ID: 672062
Sample Name: 548IrCt4hj.dll
Cookbook: default.jbs
Time: 05:06:03
Date: 23/07/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report 548IrCt4hj.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Stealing of Sensitive Information 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 13
Public IPs 14
Private 14
General Information 15
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\ProgramData\Microsoft\Network\Downloader\edb.chk 16
C:\ProgramData\Microsoft\Network\Downloader\edb.log 16
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db 17
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm 17
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 17
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 18
C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp 18
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log 18
Static File Info 18
General 18
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 19
Data Directories 20
Sections 20
Resources 21
Imports 21
Exports 21
Possible Origin 21
Network Behavior 22
Snort IDS Alerts 22
TCP Packets 22
Statistics 22

Behavior 22
System Behavior 23
Analysis Process: loaddll64.exePID: 5724, Parent PID: 3608 23
General 23
File Activities 23
Analysis Process: cmd.exePID: 244, Parent PID: 5724 23
General 23
File Activities 23
Analysis Process: regsvr32.exePID: 4760, Parent PID: 5724 23
General 23
File Activities 24
File Deleted 24
Analysis Process: rundll32.exePID: 3080, Parent PID: 244 24
General 24
Analysis Process: rundll32.exePID: 2924, Parent PID: 5724 24
General 24
Analysis Process: regsvr32.exePID: 5996, Parent PID: 4760 25
General 25
File Activities 25
Analysis Process: rundll32.exePID: 3740, Parent PID: 5724 25
General 25
File Activities 25
Analysis Process: rundll32.exePID: 2560, Parent PID: 5724 26
General 26
File Activities 26
Analysis Process: svchost.exePID: 1012, Parent PID: 564 26
General 26
Analysis Process: svchost.exePID: 1428, Parent PID: 564 26
General 26
File Activities 26
Registry Activities 27
Analysis Process: svchost.exePID: 5892, Parent PID: 564 27
General 27
File Activities 27
Analysis Process: svchost.exePID: 4348, Parent PID: 564 27
General 27
Registry Activities 27
Analysis Process: svchost.exePID: 2572, Parent PID: 564 27
General 27
Analysis Process: SgrmBroker.exePID: 3628, Parent PID: 564 28
General 28
Analysis Process: svchost.exePID: 3532, Parent PID: 564 28
General 28
Registry Activities 28
Analysis Process: svchost.exePID: 5732, Parent PID: 564 28
General 28
File Activities 29
Analysis Process: svchost.exePID: 5244, Parent PID: 564 29
General 29
File Activities 29
Analysis Process: svchost.exePID: 6272, Parent PID: 564 29
General 29
File Activities 30
Registry Activities 30
Analysis Process: svchost.exePID: 6280, Parent PID: 564 30
General 30
File Activities 30
Analysis Process: svchost.exePID: 6532, Parent PID: 564 30
General 30
File Activities 30
Analysis Process: svchost.exePID: 6756, Parent PID: 564 31
General 31
File Activities 31
Analysis Process: MpCmdRun.exePID: 6056, Parent PID: 3532 31
General 31
File Activities 31
File Written 31
Analysis Process: conhost.exePID: 5948, Parent PID: 6056 33
General 33
Disassembly 33

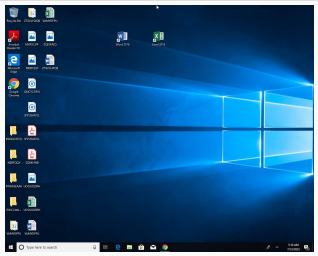
Windows Analysis Report

548IrCt4hj.dll

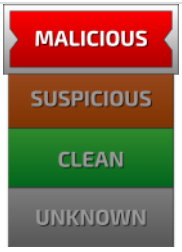
Overview

General Information

Sample Name:	548IrCt4hj.dll
Analysis ID:	672062
MD5:	7301880b88f87c..
SHA1:	c8a2b0ae061b61..
SHA256:	c409ad4f64a1ad..
Tags:	exe OpenCTIBR Sandboxed
Infos:	



Detection



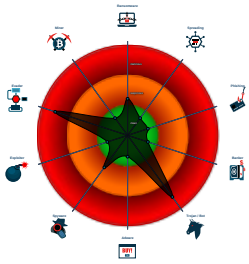
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Changes security center settings (n…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query local…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5724 cmdline: loaddll64.exe "C:\Users\user\Desktop\548IrCt4hj.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 244 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3080 cmdline: rundll32.exe "C:\Users\user\Desktop\548IrCt4hj.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 4760 cmdline: regsvr32.exe /s C:\Users\user\Desktop\548IrCt4hj.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5996 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MbnmzGnNg\joXcB.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 2924 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllCanUnloadNow MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3740 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2560 cmdline: rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 1012 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1428 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5892 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4348 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2572 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3628 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 3532 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6056 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 5732 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5244 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6272 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6280 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6532 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "118.98.72.86:443",
    "85.214.67.203:8080",
    "103.254.12.236:7080",
    "43.129.209.178:443",
    "88.217.172.165:8080",
    "78.47.204.80:443",
    "103.41.204.169:8080",
    "178.238.225.252:8080",
    "188.165.79.151:443",
    "104.244.79.94:443",
    "157.245.111.0:8080",
    "93.104.209.107:8080",
    "178.62.112.199:8080",
    "103.56.149.105:8080",
    "198.199.70.22:8080",
    "175.126.176.79:8080",
    "46.101.98.60:8080",
    "202.28.34.99:8080",
    "165.22.254.236:8080",
    "139.59.80.108:8080",
    "5.253.30.17:7080",
    "190.145.8.4:443",
    "54.37.228.122:443",
    "54.37.106.167:8080",
    "188.225.32.231:4143",
    "103.126.216.86:443",
    "196.44.98.190:8080",
    "104.248.225.227:8080",
    "37.44.244.177:8080",
    "87.106.97.83:7080",
    "64.227.55.231:8080",
    "210.57.209.142:8080",
    "83.229.80.93:8080",
    "174.138.33.49:7080",
    "85.25.120.45:8080",
    "139.196.72.155:8080",
    "190.107.19.179:443",
    "103.85.95.4:8080",
    "157.230.99.206:8080",
    "195.77.239.39:8080",
    "128.199.242.164:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0ObJw/wAXAJA=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWwrKX/wAcAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.637949653.0000000000E40000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.249040025.000001C7434E0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.638413256.0000000000EA8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3		Joe Security	
00000003.00000002.248792041.000001F26FD71000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.638139112.0000000000E71000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.2060000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.1f26fd40000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.e40000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.2060000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.regsvr32.exe.e40000.0.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)

Lowering of HIPS / PFW / Operating System Security Settings

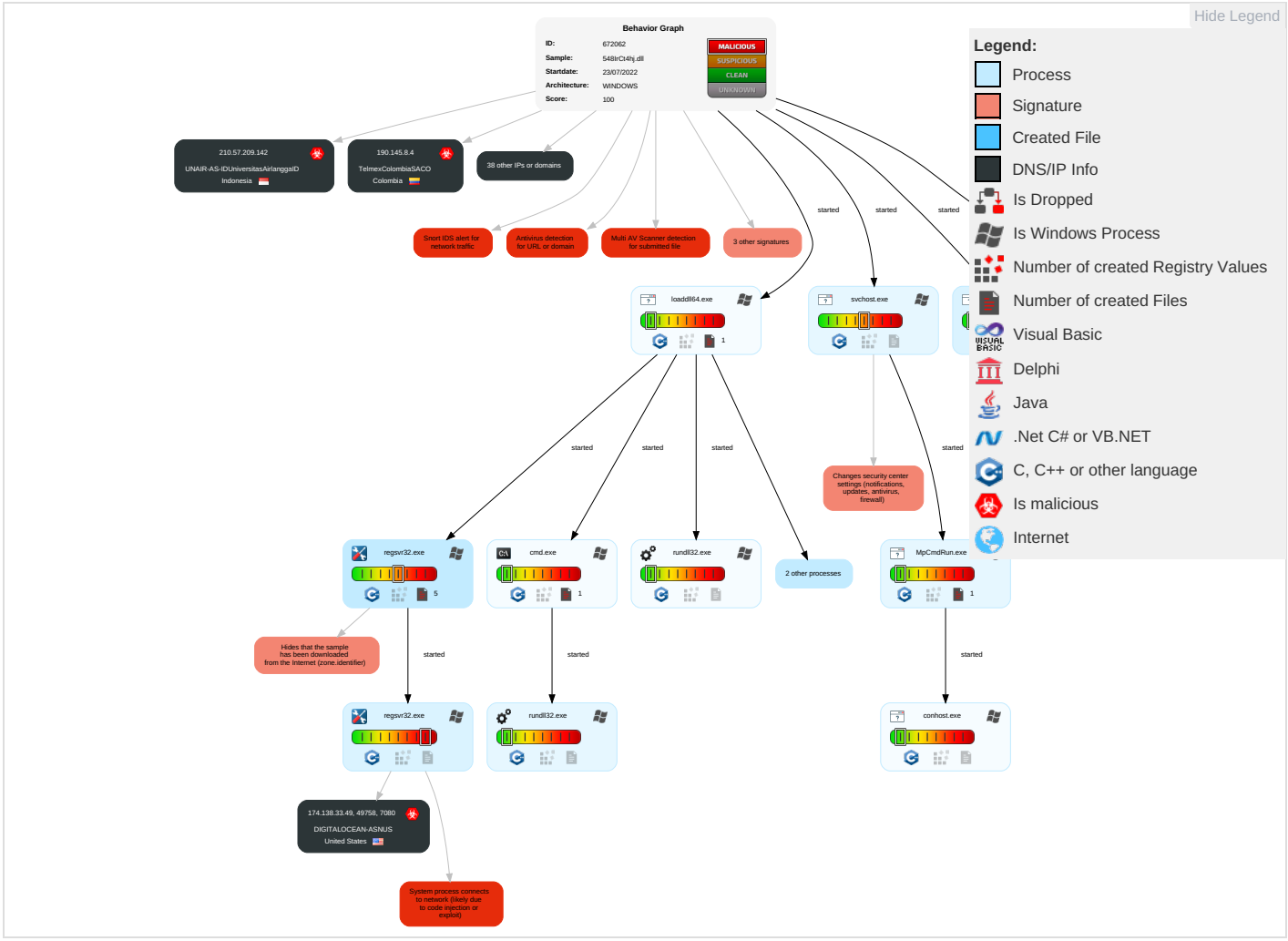
Changes security center settings (notifications, updates, antivirus, firewall)

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 1 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	1 Disable or Modify Tools	LSASS Memory	7 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)	3 Virtualization/Sandbox Evasion	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 1 1 Process Injection	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 Deobfuscate/Decode Files or Information	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	1 Hidden Files and Directories	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	2 Obfuscated Files or Information	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 Regsvr32	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 Rundll32	/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 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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
4.2.rundll32.exe.1c7434e0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.1f26fd40000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.regsvr32.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.regsvr32.exe.2060000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://174.138.33.49:7080/	0%	URL Reputation	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://174.138.33.49/U	100%	Avira URL Cloud	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://174.138.33.49:7080/hIn	100%	Avira URL Cloud	malware	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://174.138.33.49/Q	100%	Avira URL Cloud	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

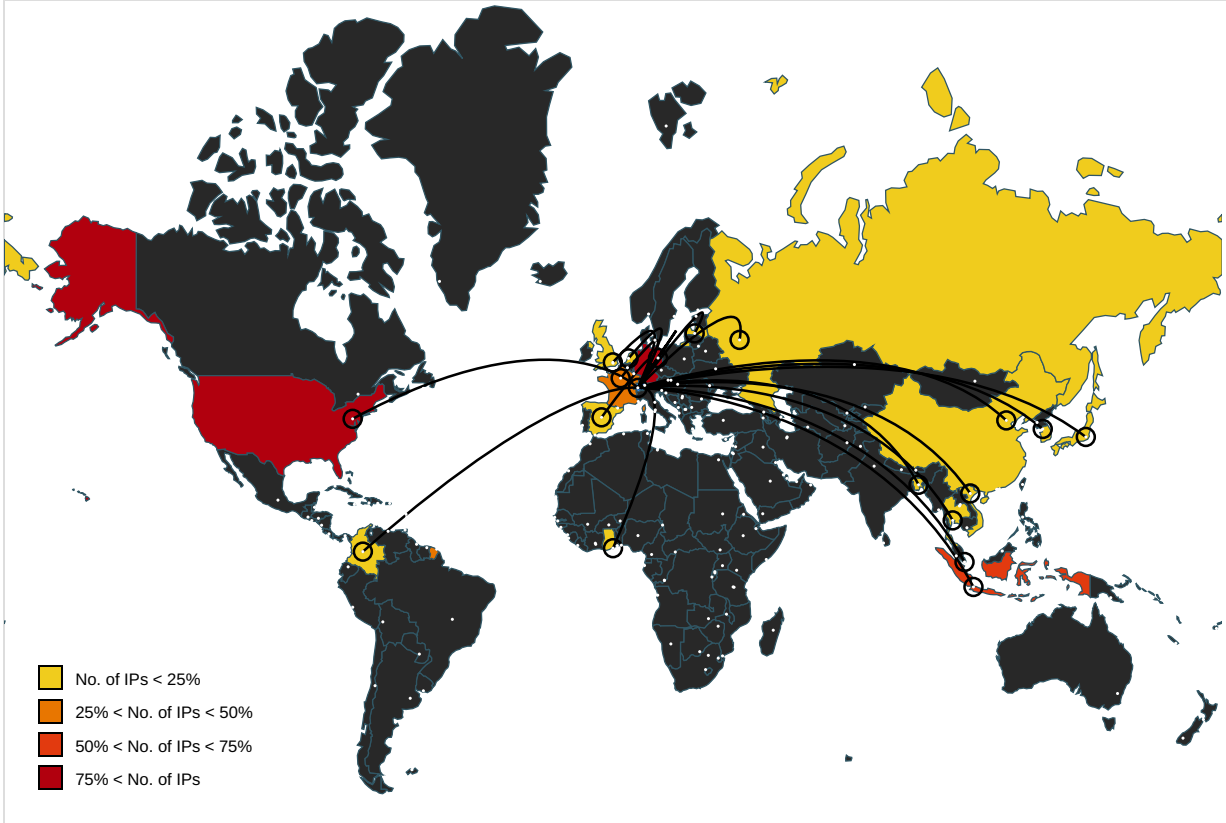
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000F.00000002.316427386.00000226FA03D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000F.00000002.316440979.00000226FA040000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000F.00000002.316383374.00000226FA029000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000F.00000002.316448338.00000226FA042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316054783.00000226FA041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000F.00000003.315949220.00000226FA04B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000F.00000002.316448338.00000226FA042000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316054783.00000226FA041000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/	regsvr32.exe, 00000005.00000003.543111893.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.638413256.0000000000EA8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.638784137.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000019.00000003.404927903.000001A111A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.404982809.000001A111593000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405001225.000001A1115A4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405032312.000001A111A02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000019.00000003.404927903.000001A111A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.404982809.000001A111593000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405001225.000001A1115A4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405032312.000001A111A02000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/mapcontrol/roadshield.ashx?bucket=	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000F.00000002.316348056.00000226FA013000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000F.00000002.316427386.00000226FA03D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000019.00000003.408103656.000001A111599000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://174.138.33.49/U	regsvr32.exe, 00000005.00000003.543111893.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.638784137.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000F.00000003.316049267.00000226FA045000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000F.00000002.316427386.00000226FA03D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000F.00000003.316049267.00000226FA045000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Stops/	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.ver)	svchost.exe, 00000015.00000002.603534517.0000019CF2E11000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000002.428413004.000001A110CEC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000F.00000002.316465691.00000226FA047000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316032557.00000226FA046000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000019.00000003.410454678.000001A11159B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.410402002.000001A1115B1000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.410518422.000001A111A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.410348749.000001A1115B1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000F.00000002.316427386.00000226FA03D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000002.316348056.00000226FA013000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49:7080/hIn	regsvr32.exe, 00000005.00000002.638413256.0000000000EA8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://%s.xboxlive.com	svchost.exe, 0000000C.00000002.638484661.0000024093E3E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://174.138.33.49/Q	regsvr32.exe, 00000005.00000003.543111893.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000005.00000002.638784137.0000000000EE2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000019.00000003.404927903.000001A111A02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.404982809.000001A111593000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405001225.000001A1115A4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000019.00000003.405032312.000001A111A02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000F.00000002.316465691.00000226FA047000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316032557.00000226FA046000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000019.00000003.408103656.000001A111599000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t	svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316054783.00000226FA041000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.315949220.00000226FA04B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 00000019.00000003.408103656.000001A111599000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000F.00000002.316383374.00000226FA029000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.291933590.00000226FA02F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000F.00000002.316465691.00000226FA047000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316013437.00000226FA03F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000F.00000003.316032557.00000226FA046000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000C.00000002.638484661.0000024093E3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000F.00000003.315897201.00000226FA04F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000019.00000003.408103656.000001A111599000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000C.00000002.638484661.0000024093E3E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000F.00000003.315949220.00000226FA04B000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
157.230.99.206	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
196.44.98.190	unknown	Ghana		327814	EcobandGH	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
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
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	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
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
178.238.225.252	unknown	Germany		51167	CONTABODE	true
46.101.98.60	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
190.145.8.4	unknown	Colombia		14080	TelmexColombiaSACO	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
190.107.19.179	unknown	Colombia		27951	MediaCommercePartnersSACO	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
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
139.59.80.108	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
104.244.79.94	unknown	United States		53667	PONYNETUS	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	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: 23/07/202205:06:03	2022-07-23 05:06:03 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	548IrCt4hj.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@31/8@0/43
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:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 300000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 93.184.221.240, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, wu.ec.azureedge.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, wu-bg-shim.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 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

No simulations

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):	0.24946602151942124
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4F:BJiRdwfu2SRU4F
MD5:	C6415F458A864CEDDB363410A92D8D55
SHA1:	7FAC7104DAE76F30E1C2D7251634F0B3E94DE7D2
SHA-256:	FE8A2F90EA9F564593FA5CE40785FF4B7290A616C04419105935BA5AA2AA0DA0
SHA-512:	FCDA8CBF3F18589B92197F0DD336D5A08278E8B5433C7055C8F3FE4A136B86A9CB31D9941F53A492CD16ECFC4921AF4031A513B86051618D76693B4B8058CAE
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 0xd83bc39c, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506456520125299
Encrypted:	false
SSDEEP:	384:h7O+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:h7hSB2nSB2RSjlK/+mLesOj1J2
MD5:	5A9C0B5046F21CA3203E4C7CA991BC85
SHA1:	82DA25512FE649527023E0FD56208FE354FAEE69
SHA-256:	2FA2DD6B161A541D4723B392BE5501EA6C0F435FD3C2DB3572449E71E8EBEA1A
SHA-512:	9FFB384C4259C2173440C0AD29342CE7940E7C01C50D060CEC6B380A516820E6B774C15B96A047DE9B087AA4B620693E9EAF1FABA674F7BF52F6E486FBA6018A
Malicious:	false
Preview:	.;.... .....e.f.3...w.....)....8....zC.....z..h.(....8....zC...).....3...w.....B.....@..... ....i.e%8....zC.....0q8....zC..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07614715333539902
Encrypted:	false
SSDEEP:	3:flltJ7vLInHYZlZy3WbydHZmtFS3ZlAll3VkttlmlnI:f1Jrkn4baWbOHW4bA3
MD5:	EC975F51AC789503AD0B2BE6FA5651B7
SHA1:	4D216416428EDF7EB6330B88E653F48291942021
SHA-256:	D203AB6EDC934A92C5A43B9DB3BCCA113E60600FD39B6570933C3E647BCAB278
SHA-512:	BD2FF982509FB909FA82BBC0747F591888EBC344420A06038DCF09741C29642A18F846990A4AF721990C42804E6C9AE00A4D1D2D97A5A057E75A07EDC5A84364
Malicious:	false
Preview:	N'.....3...w.....z..8....zC.....8....zC.8....zC.+@..8....z.....0q8....zC..... ....

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

Process:	C:\Windows\System32\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\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1358915940078624
Encrypted:	false
SSDEEP:	6:kKvKd+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:nKdNkPlE99SNxAhUeE1
MD5:	D3EA7BE178C2678C7617C7A602F7FE1C
SHA1:	416D50C68F46B1F492707337BFE8A319C4F33C84
SHA-256:	40D60CE3DC1CD35532CA36A49B555318C03B0510ADEED9F62FC14F44817067AB
SHA-512:	5696EA73B8CB20E9C6C528FE506EE808B8D6618B0C83CA7CD4DE349BEE08A522DE183CA7BBE93E8070FCA74783B182AC94FDCCB40D6A5E8F0147FDA6457132CD
Malicious:	false
Preview:	p...... ...._A...(... ....L.........$...............h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.162183525338945
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+EwF3+et:j+s+i+Z+z+B+c+Y+0g+J+j+p3+et
MD5:	D39A3BDD050BA8CF9774D1E1A6F7A651
SHA1:	47003AC294BE61B57D2AB37C7F4AB314CB967C1F
SHA-256:	312A42E0C253625E4FC102E21E7761D1F718E195A7E1A7588B9AEF2E27B5CD09
SHA-512:	948B948AFD7D2A83B18ED51E800FB3E4601DC989FA406B39A52FFA4207DDF26A09C571B2AC31ED39DD044C32A43A5CB58043DD613CA0AA3B40D71A941424091
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) 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:	548lrCt4hj.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 00007FCE50787EDEh
jmp 00007FCE507DECC5h
jmp 00007FCE5079C6ECh
jmp 00007FCE507C7DABh
jmp 00007FCE507BB822h
jmp 00007FCE5079FBE1h
jmp 00007FCE50786570h
jmp 00007FCE5079AC33h
jmp 00007FCE5077B0EAh
jmp 00007FCE507A8431h
jmp 00007FCE507A626Ch
jmp 00007FCE507A850Bh
jmp 00007FCE507CA986h
jmp 00007FCE507807E1h
jmp 00007FCE50788594h
jmp 00007FCE5079AC37h
jmp 00007FCE507E96DEh

Instruction
jmp 00007FCE507A1A81h
jmp 00007FCE507C5E98h
jmp 00007FCE507B9013h
jmp 00007FCE507D9E16h
jmp 00007FCE507D36B5h
jmp 00007FCE507B3144h
jmp 00007FCE507C50C3h
jmp 00007FCE507C54A6h
jmp 00007FCE507E9785h
jmp 00007FCE507D30E0h
jmp 00007FCE5078B5FFh
jmp 00007FCE5078A116h
jmp 00007FCE507C6D9Dh
jmp 00007FCE5078BAA4h
jmp 00007FCE507D09C3h
jmp 00007FCE507CEEE6h
jmp 00007FCE5079B9FDh
jmp 00007FCE50790128h
jmp 00007FCE507C9133h
jmp 00007FCE5079BC02h
jmp 00007FCE507DC949h
jmp 00007FCE507B8F9Ch
jmp 00007FCE5079AD3Fh

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.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

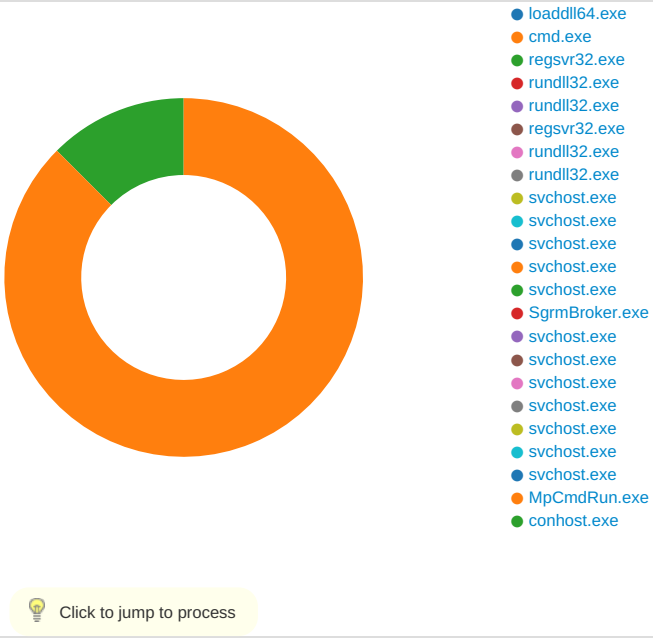
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5174.138.33.49 4976870802404316 07/23/22-04:56:42.473067	TCP	2404316	ET CNC Feodo Tracker Reported CnC Server TCP group 9	49768	7080	192.168.2.5	174.138.33.49

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 23, 2022 05:07:40.757388115 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:40.859507084 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:40.859658003 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:40.889399052 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:40.994549036 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:41.014581919 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:41.014671087 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:41.014766932 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:41.015188932 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:45.621840000 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:45.726568937 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:45.726685047 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:45.730561018 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:45.872215986 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:46.269582987 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:46.269676924 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:49.276211023 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:49.276302099 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:07:49.276330948 CEST	7080	49758	174.138.33.49	192.168.2.4
Jul 23, 2022 05:07:49.276375055 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:09:31.102890968 CEST	49758	7080	192.168.2.4	174.138.33.49
Jul 23, 2022 05:09:31.102929115 CEST	49758	7080	192.168.2.4	174.138.33.49

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **5724**, Parent PID: **3608**

General

Target ID:	0
Start time:	05:07:10
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:	0x7ff6005f0000
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: **244**, Parent PID: **5724**

General

Target ID:	1
Start time:	05:07:10
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:	0x7ff7bb450000
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: **4760**, Parent PID: **5724**

General

Target ID:	2
Start time:	05:07:11
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:	0x7ff7f12b0000
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: 00000002.00000002.252638967.0000000002091000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.252607659.0000000002060000.00000040.00001000.00020000.00000000.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\System32\MbnmzGnNg\joXcB.dll:Zone.Identifier	success or wait	1	20AED93	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: **3080**, Parent PID: **244**

General

Target ID:	3
Start time:	05:07:11
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:	0x7ff7174b0000
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: 00000003.00000002.248792041.000001F26FD71000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.248763264.000001F26FD40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **2924**, Parent PID: **5724**

General

Target ID:	4
Start time:	05:07:11
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:	0x7ff7174b0000
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: 00000004.00000002.249040025.000001C7434E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.249084413.000001C743541000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **5996**, Parent PID: **4760**

General

Target ID:	5
Start time:	05:07:14
Start date:	23/07/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\MbnmzGnNg\joXcB.dll"
Imagebase:	0x7ff7f12b0000
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: 00000005.00000002.637949653.0000000000E40000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_3, Description: , Source: 00000005.00000002.638413256.0000000000EA8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.638139112.0000000000E71000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3740**, Parent PID: **5724**

General

Target ID:	6
Start time:	05:07:15
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:	0x7ff7174b0000
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: **2560**, Parent PID: **5724**

General	
Target ID:	8
Start time:	05:07:18
Start date:	23/07/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\548IrCt4hj.dll,DllRegisterServer
Imagebase:	0x7ff7174b0000
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: **1012**, Parent PID: **564**

General	
Target ID:	11
Start time:	05:07:31
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **1428**, Parent PID: **564**

General	
Target ID:	12
Start time:	05:07:31
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5892**, Parent PID: **564**

General

Target ID:	13
Start time:	05:07:32
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4348**, Parent PID: **564**

General

Target ID:	14
Start time:	05:07:33
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

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

Analysis Process: svchost.exe PID: **2572**, Parent PID: **564**

General

Target ID:	15

Start time:	05:07:33
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **3628**, Parent PID: **564**

General

Target ID:	16
Start time:	05:07:34
Start date:	23/07/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7e4e90000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **3532**, Parent PID: **564**

General

Target ID:	17
Start time:	05:07:35
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: **5732**, Parent PID: **564**

General

Target ID:	18

Start time:	05:07:35
Start date:	23/07/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5244**, Parent PID: **564**

General

Target ID:	20
Start time:	05:07:39
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6272**, Parent PID: **564**

General

Target ID:	21
Start time:	05:07:45
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6280**, Parent PID: **564**

General

Target ID:	22
Start time:	05:07:46
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6532**, Parent PID: **564**

General

Target ID:	23
Start time:	05:08:06
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6756, Parent PID: 564

General

Target ID:	25
Start time:	05:08:18
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 6056, Parent PID: 3532

General

Target ID:	29
Start time:	05:08:35
Start date:	23/07/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff626d40000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 61 00 74 00 20 00 0e 20 4a 00 75 00 6c 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 35 00 3a 00 30 00 38 00 3a 00 33 00 37 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat Jul 23 2022 05:08 :37	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 61 00 74 00 20 00 0e 20 4a 00 75 00 6c 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 35 00 3a 00 30 00 38 00 3a 00 33 00 37 00 0d 00 0a 00	MpCmdRun: End Time: Sat Jul 23 2022 05:08:37	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **5948**, Parent PID: **6056**

General

Target ID:	30
Start time:	05:08:36
Start date:	23/07/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly