ID: 562461
Sample Name: Bg6DyC7lDh
Cookbook: default.jbs
Time: 22:20:13
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

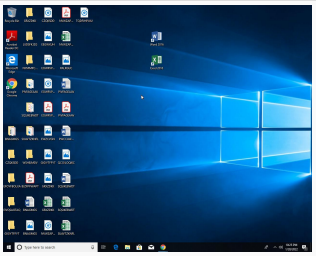
Windows Analysis Report

Bg6DyC7lDh

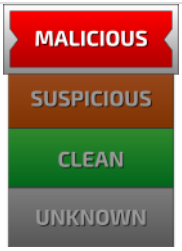
Overview

General Information

Sample Name:	Bg6DyC7lDh (renamed file extension from none to dll)
Analysis ID:	562461
MD5:	3fa1bec287b995..
SHA1:	c721507f4a11e0..
SHA256:	f7a5f6bc0833474..
Tags:	32 dll exe trojan
Infos:	



Detection



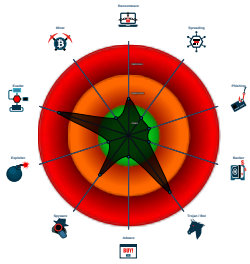
Emotet

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Changes security center settings (n…
- Machine Learning detection for sam…
- Sigma detected: Suspicious Call by…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 972 cmdline: loaddll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6152 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6176 cmdline: rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6380 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - BackgroundTransferHost.exe (PID: 6380 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
  - regsvr32.exe (PID: 6164 cmdline: regsvr32.exe /s C:\Users\user\Desktop\Bg6DyC7lDh.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6324 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6184 cmdline: rundll32.exe C:\Users\user\Desktop\Bg6DyC7lDh.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6484 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lvetlyszixrl\grmpeubxplti.rrq",FloWMCkThX MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6524 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lvetlyszixrl\grmpeubxplti.rrq",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6388 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 6300 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6504 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6600 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6808 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6872 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6900 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5556 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6168 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6704 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6852 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "C2 list": [
    "74.207.230.120:8080",
    "139.196.72.155:8080",
    "37.44.244.177:8080",
    "37.59.209.141:8080",
    "116.124.128.206:8080",
    "217.182.143.207:443",
    "54.37.228.122:443",
    "203.153.216.46:443",
    "168.197.250.14:80",
    "207.148.81.119:8080",
    "195.154.146.35:443",
    "78.46.73.125:443",
    "191.252.103.16:80",
    "210.57.209.142:8080",
    "185.168.130.138:443",
    "142.4.219.173:8080",
    "118.98.72.86:443",
    "78.47.204.80:443",
    "159.69.237.188:443",
    "190.90.233.66:443",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "185.148.168.15:8080",
    "54.38.242.185:443",
    "198.199.98.78:8080",
    "194.9.172.107:8080",
    "85.214.67.203:8080",
    "66.42.57.149:443",
    "185.148.168.220:8080",
    "103.41.204.169:8080",
    "128.199.192.135:8080",
    "195.77.239.39:8080",
    "59.148.253.194:443"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Bg6DyC7lDh.dll	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.287494272.0000000005381000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.780209080.0000000005701000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.296338746.0000000004F71000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000B.00000002.779999636.0000000005491000.00000020.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.268531340.0000000000DE0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 60 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.rundll32.exe.5250000.12.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.5700000.21.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
11.2.rundll32.exe.46f0000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
11.2.rundll32.exe.5000000.8.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.4c00000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 89 entries				

Sigma Overview

System Summary

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

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

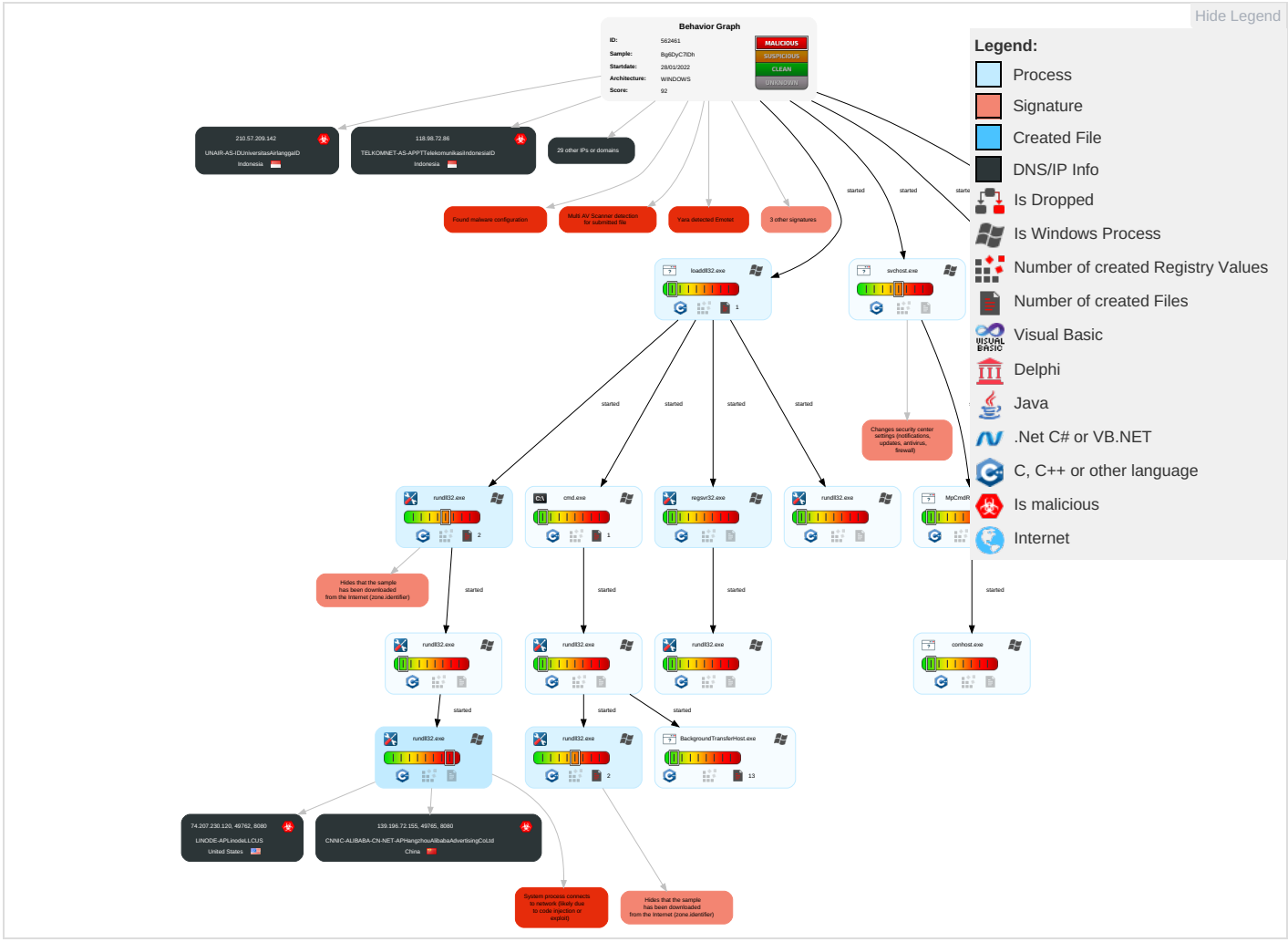
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	2 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	4 6 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	5 1 Security Software 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 Masquerading	Cached Domain Credentials	2 Virtualization/Sandbox Evasion	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 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Regsvr32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

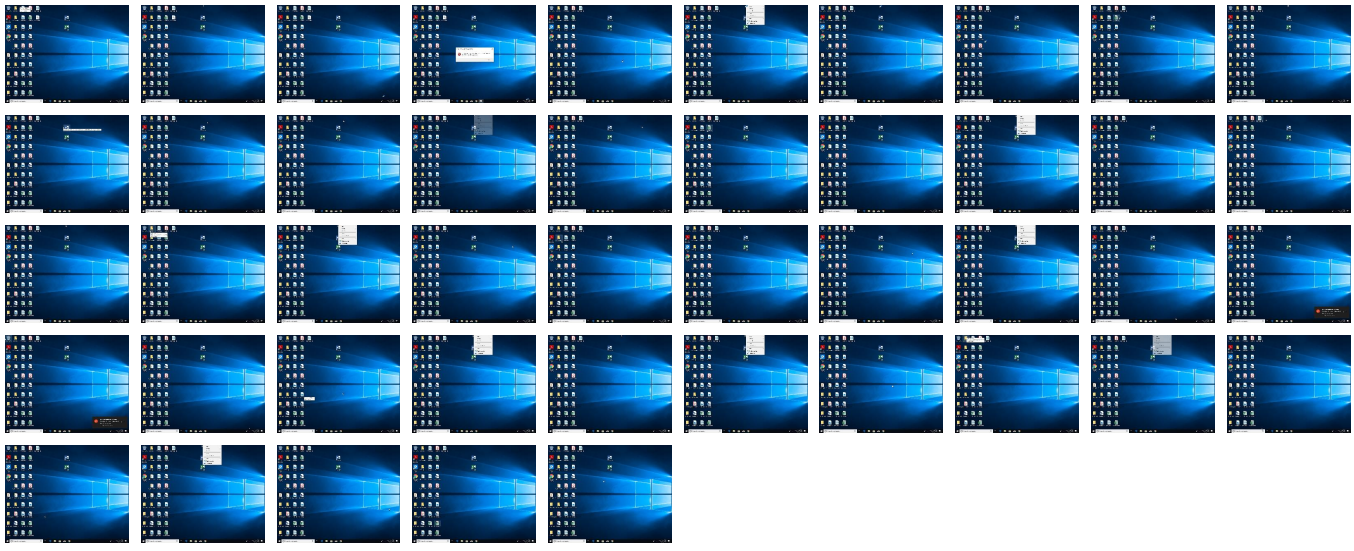
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Bg6DyC7lDh.dll	15%	Virustotal		Browse
Bg6DyC7lDh.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.4e40000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4fa0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
3.2.rundll32.exe.de0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4f70000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4cd0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5380000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.5460000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.54e0000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5700000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.53a0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.5170000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4de0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5510000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.11c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5280000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.4e10000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.51a0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.1280000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4fd0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.5100000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5670000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
9.2.rundll32.exe.4870000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.5650000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.5350000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.53b0000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.46f0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4af0000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4c30000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.4af0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5370000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
0.2.loaddll32.exe.1500000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5190000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.5130000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.48a0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.4ea0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
7.2.rundll32.exe.56a0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.4dc0000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.c40000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
3.2.rundll32.exe.e10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5490000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5680000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
11.2.rundll32.exe.5000000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.e50000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.5070000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.1180000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4ed0000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.50c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5250000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.56d0000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
4.2.rundll32.exe.4b20000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.4d10000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.14d0000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4df0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5030000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.5540000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.4c00000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
11.2.rundll32.exe.4730000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.exe.5060000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://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

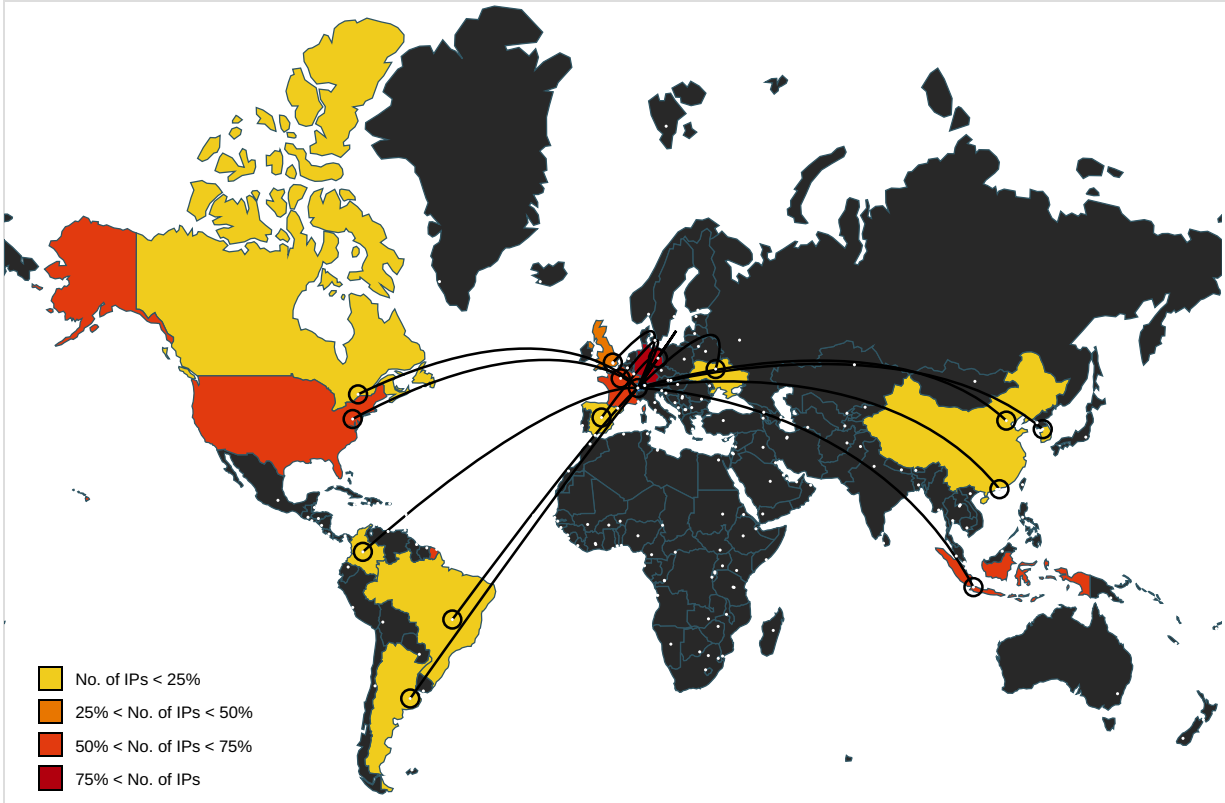
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001A.00000003.443630985.000002DEDAF90000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.444014442.000002DEDAF7E000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000003.321367338.000001A9C1445000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000D.00000002.322108516.000001A9C143E000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000D.00000002.322108516.000001A9C143E000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000002.322127503.000001A9C144D000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000D.00000003.320908225.000001A9C1467000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.322149285.000001A9C146A000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000D.00000002.322127503.000001A9C144D000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000D.00000002.322108516.000001A9C143E000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000D.00000003.299068688.000001A9C1431000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000003.299068688.000001A9C1431000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000005.00000002.614917318.000002FA99012000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000002.473526103.000002DEDA6ED000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000D.00000002.322122135.000001A9C1447000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.322090596.000001A9C1429000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321252960.000001A9C1446000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001A.00000003.447105193.000002DEDB402000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.446901322.000002DEDAFC2000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.446829559.000002DEDAF8A000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.446821206.000002DEDAF79000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.447041610.000002DEDAFAB000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.446970410.000002DEDAFC2000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://activity.windows.comr	svchost.exe, 0000000A.00000002.779027574.000001FEA5042000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000002.322108516.000001A9C143E000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.322076624.000001A9C1413000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000D.00000002.322115623.000001A9C1442000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321477876.000001A9C1441000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000A.00000002.779027574.000001FEA5042000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000D.00000003.299068688.000001A9C1431000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000D.00000003.299068688.000001A9C1431000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000D.00000002.322122135.000001A9C1447000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321252960.000001A9C1446000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001A.00000003.443630985.000002DEDAF90000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.444014442.000002DEDAF7E000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.322127503.000001A9C144D000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000D.00000002.322115623.000001A9C1442000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321477876.000001A9C1441000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000002.322115623.000001A9C1442000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321477876.000001A9C1441000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 0000001A.00000003.443630985.000002DEDAF90000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.444014442.000002DEDAF7E000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000D.00000003.299068688.000001A9C1431000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321593288.000001A9C143A000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000D.00000002.322122135.000001A9C1447000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321252960.000001A9C1446000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://activity.windows.com	svchost.exe, 0000000A.00000002.779027574.000001FEA5042000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000D.00000002.322076624.000001A9C1413000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000D.00000003.321017680.000001A9C1460000.00000004.00000001.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 0000001A.00000003.443630985.000002DEDAF90000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000001A.00000003.444014442.000002DEDAF7E000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000D.00000002.322108516.000001A9C143E000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000A.00000002.779027574.000001FEA5042000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000D.00000002.322127503.000001A9C144D000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000D.00000003.321127969.000001A9C144B000.00000004.00000001.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.148.81.119	unknown	United States		20473	AS-CHOOPAUS	true
104.131.62.48	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
198.199.98.78	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
194.9.172.107	unknown	unknown		207992	FEELBFR	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
74.207.230.120	unknown	United States		63949	LINODE-APLinodeLLCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternetSABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNETAR	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
217.182.143.207	unknown	France		16276	OVHFR	true
203.153.216.46	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
37.59.209.141	unknown	France		16276	OVHFR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
185.148.168.220	unknown	Germany		44780	EVERSCALE-ASDE	true
54.37.228.122	unknown	France		16276	OVHFR	true
185.168.130.138	unknown	Ukraine		49720	GIGACLOUD-ASUA	true
190.90.233.66	unknown	Colombia		18678	INTERNEXASAESPCO	true
142.4.219.173	unknown	Canada		16276	OVHFR	true
54.38.242.185	unknown	France		16276	OVHFR	true
195.154.146.35	unknown	France		12876	OnlineSASFR	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
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
128.199.192.135	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562461
Start date:	28.01.2022
Start time:	22:20:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bg6DyC7lDh (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.evad.winDLL@32/9@0/34
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 93.4%) • Quality average: 71.5% • Quality standard deviation: 26.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 2.20.156.69, 92.123.101.210, 92.123.101.170, 92.123.101.179, 92.123.101.169, 40.91.112.76, 20.54.7.98, 20.54.104.15
- Excluded domains from analysis (whitelisted): displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wus2-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, www-bing-com.dual-a-0001.a-msedge.net, consumer-displaycatalogrp-aks2aks-uswest.md.mp.microsoft.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu-shim.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-micro
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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
22:21:17	API Interceptor	10x Sleep call for process: svchost.exe modified
22:22:37	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

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

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2494418280042947
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4p:BJiRdwfu2SRU4p
MD5:	D4CE4F78B74CC0908941E8735F1CF295
SHA1:	FF53DF2E0C8F9BEC427525A3A44AF8757CBDFD15
SHA-256:	625135E85A1E34931F3EF6426E0D42B77A97BDF07C69EC9FD27BA95353673A1F
SHA-512:	829C1B935198054D4013F0E63F9DDFE0689F17B890296624F945BAAD41002540DAF512F39F9E9AC64A8A805C7AAAB6B9ECF3D64F0B222A0EE36B503B957A9021
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 0x0f7c94ec, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506229908050935
Encrypted:	false
SSDEEP:	384:g/N+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:g/uSB2nSB2RSjlK/+mLesOj1J2
MD5:	45415639C5303A0C1C09FED273A52481
SHA1:	AF6E77DD80387C01E0DC53EFCF6BF65ABFFC4AB3
SHA-256:	EFB44260505B02062337CD61A88FA3DC6A695FF821511AF1765AF8081259123B
SHA-512:	A0D0C7DD4DB82C028C1137079717D3E71EBC8969A620E2CDDCB4D9FB262B369DC1B1F6523B07F426FD65B77D0EA73DD25A5558C2EF026F7056EC48E9B6920 FD
Malicious:	false

Preview:	.|..... .....e.f.3...w.....).....zI.....zQ.h.(.....zI...).....3...w.....B.....@..... ....5.....zI.....:....zI..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07576484657716591
Encrypted:	false
SSDEEP:	3:ynZ7v3+UNG/ts5NfOOrg7///qkrO/tall3VkttlmlnI:yZrOi9sXZr73
MD5:	7E267D71A3A2924510CB2275C9135446
SHA1:	F92E6283962D1DF967966ABFE5685BD0F6223552
SHA-256:	3244F40C786FC3759E9FE37221A6AFD7E3539EA1563C601EE2F4C53BF5CA6345
SHA-512:	00F588D5696E3F55365D320D318F5404E76F35774B3F57D2AE4BF89A27C053638F2F4696FD69DF0A8F76D624D5F2C7B8218C1EF7011BAA46A93904C2E1FA895C
Malicious:	false
Preview:	`.....3...w.....z.....zI.....zI.....zI.kN_.....z.....:....zI..... ....

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

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD898447614l7C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090 0
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....l.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;..Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.l..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z.....,_...gY..!Z..?l....vp.l.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c../.;....g&.....

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

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1122616792999316
Encrypted:	false
SSDEEP:	6:kKdptk8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:Tt9kPlE99SNxAhUeYlUSA/t
MD5:	1E4ED718E0D2EF47370B4567A1C2B750
SHA1:	F359C1AC5B4A3CE402415DF418E0A834926CBDB1
SHA-256:	B24509D0D688AB01F9332DAC5708DAA58319DCE5D48215C66BEBF3682F513A93
SHA-512:	D25E0517EB93172332EB284C47BDB5AA9C710B58F25B5CE02C0066289671A0ACEB8508C2BFA19404672566B317B1D369227756C5223ABE9D38634A2132E884C1
Malicious:	false
Preview:	p..... .....L.....(..... ....q.\].....&.....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...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

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

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators

Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.166114821808174
Encrypted:	false
SSDEEP:	192:cY+38+DJDD+iDtJC+iw3+gF+O5+6tw+EStN+Ej23+dt:j+s+5D+Me+X+u+M+j+l+73+dt
MD5:	F095B293720409934FBE10DAF412A8A1
SHA1:	FAE8DCB76639C9CE658E43703C3B821E82EC852D
SHA-256:	228B5DD614F3486781CC7A7F4EBDC81CB0FC20A9B2BAF25ED54D9DB5B2A7B0DE
SHA-512:	3400E5A1CCBFA58FDCDCEA7BA2426BCB8A5E574959EDAB97E91B5D7DD7ADAA5970D310E2C57798AD4E2DC99F35D50BB007ADDA01A3BD535C8F421C1F0C04DA8
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.....-............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220129_062134_900.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	3.7803076993140294
Encrypted:	false
SSDEEP:	96:dTCgblgo+h/5uD9S/YAVCACI2lzfkHc4c+T2hjFzMNMCgGdJRA7dj5EUMCDY5QU8:8Pe4Ee2BltCg2fCpCKC2CUCo
MD5:	799E7659320F37DDC20C480DB77CCE14
SHA1:	DAF693FA4F3C2411D096690CA673836F403EDB50
SHA-256:	5D39D3DA4BB584E3D96B8F0B53205D146D3A01B9ACB2355BA6B63DFA108DB9C8
SHA-512:	1A1134DC7EE0AFFD43D0812E556B20491030547098968194769 79EA933DC8367E4A949939D0099F768D3B1314E6CED77E9309E8890ADB4842C5BC631CD2583B6
Malicious:	false
Preview:	....!...B.............Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..N...=..... .....P..v...........8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.2.9._.0.6.2.1.3.4._.9.0.0...e.t.l.........P.P...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.004123659336167
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

File name:	Bg6DyC7lDh.dll
File size:	557056
MD5:	3fa1bec287b995a7f96dc3866eff577d
SHA1:	c721507f4a11e090f107d071a99aaeffbdc0ea43
SHA256:	f7a5f6bc0833474da5450e33786893ac7b996ba5e91ed0f7d3243dc4d7db5486
SHA512:	70304fcf6f6ea1cc3cca75ff01475f97451500d0114f94f19119573c4e34f6f33e4c54de3481d74c37100360ac72720675725bc230ed68d0e8e5a12e84b443b5
SSDEEP:	6144:HUNF4UQXTkkAiBuGKDU5PSczbmOTT0DaTMGbUylbdTN1itwRClN6RfcjJxX4R0Zq:AeAa4DU5PSczbmmTzTnwyDx6BrWt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....hs.a,..2,..2,...2...2&..2...27..2,..2...2...26..2...2...2...2...2...2-..2...2-..2...2-..2...2Rich,..2.....PE..L.....a...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10030d06
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61F3FA91 [Fri Jan 28 14:15:45 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f4d2f65566a93075f8824e97bf321580

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007F37F496D067h
call 00007F37F49753C0h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007F37F496CF52h
pop ecx
retn 000Ch
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax

Instruction
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], esp
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [100545D4h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x52d40	0x52	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x51034	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x27650	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	0x4e30	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4bd90	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x46000	0x594	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x50fac	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44539	0x45000	False	0.469910552536	data	6.61687356024	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x46000	0xcd92	0xd000	False	0.337834284856	data	5.22670579455	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x53000	0x6580	0x3000	False	0.2626953125	PGP symmetric key encrypted data -	4.05367526692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x27650	0x28000	False	0.916259765625	data	7.8318744089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0x9376	0xa000	False	0.346923828125	data	4.18220950375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
DASHBOARD	0x5ab04	0x23600	data	Chinese	Taiwan
RT_CURSOR	0x7e104	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e238	0xb4	data	Chinese	Taiwan
RT_CURSOR	0x7e2ec	0x134	AmigaOS bitmap font	Chinese	Taiwan
RT_CURSOR	0x7e420	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e554	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e688	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e7bc	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7e8f0	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7ea24	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7eb58	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7ec8c	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7edc0	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7eef4	0x134	AmigaOS bitmap font	Chinese	Taiwan
RT_CURSOR	0x7f028	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7f15c	0x134	data	Chinese	Taiwan
RT_CURSOR	0x7f290	0x134	data	Chinese	Taiwan
RT_BITMAP	0x7f3c4	0xb8	data	Chinese	Taiwan
RT_BITMAP	0x7f47c	0x144	data	Chinese	Taiwan
RT_DIALOG	0x7f5c0	0x148	data	Chinese	Taiwan
RT_DIALOG	0x7f708	0x26a	data	Chinese	Taiwan
RT_DIALOG	0x7f974	0xe8	data	Chinese	Taiwan
RT_DIALOG	0x7fa5c	0x34	data	Chinese	Taiwan
RT_STRING	0x7fa90	0x58	data	Chinese	Taiwan
RT_STRING	0x7fae8	0x82	data	Chinese	Taiwan
RT_STRING	0x7fb6c	0x2a	data	Chinese	Taiwan
RT_STRING	0x7fb98	0x192	data	Chinese	Taiwan
RT_STRING	0x7fd2c	0x4e2	data	Chinese	Taiwan
RT_STRING	0x80210	0x31a	data	Chinese	Taiwan

Name	RVA	Size	Type	Language	Country
RT_STRING	0x8052c	0x2dc	data	Chinese	Taiwan
RT_STRING	0x80808	0x8a	data	Chinese	Taiwan
RT_STRING	0x80894	0xac	data	Chinese	Taiwan
RT_STRING	0x80940	0xde	data	Chinese	Taiwan
RT_STRING	0x80a20	0x4c4	data	Chinese	Taiwan
RT_STRING	0x80ee4	0x264	data	Chinese	Taiwan
RT_STRING	0x81148	0x2c	data	Chinese	Taiwan
RT_STRING	0x81174	0x42	data	Chinese	Taiwan
RT_GROUP_CURSOR	0x811b8	0x22	Lotus unknown worksheet or configuration, revision 0x2	Chinese	Taiwan
RT_GROUP_CURSOR	0x811dc	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x811f0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81204	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81218	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x8122c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81240	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81254	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81268	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x8127c	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x81290	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812a4	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812b8	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812cc	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_GROUP_CURSOR	0x812e0	0x14	Lotus unknown worksheet or configuration, revision 0x1	Chinese	Taiwan
RT_VERSION	0x812f4	0x304	data	Chinese	Taiwan
RT_MANIFEST	0x815f8	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	FileTimeToSystemTime, FileTimeToLocalFileTime, GetFileAttributesA, GetFileTime, GetTickCount, RtlUnwind, GetSystemInfo, HeapReAlloc, GetCommandLineA, ExitProcess, ExitThread, CreateThread, RaiseException, HeapSize, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, Sleep, HeapDestroy, HeapCreate, GetStdHandle, GetOEMCP, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetSystemTimeAsFileTime, GetACP, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, GetConsoleCP, GetConsoleMode, LCMapStringA, LCMapStringW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetEnvironmentVariableA, GetCPInfo, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetThreadLocale, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, InterlockedIncrement, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, LocalAlloc, GlobalFlags, FormatMessageA, LocalFree, InterlockedDecrement, MulDiv, GlobalGetAtomNameA, GlobalFindAtomA, lstrcmpW, GetVersionExA, WritePrivateProfileStringA, GlobalUnlock, GlobalFree, FreeResource, GetCurrentProcessId, GlobalAddAtomA, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, GetCurrentThreadId, ConvertDefaultLocale, GetModuleFileNameA, EnumResourceLanguagesA, GetLocaleInfoA, GlobalLock, lstrcmpA, GlobalAlloc, GlobalDeleteAtom, GetModuleHandleA, GetLastError, lstrlenA, CompareStringA, CompareStringW, MultiByteToWideChar, InterlockedExchange, GetVersion, WideCharToMultiByte, LockResource, FindResourceA, FindResourceW, LoadResource, SizeofResource, HeapFree, GetNativeSystemInfo, GetProcessHeap, HeapAlloc, FreeLibrary, GetProcAddress, LoadLibraryA, IsBadReadPtr, VirtualProtect, SetLastError, VirtualAlloc, VirtualFree, SetHandleCount, VirtualQuery

DLL	Import
USER32.dll	GetNextDlgGroupItem, MessageBeep, UnregisterClassA, RegisterClipboardFormatA, PostThreadMessageA, LoadCursorA, SetCapture, DestroyMenu, EndPaint, BeginPaint, GetWindowDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, RegisterWindowMessageA, SendDlgItemMessageA, WinHelpA, GetCapture, GetClassLongA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SetFocus, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, InvalidateRgn, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, GetSubMenu, GetMenuItemID, GetMenuItemCount, CreateWindowExA, GetClassInfoExA, GetClassInfoA, RegisterClassA, GetSysColor, AdjustWindowRectEx, EqualRect, PtInRect, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, ReleaseDC, GetDC, CopyRect, SetWindowLongA, GetWindowLongA, GetSystemMetrics, DrawIcon, AppendMenuA, SendMessageA, GetWindow, SetWindowContextHelpId, MapDialogRect, SetWindowPos, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamA, DestroyWindow, IsWindow, GetDlgItem, GetNextDlgTabItem, EndDialog, GetWindowThreadProcessId, InvalidateRect, SetRect, IsRectEmpty, CopyAcceleratorTableA, CharNextA, GetLastActivePopup, IsWindowEnabled, GetSysColorBrush, ReleaseCapture, GetSystemMenu, IsIconic, GetClientRect, EnableWindow, LoadIconA, CharUpperA, PostQuitMessage, PostMessageA, CheckMenuItem, EnableMenuItem, GetMenuState, ModifyMenuA, GetParent, GetFocus, LoadBitmapA, GetMenuCheckMarkDimensions, SetMenuItemBitmaps, ValidateRect, GetCursorPos, PeekMessageA, GetKeyState, IsWindowVisible, GetActiveWindow, DispatchMessageA, TranslateMessage, GetMessageA, CallNextHookEx, SetWindowsHookExA, SetCursor, MessageBoxA, IsChild
GDI32.dll	ExtSelectClipRgn, DeleteDC, GetStockObject, GetDeviceCaps, GetBkColor, GetTextColor, GetRgnBox, GetMapMode, ScaleWindowExtEx, SetWindowExtEx, ScaleViewportExtEx, SetViewportExtEx, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, Escape, ExtTextOutA, CreateBitmap, RectVisible, PtVisible, GetWindowExtEx, GetViewportExtEx, DeleteObject, SetMapMode, RestoreDC, SaveDC, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateRectRgnIndirect, TextOutA
comdlg32.dll	GetFileTitleA
WINSPOOL.DRV	DocumentPropertiesA, OpenPrinterA, ClosePrinter
ADVAPI32.dll	RegQueryValueA, RegSetValueExA, RegCreateKeyExA, RegCloseKey, RegOpenKeyA, RegEnumKeyA, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA
COMCTL32.dll	InitCommonControlsEx
SHLWAPI.dll	PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
WS2_32.dll	recv, connect, WSACleanup, socket, WSAStartup, htons, inet_addr, closesocket, send
oledlg.dll	
ole32.dll	StgOpenStorageOnILockBytes, CoGetClassObject, CoTaskMemAlloc, StgCreateDocfileOnILockBytes, CoTaskMemFree, CLSIDFromString, CLSIDFromProgID, CreateILockBytesOnHGlobal, CoRegisterMessageFilter, OleFlushClipboard, OleIsCurrentClipboard, CoRevokeClassObject, OleInitialize, CoFreeUnusedLibraries, OleUninitialize
OLEAUT32.dll	SysAllocStringLen, VariantClear, VariantChangeType, VariantInit, SysStringLen, SysAllocStringByteLen, OleCreateFontIndirect, VariantTimeToSystemTime, SystemTimeToVariantTime, SafeArrayDestroy, SysAllocString, VariantCopy, SysFreeString

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10012860

Version Infos

Description	Data
LegalCopyright	Innoversal. All rights reserved.
InternalName	FinalChatSocketCli.exe
FileVersion	1.0.2.4
CompanyName	Innoversal
ProductName	Char room only
ProductVersion	1.0.2.4
FileDescription	Chat room
OriginalFilename	FinalChatSocketCli.exe
Translation	0x0404 0x03b6

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

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

Network Behavior

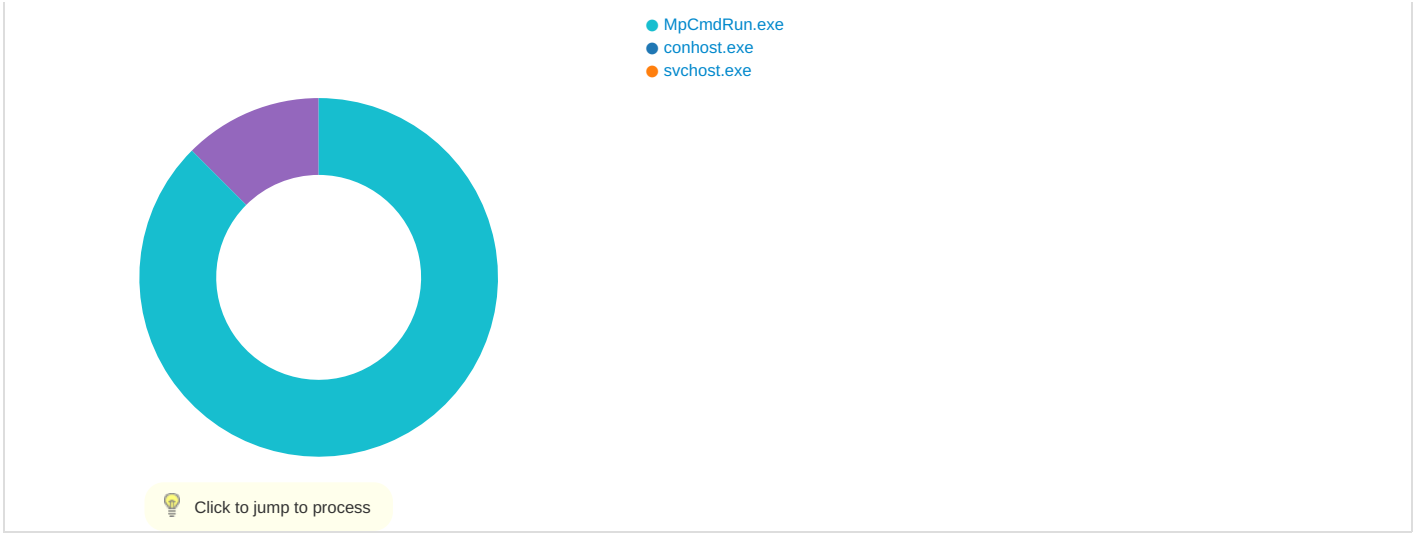
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:21:45.634107113 CET	49762	8080	192.168.2.7	74.207.230.120
Jan 28, 2022 22:21:45.783974886 CET	8080	49762	74.207.230.120	192.168.2.7
Jan 28, 2022 22:21:46.348982096 CET	49762	8080	192.168.2.7	74.207.230.120
Jan 28, 2022 22:21:46.498123884 CET	8080	49762	74.207.230.120	192.168.2.7
Jan 28, 2022 22:21:47.036732912 CET	49762	8080	192.168.2.7	74.207.230.120
Jan 28, 2022 22:21:47.187123060 CET	8080	49762	74.207.230.120	192.168.2.7
Jan 28, 2022 22:21:47.196436882 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:47.440165043 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:47.440510988 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:47.715660095 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:47.959338903 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:47.970019102 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:47.970052004 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:47.970172882 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:54.870376110 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:55.114665031 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:55.114808083 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:55.119724035 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:55.403013945 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:56.240480900 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:56.240611076 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:59.240741014 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:59.240775108 CET	8080	49765	139.196.72.155	192.168.2.7
Jan 28, 2022 22:21:59.240861893 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:21:59.240910053 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:23:35.577542067 CET	49765	8080	192.168.2.7	139.196.72.155
Jan 28, 2022 22:23:35.577588081 CET	49765	8080	192.168.2.7	139.196.72.155

Statistics

Behavior

- loaddll32.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- svchost.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- svchost.exe
- rundll32.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- BackgroundTransferHost.exe
- svchost.exe



System Behavior

Analysis Process: loaddll32.exe PID: **972**, Parent PID: **2388**

General

Target ID:	0
Start time:	22:21:14
Start date:	28/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll"
Imagebase:	0x910000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000000.00000002.274458477.0000000001501000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.271956434.00000000014D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.276915244.0000000010001000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6152**, Parent PID: **972**

General

Target ID:	1
Start time:	22:21:14
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",#1
Imagebase:	0x870000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6164, Parent PID: 972

General

Target ID:	2
Start time:	22:21:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\Bg6DyC7lDh.dll
Imagebase:	0x60000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.266354631.0000000004D11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.262826472.0000000004CD0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.266639849.0000000010001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6176, Parent PID: 6152

General

Target ID:	3
Start time:	22:21:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",#1
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.268531340.0000000000DE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.268562280.0000000000E11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.268591855.0000000010001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6184, Parent PID: 972

General	
Target ID:	4
Start time:	22:21:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Bg6DyC7lDh.dll,DllRegisterServer
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296338746.0000000004F71000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296293943.0000000004E11000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.294626282.0000000001180000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296431152.0000000005131000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296459967.0000000010001000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296356591.0000000004FA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.295961219.0000000004C00000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296375902.0000000004FD1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.295334948.0000000004B21000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.295156896.0000000004AF0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296406434.0000000005100000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296276538.0000000004DE0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296314729.0000000004E40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.296141210.0000000004C31000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.294816386.00000000011C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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

File Deleted				
File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\Lvetlyszixrl\grmpeubxplti.rrq:Zone.Identifier	success or wait	1	11CBB46	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6300, Parent PID: 560

General	
Target ID:	5
Start time:	22:21:16
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000
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

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: rundll32.exe PID: **6324**, Parent PID: **6164**

General

Target ID:	6
Start time:	22:21:17
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6380**, Parent PID: **6176**

General

Target ID:	7
Start time:	22:21:20
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287494272.0000000005381000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287862922.0000000005541000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287111363.0000000005170000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287132788.00000000051A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287038579.0000000005070000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.285682496.0000000001280000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287469423.0000000005350000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287075796.00000000050C1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.285736531.0000000004AF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287604820.00000000053B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287829918.0000000005510000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.287729935.00000000054E1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.288375637.0000000010001000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.288125580.00000000056A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.288102612.0000000005670000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **6388**, Parent PID: **972**

General

Target ID:	8
Start time:	22:21:20
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\Bg6DyC7lDh.dll",DllRegisterServer
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **6484**, Parent PID: **6184**

General

Target ID:	9
Start time:	22:21:25
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Lvetlyszixrl\grmpeubxplti.rrq",FloWMCkThX
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.288455858.0000000004870000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.288482327.00000000048A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.293864491.0000000010001000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: **6504**, Parent PID: **560**

General

Target ID:	10
Start time:	22:21:26
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff641cd0000
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

Analysis Process: rundll32.exe PID: **6524**, Parent PID: **6484**

General

Target ID:	11
Start time:	22:21:27
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Lvetlyszixrl\grmpeubxplti.rrq",DllRegisterServer
Imagebase:	0x12b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.780209080.0000000005701000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779999636.0000000005491000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779143719.0000000000E51000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779418909.0000000004DC0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779603939.0000000005000000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.778637126.0000000000C40000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779449781.0000000004DF1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779771482.0000000005281000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779542982.0000000004ED1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779971740.0000000005460000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779631051.0000000005031000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779317583.0000000004731000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.780141318.0000000005681000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779684590.0000000005191000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779867718.0000000005370000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779237002.00000000046F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779911189.00000000053A1000.00000020.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.780100280.0000000005650000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779726684.0000000005250000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779504243.0000000004EA0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.780181061.00000000056D0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.779651988.0000000005060000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000B.00000002.780299654.0000000010001000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security

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: svchost.exe PID: **6600**, Parent PID: **560**

General

Target ID:	12
Start time:	22:21:29
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff641cd0000
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: **6808**, Parent PID: **560**

General

Target ID:	13
Start time:	22:21:35
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff641cd0000
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: **6872**, Parent PID: **560**

General

Target ID:	14
Start time:	22:21:35
Start date:	28/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6de5a0000
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: **6900**, Parent PID: **560**

General

Target ID:	15
Start time:	22:21:36
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff641cd0000
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: 6168, Parent PID: 560

General

Target ID:	19
Start time:	22:21:59
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
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: BackgroundTransferHost.exe PID: 6380, Parent PID: 792

General

Target ID:	21
Start time:	22:22:23
Start date:	28/01/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff772bb0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6704, Parent PID: 560

General

Target ID:	22
Start time:	22:22:23
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
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: MpCmdRun.exe PID: **5556**, Parent PID: **6900**

General

Target ID:	23
Start time:	22:22:37
Start date:	28/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7bf500000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8156	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF7BF52BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 32 00 38 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 32 00 32 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: Fri Jan 28 2022 22:22:37	success or wait	1	7FF7BF52BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF7BF52BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF7BF52BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF7BF52BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 4a 00 61 00 6e 00 20 00 0e 20 32 00 38 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 32 00 32 00 3a 00 33 00 37 00 0d 00 0a 00	MpCmdRun: End Time: Fri Jan 28 2022 22:22:37	success or wait	1	7FF7BF52BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF7BF52BC96	WriteFile

Analysis Process: conhost.exe PID: **5728**, Parent PID: **5556**

General

Target ID:	24
Start time:	22:22:37
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6852**, Parent PID: **560**

General

Target ID:	26
Start time:	22:22:40
Start date:	28/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly