ID: 669372
Sample Name: bscHLGMyjW
Cookbook: default.jbs
Time: 01:05:12
Date: 20/07/2022
Version: 35.0.0 Citrine

Table of Contents

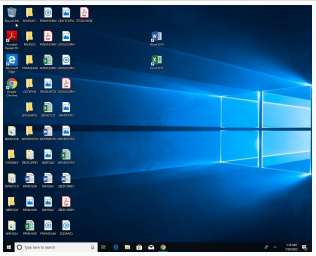
Windows Analysis Report

bscHLGMyjW

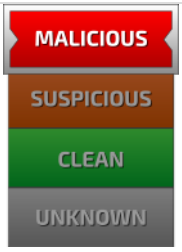
Overview

General Information

Sample Name:	bscHLGMyjW (renamed file extension from none to dll)
Analysis ID:	669372
MD5:	853c4a8922ffe40..
SHA1:	7d46327d257ff52.
SHA256:	8c58876a208132..
Tags:	32 dll exe trojan
Infos:	



Detection



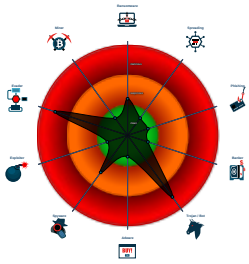
Emotet

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Query firmware table information (lik…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 7008 cmdline: loaddll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7032 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7052 cmdline: rundll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 7040 cmdline: regsvr32.exe /s C:\Users\user\Desktop\bscHLGMyjW.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 7140 cmdline: C:\Windows\SysWOW64\regsvr32.exe /s "C:\Windows\SysWOW64\Mjzwixkz\jiugg.vcz" MD5: 426E7499F6A7346F0410DEAD0805586B)
  - rundll32.exe (PID: 7064 cmdline: rundll32.exe C:\Users\user\Desktop\bscHLGMyjW.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7164 cmdline: rundll32.exe C:\Users\user\Desktop\bscHLGMyjW.dll,DllUnregisterServerr MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5504 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6412 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7068 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5600 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2320 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1640 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7164 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "216.131.66.3:1",
    "192.16.0.0:1484",
    "216.64.72.3:1",
    "248.38.74.3:1",
    "255.255.255.255:3",
    "156.4.0.0:1",
    "108.4.0.0:1",
    "152.4.0.0:1",
    "124.4.0.0:1",
    "180.4.0.0:1",
    "184.4.0.0:1",
    "128.4.0.0:1",
    "148.4.0.0:1",
    "208.185.68.3:1",
    "40.38.70.3:48",
    "32.137.69.3:48",
    "103.240.2.0:4300",
    "112.135.10.118:5",
    "91.240.2.0:4600",
    "108.240.2.0:3484",
    "114.240.2.0:2956",
    "120.240.2.0:4600",
    "224.120.66.3:1",
    "135.52.4.0:4828",
    "220.194.66.52:443"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.361541102.0000000004DB1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.361541102.0000000004DB1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.359006501.0000000003590000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.359006501.0000000003590000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.361265936.0000000003550000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.regsvr32.exe.4df0000.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.4df0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.3590000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.3590000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.3150000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 18 - Source IP: 192.168.2.7 - Destination IP: 46.55.222.11

Timestamp:	192.168.2.746.55.222.11498564432404334 07/20/22-01:08:26.357523
SID:	2404334
Source Port:	49856
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 4 - Source IP: 192.168.2.7 - Destination IP: 131.100.24.231

Timestamp:	192.168.2.7131.100.24.23149895802404306 07/20/22-01:10:07.675221
SID:	2404306
Source Port:	49895
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	192.168.2.751.91.76.894976280802404338 07/20/22-01:06:44.834560
SID:	2404338
Source Port:	49762
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

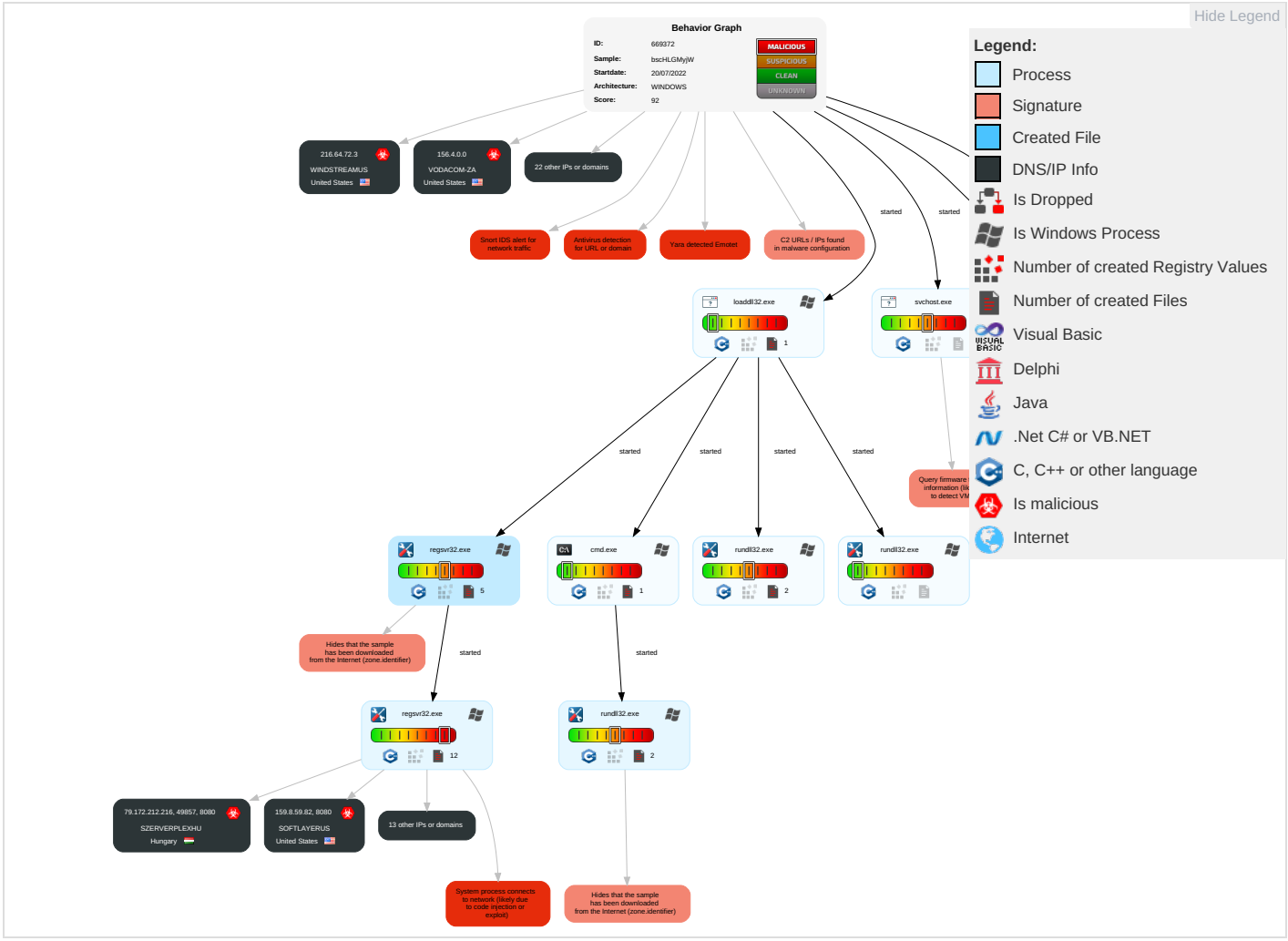
HIPS / PFW / Operating System Protection Evasion

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Input Capture	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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	2 Obfuscated Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	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)	Logon Script (Windows)	1 DLL Side-Loading	Security Account Manager	4 5 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 File Deletion	NTDS	1 5 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	1 3 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	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 Hidden Files and Directories	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 Regsvr32	/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 Rundll32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

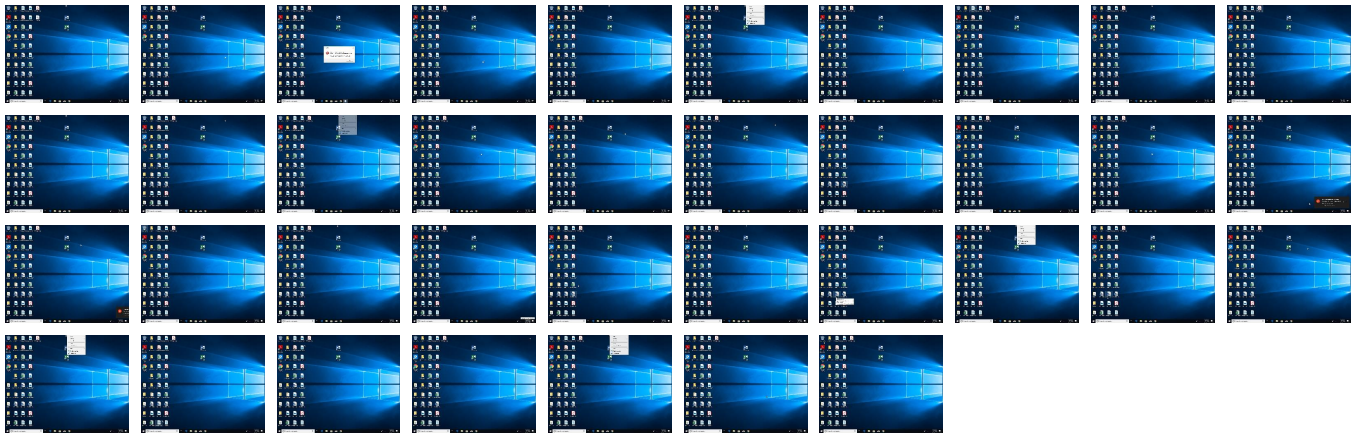
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.4dc0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.4df0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.3590000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.3550000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.regsvr32.exe.3150000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.4c20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4b80000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4db0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdb	100%	Avira URL Cloud	malware	
http://https://51.91.7.5/	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJ771D	0%	Avira URL Cloud	safe	
http://https://120.50.40.183/	100%	Avira URL Cloud	malware	
http://https://159.8.59.82/	100%	Avira URL Cloud	malware	
http://https://131.100.24.231:80/H	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/72.212.216/	0%	Avira URL Cloud	safe	
http://https://103.221.221.247:8080/gYHJIs	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/	0%	Avira URL Cloud	safe	
http://https://173.254.208.91:8080/FHNmSQhMPmUgfiGTpfRKglWV	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/0	100%	Avira URL Cloud	malware	
http://https://159.8.59.82:8080/	100%	Avira URL Cloud	malware	
http://https://79.172.212.216/9	100%	Avira URL Cloud	malware	
http://https://149.56.128.192/fSTm	100%	Avira URL Cloud	malware	
http://https://sls.upP	0%	Avira URL Cloud	safe	
http://https://131.100.24.231:80/	100%	Avira URL Cloud	malware	
http://https://51.91.7.5:8080/rxYzgkPqLyQVovawmSL	100%	Avira URL Cloud	malware	
http://https://51.91.76.89:8080/lNTCDnLEFARnzCSTbPqiarmtqBjaTTxMdOLjVhFUj	100%	Avira URL Cloud	malware	
http://https://160.16.218.63:8080/rlxtXuQTWcz	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/4	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/99.251.50/hdaVPxkDfoKJQyOXvwYhhkAy	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTYy	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/	100%	Avira URL Cloud	malware	
http://https://206.188.212.92/	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdbsI	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/gYHJIsD	100%	Avira URL Cloud	malware	
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://206.188.212.92:8080/XGoDqOmEznVckdttzjTudmbZ	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/0/wVZyzHXwzFIbSsMDkdb	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/B	100%	Avira URL Cloud	malware	
http://https://149.56.128.192/	100%	Avira URL Cloud	malware	
http://https://103.221.221.247:8080/tas	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/n	0%	Avira URL Cloud	safe	
http://https://46.55.222.11/F	100%	Avira URL Cloud	malware	
http://https://131.100.24.231:80/HjsJJresDkOtazdwjPkgeyoMeBIGInWLCajLkkcuvkifWRvynwfbRFAZdPO	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkAQ	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/wVZyzHX	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/2.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://131.100.24.231/	100%	Avira URL Cloud	malware	
http://https://51.91.7.5:8080/	100%	Avira URL Cloud	malware	
http://https://131.100.24.231/I	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdbX	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/.50.40.183/	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://103.221.221.247/	100%	Avira URL Cloud	malware	
http://https://160.16.218.63/Y	100%	Avira URL Cloud	malware	
http://https://159.8.59.82:8080/taEjAKKH	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://79.172.212.216:8080/	100%	Avira URL Cloud	malware	
http://https://185.157.82.211:8080/	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkA	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://160.16.218.63:8080/rlxtXuQTWczj	100%	Avira URL Cloud	malware	
http://https://160.16.218.63/K	100%	Avira URL Cloud	malware	
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJh	0%	Avira URL Cloud	safe	
http://https://185.157.82.211:8080/)	100%	Avira URL Cloud	malware	
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkAAppData	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/-	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdbP	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/.50.40.183:80/wVZyzHXwzFIbSsMDkdb	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJ	0%	Avira URL Cloud	safe	
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJn	0%	Avira URL Cloud	safe	
http://https://185.157.82.211/	100%	Avira URL Cloud	malware	
http://https://185.157.82.211/V	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTY=	100%	Avira URL Cloud	malware	
http://https://51.91.76.89/	100%	Avira URL Cloud	malware	
http://https://46.55.222.11/BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTY	100%	Avira URL Cloud	malware	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://79.172.212.216/	100%	Avira URL Cloud	malware	
http://https://159.8.59.82:8080/taEjAKKHJ	100%	Avira URL Cloud	malware	
http://https://79.172.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ	100%	Avira URL Cloud	malware	
http://https://159.8.59.82/5	100%	Avira URL Cloud	malware	
http://https://185.157.82.211:8080/riNpYqdQCgxyFX	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/	100%	Avira URL Cloud	malware	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://79.172.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ%	100%	Avira URL Cloud	malware	
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdb1	100%	Avira URL Cloud	malware	
http://https://58.227.42.236/3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdb	regsvr32.exe, 00000005.00000003.51713187 1.000000000347A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://51.91.7.5/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJ771D	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://120.50.40.183/	regsvr32.exe, 00000005.00000003.51713187 1.000000000347A000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82/	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://131.100.24.231:80/H	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236/72.212.216/	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://103.221.221.247:8080/gYHJIs	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://173.254.208.91:8080/FHNmSQhMPmUgfiGTpfRKglWV	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.471558713.000000000345A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.729492928.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/0	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82:8080/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.216/9	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492 928.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://sls.upP	regsvr32.exe, 00000005.00000003.60897965 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://131.100.24.231:80/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://51.91.7.5:8080/rxYzgkPqLyQVovawmSL	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://51.91.76.89:8080/INTCDnLEFARnzCSTbPqiarmtqBjaTTxMdOLjVhFUj	regsvr32.exe, 00000005.00000002.87339799 4.00000000033EA000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63:8080/rlxtXuQTWcz	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/4	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492 928.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/99.251.50/hdaVPxkDfoKJQyOXvwYhhkAy	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTYy	regsvr32.exe, 00000005.00000003.60897965 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://206.188.212.92/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/wVZyzHXwzFlbSsMDkdbsI	regsvr32.exe, 00000005.00000003.51713187 1.000000000347A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/gYHJIsD	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://173.254.208.91/	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.471558713.000000000345A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.72949292 8.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://160.16.218.63/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000015.00000003.567542287 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567572106.000001CA15A02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567792370 .000001CA15A19000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567438801.000001CA1559C000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567727159 .000001CA1558A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567687637.000001CA15A03000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567757308 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000015.00000003.567542287 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567572106.000001CA15A02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567792370 .000001CA15A19000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567438801.000001CA1559C000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567727159 .000001CA1558A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567687637.000001CA15A03000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567757308 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://206.188.212.92:8080/XGoDqOmEznVckdttzjTudmbZ	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/0/wVZyzHXwzFlbSsMDkdb	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/B	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://149.56.128.192/	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.471558713.000000000345A000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.729492928.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://103.221.221.247:8080/tas	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236/n	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492 928.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://46.55.222.11/F	regsvr32.exe, 00000005.00000003.72949292 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://131.100.24.231:80/HjsJJresDkOtazdwjPkgeyoMeBIGInWLCajLkkcuvkifWRvynwfbRFAZdPO	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492928.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkAQ	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/	regsvr32.exe, 00000005.00000003.60897965 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/wVZyzHX	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.608979 653.0000000003474000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/2.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000015.00000003.571982184 .000001CA1558E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.571561051.000001CA155A0000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://131.100.24.231/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

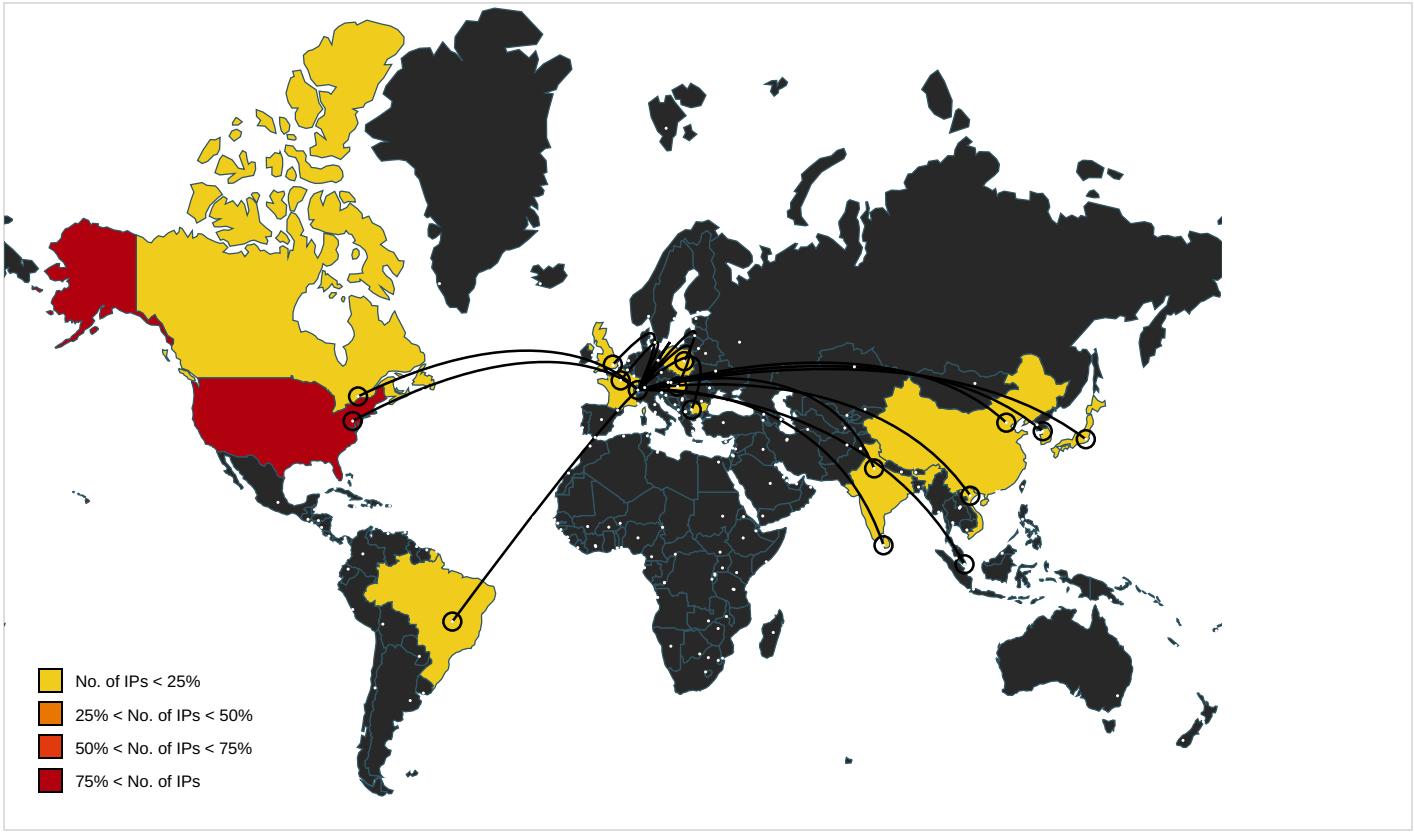
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://51.91.7.5:8080/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://131.100.24.231/l	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdbX	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.517131871.0000 00000347A000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000005.00 000002.873626561.0000000003439000.000000 04.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/.50.40.183/	regsvr32.exe, 00000005.00000003.60897965 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://103.221.221.247/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63/Y	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82:8080/taEjAKKH	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000015.00000002.596545350 .000001CA15500000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 9.00000002.875031828.000001BCA7C63000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001E.00000002.874276020 .00000249B38E3000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://79.172.212.216:8080/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://185.157.82.211:8080/	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkA	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492928.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000015.00000003.576016058 .000001CA15A02000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.575804144.000001CA155B5000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.575895200 .000001CA1558E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.575847849.000001CA155B5000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.575944148 .000001CA1559F000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://160.16.218.63:8080/rlxtXuQTWczj	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://160.16.218.63/K	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.608979653.0000000003474000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJh	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://185.157.82.211:8080/)	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.861975728.0000000003439000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626 561.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://192.99.251.50/hdaVPxkDfoKJQyOXvwYhhkAAppData	regsvr32.exe, 00000005.00000003.72931428 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://46.55.222.11/-	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://support.hotspotshield.com/	svchost.exe, 00000015.00000003.567542287 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567572106.000001CA15A02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567792370 .000001CA15A19000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567438801.000001CA1559C000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567727159 .000001CA1558A000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.567687637.000001CA15A03000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.567757308 .000001CA155AC000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://120.50.40.183:80/wVZyzHXwzFIbSsMDkdbP	regsvr32.exe, 00000005.00000003.51713187 1.000000000347A000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/.50.40.183:80/wVZyzHXwzFIbSsMDkdb	regsvr32.exe, 00000005.00000003.60897965 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000015.00000003.571982184 .000001CA1558E000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 5.00000003.571561051.000001CA155A0000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJ	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000002.873626561.000000000343900 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492928.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://58.227.42.236:80/sCQmfFGUJRcSUjROebyagzBacHzSNzxJn	regsvr32.exe, 00000005.00000003.72949292 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://185.157.82.211/	regsvr32.exe, 00000005.00000002.87362656 1.0000000003439000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://185.157.82.211/V	regsvr32.exe, 00000005.00000003.86197572 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000002.873626561.0000000003439000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://46.55.222.11/BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTY=	regsvr32.exe, 00000005.00000003.82647330 3.0000000003474000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 005.00000003.729314283.0000000003474000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975 728.0000000003439000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00005.00000003.608979653.000000000347400 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000 000003439000.00000004.00000020.00020000. 00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://51.91.76.89/	regsvr32.exe, 00000005.00000003.72949292 8.0000000003439000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://disneyplus.com/legal.	svchost.exe, 00000015.00000003.571982184.000001CA1558E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.571561051.000001CA155A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://79.172.212.216/	regsvr32.exe, 00000005.00000003.729314283.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492928.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82:8080/taEjAKKHJ	regsvr32.exe, 00000005.00000003.826473303.0000000003474000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://79.172.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ	regsvr32.exe, 00000005.00000003.826473303.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729314283.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://159.8.59.82/5	regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://185.157.82.211:8080/riNpYqdQCgxyFX	regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/	regsvr32.exe, 00000005.00000003.826473303.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729314283.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.608979653.0000000000347400.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.517131871.000000000347A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://help.disneyplus.com.	svchost.exe, 00000015.00000003.571982184.000001CA1558E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000015.00000003.571561051.000001CA155A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://79.172.212.216:8080/QLBvrKXyQhlLtOrpKVuDaNHJ%	regsvr32.exe, 00000005.00000003.826473303.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729314283.0000000003474000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://120.50.40.183:80/wVZyzHXwzFlbSsMDkdb1	regsvr32.exe, 00000005.00000003.517131871.000000000347A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://58.227.42.236/3	regsvr32.exe, 00000005.00000003.861975728.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.873626561.0000000003439000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000003.729492928.0000000003439000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
248.38.74.3	unknown	Reserved		unknown	unknown	true
208.185.68.3	unknown	United States		396173	SWA-W11-MKT-INETUS	true
185.157.82.211	unknown	Poland		42927	S-NET-ASPL	true
216.131.66.3	unknown	United States		22781	RBLHSTUS	true
180.4.0.0	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
79.172.212.216	unknown	Hungary		61998	SZERVERPLEXHU	true
114.240.2.0	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	true
220.194.66.52	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	true
91.240.2.0	unknown	United Kingdom		198863	CUP-ASGB	true
173.254.208.91	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	true
206.188.212.92	unknown	United States		55002	DEFENSE-NETUS	true
40.38.70.3	unknown	United States		4249	LILLY-ASUS	true
135.52.4.0	unknown	United States		54614	CIKTELECOM-CABLECA	true
51.91.7.5	unknown	France		16276	OVHFR	true
32.137.69.3	unknown	United States		2686	ATGS-MMD-ASUS	true
108.240.2.0	unknown	United States		7018	ATT-INTERNET4US	true
148.4.0.0	unknown	United States		6074	LIUNETUS	true
108.4.0.0	unknown	United States		701	UUNETUS	true
192.16.0.0	unknown	United States		14153	EDGECAST-IRUS	true
149.56.128.192	unknown	Canada		16276	OVHFR	true
128.4.0.0	unknown	United States		2	UDEL-DCNUS	true
120.240.2.0	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	true
131.100.24.231	unknown	Brazil		61635	GOPLEXTELECOMUNICACOESEINTERNETLTDA-MEBR	true
156.4.0.0	unknown	United States		29975	VODACOM-ZA	true
184.4.0.0	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	true
46.55.222.11	unknown	Bulgaria		34841	BALCHIKNETBG	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.91.76.89	unknown	France		16276	OVHFR	true
103.240.2.0	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	true
160.16.218.63	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
224.120.66.3	unknown	Reserved		unknown	unknown	true
192.99.251.50	unknown	Canada		16276	OVHFR	true
216.64.72.3	unknown	United States		7029	WINDSTREAMUS	true
124.4.0.0	unknown	India		18302	SKG_NW-AS-KRSKTelecomKR	true
112.135.10.118	unknown	Sri Lanka		9329	SLTINT-AS-APSriLankaTelecomInternetLK	true
152.4.0.0	unknown	United States		81	NCRENUS	true
159.8.59.82	unknown	United States		36351	SOFTLAYERUS	true
120.50.40.183	unknown	Singapore		17547	M1NET-SG-APM1NETLTDSG	true
58.227.42.236	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
103.221.221.247	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	669372
Start date and time: 20/07/202201:05:12	2022-07-20 01:05:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bscHLGMyjW (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:	31
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:	mal92.troj.evad.winDLL@20/4@0/41
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 1.2%) • Quality average: 80.7% • Quality standard deviation: 22%
HCA Information:	• Successful, ratio: 75% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, UsoClient.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 8.248.137.254, 8.238.85.254, 8.248.145.254, 8.248.119.254, 8.241.126.121, 20.223.24.244, 23.211.4.86, 40.119.249.228, 51.11.168.232, 8.248.135.254, 8.248.149.254, 8.238.189.126, 8.253.207.120
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, settings-prod-sea-2.southeastasia.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, settings-prod-uks-1.uksouth.cloudapp.azure.com, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.us eroor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, wu-bg-shim.trafficmanager.net, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, displaycatalog-rp.md.mp.microsoft.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.
- VT rate limit hit for: bscHLGMyjW.dll

Simulations

Behavior and APIs

Time	Type	Description
01:07:56	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x2c04a331, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped

Size (bytes):	786432
Entropy (8bit):	0.250704057018144
Encrypted:	false
SSDEEP:	384:E+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:7SB2nSB2RSjlK/+mLesOj1J2
MD5:	1C4553ECE074FAF7C1CBD4589F778FE5
SHA1:	56C3A250F1414B3FB0CFCD7098A3AD0F67906F07
SHA-256:	0EC64C6E3DC500EBBD29D2518A2F2ABEEADBF9B99D2685C3E2D9522AD2BF43E0
SHA-512:	A60EF4D10A72D99E42F98BC60091FA709209332D538EA9104A4CFEAEFDF7A3B4ACCDFDB3DE58AA56576A7BB84399F45F46D06274AA31B5564FE4122533B03BC3
Malicious:	false
Preview:	,..1... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... ....5..=.....z.....S.....z..... .....

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

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

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

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1050968086786974
Encrypted:	false
SSDEEP:	6:kKP1v+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:nFNkPlE99SNxAhUeE1
MD5:	99CD07B7CBA64F60AD1D768E8D35793A
SHA1:	CD04042624DC329DB9D704FA6EFFBA8A68793268
SHA-256:	EE7BDD31B8346C7B1B251091563660CBB4FE2264D9F4AAB59441200717484E53
SHA-512:	48250248B491A37EC381D3D023EC70E0D2E2431CAB87782EDE0B631A8BE7441CB6254122858B538C086E95F46999492124552A6487BAB413A7A19EBEFFDE5D7E
Malicious:	false
Preview:	p..... .....dE. ....(..... ....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b.."..0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

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

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9

SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.571573688089068
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bscHLGMyjW.dll
File size:	942080
MD5:	853c4a8922ffe407962ed618f5e5050b
SHA1:	7d46327d257ff52b5c380b521cd28935d65c4bc7
SHA256:	8c58876a208132d6ed84b2d63416bde9efa590e9ae0246a4f668bcebdc04b7a1
SHA512:	d5607fe37a1670acab8e13acfa3d7f0be2ac4d9a733a83e303a88f33f5e4a11ee0399a9438713bce73434b51a7f3ac0d7bf22535f2e76fd723dad2b830145fb2
SSDEEP:	12288:1HINAbFJ0qIOft0qsDCTOteq/XhkUqKJzlB/ooM5M7VesLZkl:qNyJTIOfADYOEgoUuoM5M7VesLZ
TLSH:	9F15E74279838E34F11F03B0DD43121AB61F9E50FA51553EABB872AAAF307A17DD921D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....aa..%...%...%...../.....2...%...3.....$.....$.....$...Rich%.....PE..L...7.;b...

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x1005801e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	
Time Stamp:	0x623B8F37 [Wed Mar 23 21:20:55 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:	39f0c91492ecdee129a7efdc73aac29f

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007FECA09D74A7h
call 00007FECA09E14ADh
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]

Instruction
mov edx, dword ptr [esp+0Ch]
call 00007FECA09D7392h
pop ecx
retn 000Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [1008675Ch]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [1008675Ch]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [1008675Ch]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x84b60	0x73	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x82efc	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8c000	0x45d70	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	0x132f8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x7cdc0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x72000	0x55c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x82e74	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x70e79	0x71000	False	0.33150407909292035	data	6.159544480920374	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x72000	0x12bd3	0x13000	False	0.39717824835526316	data	5.546150396900126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x85000	0x6b98	0x3000	False	0.301025390625	data	4.396397855204817	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x8c000	0x45d70	0x46000	False	0.5704938616071429	data	6.319202698969252	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0x1784e	0x18000	False	0.4889424641927083	data	6.127097386348335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
	0x8cc88	0x20800	data	English	United States
RT_CURSOR	0xad488	0x134	data	English	United States
RT_CURSOR	0xad5bc	0xb4	data	English	United States
RT_CURSOR	0xad670	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0xad7a4	0x134	data	English	United States
RT_CURSOR	0xad8d8	0x134	data	English	United States
RT_CURSOR	0xada0c	0x134	data	English	United States
RT_CURSOR	0xadb40	0x134	data	English	United States
RT_CURSOR	0xadc74	0x134	data	English	United States
RT_CURSOR	0xadda8	0x134	data	English	United States
RT_CURSOR	0xadedc	0x134	data	English	United States
RT_CURSOR	0xae010	0x134	data	English	United States
RT_CURSOR	0xae144	0x134	data	English	United States
RT_CURSOR	0xae278	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0xae3ac	0x134	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xae4e0	0x134	data	English	United States
RT_CURSOR	0xae614	0x134	data	English	United States
RT_BITMAP	0xae748	0xb8	data	English	United States
RT_BITMAP	0xae800	0x144	data	English	United States
RT_ICON	0xae944	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	English	United States
RT_ICON	0xaec2c	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xaed54	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0xbf57c	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_DIALOG	0xcfda4	0x11a	data	English	United States
RT_DIALOG	0xcfec0	0x182	data	English	United States
RT_DIALOG	0xd0044	0xe8	data	English	United States
RT_DIALOG	0xd012c	0x34	data	English	United States
RT_STRING	0xd0160	0x4a	data	English	United States
RT_STRING	0xd01ac	0x82	data	English	United States
RT_STRING	0xd0230	0x2a	data	English	United States
RT_STRING	0xd025c	0x192	data	English	United States
RT_STRING	0xd03f0	0x4e2	data	English	United States
RT_STRING	0xd08d4	0x31a	data	English	United States
RT_STRING	0xd0bf0	0x2dc	data	English	United States
RT_STRING	0xd0ecc	0x8a	data	English	United States
RT_STRING	0xd0f58	0xac	data	English	United States
RT_STRING	0xd1004	0xde	data	English	United States
RT_STRING	0xd10e4	0x4c4	data	English	United States
RT_STRING	0xd15a8	0x264	data	English	United States
RT_STRING	0xd180c	0x2c	data	English	United States
RT_STRING	0xd1838	0x42	data	English	United States
RT_GROUP_CURSOR	0xd187c	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0xd18a0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd18b4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd18c8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd18dc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd18f0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1904	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1918	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd192c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1940	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1954	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1968	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd197c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd1990	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xd19a4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xd19b8	0x22	data	English	United States
RT_GROUP_ICON	0xd19dc	0x14	data	English	United States
RT_GROUP_ICON	0xd19f0	0x14	data	English	United States
RT_VERSION	0xd1a04	0x314	data	English	United States
RT_MANIFEST	0xd1d18	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	HeapFree, HeapAlloc, GetCommandLineA, GetProcessHeap, RaiseException, HeapReAlloc, HeapSize, VirtualProtect, VirtualAlloc, GetSystemInfo, VirtualQuery, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, Sleep, HeapDestroy, HeapCreate, VirtualFree, GetStdHandle, GetModuleFileNameA, SetHandleCount, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, RtlUnwind, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, GetTimeZoneInformation, GetLocaleInfoA, GetConsoleCP, GetConsoleMode, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, CreateFileA, SetEnvironmentVariableA, GetTickCount, GetFileTime, GetFileAttributesW, FileTimeToLocalFileTime, FileTimeToSystemTime, lstrlenA, CreateFileW, GetFullPathNameW, GetVolumeInformationW, FindFirstFileW, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, GetThreadLocale, InterlockedIncrement, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, WritePrivateProfileStringW, FormatMessageW, LocalFree, MulDiv, GetModuleHandleA, InterlockedDecrement, lstrlenW, GlobalFindAtomW, CompareStringW, LoadLibraryA, GetVersionExA, GlobalUnlock, GlobalFree, FreeResource, GetCurrentProcessId, GetLastError, SetLastError, GlobalAddAtomW, CloseHandle, GetCurrentThread, GetCurrentThreadId, ConvertDefaultLocale, GetModuleFileNameW, GetVersion, EnumResourceLanguagesW, lstrcmpA, GetLocaleInfoW, LoadLibraryW, WideCharToMultiByte, CompareStringA, MultiByteToWideChar, InterlockedExchange, GlobalLock, lstrcmpW, GlobalAlloc, FreeLibrary, GlobalDeleteAtom, GetModuleHandleW, GetProcAddress, LoadResource, LockResource, SizeofResource, FindResourceW, GetEnvironmentStrings, ExitProcess
USER32.dll	RegisterClipboardFormatW, PostThreadMessageW, ReleaseCapture, LoadCursorW, SetCapture, EndPaint, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GrayStringW, DrawTextExW, DrawTextW, TabbedTextOutW, DestroyMenu, ShowWindow, MoveWindow, SetWindowTextW, IsDialogMessageW, RegisterWindowMessageW, SendDlgItemMessageW, SendDlgItemMessageA, WinHelpW, IsChild, GetCapture, GetClassLongW, GetClassNameW, MessageBeep, GetPropW, RemovePropW, SetFocus, GetWindowTextW, GetForegroundWindow, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreateWindowExW, GetClassInfoExW, GetClassInfoW, RegisterClassW, GetSysColor, AdjustWindowRectEx, EqualRect, CopyRect, PtInRect, GetDlgCtrlID, DefWindowProcW, CallWindowProcW, SetWindowLongW, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamW, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, GetWindowThreadProcessId, GetWindowLongW, GetLastActivePopup, IsWindowEnabled, MessageBoxW, GetNextDlgGroupItem, InvalidateRgn, SetRect, IsRectEmpty, CopyAcceleratorTableW, CharNextW, CharUpperW, SetPropW, GetSysColorBrush, SetCursor, SetWindowsHookExW, CallNextHookEx, GetMessageW, TranslateMessage, DispatchMessageW, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageW, GetCursorPos, ValidateRect, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, GetFocus, ModifyMenuW, GetMenuState, EnableMenuItem, CheckMenuItem, PostMessageW, PostQuitMessage, InvalidateRect, LoadBitmapW, GetParent, GetClientRect, IsIconic, DrawIcon, GetSystemMetrics, SendMessageW, GetSystemMenu, AppendMenuW, LoadIconW, EnableWindow, UnregisterClassA
GDI32.dll	ScaleWindowExtEx, GetWindowExtEx, ExtSelectClipRgn, DeleteDC, GetStockObject, GetDeviceCaps, SetWindowExtEx, GetBkColor, GetTextColor, CreateRectRgnIndirect, GetRgnBox, GetMapMode, GetViewportExtEx, DeleteObject, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, Escape, TextOutW, RectVisible, PtVisible, BitBlt, SetMapMode, RestoreDC, SaveDC, ExtTextOutW, SetBkColor, SetTextColor, GetClipBox, CreateBitmap, GetPixel, GetObjectW, CreateCompatibleDC, CreateCompatibleBitmap, SetPixelV
comdlg32.dll	GetFileTitleW
WINSPOOL.DRV	DocumentPropertiesW, OpenPrinterW, ClosePrinter
ADVAPI32.dll	RegSetValueExW, RegCreateKeyExW, RegQueryValueW, RegOpenKeyW, RegEnumKeyW, RegDeleteKeyW, RegOpenKeyExW, RegQueryValueExW, RegCloseKey
SHLWAPI.dll	PathFindFileNameW, PathStripToRootW, PathFindExtensionW, PathIsUNCW
oledlg.dll	OleUIBusyW
ole32.dll	OleInitialize, CoFreeUnusedLibraries, OleUninitialize, CreateILockBytesOnHGlobal, StgCreateDocfileOnILockBytes, StgOpenStorageOnILockBytes, CoGetClassObject, CoRevokeClassObject, CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, CLSIDFromProgID, OleIsCurrentClipboard, OleFlushClipboard, CoRegisterMessageFilter
OLEAUT32.dll	VariantCopy, SysAllocString, SafeArrayDestroy, SystemTimeToVariantTime, VariantTimeToSystemTime, OleCreateFontIndirect, SysStringLen, VariantInit, VariantChangeType, VariantClear, SysAllocStringLen, SysFreeString

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10039b80
DllUnregisterServerr	2	0x10039bc0

Possible Origin

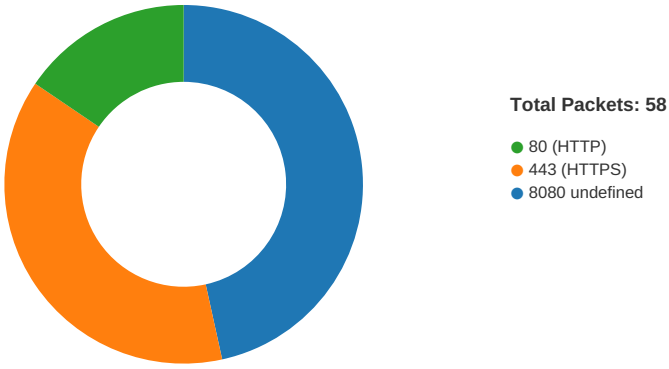
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.746.55.222.114 98564432404334 07/20/22-01:08:26.357523	TCP	2404334	ET CNC Feodo Tracker Reported CnC Server TCP group 18	49856	443	192.168.2.7	46.55.222.11
192.168.2.7131.100.24.23 149895802404306 07/20/22-01:10:07.675221	TCP	2404306	ET CNC Feodo Tracker Reported CnC Server TCP group 4	49895	80	192.168.2.7	131.100.24.231
192.168.2.751.91.76.8949 76280802404338 07/20/22-01:06:44.834560	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49762	8080	192.168.2.7	51.91.76.89

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:06:44.834559917 CEST	49762	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:06:44.856633902 CEST	8080	49762	51.91.76.89	192.168.2.7
Jul 20, 2022 01:06:45.503371000 CEST	49762	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:06:45.523595095 CEST	8080	49762	51.91.76.89	192.168.2.7
Jul 20, 2022 01:06:46.206505060 CEST	49762	8080	192.168.2.7	51.91.76.89
Jul 20, 2022 01:06:46.226511955 CEST	8080	49762	51.91.76.89	192.168.2.7
Jul 20, 2022 01:06:46.242204905 CEST	49763	8080	192.168.2.7	173.254.208.91
Jul 20, 2022 01:06:46.406214952 CEST	8080	49763	173.254.208.91	192.168.2.7
Jul 20, 2022 01:06:46.909936905 CEST	49763	8080	192.168.2.7	173.254.208.91
Jul 20, 2022 01:06:47.073618889 CEST	8080	49763	173.254.208.91	192.168.2.7
Jul 20, 2022 01:06:47.722201109 CEST	49763	8080	192.168.2.7	173.254.208.91
Jul 20, 2022 01:06:47.891154051 CEST	8080	49763	173.254.208.91	192.168.2.7
Jul 20, 2022 01:06:47.906995058 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:47.907058001 CEST	443	49764	149.56.128.192	192.168.2.7
Jul 20, 2022 01:06:47.908020020 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:47.930125952 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:47.930171013 CEST	443	49764	149.56.128.192	192.168.2.7
Jul 20, 2022 01:06:48.282975912 CEST	443	49764	149.56.128.192	192.168.2.7
Jul 20, 2022 01:06:48.283132076 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:48.685695887 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:48.685745955 CEST	443	49764	149.56.128.192	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:06:48.685997963 CEST	443	49764	149.56.128.192	192.168.2.7
Jul 20, 2022 01:06:48.686086893 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:48.690339088 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:06:48.736499071 CEST	443	49764	149.56.128.192	192.168.2.7
Jul 20, 2022 01:07:22.296195030 CEST	49764	443	192.168.2.7	149.56.128.192
Jul 20, 2022 01:07:22.771351099 CEST	49783	80	192.168.2.7	120.50.40.183
Jul 20, 2022 01:07:25.808518887 CEST	49783	80	192.168.2.7	120.50.40.183
Jul 20, 2022 01:07:31.819861889 CEST	49783	80	192.168.2.7	120.50.40.183
Jul 20, 2022 01:07:44.009496927 CEST	49792	8080	192.168.2.7	160.16.218.63
Jul 20, 2022 01:07:47.149231911 CEST	49792	8080	192.168.2.7	160.16.218.63
Jul 20, 2022 01:07:53.290525913 CEST	49792	8080	192.168.2.7	160.16.218.63
Jul 20, 2022 01:08:05.308933020 CEST	49822	8080	192.168.2.7	206.188.212.92
Jul 20, 2022 01:08:08.312422991 CEST	49822	8080	192.168.2.7	206.188.212.92
Jul 20, 2022 01:08:14.312891006 CEST	49822	8080	192.168.2.7	206.188.212.92
Jul 20, 2022 01:08:26.357522964 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.357578039 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.357676029 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.359740019 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.359776020 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.532005072 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.532187939 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.630074024 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.630100012 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.630712032 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.630785942 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.631612062 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.672494888 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.804231882 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.804380894 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.804405928 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.804501057 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.804526091 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.804562092 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.804629087 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.804647923 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.827383995 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.827428102 CEST	443	49856	46.55.222.11	192.168.2.7
Jul 20, 2022 01:08:26.827442884 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.827522993 CEST	49856	443	192.168.2.7	46.55.222.11
Jul 20, 2022 01:08:26.874392986 CEST	49857	8080	192.168.2.7	79.172.212.216
Jul 20, 2022 01:08:26.907696962 CEST	8080	49857	79.172.212.216	192.168.2.7
Jul 20, 2022 01:08:27.407752991 CEST	49857	8080	192.168.2.7	79.172.212.216
Jul 20, 2022 01:08:27.441828012 CEST	8080	49857	79.172.212.216	192.168.2.7
Jul 20, 2022 01:08:27.954648972 CEST	49857	8080	192.168.2.7	79.172.212.216
Jul 20, 2022 01:08:27.989011049 CEST	8080	49857	79.172.212.216	192.168.2.7
Jul 20, 2022 01:08:27.993065119 CEST	49858	8080	192.168.2.7	103.221.221.247
Jul 20, 2022 01:08:28.205580950 CEST	8080	49858	103.221.221.247	192.168.2.7
Jul 20, 2022 01:08:28.720330954 CEST	49858	8080	192.168.2.7	103.221.221.247
Jul 20, 2022 01:08:28.933847904 CEST	8080	49858	103.221.221.247	192.168.2.7
Jul 20, 2022 01:08:29.439251900 CEST	49858	8080	192.168.2.7	103.221.221.247
Jul 20, 2022 01:08:29.650430918 CEST	8080	49858	103.221.221.247	192.168.2.7
Jul 20, 2022 01:08:29.655344963 CEST	49859	80	192.168.2.7	58.227.42.236
Jul 20, 2022 01:08:32.642461061 CEST	49859	80	192.168.2.7	58.227.42.236
Jul 20, 2022 01:08:38.643042088 CEST	49859	80	192.168.2.7	58.227.42.236
Jul 20, 2022 01:08:50.653744936 CEST	49884	443	192.168.2.7	192.99.251.50
Jul 20, 2022 01:08:50.653812885 CEST	443	49884	192.99.251.50	192.168.2.7
Jul 20, 2022 01:08:50.653953075 CEST	49884	443	192.168.2.7	192.99.251.50
Jul 20, 2022 01:08:50.654799938 CEST	49884	443	192.168.2.7	192.99.251.50
Jul 20, 2022 01:08:50.654838085 CEST	443	49884	192.99.251.50	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 20, 2022 01:09:22.978303909 CEST	49884	443	192.168.2.7	192.99.251.50
Jul 20, 2022 01:09:23.103354931 CEST	49890	8080	192.168.2.7	185.157.82.211
Jul 20, 2022 01:09:26.115669966 CEST	49890	8080	192.168.2.7	185.157.82.211
Jul 20, 2022 01:09:32.131822109 CEST	49890	8080	192.168.2.7	185.157.82.211
Jul 20, 2022 01:09:44.142637968 CEST	49893	8080	192.168.2.7	159.8.59.82
Jul 20, 2022 01:09:47.148674011 CEST	49893	8080	192.168.2.7	159.8.59.82
Jul 20, 2022 01:09:53.156699896 CEST	49893	8080	192.168.2.7	159.8.59.82
Jul 20, 2022 01:10:05.302692890 CEST	49894	8080	192.168.2.7	51.91.7.5
Jul 20, 2022 01:10:05.330826998 CEST	8080	49894	51.91.7.5	192.168.2.7
Jul 20, 2022 01:10:05.837692022 CEST	49894	8080	192.168.2.7	51.91.7.5
Jul 20, 2022 01:10:05.868336916 CEST	8080	49894	51.91.7.5	192.168.2.7
Jul 20, 2022 01:10:06.384687901 CEST	49894	8080	192.168.2.7	51.91.7.5
Jul 20, 2022 01:10:06.413839102 CEST	8080	49894	51.91.7.5	192.168.2.7
Jul 20, 2022 01:10:07.675220966 CEST	49895	80	192.168.2.7	131.100.24.231
Jul 20, 2022 01:10:07.809349060 CEST	80	49895	131.100.24.231	192.168.2.7
Jul 20, 2022 01:10:07.809556961 CEST	49895	80	192.168.2.7	131.100.24.231
Jul 20, 2022 01:10:07.963644981 CEST	49895	80	192.168.2.7	131.100.24.231
Jul 20, 2022 01:10:08.096733093 CEST	80	49895	131.100.24.231	192.168.2.7
Jul 20, 2022 01:10:08.117975950 CEST	80	49895	131.100.24.231	192.168.2.7
Jul 20, 2022 01:10:08.118000984 CEST	80	49895	131.100.24.231	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jul 20, 2022 01:07:22.943972111 CEST	120.50.40.183	192.168.2.7	60b5	(Unknown)	Destination Unreachable
Jul 20, 2022 01:07:25.979613066 CEST	120.50.40.183	192.168.2.7	60b5	(Unknown)	Destination Unreachable
Jul 20, 2022 01:07:31.993840933 CEST	120.50.40.183	192.168.2.7	60b5	(Unknown)	Destination Unreachable

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	192.168.2.7	49764	149.56.128.192	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-19 23:06:48 UTC	0	OUT	GET /fSTm HTTP/1.1 Cookie: RCgcztBeyqV=lnFDO8M7QZ1oPgB4nY1cj9kEItiu+1lC4kYVxBoxBllfbtHBCudUYjnRoBy8SYXV1srkUR bSy/IsFNQ+ucZuSoKtKE0A5BmVzVszJ57xNbQiII6AXjiVwF9fZa5yKYDVvPEpBhl22lgyuByb+bvkutsXjB2JpqNE fh4g+cnQNOBmZjpGug7GM9O03vTF2D7uGgC81sfYU6tCwLuyKOvpdyEei5sFj+shvwDs+JDlyi5zLxE/FuyzCk3X+e flKtNFb5X94ruZkldL Host: 149.56.128.192 Connection: Keep-Alive Cache-Control: no-cache

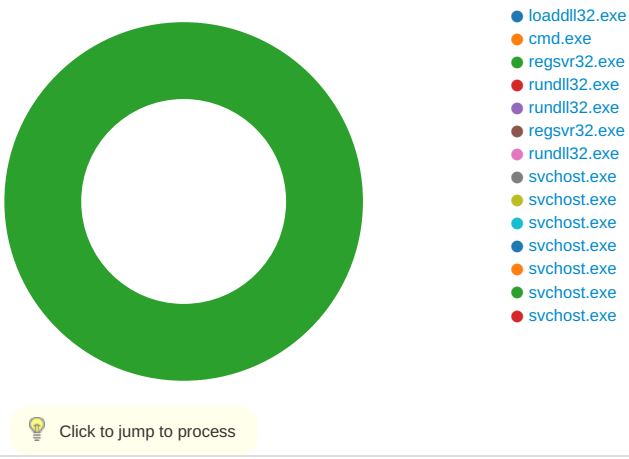
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49856	46.55.222.11	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-07-19 23:08:26 UTC	0	OUT	GET /BiEgOdFqxzyfFPqwAOweHeXemJBZKjqwNwwVobqyTY HTTP/1.1 Cookie: hwPnhB=lnFDO8M7QZ1oPgB4nY1cj9kEItiu+1IC4kYVxBoxBllfbtHBCudUYjnRoBy8SYXV1srkURbSy/IsFNQ+ucZuSoKtKE0A5BmVzVszJ57xNbQiIl6AXjiVwF9fZa5yKYDVvPEpBhl22lgyuByb+bvkutsXjB2JpqNEfh4g+cnQNOBmZjpGug7GM9O03vTF2D7uGgC81sfYU6tCwLuyKOvpd81D4rN1AGkvWGjCmOQEyJVKCjHD95//Nxae/txUYJ5SwYpA/5OYvY6zhTXw98PfWocrrg1l/8T7yt9faC2eGs5YaD2HKU6Z4U7+QDaKwy9bRKPIQC74SA== Host: 46.55.222.11 Connection: Keep-Alive Cache-Control: no-cache
2022-07-19 23:08:26 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 19 Jul 2022 23:08:26 GMT Content-Type: text/html Content-Length: 162 Connection: close
2022-07-19 23:08:26 UTC	0	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



System Behavior

Analysis Process: loaddll32.exe PID: **7008**, Parent PID: **1556**

General

Target ID:	0
Start time:	01:06:25
Start date:	20/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll"
Imagebase:	0x320000
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: 7032, Parent PID: 7008

General

Target ID:	1
Start time:	01:06:25
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll",#1
Imagebase:	0xdd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 7040, Parent PID: 7008

General

Target ID:	2
Start time:	01:06:25
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\bscHLGMyjW.dll
Imagebase:	0x970000
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: 00000002.00000002.363189239.0000000004B81000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.363189239.0000000004B81000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.361757163.0000000003150000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.361757163.0000000003150000.00000040.00001000.00020000.00000000.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\Mjzwixkz\jiugg.vcz:Zone.Identifier	success or wait	1	4B9594F	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: **7052**, Parent PID: **7032**

General

Target ID:	3
Start time:	01:06:26
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\bscHLGMyjW.dll",#1
Imagebase:	0x13e0000
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: 00000003.00000002.359006501.0000000003590000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.359006501.0000000003590000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.359233383.0000000004C21000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.359233383.0000000004C21000.00000020.00001000.00020000.00000000.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: **7064**, Parent PID: **7008**

General

Target ID:	4
Start time:	01:06:26
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\bscHLGMyjW.dll,DllRegisterServer
Imagebase:	0x13e0000
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: 00000004.00000002.361541102.0000000004DB1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.361541102.0000000004DB1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.361265936.0000000003550000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.361265936.0000000003550000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **7140**, Parent PID: **7040**

General

Target ID:	5
Start time:	01:06:29
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\Mjzwixkz\jiugg.vcz"
Imagebase:	0x970000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.874265286.0000000004DF1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.874265286.0000000004DF1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.874183013.0000000004DC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.874183013.0000000004DC0000.00000040.00001000.00020000.00000000.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: rundll32.exe PID: **7164**, Parent PID: **7008**

General

Target ID:	6
Start time:	01:06:30
Start date:	20/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\bscHLGMyjW.dll,DllUnregisterServerr
Imagebase:	0x13e0000
File size:	61952 bytes

MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5504, Parent PID: 604

General

Target ID:	10
Start time:	01:06:50
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6412, Parent PID: 604

General

Target ID:	13
Start time:	01:07:03
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7068, Parent PID: 604

General

Target ID:	15
Start time:	01:07:13
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p

Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5600, Parent PID: 604

General

Target ID:	19
Start time:	01:07:36
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:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2320, Parent PID: 604

General

Target ID:	21
Start time:	01:07:51
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **1640**, Parent PID: **604**

General

Target ID:	25
Start time:	01:08:07
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **7164**, Parent PID: **604**

General

Target ID:	30
Start time:	01:08:54
Start date:	20/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Disassembly

No disassembly