



ID: 553129
Sample Name: 7MhGa3iotM
Cookbook: default.jbs
Time: 11:06:47
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 7MhGa3iotM 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 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: 6
Mitre Att&ck Matrix 6
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 11
Contacted IPs 11
Public 11
Private 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Rich Headers 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Exports 16
Version Infos 16
Possible Origin 16
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 17
DNS Answers 17
Code Manipulations 17
Statistics 17
Behavior 17
System Behavior 17
Analysis Process: SgrmBroker.exe PID: 7124 Parent PID: 572 17

Copyright Joe Security LLC 2022

General 17
Analysis Process: svchost.exe PID: 7152 Parent PID: 572 18
General 18
File Activities 18
Analysis Process: loaddll32.exe PID: 6180 Parent PID: 4248 18
General 18
File Activities 18
Analysis Process: svchost.exe PID: 5808 Parent PID: 572 18
General 18
Registry Activities 19
Analysis Process: cmd.exe PID: 1496 Parent PID: 6180 19
General 19
File Activities 19
Analysis Process: regsvr32.exe PID: 3348 Parent PID: 6180 19
General 19
Analysis Process: rundll32.exe PID: 5732 Parent PID: 1496 19
General 19
Analysis Process: rundll32.exe PID: 6388 Parent PID: 6180 20
General 20
File Activities 20
File Deleted 20
Analysis Process: rundll32.exe PID: 5388 Parent PID: 3348 21
General 21
Analysis Process: rundll32.exe PID: 3360 Parent PID: 5732 21
General 21
File Activities 21
Analysis Process: rundll32.exe PID: 2172 Parent PID: 6388 21
General 21
Analysis Process: rundll32.exe PID: 6512 Parent PID: 2172 22
General 22
File Activities 23
Analysis Process: svchost.exe PID: 3396 Parent PID: 572 23
General 23
File Activities 24
Analysis Process: svchost.exe PID: 6640 Parent PID: 572 24
General 24
File Activities 24
Analysis Process: svchost.exe PID: 1496 Parent PID: 572 24
General 24
File Activities 24
Analysis Process: svchost.exe PID: 1460 Parent PID: 572 24
General 24
File Activities 25
Analysis Process: MpCmdRun.exe PID: 6456 Parent PID: 5808 25
General 25
File Activities 25
File Written 25
Analysis Process: conhost.exe PID: 5952 Parent PID: 6456 25
General 25
Disassembly 25
Code Analysis 25

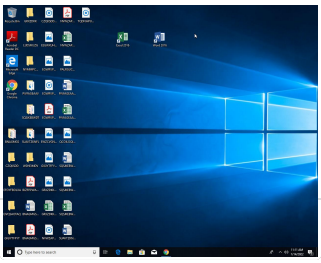
Windows Analysis Report 7MhGa3iotM

Overview

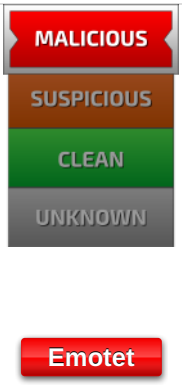
General Information

Sample Name:	7MhGa3iotM (renamed file extension from none to dll)
Analysis ID:	553129
MD5:	752a2613b2b71fc.
SHA1:	7d59cf93d7b7644.
SHA256:	2df1bd696a635b1.
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

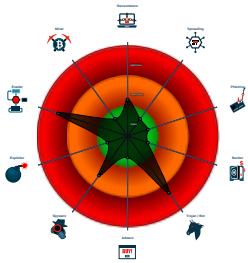


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Changes security center settings (no…
- Machine Learning detection for samp…
- 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…

Classification



Process Tree

- **System is w10x64**
- SgrmBroker.exe (PID: 7124 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 7152 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- loaddll32.exe (PID: 6180 cmdline: loaddll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1496 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5732 cmdline: rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 3360 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 3348 cmdline: regsvr32.exe /s C:\Users\user\Desktop\7MhGa3iotM.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 5388 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6388 cmdline: rundll32.exe C:\Users\user\Desktop\7MhGa3iotM.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 2172 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kgiezrb\edgitxrppqaf.tym",JFlwYpDQ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 6512 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Kgiezrb\edgitxrppqaf.tym",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- svchost.exe (PID: 5808 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 6456 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 3396 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6640 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1496 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1460 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "45.138.98.34:80",
    "69.16.218.101:8080",
    "51.210.242.234:8080",
    "185.148.168.220:8080",
    "142.4.219.173:8080",
    "54.38.242.185:443",
    "191.252.103.16:80",
    "104.131.62.48:8080",
    "62.171.178.147:8080",
    "217.182.143.207:443",
    "168.197.250.14:80",
    "37.44.244.177:8080",
    "66.42.57.149:443",
    "210.57.209.142:8080",
    "159.69.237.188:443",
    "116.124.128.206:8080",
    "128.199.192.135:8080",
    "195.154.146.35:443",
    "185.148.168.15:8080",
    "195.77.239.39:8080",
    "207.148.81.119:8080",
    "85.214.67.203:8080",
    "190.90.233.66:443",
    "78.46.73.125:443",
    "78.47.204.80:443",
    "37.59.209.141:8080",
    "54.37.228.122:443"
  ],
  "Public Key": [
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCW",
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.298606993.00000000056B0000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.294428773.0000000004E31000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.815959143.0000000004E91000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.298670924.00000000056E1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000D.00000002.816961696.00000000050F1000.00000020.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 43 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.rundll32.exe.53a0000.18.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.4ec0000.10.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.rundll32.exe.54f0000.6.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.2d50000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
13.2.rundll32.exe.4ef0000.11.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Click to see the 67 entries

Sigma Overview

System Summary:



Copyright Joe Security LLC 2022

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:



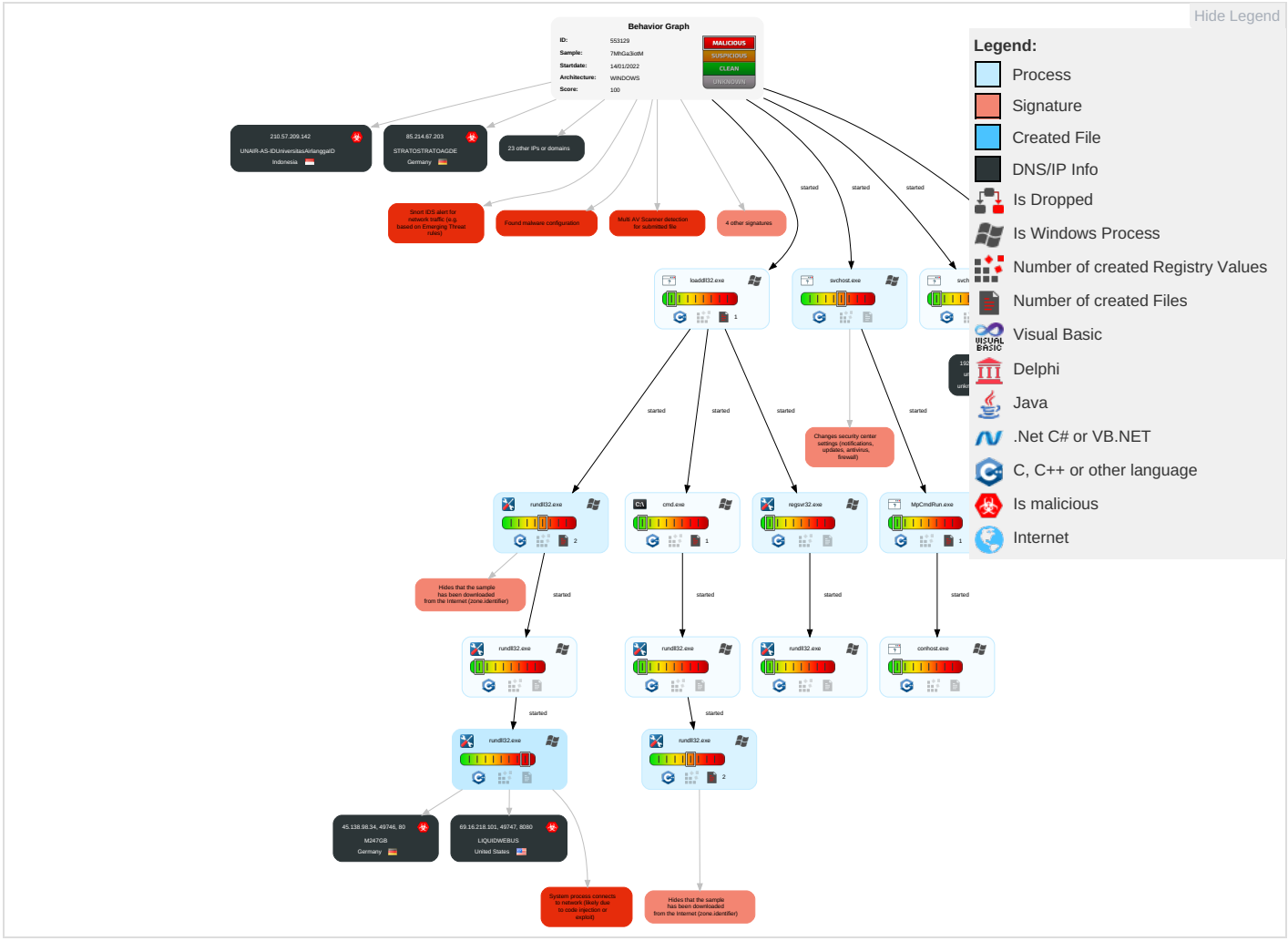
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

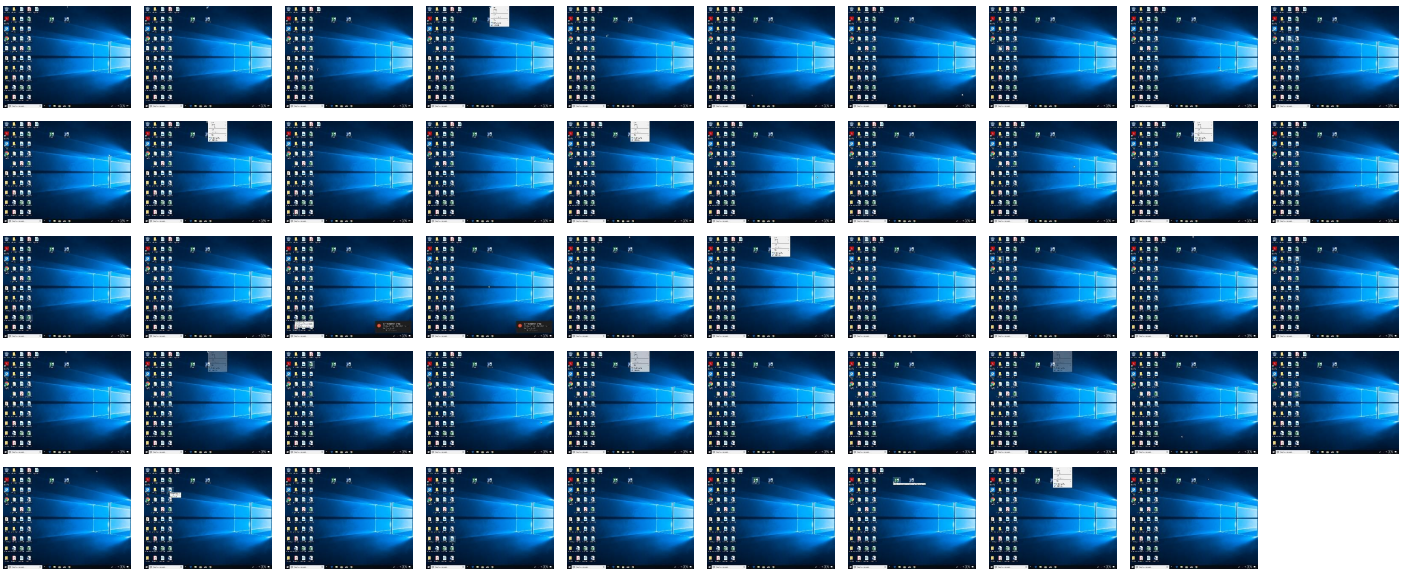
Behavior Graph



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
7MhGa3iotM.dll	30%	Virustotal		Browse
7MhGa3iotM.dll	42%	ReversingLabs	Win32.Trojan.Emotet	
7MhGa3iotM.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.4d30000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.4ef0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4ac0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.54f0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4ec0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.5580000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.52e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.43d0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.5280000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4c50000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.4e90000.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.5520000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.2d50000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.4d90000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.4fa0000.12.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.56b0000.10.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4fd0000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.5620000.20.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.53a0000.18.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.4a40000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4480000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.3430000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.50f0000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4af0000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.53d0000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.51a0000.16.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.43c0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.regsvr32.exe.4e30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.2990000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.5550000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.50c0000.14.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.2.rundll32.exe.4a70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.4d00000.6.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
5.2.regsvr32.exe.4e00000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.53c0000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.51d0000.17.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4a90000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.850000.0.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4e60000.8.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
13.2.rundll32.exe.4c20000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
8.2.rundll32.exe.56e0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.45d0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.880000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.5390000.4.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
10.2.rundll32.exe.49c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.5650000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4b20000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.4990000.2.unpack	100%	Avira	HEUR/AGEN.1145233		Download File

Domains

Source	Detection	Scanner	Label	Link
windowsupdate.s.llnwi.net	0%	Virustotal		Browse

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.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	41.63.96.128	true	false	• 0%, Virustotal, Browse	unknown

Copyright Joe Security LLC 2022

URLs from Memory and Binaries

Contacted IPs

Public

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
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
191.252.103.16	unknown	Brazil		27715	LocawebServicosdeInternet SABR	true
168.197.250.14	unknown	Argentina		264776	OmarAnselmoRipollTDCNET AR	true
66.42.57.149	unknown	United States		20473	AS-CHOOPAUS	true
185.148.168.15	unknown	Germany		44780	EVERSCALE-ASDE	true
51.210.242.234	unknown	France		16276	OVHFR	true
217.182.143.207	unknown	France		16276	OVHFR	true
69.16.218.101	unknown	United States		32244	LIQUIDWEBUS	true
159.69.237.188	unknown	Germany		24940	HETZNER-ASDE	true
45.138.98.34	unknown	Germany		9009	M247GB	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
78.46.73.125	unknown	Germany		24940	HETZNER-ASDE	true
37.59.209.141	unknown	France		16276	OVHFR	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
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
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
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553129
Start date:	14.01.2022
Start time:	11:06:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7MhGa3iotM (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

Copyright Joe Security LLC 2022

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@27/9@0/28
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 35.7% (good quality ratio 34%) • Quality average: 75% • Quality standard deviation: 26%
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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:08:32	API Interceptor	7x Sleep call for process: svchost.exe modified
11:08:44	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".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):	290
Entropy (8bit):	2.968077906394976
Encrypted:	false
SSDEEP:	6:kKhg05SN+SkQlPlEGYRMY9z+4KlDA3RUe/:LHkPlE99SNxAhUe/
MD5:	73A83B68EEC56F6FCE5D94AFE5DA3754
SHA1:	C890FCF934893E2C207F0AC9F515F939F961B2CB
SHA-256:	BA6B5262B6379BFDB13F8FB878C85EE73D2E7EA8901D062B30787C074408B8BE
SHA-512:	2BAC200648638F8C83B583CC8AE4FE9F4F319A523F9D862476BCEDBCB7F4B13F393C95AEA4EC360C9DC275FC186AEC7E4ECEE32D28D72ACD312607D4944E149
Malicious:	false
Preview:	p..... .....%..z...(..... .....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...

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101672685363626
Encrypted:	false
SSDEEP:	12:26WlXm/Ey6q9995lq3qQ10nMCldimE8eawHjcMN:26Wll68WLyMCldzE9BHjcMN
MD5:	75C2DE0C97DD15E5AC9CF377585FA04E
SHA1:	BD1A00C70BA04402662C30704E52F724E1EDFE23
SHA-256:	E6726753A68B67804E82A85CA857C472E73A8C6F544908A26D72C421CD4CEF8B
SHA-512:	98DC8FB57398E8BB10A16B046E8E9E56CF13D4D6A4C614558387746E3449A5253BE1C50C587AD4E781A4041F88C318D0FCC8C88EA7E29EB8446784F91280C807
Malicious:	false
Preview:	.....{j.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c)un}..... .....@-7.z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....G({j..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11270787281031859
Encrypted:	false
SSDEEP:	12:ikXm/Ey6q9995Q1miM3qQ10nMCldimE8eawHza1miIPxp:itl68S1tMLyMCldzE9BHza1tIPv
MD5:	C2B7134EDA03414935D4BEA1CB0ABB11
SHA1:	8F30DEA4ACDD8349EE72592EB08C80FDD66903C0
SHA-256:	8A359453C99992A0DB2003A515696AB1EF23D9269609F79ED1F72D25D8B2F56A
SHA-512:	4A76F32772F84ADAEC5A2806A67C22120CB7E7B78F9AADD94841340C3DF3DF459923FC8C091BBFA377265F41496FFB85BB59C50B235B77E6C41CA5CE0E690E42
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Preview:	.....yyj.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c)un}..... .....%.0.z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....yj..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1126590871725233
Encrypted:	false
SSDEEP:	12:iRVXm/Ey6q9995Q1mK2P3qQ10nMCldimE8eawHza1mK63oN:iR4l68S1iPLyMCldzE9BHza123oN
MD5:	E7A6CAE1C5F91225F13E66DE1D75FFCF
SHA1:	23AC2F55B12BEF143E76D1B8E8AC89CB8099C26D
SHA-256:	65A61535E5289512E2DE344CD19EE17E79ECFD3618AEB32927EFA320203C16AD
SHA-512:	CC3FDC6B3CF426A252B39E049B72D49B48BAA13FFC73A4E2A8727175BFF7AC75FEEC0EC95087FE121932E872A206EBF1E41CD190D1CCE13D7F89D1EE0178F9 B2
Malicious:	false
Preview:	.....Cxj.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c)un}..... .....%.0.z.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....Sxj..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001@` (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1101672685363626
Encrypted:	false
SSDEEP:	12:26WlXm/Ey6q9995lq3qQ10nMCldimE8eawHjcMN:26WIl68WLyMCldzE9BHjcMN
MD5:	75C2DE0C97DD15E5AC9CF377585FA04E
SHA1:	BD1A00C70BA04402662C30704E52F724E1EDFE23
SHA-256:	E6726753A68B67804E82A85CA857C472E73A8C6F544908A26D72C421CD4CEF8B
SHA-512:	98DC8FB57398E8BB10A16B046E8E9E56CF13D4D6A4C614558387746E3449A5253BE1C50C587AD4E781A4041F88C318D0FCC8C88EA7E29EB8446784F91280C807
Malicious:	false
Preview:	.....{j.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c)un}..... .....@-7.z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....G({j..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11270787281031859
Encrypted:	false
SSDEEP:	12:ikXm/Ey6q9995Q1miM3qQ10nMCldimE8eawHza1miIPxp:itl68S1tMLyMCldzE9BHza1tIPv
MD5:	C2B7134EDA03414935D4BEA1CB0ABB11
SHA1:	8F30DEA4ACDD8349EE72592EB08C80FDD66903C0
SHA-256:	8A359453C99992A0DB2003A515696AB1EF23D9269609F79ED1F72D25D8B2F56A
SHA-512:	4A76F32772F84ADAEC5A2806A67C22120CB7E7B78F9AADD94841340C3DF3DF459923FC8C091BBFA377265F41496FFB85BB59C50B235B77E6C41CA5CE0E690E4 2
Malicious:	false
Preview:	.....yyj.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c)un}..... .....%.0.z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....yj..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001C8 (copy)	
Process:	C:\Windows\System32\svchost.exe

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001C8 (copy)	
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1126590871725233
Encrypted:	false
SSDEEP:	12:iRVXm/Ey6q9995Q1mK2P3qQ10nMCldimE8eawHza1mK63oN:iR4l68S1iPLyMCldzE9BHza123oN
MD5:	E7A6CAE1C5F91225F13E66DE1D75FFCF
SHA1:	23AC2F55B12BEF143E76D1B8E8AC89CB8099C26D
SHA-256:	65A61535E5289512E2DE344CD19EE17E79ECFD3618AEB32927EFA320203C16AD
SHA-512:	CC3FDC6B3CF426A252B39E049B72D49B48BAA13FFC73A4E2A8727175BFF7AC75FEEC0EC95087FE121932E872A206EBF1E41CD190D1CCE13D7F89D1EE0178F9B2
Malicious:	false
Preview:	.....Cxj.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c)un}..... .....%.0.z.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....Sxj.....

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):	3.162897933838449
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zl+q:j+s+v+b+P+m+0+Q+q+u+q
MD5:	593A937962715FDBD857B705A9988F7F
SHA1:	9AC262E6FD279F69ED37720956C9E545CC6EF56A
SHA-256:	9B633FC8F9952A7B752D245CD68447D047A72728075ECEDA08A73D96780A94AE
SHA-512:	690A19B0F33B26893B3E70E61E05B7C31BA9B6FD770381385C78A820DD5875A4F5CF9A37872AE898750D84E5F1F50054B19DD1393E02B6929FE26EA023923DE1
Malicious:	false
Preview:	.....-.-.-.

File Icon



Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x10017b85
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x61E02B6B [Thu Jan 13 13:38:51 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:	90add561a8bf6976696c056c199a41b8

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x27f5e	0x28000	False	0.514996337891	data	6.66251942868	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x29000	0x8410	0x9000	False	0.308946397569	data	4.83100368645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x2a9a0	0x27000	False	0.963572966747	data	7.93281036967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x5d000	0x3664	0x4000	False	0.274780273438	data	4.49622273105	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x61000	0x8284	0x9000	False	0.33251953125	data	3.82081999119	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

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
01/14/22-11:07:56.625038	TCP	2404332	ET CNC Feodo Tracker Reported CnC Server TCP group 17	49746	80	192.168.2.3	45.138.98.34
01/14/22-11:07:57.706065	TCP	2404338	ET CNC Feodo Tracker Reported CnC Server TCP group 20	49747	8080	192.168.2.3	69.16.218.101

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 11:08:00.934662104 CET	8.8.8.8	192.168.2.3	0x14b3	No error (0)	windowsupdate.s.llnwi.net		41.63.96.128	A (IP address)	IN (0x0001)
Jan 14, 2022 11:08:00.934662104 CET	8.8.8.8	192.168.2.3	0x14b3	No error (0)	windowsupdate.s.llnwi.net		41.63.96.0	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SgrmBroker.exe PID: 7124 Parent PID: 572

General

Start time:	11:07:42
Start date:	14/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false

Copyright Joe Security LLC 2022

Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7a43c0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 7152 Parent PID: 572

General

Start time:	11:07:42
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: loaddll32.exe PID: 6180 Parent PID: 4248

General

Start time:	11:07:43
Start date:	14/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll"
Imagebase:	0x880000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5808 Parent PID: 572

General

Start time:	11:07:43
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: cmd.exe PID: 1496 Parent PID: 6180

General

Start time:	11:07:43
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",#1
Imagebase:	0xd80000
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 Show Windows behavior

Analysis Process: regsvr32.exe PID: 3348 Parent PID: 6180

General

Start time:	11:07:43
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\7MhGa3iotM.dll
Imagebase:	0xb70000
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: 00000005.00000002.294428773.0000000004E31000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.294337664.0000000004E00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 5732 Parent PID: 1496

General

Start time:	11:07:43
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",#1
Imagebase:	0x8b0000
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: 00000006.00000002.294757561.00000000043D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.294482062.0000000002990000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6388 Parent PID: 6180

General

Start time:	11:07:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\7MhGa3iotM.dll,DllRegisterServer
Imagebase:	0x8b0000
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: 00000008.00000002.298606993.00000000056B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298670924.00000000056E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.297938888.00000000052E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298239999.00000000054F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.297893846.0000000005280000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298028546.0000000005390000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298441375.0000000005550000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.297464641.0000000003430000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298510030.0000000005581000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.297668150.0000000004D91000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298093850.00000000053C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.298383199.0000000005521000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: rundll32.exe PID: 5388 Parent PID: 3348

General

Start time:	11:07:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",DllRegisterServer
Imagebase:	0x8b0000
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: 3360 Parent PID: 5732

General

Start time:	11:07:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\7MhGa3iotM.dll",DllRegisterServer
Imagebase:	0x8b0000
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: 0000000A.00000002.297817521.0000000004AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.297755557.0000000004AC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.297710814.0000000004A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.295787483.0000000000850000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.297638381.000000000049C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.297863633.0000000004B21000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.297583118.0000000004990000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000A.00000002.295818674.0000000000881000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 2172 Parent PID: 6388

General

Start time:	11:07:47
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Kgiezrb\edgitxrppqaf.tym", JFlwYpDQ
Imagebase:	0x8b0000
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: 0000000C.00000002.301385832.0000000004A71000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.301361900.0000000004A40000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6512 Parent PID: 2172

General

Start time:	11:07:48
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Kgiezrb\edgitxrppqaf.tym", DllRegisterServer
Imagebase:	0x8b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815959143.0000000004E91000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816961696.00000000050F1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.814399683.0000000002D50000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815700731.0000000004D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815587816.0000000004C51000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817960495.0000000005651000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815509685.0000000004C20000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815776896.0000000004D31000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817419709.00000000051D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816312049.0000000004FD1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816141431.0000000004EF1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.814627918.00000000043C1000.00000020.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816054659.0000000004EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.814701416.0000000004480000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816243405.0000000004FA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817244449.00000000051A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815880931.0000000004E60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817694741.00000000053A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817922483.0000000005620000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.816664369.00000000050C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.815012363.00000000045D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000D.00000002.817778819.00000000053D1000.00000020.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3396 Parent PID: 572

General

Start time:	11:07:55
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes

MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6640 Parent PID: 572

General

Start time:	11:08:06
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1496 Parent PID: 572

General

Start time:	11:08:19
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1460 Parent PID: 572

General

Start time:	11:08:30
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2022

Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 6456 Parent PID: 5808

General

Start time:	11:08:43
Start date:	14/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff6b2fd0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 5952 Parent PID: 6456

General

Start time:	11:08:44
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022