID:	16
Start time:	01:07:12
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **2060**, Parent PID: **588**

General	
Target ID:	19
Start time:	01:07:33
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

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

File Activities							
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.							
File Path	**Access**	**Attributes**	**Options**	**Completion**	**Count**	**Source Address**	**Symbol**

Analysis Process: svchost.exe PID: **5116**, Parent PID: **588**

General	
Target ID:	23
Start time:	01:07:48
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff726010000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities							
There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.							
File Path	**Access**	**Attributes**	**Options**	**Completion**	**Count**	**Source Address**	**Symbol**

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly