ID: 463770
Sample Name:
KNEa2w7v3a.exe
Cookbook: default.jbs
Time: 03:55:37
Date: 12/08/2021
Version: 33.0.0 White Diamond

Table of Contents

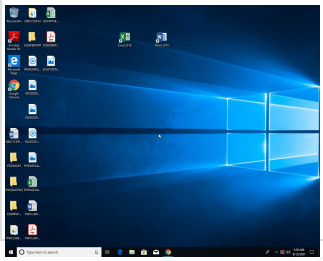
Windows Analysis Report KNEa2w7v3a.exe

Overview

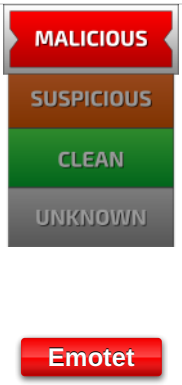
General Information

Sample Name:	KNEa2w7v3a.exe
Analysis ID:	463770
MD5:	f8adcf71a8c4e5c…
SHA1:	2246c5925aca14..
SHA256:	5303823581f2696.
Infos:	

Most interesting Screenshot:



Detection

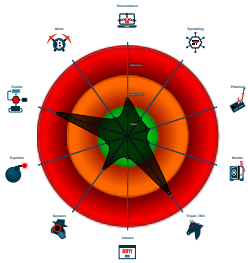


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- 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…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Checks if Antivirus/Antispyware/Fire…

Classification



Process Tree

- **System is w10x64**
- svchost.exe (PID: 5868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- KNEa2w7v3a.exe (PID: 5700 cmdline: 'C:\Users\user\Desktop\KNEa2w7v3a.exe' MD5: F8ADCF71A8C4E5C16D11308DFF998ECE)
  - wiaacmgr.exe (PID: 6124 cmdline: C:\Windows\SysWOW64\rdvgogl32\wiaacmgr.exe MD5: F8ADCF71A8C4E5C16D11308DFF998ECE)
    - Windows.Media.Playback.MediaPlayer.exe (PID: 6052 cmdline: C:\Windows\SysWOW64\CompPkgSup\Windows.Media.Playback.MediaPlayer.exe MD5: F8ADCF71A8C4E5C16D11308DFF998ECE)
- svchost.exe (PID: 5376 cmdline: c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s NgcSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1736 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s NgcCtnrSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4260 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5900 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4364 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6076 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4788 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5728 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 496 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1180 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 4072 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 720 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAOZ9fLJ8UrI0OZURpPsR3eijAyfPj3z6|nuS75f2igmYFW2aWgNcFIzsAYQleKzD0nlCFHOo7Zf8/4wY2UW0CJ4dJEHnE/PHlz|n6uNk3pxjm7o4eCDyiJbzf+k0Azjl0q54FQIDAQAB",
  "C2 list": [
    "190.202.229.74:80",
    "118.69.11.81:7080",
    "70.39.251.94:8080",
    "87.230.25.43:8080",
    "94.23.62.116:8080",
    "37.187.161.206:8080",
    "45.46.37.97:80",
    "138.97.60.141:7080",
    "177.144.130.105:8080",
```

```
"169.1.39.242:80",
"209.236.123.42:8080",
"202.134.4.210:7080",
"193.251.77.110:80",
"2.45.176.233:80",
"217.13.106.14:8080",
"189.223.16.99:80",
"190.101.156.139:80",
"77.238.212.227:80",
"181.58.181.9:80",
"37.183.81.217:80",
"74.58.215.226:80",
"174.118.202.24:443",
"168.197.45.36:80",
"81.215.230.173:443",
"192.175.111.212:7080",
"216.47.196.104:80",
"128.92.203.42:80",
"94.176.234.118:443",
"191.182.6.118:80",
"212.71.237.140:8080",
"24.232.228.233:80",
"177.73.0.98:443",
"177.23.7.151:80",
"24.135.69.146:80",
"83.169.21.32:7080",
"189.34.181.88:80",
"179.222.115.170:80",
"177.144.130.105:443",
"213.197.182.158:8080",
"5.89.33.136:80",
"77.78.196.173:443",
"120.72.18.91:80",
"50.28.51.143:8080",
"190.64.88.186:443",
"111.67.12.221:8080",
"12.162.84.2:8080",
"46.105.114.137:8080",
"59.148.253.194:8080",
"201.213.177.139:80",
"82.76.52.155:80",
"172.104.169.32:8080",
"188.251.213.180:80",
"46.43.2.95:8080",
"137.74.106.111:7080",
"188.135.15.49:80",
"185.94.252.27:443",
"197.232.36.108:80",
"60.249.78.226:8080",
"187.162.248.237:80",
"181.129.96.162:8080",
"46.101.58.37:8080",
"109.242.153.9:80",
"178.211.45.66:8080",
"200.59.6.174:80",
"83.103.179.156:80",
"172.86.186.21:8080",
"70.32.115.157:8080",
"81.214.253.80:443",
"201.49.239.200:443",
"149.202.72.142:7080",
"190.45.24.210:80",
"186.189.249.2:80",
"219.92.13.25:80",
"170.81.48.2:80",
"51.75.33.127:80",
"192.241.143.52:8080",
"45.33.77.42:8080",
"152.169.22.67:80",
"1.226.84.243:8080",
"78.206.229.130:80",
"37.179.145.105:80",
"68.183.170.114:8080",
"192.232.229.54:7080",
"103.236.179.162:80",
"70.32.84.74:8080",
"79.118.74.90:80",
"60.93.23.51:80",
"181.120.29.49:80",
"213.52.74.198:80",
"51.255.165.160:8080",
"183.176.82.231:80",
"186.193.229.123:80",
"98.103.204.12:443",
"129.232.220.11:8080",
"181.61.182.143:80",
"68.183.190.199:8080",
"190.115.18.139:8080",
"200.24.255.23:80",
"103.13.224.53:80",
"85.214.26.7:8080",
```

```
    "190.24.243.186:80",
    "87.106.46.107:8080",
    "177.107.79.214:8080",
    "12.163.208.58:80",
    "187.162.250.23:443",
    "109.101.137.162:8080",
    "82.76.111.249:443",
    "181.30.61.163:443",
    "5.196.35.138:7080",
    "51.15.7.145:80",
    "192.198.91.138:443",
    "188.157.101.114:80",
    "189.2.177.210:443",
    "181.123.6.86:80",
    "109.190.35.249:80",
    "45.16.226.117:443",
    "190.190.219.184:80",
    "104.131.41.185:8080",
    "101.187.81.254:80",
    "62.84.75.50:80",
    "178.250.54.208:8080",
    "201.71.228.86:80",
    "190.92.122.226:80",
    "138.97.60.140:8080"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.471191876.00000000020F0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.206004453.0000000002641000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.210049440.0000000002181000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.205611516.0000000002294000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.471538485.0000000002211000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.wiaacmgr.exe.20c052e.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.wiaacmgr.exe.2180000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.Windows.Media.Playback.MediaPlayer.exe.20f052e.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.KNEa2w7v3a.exe.223279e.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.KNEa2w7v3a.exe.223052e.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

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

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Emotet

Persistence and Installation Behavior:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

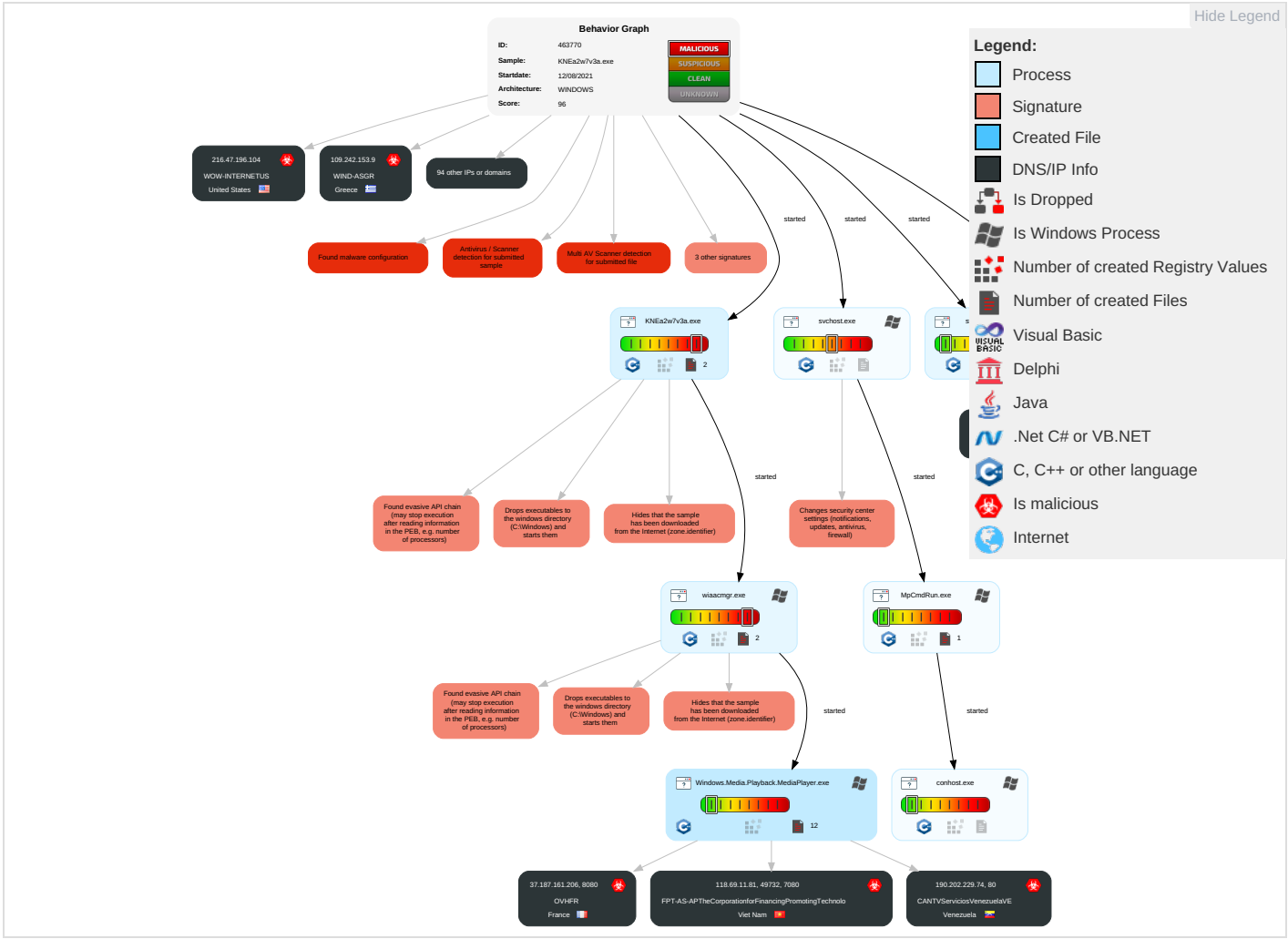
- Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Windows Service 1 2	Windows Service 1 2	Masquerading 1 2 1	Input Capture 1	Security Software Discovery 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesd Insecur Networ Commu
Default Accounts	Service Execution 1 1	DLL Side-Loading 1	Process Injection 2	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/S
Domain Accounts	Native API 1 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	System Service Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

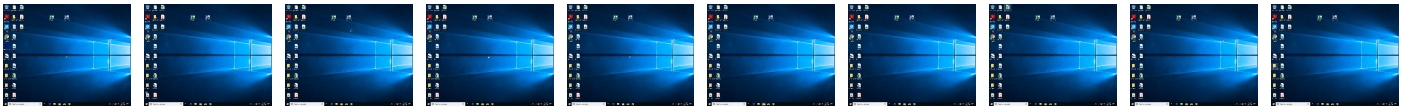
Behavior Graph



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
KNEa2w7v3a.exe	89%	Virustotal		Browse
KNEa2w7v3a.exe	57%	Metadefender		Browse
KNEa2w7v3a.exe	96%	ReversingLabs	Win32.Trojan.EmotetCrypt	
KNEa2w7v3a.exe	100%	Avira	TR/Injector.tthlz	
KNEa2w7v3a.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Windows.Media.Playback.MediaPlayer.exe.20f052e.1.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
4.2.wiaacmgr.exe.2180000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.wiaacmgr.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.KNEa2w7v3a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
1.0.KNEa2w7v3a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
4.2.wiaacmgr.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
1.2.KNEa2w7v3a.exe.223052e.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
1.2.KNEa2w7v3a.exe.223279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.Windows.Media.Playback.MediaPlayer.exe.20f279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.wiaacmgr.exe.20c052e.1.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
5.2.Windows.Media.Playback.MediaPlayer.exe.2210000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.Windows.Media.Playback.MediaPlayer.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
1.2.KNEa2w7v3a.exe.2640000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.Windows.Media.Playback.MediaPlayer.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139844		Download File
4.2.wiaacmgr.exe.20c279e.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://37.187.161.206:8080/AJT6ih/yjZb/vgDNbB0LE6VNEd/	0%	Avira URL Cloud	safe	
http://190.202.229.74/u2xUhDP9gvOFSFief0/IRiW/IMV8TOoDabstev/N	0%	Avira URL Cloud	safe	
http://118.69.11.81:7080/cLGKs29k/	0%	Avira URL Cloud	safe	
http://70.39.251.94:8080/blOro9t0iLZ/z7z	0%	Avira URL Cloud	safe	
http://118.69.11.81:7080/cLGKs29k/$	0%	Avira URL Cloud	safe	
http://118.69.11.81:7080/cLGKs29k/0	0%	Avira URL Cloud	safe	
http://190.202.229.74/u2xUhDP9gvOFSFief0/IRiW/IMV8TOoDabstev/	0%	Avira URL Cloud	safe	
http://94.23.62.116:8080/TkDGGoG/EjmXKjEQOJnYdPvRd/	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://70.39.251.94:8080/blOro9t7	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.214.253.80	unknown	Turkey		9121	TTNETTR	true
94.176.234.118	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
78.206.229.130	unknown	France		12322	PROXADFR	true
181.58.181.9	unknown	Colombia		10620	TelmexColombiaSACO	true
213.197.182.158	unknown	Lithuania		15440	BALTNETACustomersASLT	true
103.13.224.53	unknown	Bangladesh		58672	MAXNETONLINE-BDMaxnetOnlineBD	true
209.236.123.42	unknown	United States		393398	ASN-DISUS	true
79.118.74.90	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
51.15.7.145	unknown	France		12876	OnlineSASFR	true
190.45.24.210	unknown	Chile		22047	VTRBANDAANCHASACL	true
5.196.35.138	unknown	France		16276	OVHFR	true
190.190.219.184	unknown	Argentina		10481	TelecomArgentinaSAAR	true
200.59.6.174	unknown	Argentina		12150	COTELCAMAR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
181.129.96.162	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
50.28.51.143	unknown	United States		32244	LIQUIDWEBUS	true
189.34.181.88	unknown	Brazil		28573	CLAROSABR	true
149.202.72.142	unknown	France		16276	OVHFR	true
82.76.52.155	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
5.89.33.136	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
45.16.226.117	unknown	United States		7018	ATT-INTERNET4US	true
120.72.18.91	unknown	Philippines		38553	DCTECHDVO-AS-APInternetServiceProvideranddDataCenterP	true
187.162.250.23	unknown	Mexico		6503	AxtelSABdeCVMX	true
12.163.208.58	unknown	United States		7018	ATT-INTERNET4US	true
101.187.81.254	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
177.107.79.214	unknown	Brazil		52862	RedenilfServicosdeTelecomunicacoesLtdaBR	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
190.64.88.186	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	true
68.183.170.114	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
168.197.45.36	unknown	Argentina		264781	VIDEOTELSRLAR	true
1.226.84.243	unknown	Korea Republic of		9277	SKB-T-AS-KRSKBroadbandCoLtdKR	true
24.135.69.146	unknown	Serbia		31042	SERBIA-BROADBAND-ASSerbiaBroadBand-SrpskeKablovskemreze	true
137.74.106.111	unknown	France		16276	OVHFR	true
172.104.169.32	unknown	United States		63949	LINODE-APLinodeLLCUS	true
178.250.54.208	unknown	United Kingdom		20860	IOMART-ASGB	true
45.33.77.42	unknown	United States		63949	LINODE-APLinodeLLCUS	true
46.101.58.37	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
177.23.7.151	unknown	Brazil		262886	LansofNetLTDAMEBR	true
216.47.196.104	unknown	United States		12083	WOW-INTERNETUS	true
83.169.21.32	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
109.190.35.249	unknown	France		35540	OVH-TELECOMFR	true
172.86.186.21	unknown	Canada		32489	AMANAHA-NEWCA	true
70.32.115.157	unknown	United States		31815	MEDIATEMPLEUS	true
186.189.249.2	unknown	Argentina		16814	NSSSAAR	true
109.101.137.162	unknown	Romania		9050	RTDBucharestRomaniaRO	true
190.115.18.139	unknown	Belize		262254	DDOS-GUARDCORPBZ	true
189.223.16.99	unknown	Mexico		8151	UninetSAdeCVMX	true
201.49.239.200	unknown	Brazil		52532	SpeednetTelecomunicacoesLtdaMEBR	true
185.94.252.27	unknown	Germany		197890	MEGASERVERS-DE	true
178.211.45.66	unknown	Turkey		197328	INETLTDTR	true
169.1.39.242	unknown	South Africa		37611	AfrihostZA	true
188.135.15.49	unknown	Oman		50010	NAWRAS-ASSultanateofOmanOM	true
60.249.78.226	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	true
181.123.6.86	unknown	Paraguay		23201	TelecelSAPY	true
193.251.77.110	unknown	France		3215	FranceTelecom-OrangeFR	true
192.241.143.52	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
128.92.203.42	unknown	United States		20115	CHARTER-20115US	true
81.215.230.173	unknown	Turkey		9121	TTNETTR	true
111.67.12.221	unknown	Australia		55803	DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	true
46.105.114.137	unknown	France		16276	OVHFR	true
192.232.229.54	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
191.182.6.118	unknown	Brazil		28573	CLAROSABR	true
200.24.255.23	unknown	Argentina		52381	SociedadCooperativaPopularLimitadadeComodoroAR	true
177.73.0.98	unknown	Brazil		53184	INBTelecomEIRELIBR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
70.32.84.74	unknown	United States		398110	GO-DADDY-COM-LLCUS	true
12.162.84.2	unknown	United States		7018	ATT-INTERNET4US	true
181.61.182.143	unknown	Colombia		10620	TelmexColombiaSACO	true
170.81.48.2	unknown	Brazil		263634	TACNETTELECOMBR	true
181.120.29.49	unknown	Paraguay		23201	TelecelSAPY	true
219.92.13.25	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	true
98.103.204.12	unknown	United States		10796	TWC-10796-MIDWESTUS	true
190.101.156.139	unknown	Chile		22047	VTRBANDAANCHASACL	true
2.45.176.233	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
187.162.248.237	unknown	Mexico		6503	AxtelSABdeCVMX	true
186.193.229.123	unknown	Brazil		262731	CTINETSOLUCOESEMCONECTIVIDADEEINFORMATICALTDBR	true
189.2.177.210	unknown	Brazil		4230	CLAROSABR	true
37.183.81.217	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
179.222.115.170	unknown	Brazil		28573	CLAROSABR	true
37.179.145.105	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
118.69.11.81	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true
68.183.190.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
183.176.82.231	unknown	Japan		7522	STCNSTNetIncorporatedJP	true
177.144.130.105	unknown	Brazil		27699	TELEFONICABRASILSABR	true
181.30.61.163	unknown	Argentina		10318	TelecomArgentinaSAAR	true
190.202.229.74	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	true
82.76.111.249	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
77.238.212.227	unknown	Bosnia and Herzegowina		42560	BA-TELEMACH-ASTelemachdooSarajevoBA	true
217.13.106.14	unknown	Hungary		12301	INVITECHHU	true
77.78.196.173	unknown	Bosnia and Herzegowina		42560	BA-TELEMACH-ASTelemachdooSarajevoBA	true
62.84.75.50	unknown	Lebanon		42334	BBP-ASLB	true
37.187.161.206	unknown	France		16276	OVHFR	true
201.213.177.139	unknown	Argentina		10481	TelecomArgentinaSAAR	true
188.251.213.180	unknown	Portugal		3243	MEO-RESIDENCIALPT	true
109.242.153.9	unknown	Greece		25472	WIND-ASGR	true
85.214.26.7	unknown	Germany		6724	STRATOSTRATOAGDE	true
51.75.33.127	unknown	France		16276	OVHFR	true
188.157.101.114	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
46.43.2.95	unknown	United Kingdom		35425	BYTEMARK-ASGB	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
74.58.215.226	unknown	Canada		5769	VIDEOTRONCA	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	463770
Start date:	12.08.2021
Start time:	03:55:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KNEa2w7v3a.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:	25
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:	mal96.troj.evad.winEXE@21/11@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 19.7% (good quality ratio 19.2%) • Quality average: 72.3% • Quality standard deviation: 23%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
03:56:25	API Interceptor	1x Sleep call for process: KNEa2w7v3a.exe modified
03:56:51	API Interceptor	2x Sleep call for process: svchost.exe modified
03:58:07	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
81.214.253.80	http://buybywe.com/roundcube/installer/eaZ/	Get hash	malicious	Browse	• 81.214.253.80:443/BdD9uZ0nJukeWE
94.176.234.118	mormanti.exe	Get hash	malicious	Browse	
	Io8ic2291n.doc	Get hash	malicious	Browse	
	SpEQvgtnaR.exe	Get hash	malicious	Browse	
	gPEkWaJGIA.exe	Get hash	malicious	Browse	
	aXwo8YyqNu.exe	Get hash	malicious	Browse	
	aof712Ufpl.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKRAYUABRakrejusLT	PHvqpLRfRl.exe	Get hash	malicious	Browse	• 79.98.24.39
	VESSEL BOOKING DETAILS_pdf.exe	Get hash	malicious	Browse	• 194.135.89.35
	B6i30pLa8e.exe	Get hash	malicious	Browse	• 79.98.28.25
	Y7S49aaObc	Get hash	malicious	Browse	• 80.209.224.126
	CTM ARRANGEMENT.exe	Get hash	malicious	Browse	• 176.223.13 1.225
	vMd5gb1HEJ.exe	Get hash	malicious	Browse	• 80.209.229.141
	vMAjf3xZSp.exe	Get hash	malicious	Browse	• 80.209.229.141
	BANGKOK REG. SHIPMENT SUPPLY CIF BANGKOK 19-21 FULL DETAILS.exe	Get hash	malicious	Browse	• 194.135.89.35
	mormanti.exe	Get hash	malicious	Browse	• 94.176.234.118
	f3ZU8AhKs3.exe	Get hash	malicious	Browse	• 185.69.55.138
	f2c8546e61ac6f18f9d739a31134c3d47612059d16201.exe	Get hash	malicious	Browse	• 185.69.55.138
	HGIUF7881Q.exe	Get hash	malicious	Browse	• 195.181.24 6.217
	NWMEaRqF7s.exe	Get hash	malicious	Browse	• 79.98.24.39
	uNh5bTbDTa.dll	Get hash	malicious	Browse	• 194.135.90.221
	uNh5bTbDTa.dll	Get hash	malicious	Browse	• 194.135.90.221
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 80.209.231.56
	scan of invoice 4366307.xlsm	Get hash	malicious	Browse	• 94.176.239.4
	kHisp6Vo3M.exe	Get hash	malicious	Browse	• 94.176.235.200
	sk4imVdVck.exe	Get hash	malicious	Browse	• 80.209.227.207
	document-1625724940.xls	Get hash	malicious	Browse	• 194.135.87.87
TTNETTR	PHvqpLRfRl.exe	Get hash	malicious	Browse	• 78.187.156.31
	IA37ji8jpa	Get hash	malicious	Browse	• 85.97.99.130
	FD6qpyHOPI	Get hash	malicious	Browse	• 88.255.23.140
	Vjeta9CbXg	Get hash	malicious	Browse	• 95.5.58.149
	fEbFnRr00C	Get hash	malicious	Browse	• 88.241.107.42
	WDNwpnLC6z	Get hash	malicious	Browse	• 95.7.215.146
	AtzpbZmOwo	Get hash	malicious	Browse	• 95.6.137.32
	BuJw0YL8x3	Get hash	malicious	Browse	• 78.178.77.162
	g5bwzqegn4	Get hash	malicious	Browse	• 78.173.228.99
	8kNgpvKpMy	Get hash	malicious	Browse	• 85.102.2.135
	Ck4BThYsDw	Get hash	malicious	Browse	• 78.172.216.112
	6K8zK2czTn	Get hash	malicious	Browse	• 88.241.107.11
	1pXwlJR8QV	Get hash	malicious	Browse	• 88.241.107.47
	g9ikwKsuYy	Get hash	malicious	Browse	• 85.100.28.146
	X7AvBM4NoO	Get hash	malicious	Browse	• 88.225.138.222
	LDit8hIL8X	Get hash	malicious	Browse	• 88.225.186.130
	W9xJReKzmM	Get hash	malicious	Browse	• 88.248.29.152
	d5reZjGi2R	Get hash	malicious	Browse	• 95.15.253.243
	SUsQqSw8ip	Get hash	malicious	Browse	• 78.171.186.142
	OzW9U3k1r8	Get hash	malicious	Browse	• 85.111.21.252

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):	0.5950547304132587
Encrypted:	false
SSDEEP:	6:0FAk1GaD0JOCEfMuaaD0JOCEfMKQmDSaAl/gz2cE0fMbhEZolrRSQ2hyYIIT:0dGaD0JcaaD0JwQQVAg/0bjSQJ

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
MD5:	490A11F6420837D2E87F8185228C726D
SHA1:	C78B86CB11BB57114226DA2FFDA9E083ABD728E2
SHA-256:	6514574D48DEF3BFF8177A73989E405AD1EDC311789D420D51C19E2841E8A957
SHA-512:	0A45D25737AF68111E2B15884CAD1B45624E18720A01173003A4054D75B091059DCC8BA306629B59BC4B6927F8D456DB3127A6CF681FE7420B0FEE68267C9160
Malicious:	false
Preview:	.....:{..(.....38...yk..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....38...yk.....&.....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 0x8e2b3c28, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09522289101320726
Encrypted:	false
SSDEEP:	6:9zwl/+BJU1RIE11Y8TRXgtKkgKrzwl/+BJU1RIE11Y8TRXgtKkgK:90+o1O4blgQKr0+o1O4blgQK
MD5:	A4C977A7F24C1AB389C72156AC986F21
SHA1:	397A2D13ADE410D75728275C573C9E45157E6535
SHA-256:	E9F4D57C9D0DB6FEE012B95526FAA073B8618EF459F24911B40CD8142A6CAFC1
SHA-512:	E7C6B78AFA26F838FBF60D5B98BF4EFD34D939FEE5090F0F9A05D43A022E70381620E09C47D41D155F9878880D96AE3344896EAAF40DE3CFD9D1398C72C5605
Malicious:	false
Preview:	.+<(... .....e.f.3...w.....&.....w..38...yk.h.(.....3...w.....B.....@..... ....3...w..... .....Hw9]38...ykk.....x.38...yk..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10964890742971496
Encrypted:	false
SSDEEP:	3:r/9EvWdrcOiXl/bJdAtidgkr4ll:jYWmt4zkk
MD5:	E0E174397C67D567B5BB17EEE0892828
SHA1:	987912F8C0B37599354237E04905E30E813FA51A
SHA-256:	0D1429DA6459A51D057AB53F2563E485D8CB3E3FF6298ED7E82656E0A5E945FA
SHA-512:	D6C57AF3A2194788A666E48DA8672607B822C8BCCCA5F589055DEAA6ABB80E6C05182CE79EE70B40F98DC32AF87385B0E6615A3C5029A074AF6E61440310B33
Malicious:	false
Preview:	.....3...w..38...yk.....w.....w.....w....:O.....w.....x.38...yk..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1102443467453243
Encrypted:	false
SSDEEP:	12:26tXm/Ey6q9995gqwqq3qQ10nMCldimE8eawHjc1j:26Ql689wvLyMCldzE9BHjcV
MD5:	F1F2B3B98C309A9C7AEED5C63CC27753
SHA1:	10BFF7C59B16CA2A5B174C1AB90EA41294EEC545
SHA-256:	FF8F6DC09FB829F5F45675694F3D025AD3BC96F8327EA318A1AE4011A3A7FA1A
SHA-512:	7A63682FFAA6491F3FEAF6F5453E19C29F78F4847B86774BA2C9C9EB09AECE3CC3D91D17B5EB81365550D8351E167A0D2DAF6846F4540265C0256BB07FCBA47
Malicious:	false
Preview:	.....3IG.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....:.+..... .....h.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....;IG..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11276116723419126
Encrypted:	false
SSDEEP:	12:7SXm/Ey6q9995gUw1miM3qQ10nMCldimE8eawHza1miIJ:7nl68Pw1tMLyMCldzE9BHza1tIJ
MD5:	7ECF910E58D4B2A19B00926EC0D8C0BC
SHA1:	73A25F141B7DF3A22C96C3F20ACC10D6B6B7C281
SHA-256:	D297005815D6DFAF08F1E6C981856AB8D54D62661534D259D5861EDFA6CBFF14
SHA-512:	FF407A00838E6463E85D77110FF88D79EC4D73DD3D983D6AFB2C41EE5DA39E1BEA189D05F8A9A0F9CAE8EA966532493B8A352B25521ABA0320F33E8CA6F6029 9
Malicious:	false
Preview:	.....+HG.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....:.+..... .....h.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....2HG..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11256817544552042
Encrypted:	false
SSDEEP:	12:qXm/Ey6q9995gTg1mK2P3qQ10nMCldimE8eawHza1mKC:fl6891iPLyMCldzE9BHza1O
MD5:	6CB8594E9DD2938F617B9F143E790C81
SHA1:	CAB0B6F2B5554E9E3936C8FCA55EA165B921C974
SHA-256:	52C643C00A07BC1083EFA7B84BD8D3A54226A877BCA6D390E0EC9756A5F867CC
SHA-512:	2E70CB23A8FA6B34705FC08FC27A9AF67FD59CD9BA75E86955F6A2D0A74576EF9B4A06D199947FD79A863205EACDCD127195CAB98B404E1A79BA15235ABE30 C
Malicious:	false
Preview:	.....<.GG.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....:.+..... .....h.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....GG..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001YS (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1102443467453243
Encrypted:	false
SSDEEP:	12:26tXm/Ey6q9995gqwqq3qQ10nMCldimE8eawHjc1j:26Ql689wvLyMCldzE9BHjcV
MD5:	F1F2B3B98C309A9C7AEED5C63CC27753
SHA1:	10BFF7C59B16CA2A5B174C1AB90EA41294EEC545
SHA-256:	FF8F6DC09FB829F5F45675694F3D025AD3BC96F8327EA318A1AE4011A3A7FA1A
SHA-512:	7A63682FFAA6491F3FEAF6F5453E19C29F78F4847B86774BA2C9C9EB09AECE3CC3D91D17B5EB81365550D8351E167A0D2DAF6846F4540265C0256BB07FCBA47
Malicious:	false
Preview:	.....3IG.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....:.+..... .....h.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....;IG..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11276116723419126
Encrypted:	false
SSDEEP:	12:7SXm/Ey6q9995gUw1miM3qQ10nMCldimE8eawHza1miIJ:7nl68Pw1tMLyMCldzE9BHza1tIJ

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
MD5:	7ECF910E58D4B2A19B00926EC0D8C0BC
SHA1:	73A25F141B7DF3A22C96C3F20ACC10D6B6B7C281
SHA-256:	D297005815D6DFAF08F1E6C981856AB8D54D62661534D259D5861EDFA6CBFF14
SHA-512:	FF407A00838E6463E85D77110FF88D79EC4D73DD3D983D6AFB2C41EE5DA39E1BEA189D05F8A9A0F9CAE8EA966532493B8A352B25521ABA0320F33E8CA6F6029 9
Malicious:	false
Preview:	....+HG....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2....................................... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..:.+..... ....h..........U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.......P.P..........2HG.. ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001.. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11256817544552042
Encrypted:	false
SSDEEP:	12:qXm/Ey6q9995gTg1mK2P3qQ10nMCldimE8eawHza1mKC:fl6891iPLyMCldzE9BHza1O
MD5:	6CB8594E9DD2938F617B9F143E790C81
SHA1:	CAB0B6F2B5554E9E3936C8FCA55EA165B921C974
SHA-256:	52C643C00A07BC1083EFA7B84BD8D3A54226A877BCA6D390E0EC9756A5F867CC
SHA-512:	2E70CB23A8FA6B34705FC08FC27A9AF67FD59CD9BA75E86955F6A2D0A74576EF9B4A06D199947FD79A863205EACDCD127195CAB98B404E1A79BA15235ABE30 C
Malicious:	false
Preview:	....<.GG....................B.............Zb..@.t.z.r.e.s...d.l.l.,.-.2.1.2....................................... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..:.+..... ....h..........U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.......P.P...........GG.. ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
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):	3.161934255091551
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rbGsowZk9+MlWlLehB4yAq7ejCAGsoQI:OaqdmuF3r1W+kWReH4yJ7Mtw
MD5:	0A941541A681D7B2DC86079497BF7710
SHA1:	F568FA936B273843D8FD811742AA4308EE3CCA1D
SHA-256:	C2EFDEA8AB56E3C156482DDA7800D0DC4077F0592BE999D269B800B1A0AD21BB
SHA-512:	31614F8B523B7FF06526BE6951F78D17053A5B40E9219E1ED066B9261ED624F6DE23ADAD092F9CC14EB40FC48EA2EBF3751A8635722B4DBF0CC91F07298C579A
Malicious:	false
Preview:	.......-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. A.u.g. .. 1.2. .. 2.0.2.1. .0.3.:.5.8.:.0.7.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. A.u.g. .. 1.2. .. 2.0.2.1. .0.3.:.5.8.:.0.7.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.960837149454534
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:	KNEa2w7v3a.exe
File size:	479232
MD5:	f8adcf71a8c4e5c16d11308dff998ece
SHA1:	2246c5925aca1446078a4cacbafeda7076eb050a
SHA256:	5303823581f2696ae62f21e42a8b0c4d446d2fa9f820e0f04a15992d6a59c59b
SHA512:	9e997a0edfbc49bf554e708825128ab43ab292481d7d6d8d8a561fbc8270f2291dd5d577336c1262407b44b9a0f19b1dd4bb3d6ac2f7f61d0a3aa4ec9137d06c
SSDEEP:	6144:be079Bvns6+dSEDVoOhjfbJ0r0dZQ4XYo8Zv/J5QnEZgHmjihGXL/578RdBg9:bT9Z1/2GOxfbQCBURzQ4ga6U8Re
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sf!.7.O.7.O.7.O...E.<.O...A.6.O...K.3.O.U.\.3.O.#IN.4.O.7.N...O...D.4.O...I.6.O.Rich7.O.....PE..L....._.....

File Icon

Icon Hash:	3236323434089341

Static PE Info

General

Entrypoint:	0x4020ea
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5F9B1381 [Thu Oct 29 19:09:53 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:	50f8a2255c4baf188eb0098c86160f78

Entrypoint Preview

Rich Headers

Data Directories

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23bb	0x3000	False	0.187174479167	data	3.24884109022	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x10e	0x1000	False	0.009521484375	data	0.0298850891201	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5000	0x9d8	0x1000	False	0.130859375	data	1.50052137767	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x6000	0xab8	0x1000	False	0.227294921875	data	2.93333151284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7000	0x6c0f3	0x6d000	False	0.806232977351	data	7.16230757272	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0x77d	0x1000	False	0.130615234375	data	1.32281451006	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 12, 2021 03:56:48.937880039 CEST	8.8.8.8	192.168.2.3	0xcece	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: svchost.exe PID: 5868 Parent PID: 568

General

Start time:	03:56:24
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: KNEa2w7v3a.exe PID: 5700 Parent PID: 5596

General

Start time:	03:56:24
Start date:	12/08/2021
Path:	C:\Users\user\Desktop\KNEa2w7v3a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KNEa2w7v3a.exe'
Imagebase:	0x400000
File size:	479232 bytes
MD5 hash:	F8ADCF71A8C4E5C16D11308DFF998ECE
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: 00000001.00000002.206004453.0000000002641000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.205611516.0000000002294000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.205562844.0000000002230000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Deleted

Analysis Process: svchost.exe PID: 5376 Parent PID: 568

General

Start time:	03:56:25
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	c:\windows\system32\svchost.exe -k localsystemnetworkrestricted -p -s NgcSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 1736 Parent PID: 568

General

Start time:	03:56:26
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s NgcCtnrSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: wiaacmgr.exe PID: 6124 Parent PID: 5700

General

Start time:	03:56:26
Start date:	12/08/2021
Path:	C:\Windows\SysWOW64\rdvgogl32\wiaacmgr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rdvgogl32\wiaacmgr.exe
Imagebase:	0x400000
File size:	479232 bytes
MD5 hash:	F8ADCF71A8C4E5C16D11308DFF998ECE
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: 00000004.00000002.210049440.0000000002181000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.209938070.0000000002124000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.209835926.00000000020C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: Windows.Media.Playback.MediaPlayer.exe PID: 6052 Parent PID: 6124

General

Start time:	03:56:27
Start date:	12/08/2021
Path:	C:\Windows\SysWOW64\CompPkgSup\Windows.Media.Playback.MediaPlayer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\CompPkgSup\Windows.Media.Playback.MediaPlayer.exe
Imagebase:	0x400000
File size:	479232 bytes
MD5 hash:	F8ADCF71A8C4E5C16D11308DFF998ECE
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: 00000005.00000002.471191876.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.471538485.0000000002211000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.471462272.00000000021B4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 4260 Parent PID: 568

General

Start time:	03:56:48
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5900 Parent PID: 568

General

Start time:	03:56:51
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 2024 Parent PID: 568

General

Start time:	03:56:56
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4364 Parent PID: 568

General

Start time:	03:57:02
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6076 Parent PID: 568

General

Start time:	03:57:03
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4788 Parent PID: 568

General

Start time:	03:57:03
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5728 Parent PID: 568

General

Start time:	03:57:04
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 496 Parent PID: 568

General

Start time:	03:57:04
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: 1180 Parent PID: 568

General

Start time:	03:57:05
Start date:	12/08/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6665f0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4072 Parent PID: 568

General

Start time:	03:57:05
Start date:	12/08/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 720 Parent PID: 4072

General

Start time:	03:58:06
Start date:	12/08/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff6741d0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 1396 Parent PID: 720

General

Start time:	03:58:07
Start date:	12/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis