ID: 672062
Sample Name: 548IrCt4hj
Cookbook: default.jbs
Time: 04:55:07
Date: 23/07/2022
Version: 35.0.0 Citrine

Table of Contents

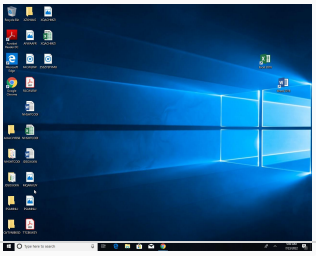
Windows Analysis Report

548IrCt4hj

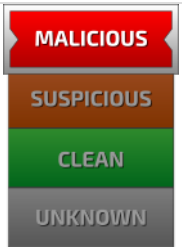
Overview

General Information

Sample Name:	548IrCt4hj (renamed file extension from none to dll)
Analysis ID:	672062
MD5:	7301880b88f87c..
SHA1:	c8a2b0ae061b61..
SHA256:	c409ad4f64a1ad..
Tags:	exe OpenCTIBR Sandboxed
Infos:	



Detection



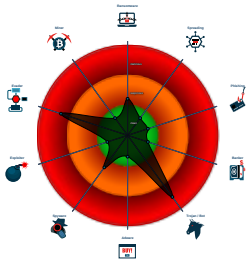
Emotet

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- 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**
- loaddll64.exe (PID: 6432 cmdline: loaddll64.exe "C:\Users\user\Desktop\548IrCt4hj.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6488 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6516 cmdline: rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6504 cmdline: regsvr32.exe /s C:\Users\user\Desktop\548IrCt4hj.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6692 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZPLPsNKH\eFntQ.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6536 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllCanUnloadNow MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6704 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6776 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 7076 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5072 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3972 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6700 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6636 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6092 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "139.59.80.108:8080",
    "83.229.80.93:8080",
    "190.107.19.179:443",
    "202.134.4.210:7080",
    "165.232.185.110:8080",
    "104.244.79.94:443",
    "198.199.70.22:8080",
    "37.44.244.177:8080",
    "195.77.239.39:8080",
    "103.85.95.4:8080",
    "85.214.67.203:8080",
    "103.41.204.169:8080",
    "78.47.204.80:443",
    "190.145.8.4:443",
    "139.196.72.155:8080",
    "87.106.97.83:7080",
    "202.29.239.162:443",
    "202.28.34.99:8080",
    "54.37.106.167:8080",
    "103.224.241.74:8080",
    "103.254.12.236:7080",
    "188.165.79.151:443",
    "43.129.209.178:443",
    "37.187.114.15:8080",
    "5.253.30.17:7080",
    "54.37.228.122:443",
    "157.230.99.206:8080",
    "103.56.149.105:8080",
    "157.245.111.0:8080",
    "128.199.242.164:8080",
    "104.248.225.227:8080",
    "88.217.172.165:8080",
    "175.126.176.79:8080",
    "85.25.120.45:8080",
    "178.62.112.199:8080",
    "178.238.225.252:8080",
    "93.104.209.107:8080",
    "210.57.209.142:8080",
    "128.199.217.206:443",
    "103.71.99.57:8080",
    "64.227.55.231:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0EZiWsQAQAIg=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW45gAsQAmAIg="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.424123479.000001E034440000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.940693332.0000000000C20000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.427012616.0000000001120000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.422757747.000001F33EB00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000A.00000002.940812969.00000000024B1000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.1e034440000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.rundll32.exe.1f33eb00000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.1120000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.1e034440000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
10.2.regsvr32.exe.c20000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.5 - Destination IP: 174.138.33.49

Timestamp:	192.168.2.5174.138.33.494976870802404316 07/23/22-04:56:42.473067
SID:	2404316
Source Port:	49768
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

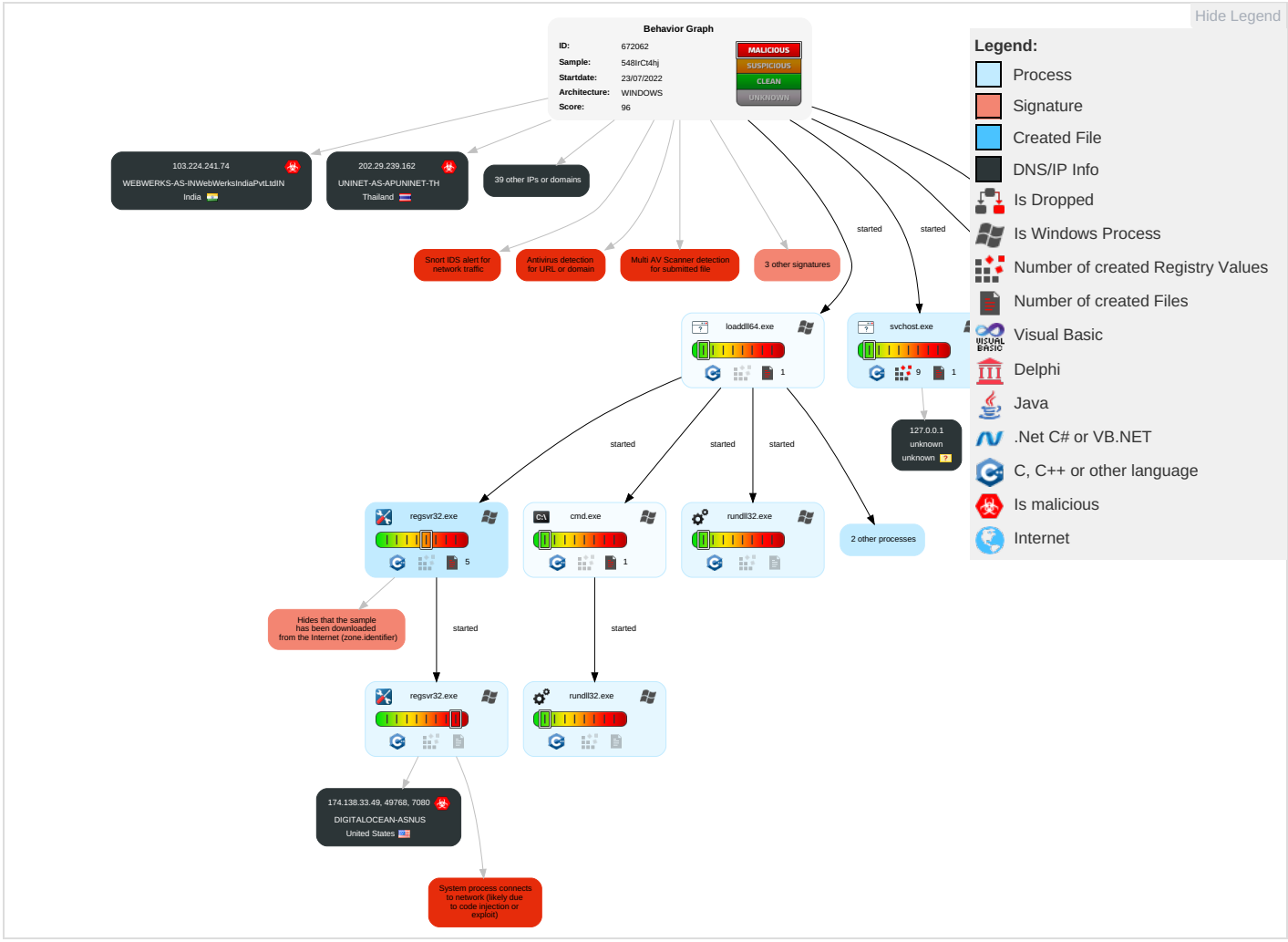
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 Virtualization/Sandbox Evasion	LSASS Memory	5 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	3 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	3 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

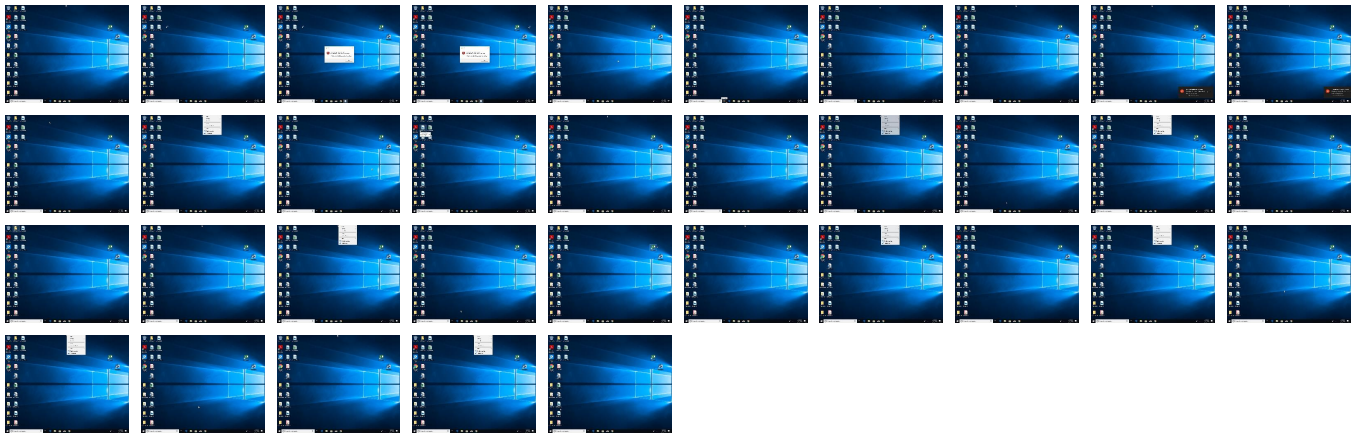
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
548IrCt4hj.dll	70%	Virustotal		Browse
548IrCt4hj.dll	46%	Metadefender		Browse
548IrCt4hj.dll	88%	ReversingLabs	Win64.Trojan.Emotet	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.regsvr32.exe.1120000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
10.2.regsvr32.exe.c20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.rundll32.exe.1f33eb00000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.rundll32.exe.1e034440000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://174.138.33.49/Z	100%	Avira URL Cloud	malware	
http://https://174.138.33.49:7080/F	100%	Avira URL Cloud	malware	
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/Only	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/r	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://174.138.33.49:7080/p	100%	Avira URL Cloud	malware	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://174.138.33.49/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

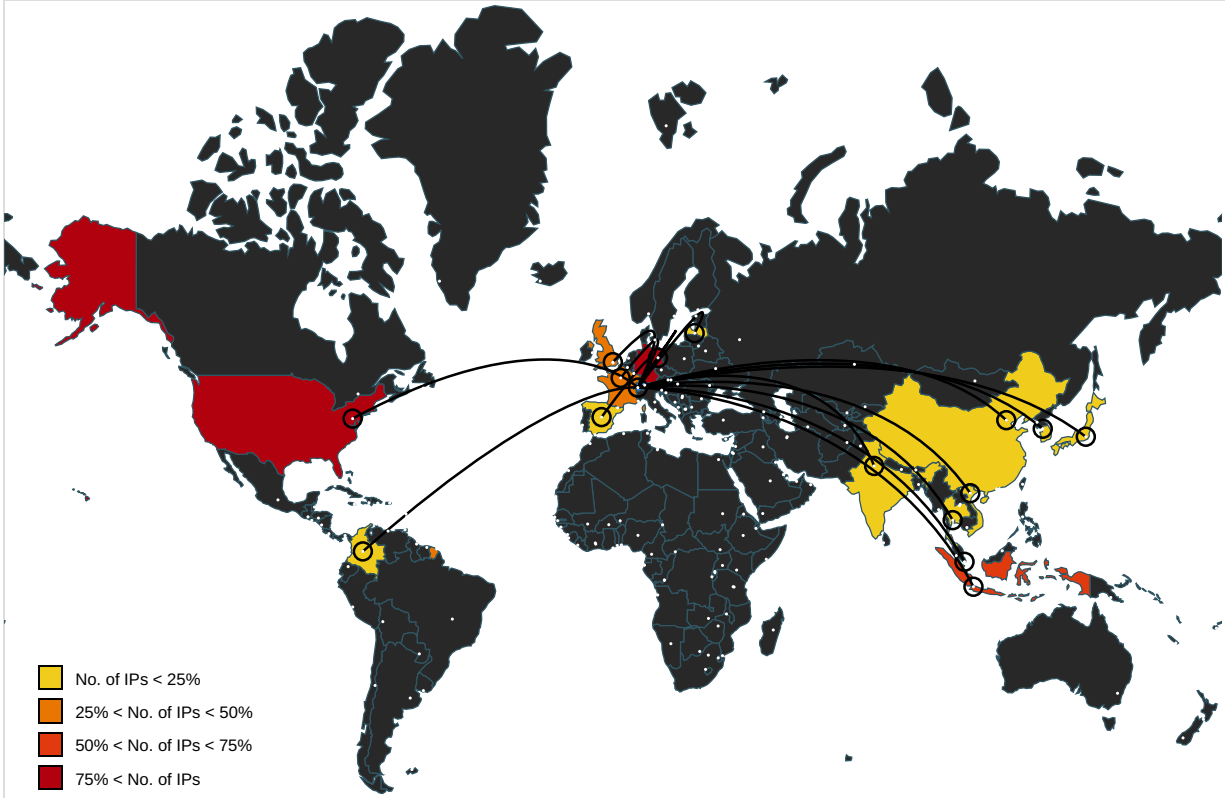
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000019.00000003.568619378.0000015F2D586000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.568197795.0000015F2D598000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000019.00000003.568619378.0000015F2D586000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.568197795.0000015F2D598000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49/Z	regsvr32.exe, 0000000A.00000002.940330437.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://174.138.33.49:7080/F	regsvr32.exe, 0000000A.00000002.940330437.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://174.138.33.49:7080/	regsvr32.exe, 0000000A.00000002.940330437.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000019.00000003.563618298.0000015F2D599000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563853374.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563634572.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563884423.0000015F2DA19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563734310.0000015F2D587000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563691195.0000015F2DA03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563660153.0000015F2DA02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/Only	regsvr32.exe, 0000000A.00000002.94033043.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.pango.co/privacy	svchost.exe, 00000019.00000003.563618298.0000015F2D599000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563853374.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563634572.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563884423.0000015F2DA19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563734310.0000015F2D587000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563691195.0000015F2DA03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563660153.0000015F2DA02000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 00000019.00000003.568619378.0000015F2D586000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.568197795.0000015F2D598000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49:7080/r	regsvr32.exe, 0000000A.00000002.94033043.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.ver)	svchost.exe, 00000013.00000002.836139820.00000188934BB000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.835512145.00000188934BB000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000002.595043128.0000015F2CCE9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://174.138.33.49:7080/p	regsvr32.exe, 0000000A.00000002.94033043.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000019.00000003.572982528.0000015F2D59A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.572906706.0000015F2D5B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.572968023.0000015F2D589000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.573008527.0000015F2DA02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.572949834.0000015F2D5B0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 00000019.00000003.568619378.0000015F2D586000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.568197795.0000015F2D598000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 00000019.00000003.563618298.0000015F2D599000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563853374.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563634572.0000015F2D5A9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563884423.0000015F2DA19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563734310.0000015F2D587000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563691195.0000015F2DA03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.563660153.0000015F2DA02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49/	regsvr32.exe, 0000000A.00000002.940330437.0000000000B21000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.480216789.0000000000B21000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.37.106.167	unknown	France		16276	OVHFR	true
188.165.79.151	unknown	France		16276	OVHFR	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
174.138.33.49	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
43.129.209.178	unknown	Japan		4249	LILLY-ASUS	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
5.253.30.17	unknown	Latvia		18978	ENZUINC-US	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
83.229.80.93	unknown	United Kingdom		8513	SKYVISIONGB	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
37.187.114.15	unknown	France		16276	OVHFR	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
128.199.242.164	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
54.37.228.122	unknown	France		16276	OVHFR	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	672062
Start date and time: 23/07/202204:55:07	2022-07-23 04:55:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	548IrCt4hj (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:	mal96.troj.evad.winDLL@21/5@0/44
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:56:49	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24948615150342127
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4X:BJiRdwfu2SRU4X
MD5:	8302100D8C0781AFFA569599554A747D
SHA1:	2AD4A77D9A42C5905F5B8FBAAACCFAB60CA60CD3
SHA-256:	8F307CAB2013948ADA4DFE98A26132AC3BDF98B917EB84BBA843DE5977A18C05
SHA-512:	66FECADDA311CE2AF81A7F4875E4F775581373BD23C1F2AA5C2136A174B6814EAB09A98DA9A98CA6834B1123A1740D2FF1524C5A643A6D16B6A4945BCE9DA0 F2
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9292e26a, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2507291590936865
Encrypted:	false

SSDEEP:	384:L7U+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:L7rSB2nSB2RSjlK/+mLesOj1J2
MD5:	C50F19CC34E36AE9D8945ECDF6CABAD5
SHA1:	15A5137868B1A5D0B8BC5E506A12052CE5CB0AA1
SHA-256:	C9A0DFC6BC8086E76E08B4237104495011053AFF5F8DC0D99735BD3A55563327
SHA-512:	E660C4EE50CD6F3DE9CF6C3F790B464CC5EE03173DF58DFF1F1D7C11D454DA880F6B85BCB5C54FCA4032D8AE62420E175CDFB8E80112EA32388DFD1DECE102E
Malicious:	false
Preview:	...j... .....e.f.3...w.....)....:;...z..18...z..h.(....:;...z....).....3...w.....B.....@..... ....E...:;...z.....\:;...z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07701426796525257
Encrypted:	false
SSDEEP:	3:kmtR7vUduyi0f2l/of7CnEe9irtlNyfeuZCl/ill3VkttlmlnI:vtRrUDf2lwf2ntI6Ole3
MD5:	3356637935306EB31EC34EF8F4F51FDE
SHA1:	C1F3106EFAB78E6B7AD03FEBEDBA313849D71462
SHA-256:	01E4C7BAED15BB1CBCB4358951970B0080D9F3CE5652A3076424C5C6F767903B
SHA-512:	F639059B00AB53B6F6473F054E9CF1540FC52EA55940320A2E960583B5E2409C89F4739AB75B03C26085FC114EC99AB35137FE0690B8E3F3A2EEB9B818102EBA
Malicious:	false
Preview:	..4.....3...w..18...z..:;...z.....:;...z..:;...z.....:;...z.g.....\:;...z..... ....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.301831913358297
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	548IrCt4hj.dll
File size:	962048
MD5:	7301880b88f87cd3a593f7106d5743cc
SHA1:	c8a2b0ae061b612f4d4a4cfc4ee3e1f7079b4240

SHA256:	c409ad4f64a1ad925ffbfdb88f57dd9177123364a1875caf6cbb6f5ba3970cc3
SHA512:	3abf4d6b0725cae5fd05edccdac75e5061ebcc033e24fbd73482fabe53bd1f914490f3bfda638bd623e642200e8499539b0541bb95d5c7040410d2ff209a640a
SSDEEP:	12288:kvyPTUfrN+lSDLV9dRCYFdVlv6jVBv4w8N6zTlvdEywUshhxmIssuqvY/J9ujv7X:k6Ufgl15qhxm1qvY2leXA
TLSH:	0515BF6677E81291D0B7D13F8AA78B49EAF2BC041734A7CB0184525D2F23BD85A3F725
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....71x.V_+.V_+.V_+p$*.V_+p$Z*&V_+.# [*.V_+.#*.V_+.#Z*.V_+p$[*.V_+p$^*.V_+.V^+ V_+b#Z*.V_+b#_*.V_+b#.+.V_+.V.+.V_+b#]*.V_+Rich.V_

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000110e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, NX_COMPAT
Time Stamp:	0x62C329A8 [Mon Jul 4 17:55:52 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c8e804de36681c3fb89b2f7688123f2b

Entrypoint Preview

Instruction
jmp 00007F2F1CD86BDEh
jmp 00007F2F1CDDD9C5h
jmp 00007F2F1CD9B3ECh
jmp 00007F2F1CDC6AABh
jmp 00007F2F1CDBA522h
jmp 00007F2F1CD9E8E1h
jmp 00007F2F1CD85270h
jmp 00007F2F1CD99933h
jmp 00007F2F1CD79DEAh
jmp 00007F2F1CDA7131h
jmp 00007F2F1CDA4F6Ch
jmp 00007F2F1CDA720Bh
jmp 00007F2F1CDC9686h
jmp 00007F2F1CD7F4E1h
jmp 00007F2F1CD87294h
jmp 00007F2F1CD99937h
jmp 00007F2F1CDE83DEh
jmp 00007F2F1CDA0781h
jmp 00007F2F1CDC4B98h
jmp 00007F2F1CDB7D13h
jmp 00007F2F1CDD8B16h
jmp 00007F2F1CDD23B5h
jmp 00007F2F1CDB1E44h
jmp 00007F2F1CDC3DC3h

Instruction
jmp 00007F2F1CDC41A6h
jmp 00007F2F1CDE8485h
jmp 00007F2F1CDD1DE0h
jmp 00007F2F1CD8A2FFh
jmp 00007F2F1CD88E16h
jmp 00007F2F1CDC5A9Dh
jmp 00007F2F1CD8A7A4h
jmp 00007F2F1CDCF6C3h
jmp 00007F2F1CDCDBE6h
jmp 00007F2F1CD9A6FDh
jmp 00007F2F1CD8EE28h
jmp 00007F2F1CDC7E33h
jmp 00007F2F1CD9A902h
jmp 00007F2F1CDDB649h
jmp 00007F2F1CDB7C9Ch
jmp 00007F2F1CD99A3Fh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xb07c0	0x1c9	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbb6e8	0x8c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x30ebd	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0xb5000	0x4ea8	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf0000	0xd78	.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	0xa6320	0x138	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xbb000	0x6e8	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0x8a5ca	0x8a600	False	0.3069634993224932	data	5.641927945052085	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8c000	0x24989	0x24a00	False	0.2668981975255973	data	4.201809080615527	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xb1000	0x3960	0x1800	False	0.13834635416666666	data	2.2672137141142894	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0xb5000	0x57a8	0x5800	False	0.5007990056818182	data	5.516669615542349	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0xbb000	0x18d1	0x1a00	False	0.2459435096153846	data	3.49134963905175	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.00cfg	0xbd000	0x151	0x200	False	0.05859375	data	0.3458273094223054	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0xbe000	0x222	0x400	False	0.16796875	data	1.4491445801684228	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x30ebd	0x31000	False	0.8592952806122449	data	7.7601261539979545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xf0000	0x194d	0x1a00	False	0.21875	data	3.637638102515201	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
REGISTRY	0xbf19c	0x1d4	ASCII text	English	United States
TYPELIB	0xbf370	0x3398	data	English	United States
RT_STRING	0xc2708	0x36	data	English	United States
RT_HTML	0xc2740	0x2d600	data	English	United States
RT_MANIFEST	0xefd40	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
ODBC32.dll	
KERNEL32.dll	FlushFileBuffers, SetStdHandle, SetFilePointerEx, EncodePointer, DecodePointer, RaiseException, GetLastError, QueryPerformanceFrequency, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, VirtualAlloc, DisableThreadLibraryCalls, WriteFile, GetModuleFileNameW, GetModuleHandleW, GetProcAddress, LoadLibraryExW, LoadResource, SizeofResource, FindResourceW, lstrcmpiW, MultiByteToWideChar, GetFileSizeEx, GetStringTypeW, SetConsoleCtrlHandler, GetProcessHeap, EnumSystemLocalesW, GetUserDefaultLCID, GetConsoleOutputCP, GetConsoleMode, ReadFile, ReadConsoleW, CloseHandle, CreateFileW, WriteConsoleW, FreeLibrary, SetUnhandledExceptionFilter, IsValidLocale, GetLocaleInfoW, LCMapStringW, CompareStringW, GetTimeFormatW, GetDateFormatW, FlsFree, FlsSetValue, FlsGetValue, FlsAlloc, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, WideCharToMultiByte, IsDebuggerPresent, OutputDebugStringW, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, RtlUnwind, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, RtlUnwindEx, InterlockedPushEntrySList, InterlockedFlushSList, SetLastError, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, ExitProcess, GetModuleHandleExW, GetCurrentThread, HeapFree, HeapAlloc, HeapSize, HeapReAlloc, GetStdHandle, GetFileType, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW
USER32.dll	ShowWindow, CharNextW, UnregisterClassW, MessageBoxA
ADVAPI32.dll	RegQueryInfoKeyW, RegOpenKeyExW, RegEnumKeyExW, RegDeleteValueW, RegDeleteKeyW, RegCreateKeyExW, RegCloseKey, RegSetValueExW
ole32.dll	CoCreateInstance, CoCreateFreeThreadedMarshaler, CoTaskMemAlloc, CoTaskMemRealloc, CoTaskMemFree, CoInitialize, StringFromGUID2
OLEAUT32.dll	LoadTypeLib, UnRegisterTypeLib, VarUI4FromStr, SysFreeString, SysAllocString

Exports

Name	Ordinal	Address
DllCanUnloadNow	1	0x180003102
DllGetClassObject	2	0x180003be3
DllRegisterServer	3	0x1800013fc
DllUnregisterServer	4	0x180003521

Possible Origin

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

Network Behavior

Snort IDS Alerts

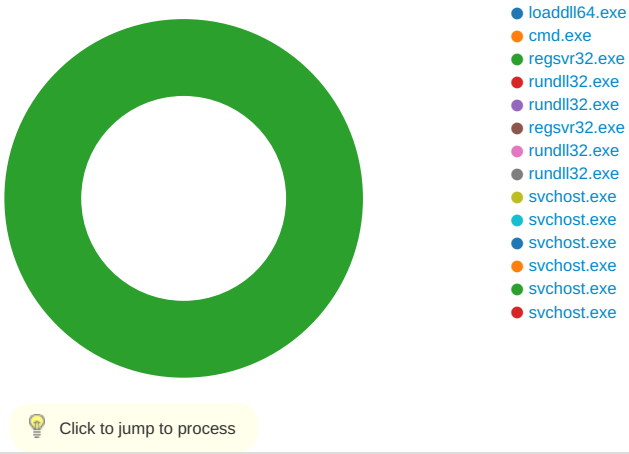
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5174.138.33.49 4976870802404316 07/23/22-04:56:42.473067	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49768	7080	192.168.2.5	174.138.33.49

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 23, 2022 04:56:42.473067045 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:42.574515104 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:42.574670076 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:42.607347012 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:42.713720083 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:42.744929075 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:42.744982958 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:42.745028019 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:42.745078087 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:43.195605040 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:43.300020933 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:43.300179005 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:43.303195000 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:43.444097042 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:43.895623922 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:43.896034956 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:46.909363031 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:46.909475088 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:56:46.909478903 CEST	7080	49768	174.138.33.49	192.168.2.5
Jul 23, 2022 04:56:46.909584045 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:58:32.400583029 CEST	49768	7080	192.168.2.5	174.138.33.49
Jul 23, 2022 04:58:32.400631905 CEST	49768	7080	192.168.2.5	174.138.33.49

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **6432**, Parent PID: **4780**

General	
Target ID:	3
Start time:	04:56:13
Start date:	23/07/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\548IrCt4hj.dll"
Imagebase:	0x7ff6044c0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: 6488, Parent PID: 6432

General	
Target ID:	4
Start time:	04:56:14
Start date:	23/07/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 6504, Parent PID: 6432

General	
Target ID:	5
Start time:	04:56:14
Start date:	23/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\548IrCt4hj.dll
Imagebase:	0x7ff776530000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.427012616.0000000001120000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.427064425.0000000001151000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\ZPLPsNKH\eFntQ.dll:Zone.Identifier	success or wait	1	116ED93	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: **6516**, Parent PID: **6488**

General

Target ID:	6
Start time:	04:56:14
Start date:	23/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1
Imagebase:	0x7ff79d320000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.422757747.000001F33EB00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.422895400.000001F33EC51000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6536**, Parent PID: **6432**

General

Target ID:	7
Start time:	04:56:14
Start date:	23/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllCanUnloadNow
Imagebase:	0x7ff79d320000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.424123479.000001E034440000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.424307117.000001E034471000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6692**, Parent PID: **6504**

General

Target ID:	10
Start time:	04:56:17
Start date:	23/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZPLPsNKH\eFntQ.dll"
Imagebase:	0x7ff776530000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.940693332.0000000000C20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.940812969.00000000024B1000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 0000000A.00000002.940180760.0000000000AEB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6704**, Parent PID: **6432**

General

Target ID:	11
Start time:	04:56:18
Start date:	23/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllGetClassObject
Imagebase:	0x7ff79d320000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6776**, Parent PID: **6432**

General

Target ID:	12
Start time:	04:56:21
Start date:	23/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllRegisterServer
Imagebase:	0x7ff79d320000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

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

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7076**, Parent PID: **580**

General

Target ID:	16
Start time:	04:56:35
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5072**, Parent PID: **580**

General

Target ID:	18
Start time:	04:56:42
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3972**, Parent PID: **580**

General

Target ID:	19

Start time:	04:56:49
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6700**, Parent PID: **580**

General

Target ID:	20
Start time:	04:56:58
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6636**, Parent PID: **580**

General

Target ID:	21
Start time:	04:56:59
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6092**, Parent PID: **580**

General

Target ID:	25
Start time:	04:57:11
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly