ID: 480340
Sample Name:
0TOEtGJHN8.exe
Cookbook: default.jbs
Time: 10:03:06
Date: 09/09/2021
Version: 33.0.0 White Diamond

Table of Contents

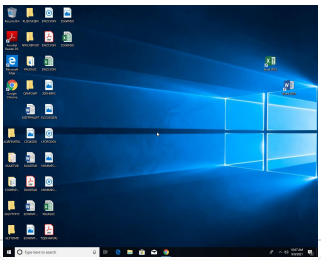
Windows Analysis Report 0TOEtGJHN8.exe

Overview

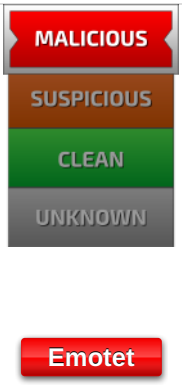
General Information

Sample Name:	0TOEtGJHN8.exe
Analysis ID:	480340
MD5:	3639d17c494474..
SHA1:	0047a882cf542b9.
SHA256:	2cb7516c937ad8..
Infos:	

Most interesting Screenshot:



Detection



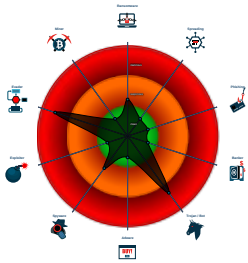
Emotet

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Query firmware table information (lik…
- Changes security center settings (no…
- Machine Learning detection for samp…
- Found evasive API chain (may stop…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Drops executables to the windows d…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- 0TOEtGJHN8.exe (PID: 360 cmdline: 'C:\Users\user\Desktop\0TOEtGJHN8.exe' MD5: 3639D17C4944743AC5C70C4E1BD30178)
  - mfnetsrc.exe (PID: 5116 cmdline: C:\Windows\SysWOW64\keyiso\mfnetsrc.exe MD5: 3639D17C4944743AC5C70C4E1BD30178)
- svchost.exe (PID: 5900 cmdline: c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s NgcSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5044 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s NgcCtnrSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6060 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6076 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5088 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3528 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4512 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4392 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1284 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1324 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5480 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5864 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 2592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6268 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6308 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhANQOcBKvh5xEW7VcJ9totsjdBwuAclxS\nQ0e09fk8V053lktpW3TRrzAW63yt6j1KWnyxMrU3igFXypBoI4lVNmkje4UPtIIS\nfkzjEIvG1v/ZNn1k0J0PfFTxbFFeUEs3AwIDAQAB",
  "C2 list": [
    "102.182.145.130:80",
    "173.173.254.105:80",
    "64.207.182.168:8080",
    "51.89.199.141:8080",
    "167.114.153.111:8080",
    "173.63.222.65:80",
    "218.147.193.146:80",
    "59.125.219.109:443",
    "172.104.97.173:8080",
    "190.162.215.233:80",
```

```
"68.115.186.26:80",
"78.188.106.53:443",
"190.240.194.77:443",
"24.133.106.23:80",
"80.227.52.78:80",
"79.137.83.50:443",
"120.150.218.241:443",
"62.171.142.179:8080",
"194.4.58.192:7080",
"62.30.7.67:443",
"134.209.144.106:443",
"24.230.141.169:80",
"194.190.67.75:80",
"172.91.208.86:80",
"201.241.127.190:80",
"185.94.252.104:443",
"104.131.11.150:443",
"71.15.245.148:8080",
"176.111.60.55:8080",
"172.86.188.251:8080",
"194.187.133.160:443",
"113.61.66.94:80",
"91.211.88.52:7080",
"202.134.4.216:8080",
"154.91.33.137:443",
"74.40.205.197:443",
"87.106.139.101:8080",
"66.76.12.94:8080",
"139.59.60.244:8080",
"112.185.64.233:80",
"85.105.111.166:80",
"74.208.45.104:8080",
"94.230.70.6:80",
"49.3.224.99:8080",
"119.59.116.21:8080",
"182.208.30.18:443",
"184.180.181.202:80",
"47.36.140.164:80",
"186.70.56.94:443",
"187.161.206.24:80",
"102.182.93.220:80",
"201.171.244.130:80",
"190.12.119.180:443",
"89.121.205.18:80",
"110.145.77.103:80",
"172.105.13.66:443",
"108.46.29.236:80",
"49.50.209.131:80",
"75.143.247.51:80",
"137.59.187.107:8080",
"188.219.31.12:80",
"61.33.119.226:443",
"209.141.54.221:7080",
"95.213.236.64:8080",
"120.150.60.189:80",
"190.164.104.62:80",
"186.74.215.34:80",
"139.99.158.11:443",
"61.19.246.238:443",
"121.7.31.214:80",
"88.153.35.32:80",
"5.39.91.110:7080",
"123.142.37.166:80",
"50.245.107.73:443",
"95.9.5.93:80",
"37.139.21.175:8080",
"157.245.99.39:8080",
"217.123.207.149:80",
"72.186.136.247:443",
"115.94.207.99:443",
"202.141.243.254:443",
"78.24.219.147:8080",
"97.82.79.83:80",
"217.20.166.178:7080",
"203.153.216.189:7080",
"220.245.198.194:80",
"168.235.67.138:7080",
"110.142.236.207:80",
"162.241.140.129:8080",
"76.175.162.101:80",
"27.114.9.93:80",
"24.178.90.49:80",
"202.134.4.211:8080",
"123.176.25.234:80",
"61.76.222.210:80",
"109.116.245.80:80",
"139.162.60.124:8080",
"190.108.228.27:443",
"94.23.237.171:443",
"2.58.16.89:8080",
"37.179.204.33:80",
```

```
    "96.245.227.43:80",
    "216.139.123.119:80",
    "89.216.122.92:80",
    "37.187.72.193:8080",
    "74.214.230.200:80",
    "93.147.212.206:80",
    "103.86.49.11:8080",
    "174.106.122.139:80",
    "138.68.87.218:443",
    "118.83.154.64:443",
    "200.116.145.225:443",
    "94.200.114.161:80",
    "62.75.141.82:80",
    "121.124.124.40:7080",
    "176.113.52.6:443",
    "24.137.76.62:80",
    "41.185.28.84:8080",
    "50.91.114.38:80",
    "46.105.131.79:8080",
    "109.74.5.95:8080",
    "67.170.250.203:443"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.642790111.0000000002A34000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.642889433.0000000002AA1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.642626999.00000000029F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.249411331.0000000002900000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.249838612.00000000029C1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.mfnetsrc.exe.29f279e.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.0TOEtGJHN8.exe.29c0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.0TOEtGJHN8.exe.290279e.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.mfnetsrc.exe.2aa0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.0TOEtGJHN8.exe.290279e.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Machine Learning detection for sample

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Emotet

Persistence and Installation Behavior:

- Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Query firmware table information (likely to detect VMs)
- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

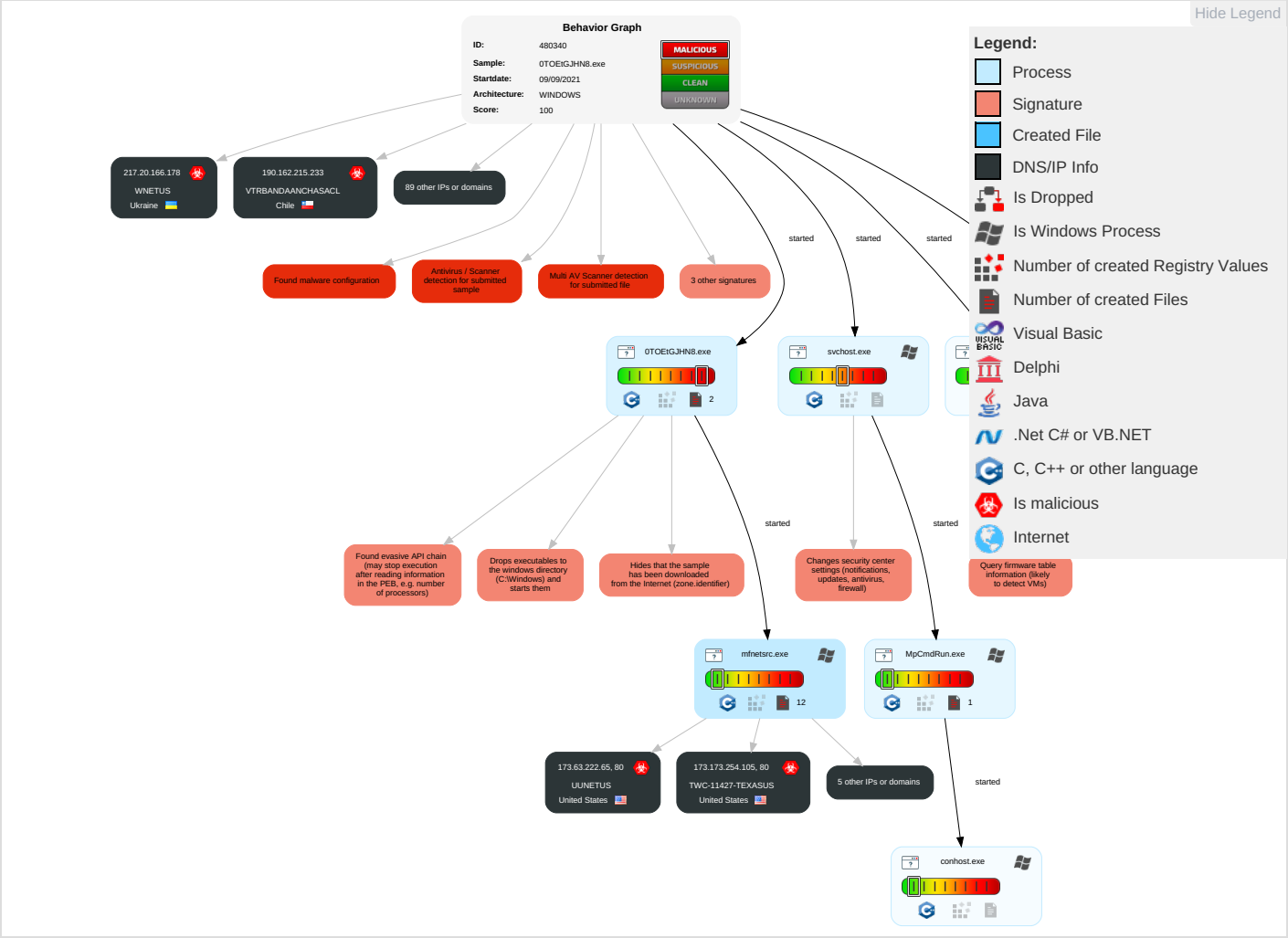
- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2 2	Eavesdr Insecure Network Commun
Default Accounts	Native API 1 1	Windows Service 2	Windows Service 2	Obfuscated Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	Service Execution 1	Logon Script (Windows)	Process Injection 2	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 2	Cached Domain Credentials	Security Software Discovery 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2	DCSync	Virtualization/Sandbox Evasion 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Sta

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
0TOEtGJHN8.exe	86%	Virustotal		Browse
0TOEtGJHN8.exe	54%	Metadefender		Browse
0TOEtGJHN8.exe	88%	ReversingLabs	Win32.Trojan.Injuke	
0TOEtGJHN8.exe	100%	Avira	TR/Crypt.Agent.hgrgz	
0TOEtGJHN8.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.0TOEtGJHN8.exe.290279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.mfnetsrc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
3.2.mfnetsrc.exe.29f279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.0TOEtGJHN8.exe.29c0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.mfnetsrc.exe.2aa0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.0TOEtGJHN8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
0.2.0TOEtGJHN8.exe.290052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
0.0.0TOEtGJHN8.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
3.2.mfnetsrc.exe.29f052e.1.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
3.2.mfnetsrc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://167.114.153.111:8080/Rbtuwk6tKXDP8l/q4Zme1rFlg/AdvdAlL/b4ILIf/Q8rZVqkkq/rDnmG2Ans/	0%	Avira URL Cloud	safe	
http://102.182.145.130/Zffxf	0%	Avira URL Cloud	safe	
http://64.207.182.168:8080/OQYP1ogFQccmQuTysw1/v0tPhparrkDhC/NKHirfkcd6IUp4b2kRd/qhg8GSGX1b4ILIf/Q8r	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/Rbtuwk6tKXDP8l/q4Zme1rFlg/AdvdAlL/A	0%	Avira URL Cloud	safe	
http://172.104.97.173:8080/NrjO6cKOEtsgnTfdu/DdqP4I6wYv/OEK9fq/iwQk9ak8yU1H9c63AU/	0%	Avira URL Cloud	safe	
http://59.125.219.109:443/VRRce6rlsw9pK/DtY9XymlLmhK7GfUco/	0%	Avira URL Cloud	safe	
http://218.147.193.146/GJXuLUUeqrq95alY1u/oD6pJ15oDS4/Z4M9h0lWKV4FEH0yB/k3vm9W8xS/TW0iKm9TEcJ7gRi0P/	0%	Avira URL Cloud	safe	
http://173.173.254.105/dVjtW6oMoXz0rsF/f6FHy9ps6/FNv98e/sYjdUx6EAD0WvYm/t	0%	Avira URL Cloud	safe	
http://173.173.254.105/dVjtW6oMoXz0rsF/f6FHy9ps6/FNv98e/sYjdUx6EAD0WvYm/u	0%	Avira URL Cloud	safe	
http://173.173.254.105/dVjtW6oMoXz0rsF/f6FHy9ps6/FNv98e/sYjdUx6EAD0WvYm/	0%	Avira URL Cloud	safe	
http://https://59.125.219.109:443/VRRce6rlsw9pK/DtY9XymlLmhK7GfUco/	0%	Avira URL Cloud	safe	
http://102.182.145.130/ZffxffN/UUQGAqPKLO/	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://51.89.199.141:8080/7zUrbHAgoGBYLL/SfmOyzopGPV6GjKjz/2Kjj2o/	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://173.63.222.65/VQIMkjZKFdAVmy/be209e2c34a9550b8LMEM	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://173.63.222.65/VQIMkjZKFdAVmy/	0%	Avira URL Cloud	safe	
http://172.104.97.173:8080/NrjO6cKOEtsgnTfdu/DdqP4I6wYv/OEK9fq/iwQk9ak8yU1H9c63AU/lication/octet-str	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://51.89.199.141:8080/7zUrbHAgoGBYLL/SfmOyzopGPV6GjKjz/2Kjj2o/r7Gp	0%	Avira URL Cloud	safe	
http://167.114.153.111:8080/Rbtuwk6tKXDP8l/q4Zme1rFlg/AdvdAlL/	0%	Avira URL Cloud	safe	
http://102.182.145.130/ZffxffN/UUQGAqPKLO/r	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://59.125.219.109:443/VRRce6rlsw9pK/DtY9XymlLmhK7GfUco/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.4.58.192	unknown	Kazakhstan		202958	HOSTER-KZ	true
102.182.93.220	unknown	South Africa		37611	AfrihostZA	true
95.9.5.93	unknown	Turkey		9121	TTNETTR	true
94.200.114.161	unknown	United Arab Emirates		15802	DU-AS1AE	true
72.186.136.247	unknown	United States		33363	BHN-33363US	true
115.94.207.99	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
24.133.106.23	unknown	Turkey		47524	TURKSAT-ASTR	true
89.121.205.18	unknown	Romania		9050	RTDBucharestRomaniaRO	true
216.139.123.119	unknown	United States		395582	GRM-NETWORKUS	true
200.116.145.225	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
172.105.13.66	unknown	United States		63949	LINODE-APLinodeLLCUS	true
138.68.87.218	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
220.245.198.194	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	true
67.170.250.203	unknown	United States		7922	COMCAST-7922US	true
104.131.11.150	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
176.111.60.55	unknown	Ukraine		24703	UN-UKRAINE-ASKievUkraineUA	true
24.178.90.49	unknown	United States		20115	CHARTER-20115US	true
94.23.237.171	unknown	France		16276	OVHFR	true
187.161.206.24	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	true
41.185.28.84	unknown	South Africa		36943	GridhostZA	true
194.190.67.75	unknown	Russian Federation		50804	BESTLINE-NET-PROTVINORU	true
186.74.215.34	unknown	Panama		11556	CableWirelessPanamaPA	true
109.116.245.80	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
202.134.4.216	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
120.150.218.241	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
202.134.4.211	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
87.106.139.101	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
62.30.7.67	unknown	United Kingdom		5089	NTLGB	true
123.142.37.166	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
51.89.199.141	unknown	France		16276	OVHFR	true
75.143.247.51	unknown	United States		20115	CHARTER-20115US	true
49.3.224.99	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	true
162.241.140.129	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
62.75.141.82	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
119.59.116.21	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
172.91.208.86	unknown	United States		20001	TWC-20001-PACWESTUS	true
113.61.66.94	unknown	Australia		45510	TELCOINABOX-AULevel109HunterStreetAU	true
96.245.227.43	unknown	United States		701	UUNETUS	true
37.139.21.175	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
194.187.133.160	unknown	Bulgaria		13124	IBGCBG	true
121.7.31.214	unknown	Singapore		9506	SINGTEL-FIBRESingtelFibreBroadbandSG	true
112.185.64.233	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
61.76.222.210	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
95.213.236.64	unknown	Russian Federation		49505	SELECTELRU	true
46.105.131.79	unknown	France		16276	OVHFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
27.114.9.93	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
74.214.230.200	unknown	United States		36728	EMERYTELCOMUS	true
190.162.215.233	unknown	Chile		22047	VTRBANDAANCHASACL	true
110.145.77.103	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
154.91.33.137	unknown	Seychelles		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	true
120.150.60.189	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
93.147.212.206	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
91.211.88.52	unknown	Ukraine		206638	HOSTFORYUA	true
172.86.188.251	unknown	Canada		32489	AMANAHA-NEWCA	true
157.245.99.39	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
167.114.153.111	unknown	Canada		16276	OVHFR	true
37.179.204.33	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
203.153.216.189	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
59.125.219.109	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	true
2.58.16.89	unknown	Latvia		64421	SERTEX-ASLV	true
62.171.142.179	unknown	United Kingdom		51167	CONTABODE	true
123.176.25.234	unknown	Maldives		7642	DHIRAAGU-MV-APDHIVEHIRAAJJEYGEGULHUNPLCMV	true
50.91.114.38	unknown	United States		33363	BHN-33363US	true
61.33.119.226	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
217.123.207.149	unknown	Netherlands		33915	TNF-ASNL	true
78.24.219.147	unknown	Russian Federation		29182	THEFIRST-ASRU	true
173.63.222.65	unknown	United States		701	UUNETUS	true
47.36.140.164	unknown	United States		20115	CHARTER-20115US	true
110.142.236.207	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
139.99.158.11	unknown	Canada		16276	OVHFR	true
201.171.244.130	unknown	Mexico		8151	UninetSAdeCVMX	true
49.50.209.131	unknown	New Zealand		55853	MEGATEL-AS-APMegatelNZ	true
190.108.228.27	unknown	Argentina		27751	NeunetSAAR	true
202.141.243.254	unknown	Pakistan		9260	MULTINET-AS-APMultinetPakistanPvtLtdPK	true
121.124.124.40	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
139.59.60.244	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
61.19.246.238	unknown	Thailand		9335	CAT-CLOUD-APCATTelecomPublicCompanyLimitedTH	true
168.235.67.138	unknown	United States		3842	RAMNODEUS	true
137.59.187.107	unknown	Hong Kong		18106	VIEWQWEST-SG-APViewqwestPteLtdSG	true
78.188.106.53	unknown	Turkey		9121	TTNETTR	true
71.15.245.148	unknown	United States		20115	CHARTER-20115US	true
188.219.31.12	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
64.207.182.168	unknown	United States		398110	GO-DADDY-COM-LLCUS	true
217.20.166.178	unknown	Ukraine		1820	WNETUS	true
24.230.141.169	unknown	United States		11232	MIDCO-NETUS	true
74.208.45.104	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
134.209.144.106	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
186.70.56.94	unknown	Ecuador		14522	SatnetEC	true
97.82.79.83	unknown	United States		20115	CHARTER-20115US	true
173.173.254.105	unknown	United States		11427	TWC-11427-TEXASUS	true
172.104.97.173	unknown	United States		63949	LINODE-APLinodeLLCUS	true
190.12.119.180	unknown	Argentina		11014	CPSAR	true
139.162.60.124	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	true
184.180.181.202	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.113.52.6	unknown	Russian Federation		8712	INTA-ASRU	true
68.115.186.26	unknown	United States		20115	CHARTER-20115US	true
201.241.127.190	unknown	Chile		22047	VTRBANDAANCHASACL	true
24.137.76.62	unknown	Canada		11260	EASTLINK-HSICA	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	480340
Start date:	09.09.2021
Start time:	10:03:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0TOEtGJHN8.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/10@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 23.2%) • Quality average: 73.5% • Quality standard deviation: 19.9%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:04:11	API Interceptor	1x Sleep call for process: svchost.exe modified
10:05:27	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.4.58.192	bol88C399w.exe	Get hash	malicious	Browse	
	bol88C399w.exe	Get hash	malicious	Browse	
	v8iFmF7XPp.dll	Get hash	malicious	Browse	
	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
102.182.93.220	0TOEtGJHN8.exe	Get hash	malicious	Browse	
	bol88C399w.exe	Get hash	malicious	Browse	
	bol88C399w.exe	Get hash	malicious	Browse	
	2ojdmC51As.exe	Get hash	malicious	Browse	
95.9.5.93	0TOEtGJHN8.exe	Get hash	malicious	Browse	
	bol88C399w.exe	Get hash	malicious	Browse	
	bol88C399w.exe	Get hash	malicious	Browse	
	v8iFmF7XPp.dll	Get hash	malicious	Browse	
	2ojdmC51As.exe	Get hash	malicious	Browse	
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	
94.200.114.161	test-emotet.exe	Get hash	malicious	Browse	• 94.200.114.161/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTER-KZ	0TOEtGJHN8.exe	Get hash	malicious	Browse	• 194.4.58.192
	bol88C399w.exe	Get hash	malicious	Browse	• 194.4.58.192
	bol88C399w.exe	Get hash	malicious	Browse	• 194.4.58.192
	jax.k.dll	Get hash	malicious	Browse	• 185.100.65.29
	0519_3361871008218.doc	Get hash	malicious	Browse	• 185.100.65.29
	fax.f.dll	Get hash	malicious	Browse	• 185.100.65.29
	0513_3111026702554.doc	Get hash	malicious	Browse	• 185.100.65.29
	0513_1360918519077.doc	Get hash	malicious	Browse	• 185.100.65.29
	581a98e7_by_Libranalysis.docm	Get hash	malicious	Browse	• 185.100.65.29
	Win32.exe	Get hash	malicious	Browse	• 185.113.134.179
	jers.dll	Get hash	malicious	Browse	• 185.100.65.29
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 194.4.58.192
	wininit.dll	Get hash	malicious	Browse	• 185.100.65.29
	0408_391585988029.doc	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.pumpl.dll	Get hash	malicious	Browse	• 185.100.65.29
	msals.dll	Get hash	malicious	Browse	• 185.100.65.29
	NvContainer.exe	Get hash	malicious	Browse	• 185.113.134.179
	0318_45657944978421.doc	Get hash	malicious	Browse	• 185.100.65.29
	2ojdmC51As.exe	Get hash	malicious	Browse	• 194.4.58.192
AfrihostZA	0TOEtGJHN8.exe	Get hash	malicious	Browse	• 102.182.145.130
	2JOGBbciho	Get hash	malicious	Browse	• 169.85.189.226
	hzD4UBTK5H	Get hash	malicious	Browse	• 169.209.50.42
	N2fpnW8P5q	Get hash	malicious	Browse	• 169.212.193.44
	Darknet.arm7	Get hash	malicious	Browse	• 102.182.120.199
	7bkrFirKok	Get hash	malicious	Browse	• 169.82.184.30
	uxHuQqDuZc	Get hash	malicious	Browse	• 169.217.110.44
	OnRFDWqdnF	Get hash	malicious	Browse	• 169.43.0.8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2vMBHaZcM5	Get hash	malicious	Browse	• 156.155.120.122
	b3astmode.x86	Get hash	malicious	Browse	• 169.185.9.1
	re.a1rmv4l	Get hash	malicious	Browse	• 169.174.32.208
	sora.arm7	Get hash	malicious	Browse	• 169.202.152.130
	AJK7j832D2	Get hash	malicious	Browse	• 169.108.199.40
	YlmvKUJ5gK	Get hash	malicious	Browse	• 169.18.199.19
	ENQUIRYSMRT119862021-ERW PIPES.pdf.exe	Get hash	malicious	Browse	• 169.1.24.244
	mips	Get hash	malicious	Browse	• 169.108.199.16
	brZRQRhRpd	Get hash	malicious	Browse	• 169.213.200.228
	0bqzNIp9PV	Get hash	malicious	Browse	• 169.87.203.46
	KSzA1ujvlV	Get hash	malicious	Browse	• 169.221.72.136
	y66dLhUn0G	Get hash	malicious	Browse	• 169.30.45.120

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):	24576
Entropy (8bit):	0.36205444996716485
Encrypted:	false
SSDEEP:	48:UtcctcMtcctcMtcctcMtcctcQtcctc0tcctc:UtTtDtTtDtTtDtTtTtTtbtTt
MD5:	353C0E84A6C573D30B15481706263B9A
SHA1:	4DCBF5ED97F1251EEF6E0747906368AB5639D0FA
SHA-256:	4412C6044B8C975D5BAB1F0E173339AE2A091A3B4D2DFBF771F1E9B854EF1751
SHA-512:	210B6E533923CF5F3FE255C39E1B2D243F675D2C022FA613E3ABD680FB552A2FD9079BF1699C91A5033AED47E29EE0191CF6E307429554A3128D2C009E047AFD
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:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.23858527923611406
Encrypted:	false
SSDEEP:	12:bNGaD0JcaaD0JwQQD8JtAg/0bjSQJ2Ali/HsRAls1sOAlTHsRAls1sOAl:bTgJctgJwb8JurjSu230Rf5zRf5
MD5:	3E95B62FD1FF65BF1D1451561D37D781
SHA1:	C061157BDDF36910FB72C06229E257DD79345F0E
SHA-256:	AFEE1D49362E794B42859C5FD7C54AD0EB7B2A3A91F684650D524A886F477C4C
SHA-512:	D2E743919C1707A3C22503690E813A1A70F0AFFCC76245C29B3D4C937B13F29C7EBF1668CB8AEEEAFD0101EB78BE8E404AFD2774AEC162097270A8D4A4C53FAB
Malicious:	false
Preview:	....E..h..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x8681bdb8, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0974673952193926
Encrypted:	false
SSDEEP:	12:Y/0+9XO4blKZGKy/0+9XO4blKZGKu0+9XO4bl2OMZGKu0+9XO4bl2OMZGK2t0+9A:Xf3f3Gw3GwF0lmF0lm5TzTTTzT
MD5:	7EF4473B7A34C26F39DC7F4177D84948
SHA1:	389A8362016E5078CFFDF3A4D1B37A3001D7628E
SHA-256:	905E233BAC7F289623635640280C03246C4BCBE383C3BAF3CB76AE972F494C9B
SHA-512:	8E778B66A10D806DF868C3E936541B7AC950B2492F82B95D48F0EDDE1374FB562085BDDC65691BC3CE2E5FD453565386601DF117B5C604BB57758A3B7DA45E0
Malicious:	false
Preview:	....e.f.3...w.....&.....w.....yQ.h.(.....3...w.....B.....@..... ....3...w..... .....yQ.....pwY.....yQ..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.11588758009323032
Encrypted:	false
SSDEEP:	12:8yNxt43Zx/NxUbteRldTlPxtWOmsRlmWlp6Al+OmsRlZl:8+xOpx/NxUSldZxLDlm27Dl
MD5:	E24DE8A56B2D3CD6849B0FC93667ABB2
SHA1:	099D3BB916A3C0518B4BDFBE88CDAFE8029F15C3
SHA-256:	81ECADE1DDB1325139A5B39D9893B03253B1AE8D98BE4DC20C85C4F19CD4B627
SHA-512:	FA408FD6A75DB8A9181552A6DD6CCC3713ECB823BE573383C0D9F005C393509C1202378A8689E4F0242827A42DB4CD9F41F2F05B82D4D74146A8B1F625125277
Malicious:	false
Preview:	;(.....3...w.....yQ.....w.....w.....w....:O.....w.....pwY.....yQ..... ....

C:\ProgramData\USOPrivate\UpdateStore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml.d (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	5.231597010571246
Encrypted:	false
SSDEEP:	24:2dS48pX4y/DvKWDkQpydX8ICDKbnTiTBMuT52YGP8EqXpWfKFghR4p/BzceFYMf9:cAn/TLtpuQ6Zhip/B4VM0SkC9+Tu8s
MD5:	B7D5597DC78BA1205B59EA0B1CD8FE77
SHA1:	436E94F5A3157D7DF0FC72CAD7703678A6089536
SHA-256:	2EED515C570006123233A8CBE9455A00C2D6C16823CE505FD5AEB33B46A719B8
SHA-512:	E6B09ECBA06E37C67D55660C09D94736AAB24B355350EBF053859851AB260BF989AE657F3ABB77E346833ACB8D31BADC045455E70979493E322A4FC1768B4A5E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399985333469120</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399985333781637</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399985333469120</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">132459503442223904</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml	
Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2493
Entropy (8bit):	5.231597010571246
Encrypted:	false
SSDEEP:	24:2dS48pX4y/DvKWDkQpydX8ICDKbnTiTBMuT52YGP8EqXpWfKFghR4p/BzceFYMf9:cAn/TLtpuQ6Zhip/B4VM0SkC9+Tu8s
MD5:	B7D5597DC78BA1205B59EA0B1CD8FE77
SHA1:	436E94F5A3157D7DF0FC72CAD7703678A6089536

C:\ProgramData\USOPrivate\UpdateStore\updatestoretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml	
SHA-256:	2EED515C570006123233A8CBE9455A00C2D6C16823CE505FD5AEB33B46A719B8
SHA-512:	E6B09ECBA06E37C67D55660C09D94736AAB24B355350EBF053859851AB260BF989AE657F3ABB77E346833ACB8D31BADC045455E70979493E322A4FC1768B4A5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?><updateStore><sessionVariables><permanent><AUOptions dataType="3">1</AUOptions><AllowMUUpdateService dataType="3">0</AllowMUUpdateService><AreUpdatesPausedByPolicy dataType="11">False</AreUpdatesPausedByPolicy><AttentionRequiredReason dataType="19">0</AttentionRequiredReason><CurrentState dataType="19">1</CurrentState><FirstScanAttemptTime dataType="21">132399985333469120</FirstScanAttemptTime><FlightEnabled dataType="3">0</FlightEnabled><LastError dataType="19">0</LastError><LastErrorState dataType="19">0</LastErrorState><LastErrorStateType dataType="11">False</LastErrorStateType><LastMeteredScanTime dataType="21">132399985333781637</LastMeteredScanTime><LastScanAttemptTime dataType="21">132399985333469120</LastScanAttemptTime><LastScanDeferredReason dataType="19">1</LastScanDeferredReason><LastScanDeferredTime dataType="21">132459503442223904</LastScanDeferredTime><LastScanFailureError dataType="3">-2147023838</LastScanFailureError><LastScanFailu

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.001.etl (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.7686197435894364
Encrypted:	false
SSDEEP:	96:Wi8i0pVZRgZNnAeZ6aZKZ5k907HUZFZoZ0ZAZLpV2ZtZeA3+ZMTn:Wi8i0pPcNnvREKSOKLpqHdoMj
MD5:	2B5184502C6E66FB07BF2F39B708B356
SHA1:	621BC0C77E9F16F4A6B5CE63C554DA035FF457C1
SHA-256:	6F681B095DA38ADD487AF3166A2558579789285B34E394D45522C69052B66BB8
SHA-512:	5CE350A3FDC1D5CA58B0430BF1434B5DDECD83DC17EFE09ECD515051E2DA9838AEA369FB3C655339662C6DCED7DBE59BD090E94E9B365EDF09A3C774731F A0A
Malicious:	false
Preview:	.....,....S.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....g...(..... .....S.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....,...S..... ....

C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration_Temp.1.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.7686197435894364
Encrypted:	false
SSDEEP:	96:Wi8i0pVZRgZNnAeZ6aZKZ5k907HUZFZoZ0ZAZLpV2ZtZeA3+ZMTn:Wi8i0pPcNnvREKSOKLpqHdoMj
MD5:	2B5184502C6E66FB07BF2F39B708B356
SHA1:	621BC0C77E9F16F4A6B5CE63C554DA035FF457C1
SHA-256:	6F681B095DA38ADD487AF3166A2558579789285B34E394D45522C69052B66BB8
SHA-512:	5CE350A3FDC1D5CA58B0430BF1434B5DDECD83DC17EFE09ECD515051E2DA9838AEA369FB3C655339662C6DCED7DBE59BD090E94E9B365EDF09A3C774731F A0A
Malicious:	false
Preview:	.....,....S.....B.....Zb..K....(.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....g...(..... .....S.....U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.U.S.O.S.h.a.r.e.d.\.L.o.g.s.\.U.p.d.a.t.e.S.e.s.s.i.o.n.O.r.c.h.e.s.t.r.a.t.i.o.n._.T.e.m.p...1...e.t.l.....P.P.....,...S..... ....

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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
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:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1482360894513364
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rkw/L1YZk9+MlWlLehB4yAq7ejC9w/L14l:OaqdmuF3rrj1f+kWReH4yJ7MTj1F
MD5:	94C47122414C60C3C6F9DB839DBD81E5
SHA1:	C2DED01A6605A35454F67EB97AF6BAB732E35321
SHA-256:	3111835B48E9F72B3DD2AD1B8D2655783CE3E1CE3B560834D2B9560466D30E3F
SHA-512:	A57065E4A286A1030E9BB642036301062C33D0E0B6853901CEA8476D30DCE37B87BFB636E66D273DFB13A61A7BE5772588797FB026D1A64C71EAEF2E19B0D74
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. .. S.e.p. .. 0.9. .. 2.0.2.1. .1.0.:.0.5.:.2. 7.........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. .. S.e.p. .. 0.9. .. 2.0.2.1. .1.0.:.0.5.:.2.7.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.4617069558872
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	0TOEtGJHN8.exe
File size:	364544
MD5:	3639d17c4944743ac5c70c4e1bd30178
SHA1:	0047a882cf542b94754496c8cb985ab64561f72c
SHA256:	2cb7516c937ad8b9467ca417530651e34340d231c36961 49c7d7b22e24ffaf9b
SHA512:	efbc3c75d893baa3e5fc5329ef7bc3163e686850f9196e2 ba758b486b18743fd2487476976d6c55b826da2ab1a017 ae854af0c53d4b95865a5221a387ba9ad11
SSDEEP:	6144:5uBkiwzntFj3OB0LPJQOZGhcvSSj2x+TGLNs3Et U7L:5HbFTOAQIacvSS6oqLFtsL
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......Y....c...c ...c.......c...|...c...|...c...|...c.......c...c..ic...|...c...e...c..Rich.c. .........PE..L...z.._...................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40a274
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5F9C077A [Fri Oct 30 12:30:50 2020 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:	c9f7e018b269f1b5fe81cf757d6f8e93

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa45f	0xb000	False	0.327281605114	data	5.39094221826	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0x10e	0x1000	False	0.00927734375	data	0.0298850891201	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd000	0x810a60	0x1000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x81e000	0x1168	0x2000	False	0.19482421875	data	2.91471949984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x820000	0x41d76	0x42000	False	0.752877900095	data	7.04184498603	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x862000	0x6f5e	0x7000	False	0.135777064732	data	1.65586384416	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 9, 2021 10:04:05.772666931 CEST	8.8.8.8	192.168.2.5	0x9f07	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 59.125.219.109
  - 59.125.219.109:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49818	59.125.219.109	443	C:\Windows\SysWOW64\keyiso\mfnetsrc.exe

Timestamp	kBytes transferred	Direction	Data
Sep 9, 2021 10:06:48.279891014 CEST	10528	OUT	POST /VRRce6rlsw9pK/DtY9XymlLmhK7GfUco/ HTTP/1.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate DNT: 1 Connection: keep-alive Referer: 59.125.219.109/ Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=----------vX8jXrCzouVUfgwE User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 59.125.219.109:443 Content-Length: 4580 Cache-Control: no-cache

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 0TOEtGJHN8.exe PID: 360 Parent PID: 5832

General

Start time:	10:04:03
Start date:	09/09/2021
Path:	C:\Users\user\Desktop\0TOEtGJHN8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\0TOEtGJHN8.exe'
Imagebase:	0x400000
File size:	364544 bytes
MD5 hash:	3639D17C4944743AC5C70C4E1BD30178
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.249411331.0000000002900000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.249838612.00000000029C1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.249721472.0000000002944000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Deleted

Analysis Process: svchost.exe PID: 5900 Parent PID: 556

General

Start time:	10:04:04
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s NgcSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5044 Parent PID: 556

General

Start time:	10:04:04
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s NgcCtnrSvc
Imagebase:	0x7ff797770000
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: mfnetsrc.exe PID: 5116 Parent PID: 360

General

Start time:	10:04:06
Start date:	09/09/2021
Path:	C:\Windows\SysWOW64\keyiso\mfnetsrc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\keyiso\mfnetsrc.exe
Imagebase:	0x400000
File size:	364544 bytes
MD5 hash:	3639D17C4944743AC5C70C4E1BD30178
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.642790111.0000000002A34000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.642889433.0000000002AA1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.642626999.00000000029F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 6060 Parent PID: 556

General

Start time:	10:04:06
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6076 Parent PID: 556

General

Start time:	10:04:11
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5088 Parent PID: 556

General

Start time:	10:04:16
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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

Show Windows behavior

Analysis Process: svchost.exe PID: 3528 Parent PID: 556

General

Start time:	10:04:21
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4512 Parent PID: 556

General

Start time:	10:04:22
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 4392 Parent PID: 556

General

Start time:	10:04:22
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
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: 1284 Parent PID: 556

General

Start time:	10:04:23
Start date:	09/09/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7360f0000
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: 1324 Parent PID: 556

General

Start time:	10:04:23
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5480 Parent PID: 556

General

Start time:	10:04:24
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6268 Parent PID: 556

General

Start time:	10:04:29
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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: 6308 Parent PID: 556

General

Start time:	10:04:39
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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: MpCmdRun.exe PID: 5864 Parent PID: 5480

General

Start time:	10:05:25
Start date:	09/09/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff74ef30000

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: 2592 Parent PID: 5864

General

Start time:	10:05:26
Start date:	09/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 7024 Parent PID: 556

General

Start time:	10:06:33
Start date:	09/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
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

Disassembly

Code Analysis