ID: 669368
Sample Name: CUfsVUDkr6
Cookbook: default.jbs
Time: 01:04:09
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

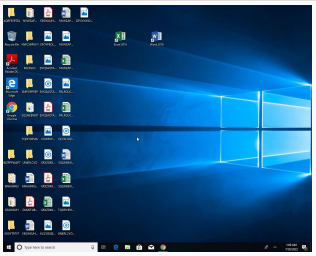
Windows Analysis Report

CUfsVUDkr6

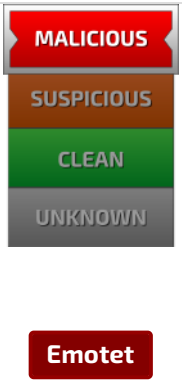
Overview

General Information

Sample Name:	CUfsVUDkr6 (renamed file extension from none to dll)
Analysis ID:	669368
MD5:	543b633663f404..
SHA1:	0d7e681d49a1ed.
SHA256:	aa0bfc40ca7a27…
Tags:	32 dll exe trojan
Infos:	



Detection



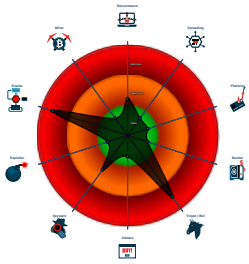
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- System process connects to networ…
- Snort IDS alert for network traffic
- Query firmware table information (lik…
- Changes security center settings (n…
- 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: 6380 cmdline: loaddll32.exe "C:\Users\user\Desktop\CUfsVUDkr6.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6388 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\CUfsVUDkr6.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6408 cmdline: rundll32.exe "C:\Users\user\Desktop\CUfsVUDkr6.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6400 cmdline: regsvr32.exe /s C:\Users\user\Desktop\CUfsVUDkr6.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Ofpagmb\vfvyklscua.sam" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 6420 cmdline: rundll32.exe C:\Users\user\Desktop\CUfsVUDkr6.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6588 cmdline: rundll32.exe C:\Users\user\Desktop\CUfsVUDkr6.dll,DllUnregisterServerr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6936 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6972 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7040 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7068 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7120 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 2492 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6248 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5568 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6484 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6388 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5000 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2932 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4432 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "160.135.187.2:6",
    "48.126.193.2:1",
    "224.130.193.2:1",
    "128.130.193.2:1",
    "136.206.195.2:153",
    "128.154.195.2:130",
    "176.130.193.2:1",
    "128.127.193.2:1",
    "8.109.194.2:2",
    "120.8.0.0:1",
    "56.8.0.0:1",
    "176.7.0.0:1",
    "172.7.0.0:1",
    "96.7.0.0:1",
    "200.7.0.0:1",
    "156.7.0.0:1",
    "240.7.0.0:1",
    "124.7.0.0:1",
    "140.7.0.0:1",
    "144.7.0.0:1",
    "60.7.0.0:1",
    "128.7.0.0:1",
    "224.7.0.0:1",
    "160.7.0.0:1",
    "228.7.0.0:1",
    "244.7.0.0:1",
    "4.8.0.0:1",
    "8.8.0.0:1",
    "72.7.0.0:1",
    "76.7.0.0:1",
    "44.7.0.0:1"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.774599292.00000000046C1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.774599292.00000000046C1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.261732368.0000000004760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000002.261732368.0000000004760000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.258847425.0000000003390000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.4ce0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4ce0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.4690000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.4690000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.940000.0.raw.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: 192.168.2.3 - Destination IP: 119.193.124.41

Timestamp:	192.168.2.3119.193.124.414976570802404304 07/20/22-01:06:02.271940
SID:	2404304
Source Port:	49765
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.3 - Destination IP: 51.91.76.89

Timestamp:	192.168.2.351.91.76.894976380802404338 07/20/22-01:06:00.016852
SID:	2404338
Source Port:	49763
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

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)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion

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

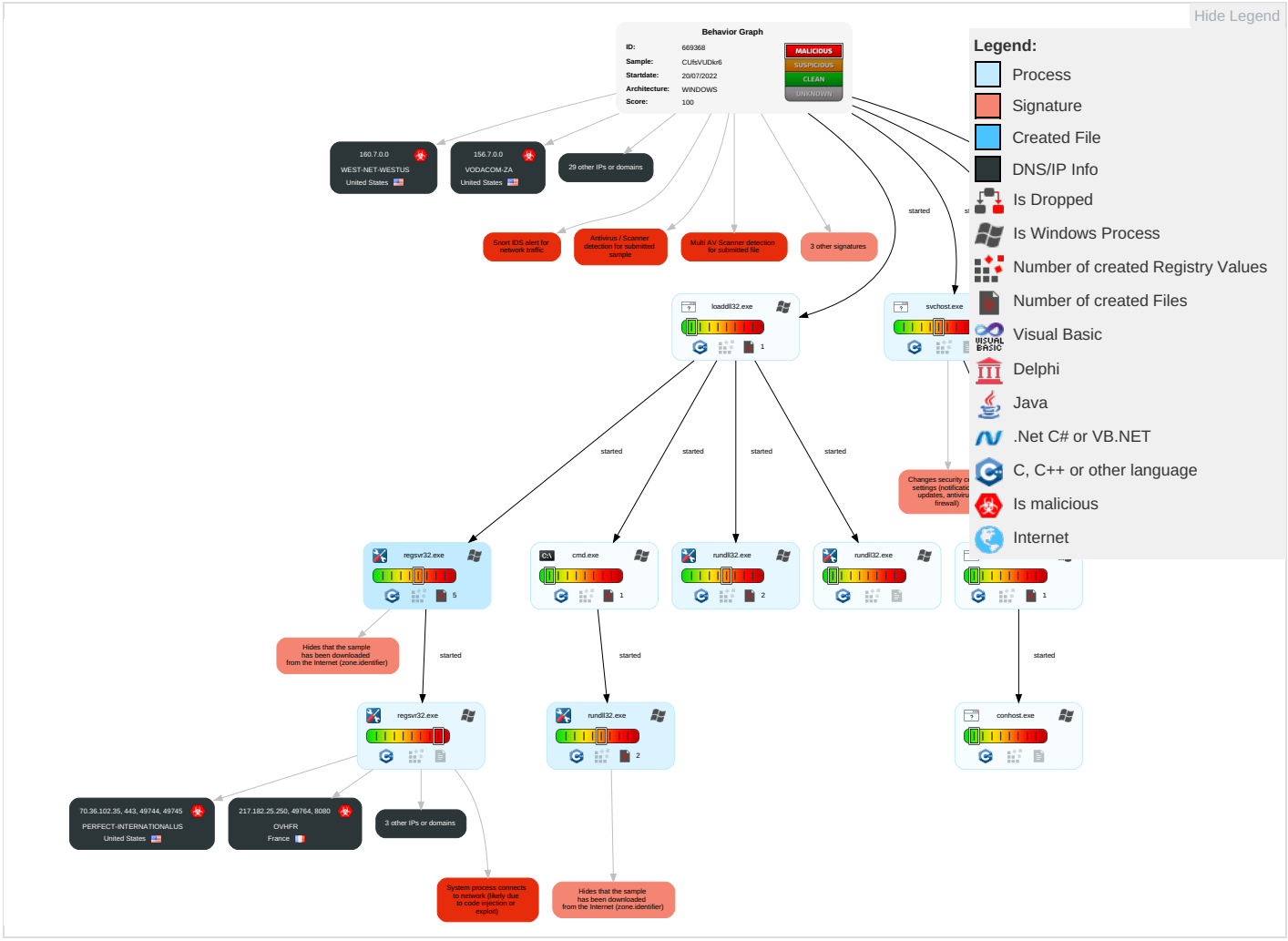
Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	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)	2 Obfuscated Files or Information	Security Account Manager	3 6 System Information Discovery	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 DLL Side-Loading	NTDS	1 5 1 Security Software 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 File Deletion	LSA Secrets	1 3 Virtualization/Sandbox Evasion	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 Masquerading	Cached Domain Credentials	1 Process 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 3 Virtualization/Sandbox Evasion	DCSync	1 Application Window 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 1 1 Process Injection	Proc Filesystem	1 Remote System 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 Hidden Files and Directories	/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 Regsvr32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

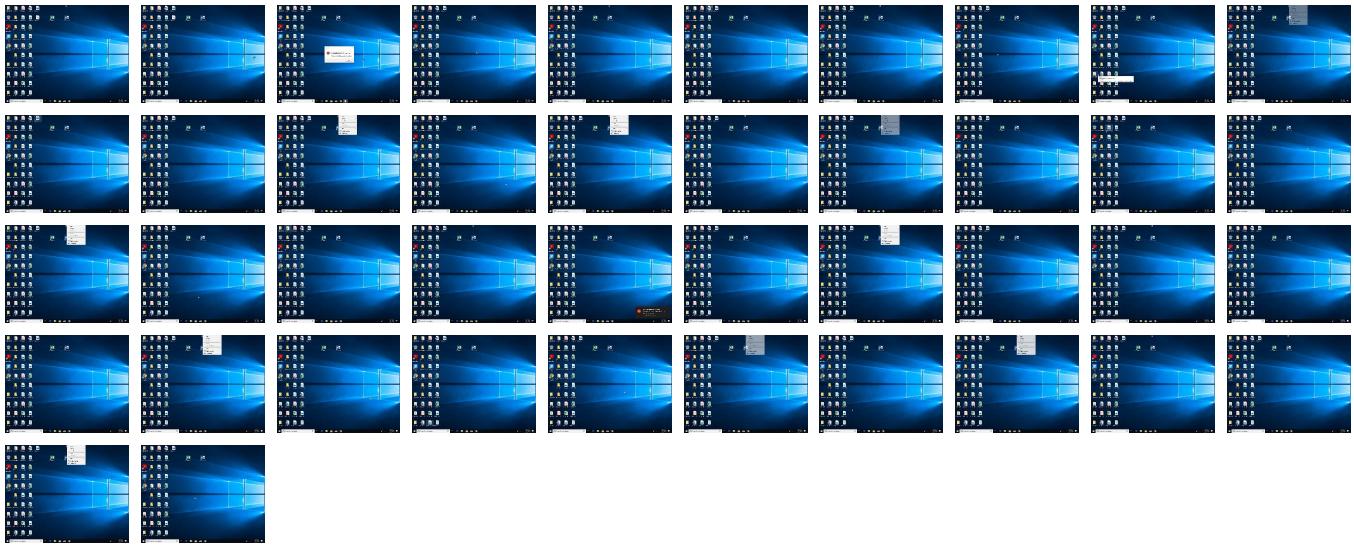
Behavior Graph



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
CUfsVUDkr6.dll	67%	Virustotal		Browse
CUfsVUDkr6.dll	100%	Avira	TR/AD.Nekark.bnwrm	
CUfsVUDkr6.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4ce0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.43a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4760000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.4690000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.3390000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.940000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.46c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4790000.1.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://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

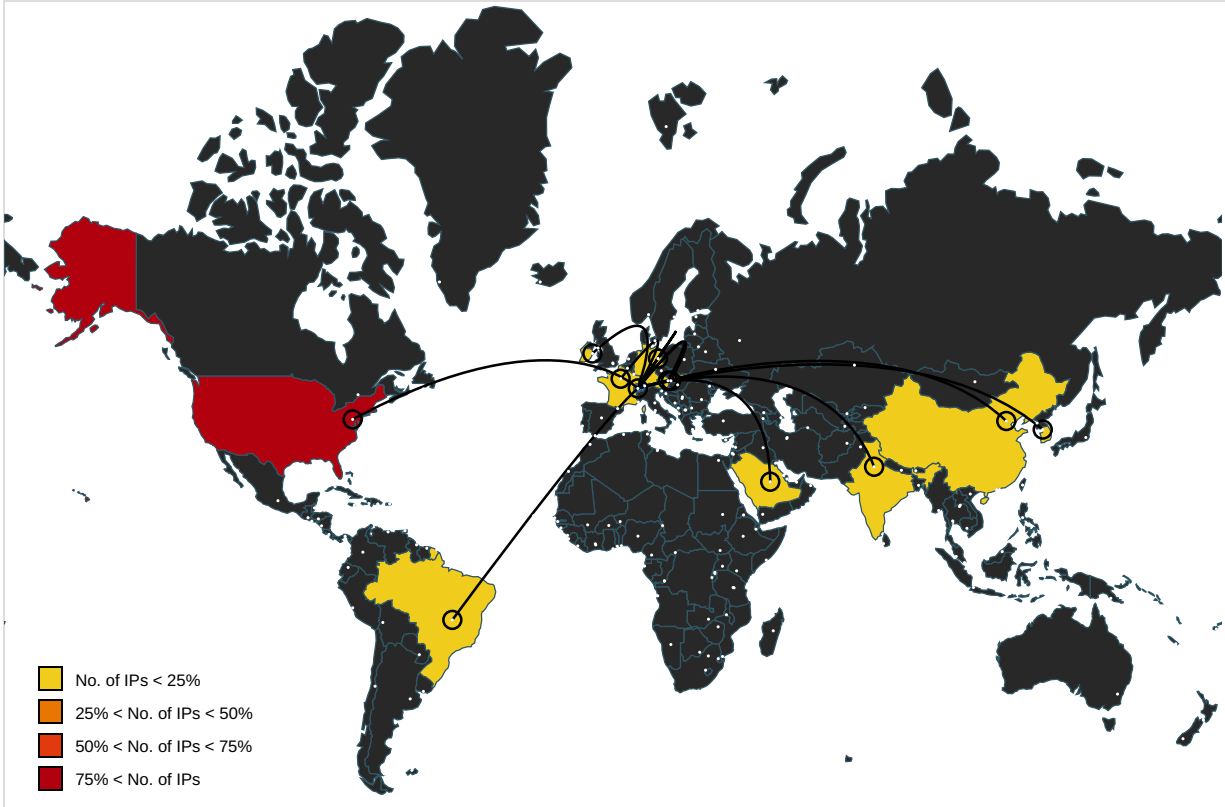
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000016.00000003.394883729.0000023CC03AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.394786236.0000023CC038D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000003.318472678.000002516B456000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000E.00000002.318770388.000002516B43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000E.00000002.318770388.000002516B43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000E.00000002.318836178.000002516B45C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000E.00000002.318818550.000002516B44D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318337851.000002516B449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000E.00000002.318770388.000002516B43D000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000013.00000002.676785569.000002799FC89000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000002.419799470.0000023CBFAE8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.318836178.000002516B45C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000016.00000003.398796153.0000023CC038D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.398927241.0000023CC0818000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000002.318770388.000002516B43D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.318685600.000002516B413000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000E.00000002.318795830.000002516B442000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318477372.000002516B441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000B.00000002.774092172.00000175ABA44000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000E.00000002.318818550.000002516B44D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318337851.000002516B449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000016.00000003.389730375.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389593585.0000023CC03AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389883804.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389629399.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389660788.0000023CC03B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389642184.0000023CC039A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389783418.0000023CC0802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389683950.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000016.00000003.394883729.0000023CC03AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.394786236.0000023CC038D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000002.318836178.000002516B45C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000E.00000002.318795830.000002516B442000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318450731.000002516B440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318477372.000002516B441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/enumeration	svchost.exe, 00000013.00000002.676470792.000002799A4B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.675741527.000002799A4AC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000016.00000003.389730375.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389593585.0000023CC03AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389883804.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389629399.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389660788.0000023CC03B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389642184.0000023CC039A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389783418.0000023CC0802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389683950.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000016.00000003.389730375.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389593585.0000023CC03AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389883804.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389629399.0000023CC0389000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389660788.0000023CC03B6000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389642184.0000023CC039A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389783418.0000023CC0802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.389683950.0000023CC081A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000016.00000003.394883729.0000023CC03AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.394786236.0000023CC038D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000E.00000003.296644835.000002516B432000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.318720352.000002516B43B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/enumera	svchost.exe, 00000013.00000002.676470792.000002799A4B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.675741527.000002799A4AC000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000002.318836178.000002516B45C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000B.00000002.774092172.00000175ABA44000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000E.00000002.318685600.000002516B413000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000E.00000003.318375087.000002516B461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000016.00000003.394883729.0000023CC03AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000016.00000003.394786236.0000023CC038D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000002.318770388.000002516B43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000B.00000002.774092172.00000175ABA44000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000002.318836178.000002516B45C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000003.318434954.000002516B45A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.182.25.250	unknown	France		16276	OVHFR	true
8.8.0.0	unknown	United States		3356	LEVEL3US	true
60.7.0.0	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
70.36.102.35	unknown	United States		22439	PERFECT-INTERNATIONALUS	true
244.7.0.0	unknown	Reserved		unknown	unknown	true
144.7.0.0	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	true
128.7.0.0	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	true
176.130.193.2	unknown	France		5410	BOUYGTEL-ISPFR	true
44.7.0.0	unknown	United States		7377	UCSDUS	true
48.126.193.2	unknown	United States		2686	ATGS-MMD-ASUS	true
128.130.193.2	unknown	Austria		679	TUNET-ASTechnischeUniversitaetWienAT	true
172.7.0.0	unknown	United States		7018	ATT-INTERNET4US	true
228.7.0.0	unknown	Reserved		unknown	unknown	true
120.8.0.0	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
160.135.187.2	unknown	United States		747	DNIC-AS-00747US	true
240.7.0.0	unknown	Reserved		unknown	unknown	true
136.206.195.2	unknown	Ireland		1213	HEANETIE	true
72.7.0.0	unknown	United States		10507	SPCSUS	true
76.7.0.0	unknown	United States		22186	CENTURYLINK-LEGACY-EMBARQ-KSGRNRUS	true
200.7.0.0	unknown	Brazil		262657	DENDENAECIALTDAMEBR	true
96.7.0.0	unknown	United States		262589	INTERNEXABRASILOPERADORADETELECOMUNICACOESSABR	true
140.7.0.0	unknown	United States		668	DNIC-AS-00668US	true
160.7.0.0	unknown	United States		210	WEST-NET-WESTUS	true
224.130.193.2	unknown	Reserved		unknown	unknown	true
51.91.76.89	unknown	France		16276	OVHFR	true
4.8.0.0	unknown	United States		3356	LEVEL3US	true
124.7.0.0	unknown	India		4662	QTCN-ASN1GCNetReachRangeIncTW	true
128.127.193.2	unknown	Saudi Arabia		35753	ITCITCASnumberSA	true
56.8.0.0	unknown	United States		2686	ATGS-MMD-ASUS	true
176.7.0.0	unknown	Germany		12638	AS12638DuesseldorfDE	true
224.7.0.0	unknown	Reserved		unknown	unknown	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
128.154.195.2	unknown	United States		1749	AS1749US	true
8.109.194.2	unknown	United States		3356	LEVEL3US	true
156.7.0.0	unknown	United States		29975	VODACOM-ZA	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:	669368
Start date and time: 20/07/202201:04:09	2022-07-20 01:04:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CUfsVUDkr6 (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:	37
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@28/8@0/38
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 97.1%) • Quality average: 84.2% • Quality standard deviation: 23.9%
HCA Information:	• Successful, ratio: 88% • 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): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.211.4.86, 8.248.141.254, 8.248.115.254, 8.248.119.254, 8.248.133.254, 8.238.190.126, 8.248.137.254, 8.238.85.254, 8.248.145.254, 8.241.126.121, 20.223.24.244, 51.104.136.2, 23.205.181.161, 20.106.86.13
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, settings-prod-neu-2.northeurope.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.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, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, settings-prod-wus3-1.westus3.cloudapp.azure.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wu-bg-shim.trafficmanager.net, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.c
- 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
01:05:49	API Interceptor	12x Sleep call for process: svchost.exe modified
01:06:38	API Interceptor	1x Sleep call for process: MpCmdRun.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):	0.24943054221035757
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU42:BJiRdwfu2SRU42
MD5:	EAC6CBA78E26DFB7BB61D6EEA9CD9233
SHA1:	32F8575376F52BC02295E41ECC840AF23A6110AD
SHA-256:	6DE704A99F57D3EF3B912AC3969EDAAABDA5CB828E15F3953DBE9390A0FFD98C
SHA-512:	BA090C9488B99D4B7CC159568B2862277D0A1E50FBB857C7584E9D4C931A8197AF0B8B146EABD5CC98AE1F86D395CAF01665FD964C54C86D9A926807694F42D 8
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 0x9088c28c, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25053946589103243
Encrypted:	false
SSDEEP:	384:BDy+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:BD9SB2nSB2RSjlK/+mLesOj1J2
MD5:	6289483600CFDE69B20838D09C48B5F6
SHA1:	3A1484848D4669A3A6B3A524E2B26FCF8B154AF8
SHA-256:	AE7B6C8427542E8BEFB894172B502EC0B1B446BC520843620DB263F3AFBE0BD6
SHA-512:	1A459B02A4751B90ADE40B8DDFD9D7605B4B3D1F4D569192208F12EA4BF26D754E6954AB19F9A4FF03F2B7F5EE2086DDAFA3477EB16C5731BDDA2E688C162C09
Malicious:	false
Preview:	....e.f.3...w.....)).....z..1....z..h.(.....z....).....3...w.....B.....@..... ....l.....z.....t.7.....z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07354863233533379
Encrypted:	false
SSDEEP:	3:td51J7vUDmZGltnWsgT96tySpDiWltall3Vkttlmlnl:v51JrUhgT96o+if3
MD5:	8A1EBFE5A1B1B2F1273C515D06A3C081
SHA1:	70D374D33D986AC3BDEDCA0334CF3DFF39E48914
SHA-256:	FE34E8493F143527E8A5CD57302ACC65BDA112B4DDFD867B5DB77C1A471589DB
SHA-512:	ECA314A85B38017D105C7F997D8E58854B2D9DD80C3DC45A627229E718B2B201303FB8BA574868C10642B28BD93FF079ED321C7E9379B8F16121FC202FC962D
Malicious:	false
Preview:	..x.....3...w..1....z.....z.....z.....z....e.;....z.s.....t.7.....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):	3.1274410188478514
Encrypted:	false
SSDEEP:	6:kKF5a/o+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:dgoNkPlE99SNxAhUeE1
MD5:	9DA7953ED0490CCBFA7B4560EFF84FCF
SHA1:	7C9A7A557B675E9011E0A0D0D099A45C1D96B512
SHA-256:	22D98BC937AF79203A67FFD25E89D49F8B5CC38233047B06E24B7B106EB25E17
SHA-512:	3F4E6BFC7179FB9AC5755ECF7BA0FFFA2A49735829FA3492010B525A9B4C1CE23F6AA80247B2CFE09A8CDE2A0AC46B3C42F4227D5FC6F5025D3BFAB89AEED3EB
Malicious:	false
Preview:	p...... ....:.Z.....(.. ....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"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.162757930159871
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zj+o:j+s+v+b+P+m+0+Q+q+E+o
MD5:	B5308DCD26005B3450D279ED7FE2D820
SHA1:	394535BBEA1AA950BAEAC1C41F75BD2FD2DBE084
SHA-256:	FA6B1DF7E415AB95C4203AD01BACE2F0F1E2B698E65B501EE66526F94EBE3BE2
SHA-512:	233FED21AF981199BEB6FE0A3994229ACE6CF7C5436506CBD40D363BC7E39A28FCD6AD0F65A213CC303A5F3E7BC738048A87F14E412FB2650E7869F9F21BEDDD
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.35282778020667

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:	CUfsVUDkr6.dll
File size:	655360
MD5:	543b633663f40468263782155c1e4cdc
SHA1:	0d7e681d49a1ed2a1539845925eac533c1d0dc7c
SHA256:	aa0bfc40ca7a27bbc6491ba35ee5ac38eb5fbdf2a2d8a4ef9332d340c391ca87
SHA512:	40131975bd3baf17e921efd58bc5230e488b7444ee73b3c0ed6f7a3049811a4b011499f98df01b46281f97600331645070912beb6df16f48431e772fb33d3e36
SSDEEP:	6144:/6ZMFXzqfoSHr/mvcQYbi2HN8C8BgifO7y7QcuVqrWLWN7Ypsi6Ih9vH0/oUHahE:/8MFX47ivcQMNsrDRKJjO69cI
TLSH:	27D47C0EFFD1C1B2D36B123019D5C64823ADBF2CEAA1C5B777A8BE1D69326C14512B16
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 00007F306CBA2691h
xor eax, eax
inc eax
mov dword ptr [ebp-1Ch], eax
mov esi, dword ptr [ebp+0Ch]
xor edi, edi
cmp esi, edi
jne 00007F306CBA14AEh
cmp dword ptr [1004F3C8h], edi
je 00007F306CBA1559h
mov dword ptr [ebp-04h], edi
cmp esi, eax
je 00007F306CBA14A7h
cmp esi, 02h

Instruction
jne 00007F306CBA14D3h
mov eax, dword ptr [10050CB4h]
cmp eax, edi
je 00007F306CBA14AEh
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 00007F306CBA152Bh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007F306CBA12C7h
mov dword ptr [ebp-1Ch], eax
cmp eax, edi
je 00007F306CBA1514h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007F306CB96238h
mov dword ptr [ebp-1Ch], eax
cmp esi, 01h
jne 00007F306CBA14B0h
cmp eax, edi
jne 00007F306CBA14ACh
push ebx
push edi
push dword ptr [ebp+08h]
call 00007F306CBA129Dh
cmp esi, edi
je 00007F306CBA14A7h
cmp esi, 03h
jne 00007F306CBA14CBh
push ebx
push esi
push dword ptr [ebp+08h]
call 00007F306CBA128Ah
test eax, eax
jne 00007F306CBA14A5h
mov dword ptr [ebp-1Ch], edi
cmp dword ptr [ebp-1Ch], edi
je 00007F306CBA14B5h
mov eax, dword ptr [10050CB4h]
cmp eax, edi
je 00007F306CBA14ACh
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 00007F306CBA14BCh
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	0.32216796875	data	5.0465288460575035	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
.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		

Name	RVA	Size	Type	Language	Country
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		
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		

Name	RVA	Size	Type	Language	Country
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
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

DLL	Import
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

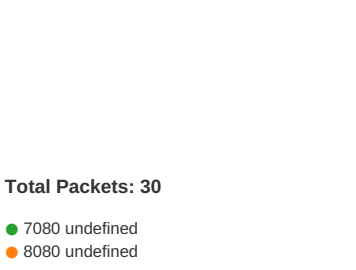
Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

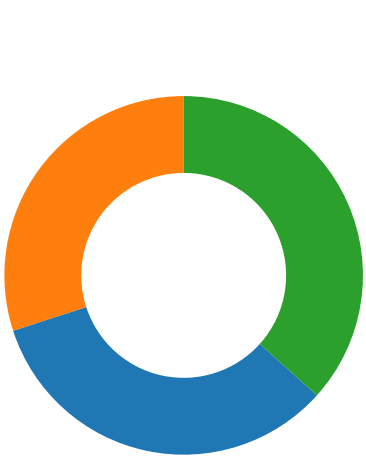
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3119.193.124.4 14976570802404304 07/20/22-01:06:02.271940	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49765	7080	192.168.2.3	119.193.124.41
192.168.2.351.91.76.8949 76380802404338 07/20/22-01:06:00.016852	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49763	8080	192.168.2.3	51.91.76.89

Network Port Distribution





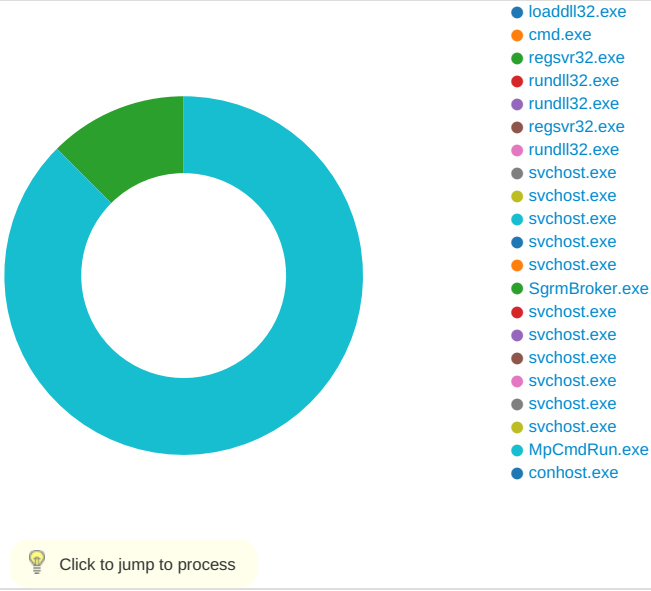
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:05:38.382345915 CEST	49744	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.382380962 CEST	443	49744	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.382472038 CEST	49744	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.401314020 CEST	49744	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.401331902 CEST	443	49744	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.574548006 CEST	443	49744	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.578385115 CEST	49745	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.578444004 CEST	443	49745	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.578576088 CEST	49745	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.579086065 CEST	49745	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.579119921 CEST	443	49745	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.752664089 CEST	443	49745	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.761722088 CEST	49746	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.761790991 CEST	443	49746	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.761930943 CEST	49746	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.762278080 CEST	49746	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.762346983 CEST	443	49746	70.36.102.35	192.168.2.3
Jul 20, 2022 01:05:38.762423992 CEST	49746	443	192.168.2.3	70.36.102.35
Jul 20, 2022 01:05:38.814444065 CEST	49747	8080	192.168.2.3	92.240.254.110
Jul 20, 2022 01:05:41.920202971 CEST	49747	8080	192.168.2.3	92.240.254.110
Jul 20, 2022 01:05:47.935970068 CEST	49747	8080	192.168.2.3	92.240.254.110
Jul 20, 2022 01:06:00.016851902 CEST	49763	8080	192.168.2.3	51.91.76.89
Jul 20, 2022 01:06:00.039036989 CEST	8080	49763	51.91.76.89	192.168.2.3
Jul 20, 2022 01:06:00.561953068 CEST	49763	8080	192.168.2.3	51.91.76.89
Jul 20, 2022 01:06:00.584394932 CEST	8080	49763	51.91.76.89	192.168.2.3
Jul 20, 2022 01:06:01.093229055 CEST	49763	8080	192.168.2.3	51.91.76.89
Jul 20, 2022 01:06:01.115122080 CEST	8080	49763	51.91.76.89	192.168.2.3
Jul 20, 2022 01:06:01.128217936 CEST	49764	8080	192.168.2.3	217.182.25.250
Jul 20, 2022 01:06:01.158274889 CEST	8080	49764	217.182.25.250	192.168.2.3
Jul 20, 2022 01:06:01.659693003 CEST	49764	8080	192.168.2.3	217.182.25.250
Jul 20, 2022 01:06:01.689210892 CEST	8080	49764	217.182.25.250	192.168.2.3
Jul 20, 2022 01:06:02.202712059 CEST	49764	8080	192.168.2.3	217.182.25.250
Jul 20, 2022 01:06:02.232880116 CEST	8080	49764	217.182.25.250	192.168.2.3
Jul 20, 2022 01:06:02.271939993 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:02.537431002 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:02.537586927 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:02.538384914 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:02.804030895 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:02.819480896 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:02.819514990 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:02.819607973 CEST	49765	7080	192.168.2.3	119.193.124.41

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:06:05.037138939 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:05.300612926 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:05.301150084 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:05.304088116 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:05.610945940 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:06.458800077 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:06.458949089 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:06:09.460608959 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:09.460654020 CEST	7080	49765	119.193.124.41	192.168.2.3
Jul 20, 2022 01:06:09.460884094 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:07:28.336844921 CEST	49765	7080	192.168.2.3	119.193.124.41
Jul 20, 2022 01:07:28.336891890 CEST	49765	7080	192.168.2.3	119.193.124.41

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **6380**, Parent PID: **3076**

General

Target ID:	0
Start time:	01:05:13
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\CUfsVUDkr6.dll"
Imagebase:	0xa70000
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: **6388**, Parent PID: **6380**

General

Target ID:	1
Start time:	01:05:13
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\CUfsVUDkr6.dll",#1
Imagebase:	0xc20000
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: **6400**, Parent PID: **6380**

General

Target ID:	2
Start time:	01:05:13
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\CUfsVUDkr6.dll
Imagebase:	0xb40000
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: 00000002.00000002.261732368.0000000004760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.261732368.0000000004760000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.261764431.0000000004791000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.261764431.0000000004791000.00000020.00001000.00020000.00000000.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\Ofpagmb\vfvyklscua.sam:Zone.Identifier	success or wait	1	47A594F	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: **6408**, Parent PID: **6388**

General

Target ID:	3
Start time:	01:05:14
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\CUfsVUDkr6.dll",#1
Imagebase:	0x970000
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: 00000003.00000002.258613972.0000000000940000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.258613972.0000000000940000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.258886140.00000000043A1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.258886140.00000000043A1000.00000020.00001000.00020000.00000000.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: **6420**, Parent PID: **6380**

General

Target ID:	4
Start time:	01:05:14
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\CUfsVUDkr6.dll,DllRegisterServer
Imagebase:	0x970000
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: 00000004.00000002.258847425.0000000003390000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.258847425.0000000003390000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.259038196.0000000004CE1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.259038196.0000000004CE1000.00000020.00001000.00020000.00000000.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: **6552**, Parent PID: **6400**

General

Target ID:	5
Start time:	01:05:17
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\Ofpagmb\vfvyklscua.sam"
Imagebase:	0xb40000
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: 00000005.00000002.774599292.00000000046C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.774599292.00000000046C1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.774512688.0000000004690000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.774512688.0000000004690000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6588**, Parent PID: **6380**

General

Target ID:	6
Start time:	01:05:18
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\CUfsVUDkr6.dll,DllUnregisterServerr
Imagebase:	0x970000
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: **6936**, Parent PID: **568**

General	
Target ID:	10
Start time:	01:05:32
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:	0x7ff73c930000
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: **6972**, Parent PID: **568**

General	
Target ID:	11
Start time:	01:05:33
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7040**, Parent PID: **568**

General	
Target ID:	12
Start time:	01:05:34
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

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

Registry Activities

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

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

Analysis Process: svchost.exe PID: 7068, Parent PID: 568

General

Target ID:	13
Start time:	01:05:34
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:	0x7ff73c930000
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: 7120, Parent PID: 568

General

Target ID:	14
Start time:	01:05:35
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 2492, Parent PID: 568

General

Target ID:	15
Start time:	01:05:35
Start date:	20/07/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff72e3a0000

File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6248**, Parent PID: **568**

General

Target ID:	16
Start time:	01:05:36
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6484**, Parent PID: **568**

General

Target ID:	18
Start time:	01:05:40
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:	0x7ff73c930000
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: **6388**, Parent PID: **568**

General

Target ID:	19
Start time:	01:05:47

Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff73c930000
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: **5000**, Parent PID: **568**

General

Target ID:	20
Start time:	01:05:57
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:	0x7ff73c930000
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: **2932**, Parent PID: **568**

General

Target ID:	22
Start time:	01:06:07
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p

Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4432, Parent PID: 568

General

Target ID:	28
Start time:	01:06:31
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: MpCmdRun.exe PID: 5568, Parent PID: 6248

General

Target ID:	30
Start time:	01:06:37
Start date:	20/07/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 57 00 65 00 64 00 20 00 0e 20 4a 00 75 00 6c 00 20 00 0e 20 32 00 30 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 31 00 3a 00 30 00 36 00 3a 00 33 00 38 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Wed Jul 20 2022 01:06 :38	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 57 00 65 00 64 00 20 00 0e 20 4a 00 75 00 6c 00 20 00 0e 20 32 00 30 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 31 00 3a 00 30 00 36 00 3a 00 33 00 38 00 0d 00 0a 00	MpCmdRun: End Time: Wed Jul 20 2022 01:06:38	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **5648**, Parent PID: **5568**

General

Target ID:	31
Start time:	01:06:38
Start date:	20/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly