ID: 449959
Sample Name: mormanti.exe
Cookbook: default.jbs
Time: 17:05:22
Date: 16/07/2021
Version: 33.0.0 White Diamond

Table of Contents

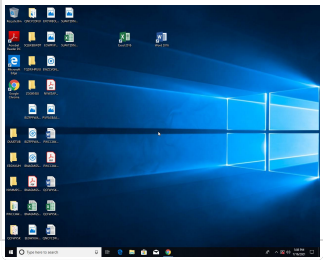
Windows Analysis Report mormanti.exe

Overview

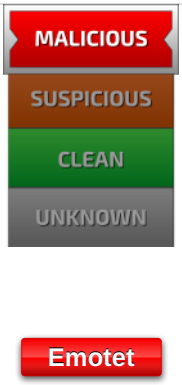
General Information

Sample Name:	mormanti.exe
Analysis ID:	449959
MD5:	6c94edfea6e5ee0.
SHA1:	a8d0cc5088ee86..
SHA256:	0154d1d06e755b..
Infos:	

Most interesting Screenshot:



Detection



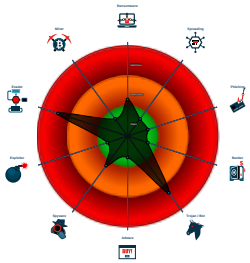
Emotet

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- 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…
- AV process strings found (often use…
- Checks if Antivirus/Antispyware/Fire…

Classification



Process Tree

- **System is w10x64**
- mormanti.exe (PID: 3412 cmdline: 'C:\Users\user\Desktop\mormanti.exe' MD5: 6C94EDFEA6E5EE001B00122C9D01BD8A)
  - eventvwr.exe (PID: 2416 cmdline: C:\Windows\SysWOW64\msmpeg2vdec\eventvwr.exe MD5: 6C94EDFEA6E5EE001B00122C9D01BD8A)
- svchost.exe (PID: 3148 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 384 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2168 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5924 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4744 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4880 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1276 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4936 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5588 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3468 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 2648 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4820 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5024 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": [
    "58.171.153.81:80",
    "104.131.103.128:443",
    "66.228.49.173:8080",
    "104.131.103.37:8080",
    "149.62.173.247:8080",
    "72.47.248.48:7080",
    "68.183.170.114:8080",
    "81.198.69.61:80",
    "217.13.106.14:8080",
    "77.90.136.129:8080",
    "217.199.160.224:7080",
    "178.79.163.131:8080",
    "2.47.112.152:80",
    "83.169.21.32:7080",
    "190.163.31.26:80",
    "185.94.252.27:443",
    "12.162.84.2:8080",
    "73.116.193.136:80",
    "177.72.13.80:80",
    "116.125.120.88:443",
    "213.181.91.224:80",
    "104.131.41.185:8080",
    "46.28.111.142:7080",
    "181.129.96.162:8080",
    "189.2.177.210:443",
    "111.67.12.221:8080",
    "189.194.58.119:80",
    "51.255.165.160:8080",
    "170.81.48.2:80",
    "177.74.228.34:80",
    "70.32.84.74:8080",
    "213.60.96.117:80",
    "186.250.52.226:8080",
    "70.32.115.157:8080",
    "190.190.148.27:8080",
    "204.225.249.100:7080",
    "192.241.143.52:8080",
    "202.62.39.111:80",
    "82.76.111.249:443",
    "190.147.137.153:443",
    "80.249.176.206:80",
    "91.219.169.180:80",
    "212.71.237.140:8080",
    "114.109.179.60:80",
    "5.196.35.138:7080",
    "87.106.46.107:8080",
    "190.6.193.152:8080",
    "172.104.169.32:8080",
    "186.103.141.250:443",
    "212.231.60.98:80",
    "147.91.184.91:80",
    "50.28.51.143:8080",
    "61.92.159.208:8080",
    "187.162.248.237:80",
    "191.182.6.118:80",
    "94.206.45.18:80",
    "219.92.13.25:80",
    "145.236.8.174:80",
    "89.32.150.160:8080",
    "93.151.186.85:80",
    "190.17.195.202:80",
    "181.120.79.227:80",
    "177.73.0.98:443",
    "192.241.146.84:8080",
    "217.160.182.191:8080",
    "68.183.190.199:8080",
    "137.74.106.111:7080",
    "177.144.135.2:80",
    "201.213.156.176:80",
    "82.196.15.205:8080",
    "104.236.161.64:8080",
    "209.236.123.42:8080",
    "77.55.211.77:8080",
    "177.66.190.130:80",
    "143.0.87.101:80",
    "94.176.234.118:443",
    "191.99.160.58:80",
    "185.94.252.12:80",
    "45.161.242.102:80",
    "181.36.42.205:443"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.465228013.0000000001140000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.203541228.0000000002DC1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.203533038.0000000002DB0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000002.465253689.0000000001151000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.mormanti.exe.2db053f.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.eventvwr.exe.114053f.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.mormanti.exe.2db053f.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.eventvwr.exe.114053f.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

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

Networking:

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

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)

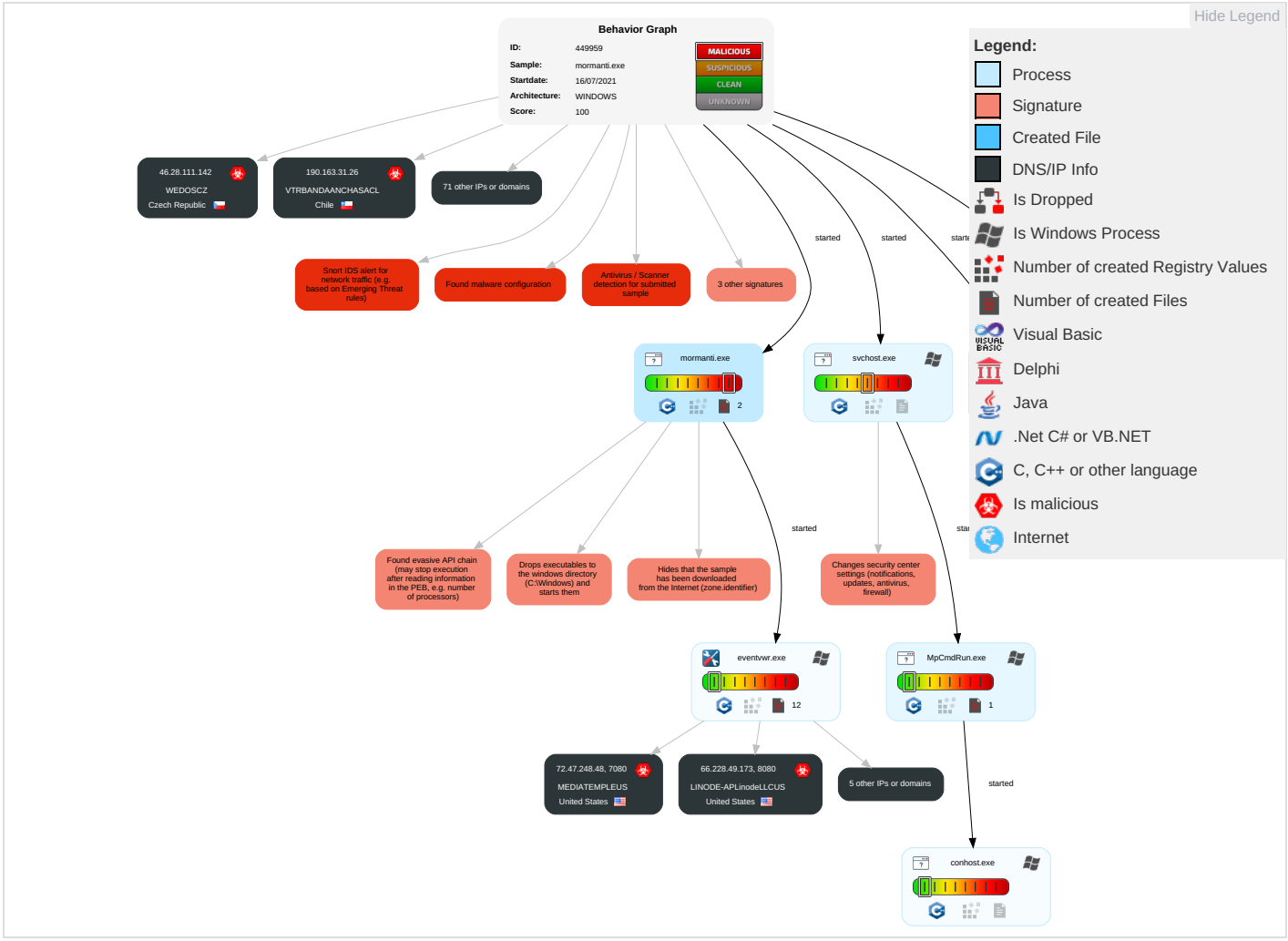
Stealing of Sensitive Information:

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	Network Effects
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communi
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
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	Manipulat Device Communi
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	Jamming Denial of 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 Wi Access P
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	Downgrad Insecure 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
mormanti.exe	75%	Virustotal		Browse
mormanti.exe	82%	ReversingLabs	Win32.Trojan.Emotet	
mormanti.exe	100%	Avira	TR/Kryptik.vhuzo	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.eventvwr.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1138886		Download File
0.0.mormanti.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1138886		Download File
0.2.mormanti.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1138886		Download File
2.0.eventvwr.exe.c10000.0.unpack	100%	Avira	HEUR/AGEN.1138886		Download File
0.2.mormanti.exe.2db053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.eventvwr.exe.114053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://68.183.170.114/nFzrf7w0/EO2pZ/MQ0xve/	0%	Avira URL Cloud	safe	
http://https://fs.microsoft.c	0%	Avira URL Cloud	safe	
http://68.183.170.114:8080/nFzrf7w0/EO2pZ/MQ0xve/	0%	Avira URL Cloud	safe	
http://72.47.248.48:7080/VTzYrEpbArBozqZBhS/	0%	Avira URL Cloud	safe	
http://66.228.49.173:8080/TyLIHl4nuj0XCeB/C12IKmccuoQw2U92z/s(KF	0%	Avira URL Cloud	safe	
http://66.228.49.173/TyLIHl4nuj0XCeB/C12IKmccuoQw2U92z/	0%	Avira URL Cloud	safe	
http://149.62.173.247:8080/kH8ALNiaGV/5bEuMKuJNKlslD3n/rvXy2RpDwZlslOQBeY7/BCLTdgbwF6J8vsIGfDq/jZ9iV	0%	Avira URL Cloud	safe	
http://68.183.170.114:8080/nFzrf7w0/EO2pZ/MQ0xve/c	0%	Avira URL Cloud	safe	
http://66.228.49.173:8080/TyLIHl4nuj0XCeB/C12IKmccuoQw2U92z/	0%	Avira URL Cloud	safe	
http://72.47.248.48:7080/VTzYrEpbArBozqZBhS/CL:	0%	Avira URL Cloud	safe	
http://149.62.173.247/kH8ALNiaGV/5bEuMKuJNKlslD3n/rvXy2RpDwZlslOQBeY7/BCLTdgbwF6J8vsIGfDq/jZ9iV8xFle	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://72.47.248.48:7080/VTzYrEpbArBozqZBhS/6O	0%	Avira URL Cloud	safe	
http://68.183.170.114:8080/nFzrf7w0/EO2pZ/MQ0xve/:	0%	Avira URL Cloud	safe	
http://58.171.153.81/j4XmHhlvX7h4pe/uu11HumRcyQn/3XzJ/ymPM07W/vKmfGodTznrrD/	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.62.173.247	unknown	Spain		50926	INFORTELECOM-ASES	true
191.182.6.118	unknown	Brazil		28573	CLAROSABR	true
104.131.103.37	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
204.225.249.100	unknown	Canada		22652	FIBRENOIRE-INTERNETCA	true
94.176.234.118	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
70.32.84.74	unknown	United States		398110	GO-DADDY-COM-LLCUS	true
177.73.0.98	unknown	Brazil		53184	INBTelecomEIRELIBR	true
12.162.84.2	unknown	United States		7018	ATT-INTERNET4US	true
116.125.120.88	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
58.171.153.81	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	true
170.81.48.2	unknown	Brazil		263634	TACNETTELECOMBR	true
219.92.13.25	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	true
202.62.39.111	unknown	Cambodia		23673	ONLINE-ASCogetelOnlineCambodiaISPKH	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.236.123.42	unknown	United States		393398	ASN-DISUS	true
213.181.91.224	unknown	Spain		49000	TELECABLEJUMILLA-ASES	true
5.196.35.138	unknown	France		16276	OVHFR	true
187.162.248.237	unknown	Mexico		6503	AxtelSABdeCVMX	true
189.2.177.210	unknown	Brazil		4230	CLAROSABR	true
93.151.186.85	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
217.199.160.224	unknown	United Kingdom		20738	GD-EMEA-DC-LD5GB	true
114.109.179.60	unknown	Thailand		17552	TRUE-AS-APTrueInternetCoLtdTH	true
143.0.87.101	unknown	Brazil		263998	MMTelecomBR	true
186.103.141.250	unknown	Chile		15311	TelefonicaEmpresasCL	true
77.90.136.129	unknown	Germany		42821	RAPIDNET-DEHaunstetterStr19DE	true
181.129.96.162	unknown	Colombia		13489	EPMTelecomunicacionesSA ESPCO	true
50.28.51.143	unknown	United States		32244	LIQUIDWEBUS	true
68.183.190.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
94.206.45.18	unknown	United Arab Emirates		15802	DU-AS1AE	true
190.17.195.202	unknown	Argentina		10318	TelecomArgentinaSAAR	true
73.116.193.136	unknown	United States		7922	COMCAST-7922US	true
82.76.111.249	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	true
189.194.58.119	unknown	Mexico		13999	MegaCableSAdeCVMX	true
80.249.176.206	unknown	Russian Federation		31376	SMART-ASRU	true
145.236.8.174	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	true
191.99.160.58	unknown	Ecuador		27738	EcuadortelecomSAEC	true
217.13.106.14	unknown	Hungary		12301	INVITECHHU	true
147.91.184.91	unknown	Serbia		13092	UB-ASRS	true
68.183.170.114	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
81.198.69.61	unknown	Latvia		12578	APOLLO-ASLatviaLV	true
177.66.190.130	unknown	Brazil		262502	FLYLinkTelecomBR	true
177.72.13.80	unknown	Brazil		52814	INTERNETPLAYLTDABR	true
61.92.159.208	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
178.79.163.131	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
46.28.111.142	unknown	Czech Republic		197019	WEDOSCZ	true
77.55.211.77	unknown	Poland		15967	NAZWAPL	true
190.163.31.26	unknown	Chile		22047	VTRBANDAANCHASACL	true
137.74.106.111	unknown	France		16276	OVHFR	true
172.104.169.32	unknown	United States		63949	LINODE-APLinodeLLCUS	true
72.47.248.48	unknown	United States		31815	MEDIATEMPLEUS	true
181.120.79.227	unknown	Paraguay		23201	TelecelSAPY	true
89.32.150.160	unknown	Romania		43927	HOSTERIONRO	true
104.131.41.185	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
186.250.52.226	unknown	Brazil		262807	RedfoxTelecomunicacoesLtdaBR	true
87.106.46.107	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
177.144.135.2	unknown	Brazil		27699	TELEFONICABRASILSABR	true
217.160.182.191	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
201.213.156.176	unknown	Argentina		10481	TelecomArgentinaSAAR	true
83.169.21.32	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
70.32.115.157	unknown	United States		31815	MEDIATEMPLEUS	true
213.60.96.117	unknown	Spain		12334	Galicia-SpainES	true
212.231.60.98	unknown	Spain		15704	AS15704ES	true
181.36.42.205	unknown	Dominican Republic		28118	ALTICEDOMINICANASADO	true
104.131.103.128	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
190.190.148.27	unknown	Argentina		10481	TelecomArgentinaSAAR	true
190.6.193.152	unknown	Honduras		27884	CABLECOLORSAHN	true
51.255.165.160	unknown	France		16276	OVHFR	true
212.71.237.140	unknown	United Kingdom		63949	LINODE-APLinodeLLCUS	true
185.94.252.27	unknown	Germany		197890	MEGASERVERS-DE	true
2.47.112.152	unknown	Italy		30722	VODAFONE-IT-ASNIT	true
104.236.161.64	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.241.143.52	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
192.241.146.84	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
45.161.242.102	unknown	Brazil		268479	AntonioMarcosdosSantos-MEBR	true
66.228.49.173	unknown	United States		63949	LINODE-APLinodeLLCUS	true
190.147.137.153	unknown	Colombia		10620	TelmexColombiaSACO	true
82.196.15.205	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
111.67.12.221	unknown	Australia		55803	DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	true
177.74.228.34	unknown	Brazil		263652	CMDNETInternetInformaticaLtdaBR	true
91.219.169.180	unknown	Ukraine		52191	LOCALKA-NET-AS	true
185.94.252.12	unknown	Germany		197890	MEGASERVERS-DE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	449959
Start date:	16.07.2021
Start time:	17:05:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mormanti.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:	mal100.troj.evad.winEXE@17/8@0/81
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.8% (good quality ratio 34%) • Quality average: 59.9% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 89% • 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
17:06:35	API Interceptor	2x Sleep call for process: svchost.exe modified
17:07:51	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
149.62.173.247	4IyFGqHAVD.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/IBsG2ITcQO3MqUs1a/eWW1CTn3/VLHN/zvqFvAYTs8Wn1umCE/
	3svzK4vdKM.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/V3H3/psfTQ/T6gzY4u9nPfs/
	2ToKPHUu99.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/87Cxqpcon5mO7BWL/kNWYVSfiQZ1/XJcpkT2gFE/Hco5ZCWlpmRP/zLI7rXAgPV20IUMXnp0/
	kzE7zbx.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/dlbDdKCLEFM/kILzAtumIq4D8Z50q/
	CKPeR3qE.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/Gb1SCLpYr1nryoMy/
	FhkjwhQzcCHjL5eJAPSd.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/O3IlwiDkTOJb9kSszV/
	PWALJSok9Jmx.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/UEN3UQF/RPhkq/Thdgzp8FPfhtu5Kzeq/jbAoM9TOYekxcG3f/
	XmlHuNZL0oAoQ.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/09OFIpDnBnX6Ch9VQR/
	zH2RXXcJJRwzkFPvoiO.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/TUUPUH/g2IoLl6V0MswbJJvtr/zFXxOI/
	List-20200731-79226.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/gC8G5H3mS6JLGBy7kW/eFDaGGEbn/6oQ6Pr5pkoT/
	LIST-20200731-88494.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/1COfPTBiLdjTj/3uD573T7jVFWo/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Rep_20200731.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/16fP0l2bHkKP/yllWZmZ8qJUp3b5wMA5/8jJDZebNHK64THon/
	messaggio_072020.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/HwFR5iVEHHADWDZIQtY/JEbgpm3H3Dba/F68osD9sJD6glZa/EYYDB32/uZcdM8DI/ONVv5X8DQM593V/
	File 072020.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/B4RsHPT/aFO997jDYlKpx/
	SecuriteInfo.com.Emotet-FROC3EC4AC84139.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/ezcsx8phECXl/oUCR96bNNx/gxL6EXuCo05e1gD/
	SecuriteInfo.com.Emotet-FRO9F97F1034DC9.exe	Get hash	malicious	Browse	• 149.62.173.247:8080/XBUhtV6sX6/m779xLLC04UeYEs/ScItlmqyP4XZ8/5A8BpJp5AfE/SY44egi1/
	doc-20200730-FFF8570.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/aXKPKdd3SCmd/
	Rep_20200730_K264404.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/ynBo0VuXDLlNeLaPaE/
	rep-0168630.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/6ozhezxENEAqUETEyn/
	00_29_G-087448.doc	Get hash	malicious	Browse	• 149.62.173.247:8080/J6jxvFJ3SOWdv/80iHzW50w9Thz/N513Uqua/ddyHLa4nW7VJ9x9/
104.131.103.37	2ToKPHUu99.exe	Get hash	malicious	Browse	
	tvNMxIhI.exe	Get hash	malicious	Browse	
	YpVLv2JU.exe	Get hash	malicious	Browse	
204.225.249.100	http://204.225.249.100	Get hash	malicious	Browse	• 204.225.249.100/favicon.ico

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLAROSABR	i	Get hash	malicious	Browse	• 189.33.64.216
	Q8qbmLCf1b	Get hash	malicious	Browse	• 201.65.97.21
	segYCksCNt.exe	Get hash	malicious	Browse	• 189.103.150.9
	mssecsvr.exe	Get hash	malicious	Browse	• 179.211.205.91
	fraps.exe	Get hash	malicious	Browse	• 187.69.114.104
	2126316AB22061FED599E07630759E814DB86A71B0001.exe	Get hash	malicious	Browse	• 201.80.87.3
	mon117_cr(1).dll	Get hash	malicious	Browse	• 187.20.217.129
	x86_unpacked	Get hash	malicious	Browse	• 191.186.71.139

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ppc_unpacked	Get hash	malicious	Browse	• 179.217.83.5
	ldr.sh	Get hash	malicious	Browse	• 201.30.209.174
	MGuvcs6Ocz	Get hash	malicious	Browse	• 189.52.247.3
	z3hir.x86	Get hash	malicious	Browse	• 201.39.243.114
	YPJ9DZYIpO	Get hash	malicious	Browse	• 179.211.54.16
	godrop.exe	Get hash	malicious	Browse	• 189.53.70.50
	SecuriteInfo.com.Heur.4905.xls	Get hash	malicious	Browse	• 187.20.217.129
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	• 200.243.153.66
	wEcncyxrEe	Get hash	malicious	Browse	• 187.68.37.156
	WUHU95Apq3	Get hash	malicious	Browse	• 179.219.28.135
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 189.34.127.42
	svchost.exe	Get hash	malicious	Browse	• 179.216.19 9.141
DIGITALOCEAN-ASNUS	deepRats.exe	Get hash	malicious	Browse	• 37.139.8.104
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 157.245.12 7.231
	Loader.exe	Get hash	malicious	Browse	• 157.245.5.40
	Machine Service.xlsx	Get hash	malicious	Browse	• 188.166.192.89
	Machine Service.xlsx	Get hash	malicious	Browse	• 188.166.192.89
	c22MANsVPI.xls	Get hash	malicious	Browse	• 128.199.24 3.169
	document.xlsm	Get hash	malicious	Browse	• 138.68.174.10
	document.xlsm	Get hash	malicious	Browse	• 138.68.174.10
	document.xlsm	Get hash	malicious	Browse	• 138.68.174.10
	document.xlsm	Get hash	malicious	Browse	• 138.68.174.10
	lNiby9ahcU.jar	Get hash	malicious	Browse	• 157.230.10.241
	2UUlKfJYJN.exe	Get hash	malicious	Browse	• 162.243.17 3.152
	r3Bdb4R6aX.exe	Get hash	malicious	Browse	• 68.183.192.109
	P7bm3wqSDh.xls	Get hash	malicious	Browse	• 128.199.24 3.169
	T7lwV5Cutg.exe	Get hash	malicious	Browse	• 178.62.61.85
	RFQ_GS_45_009_GlobalSuppl_.xlsx	Get hash	malicious	Browse	• 178.62.61.85
	9yW6QklfU7.exe	Get hash	malicious	Browse	• 178.62.61.85
	SPARE PARTS Provision List.xlsx	Get hash	malicious	Browse	• 178.62.61.85
	04006279e16979c72a6ffa4266149e911d3f3399183b3.exe	Get hash	malicious	Browse	• 165.22.105.227
	748dYNDiTO.exe	Get hash	malicious	Browse	• 68.183.192.109
INFORTELECOM-ASES	005AS7SD44F4H7J7I4D7DF4s44ffg7hj44g4d7d44d.js	Get hash	malicious	Browse	• 149.62.168.145
	005AS7SD44F4H7J7I4D7DF4s44ffg7hj44g4d7d44d.js	Get hash	malicious	Browse	• 149.62.168.145
	56UDmImzPe.dll	Get hash	malicious	Browse	• 31.24.158.56
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 5.175.41.244
	Sample.doc	Get hash	malicious	Browse	• 5.175.41.244
	Sample.doc	Get hash	malicious	Browse	• 5.175.41.244
	3zuPInon2U.dll	Get hash	malicious	Browse	• 31.24.158.56
	3zuPInon2U.dll	Get hash	malicious	Browse	• 31.24.158.56
	lZyOllK1Rs.dll	Get hash	malicious	Browse	• 31.24.158.56
	lZyOllK1Rs.dll	Get hash	malicious	Browse	• 31.24.158.56
	3ZXUCm62TH.dll	Get hash	malicious	Browse	• 31.24.158.56
	3ZXUCm62TH.dll	Get hash	malicious	Browse	• 31.24.158.56
	y3JQD3Xzos.dll	Get hash	malicious	Browse	• 31.24.158.56
	y3JQD3Xzos.dll	Get hash	malicious	Browse	• 31.24.158.56
	MmTsqqQREG.dll	Get hash	malicious	Browse	• 31.24.158.56
	MmTsqqQREG.dll	Get hash	malicious	Browse	• 31.24.158.56
	ZchEM36552.dll	Get hash	malicious	Browse	• 31.24.158.56
	yLmDpCx1xp.dll	Get hash	malicious	Browse	• 31.24.158.56
	dnW1mfW27L.dll	Get hash	malicious	Browse	• 31.24.158.56
	K0or0EZubp.dll	Get hash	malicious	Browse	• 31.24.158.56

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):	0.5918524708219107
Encrypted:	false
SSDEEP:	6:b8ek1GaD0JOCEfMuaaD0JOCEfMKQmDjjAl/gz2cE0fMbhEZolrRSQ2hyYIIT:b8NGaD0JcaaD0JwQQjjAg/0bjSQJ
MD5:	9EB1288EAAF777CF31B19FC8052D9DDD
SHA1:	D0366555B0FF7D5F716C215B7253373231FE1F4B
SHA-256:	1AB4A321F9958011E0E2AA7DF522A3567EFC956F36513C512EEA3BBA3F7E2F22
SHA-512:	E916EAE79313765EBED1A5A407594EEBAD546A7963C3E6E96FBC869B431BB491C40E973D58FC69D1D9977855B8FAC8002D1C435E855378A1508DF71343C6752
Malicious:	false
Preview:	....E..h..(.....#....yq..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....#....yq.....&.....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 0x0656ce7e, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09325297057693027
Encrypted:	false
SSDEEP:	6:agAzwl/+z6RIE11Y8TRXuo/Xx1qKIgAzwl/+z6RIE11Y8TRXuo/Xx1qK:aX0++O4blj/h1qKIX0++O4blj/h1qK
MD5:	01DC05B086437F44DADEBE72F42AE6E4
SHA1:	5ED9C40BDF29C734FDB24E80573BFAB46285828A
SHA-256:	88194003F7E242AECDD75F00695B39A37441BF6C57A9812A12F9F7735BD43BA3
SHA-512:	C1CFDEBA81E79AC3C92B208FD5E625E9625D853F518F0114FB6DF66EA1530A87F10A125A99E9E6FF3E6556568B0DC84B4C356173A2362B656E7B81698EDAB9B
Malicious:	false
Preview:	.V.~... .....e.f.3...w.....&.....w..#....yq.h.(.....3...w.....B.....@..... ....3...w..... .....t\..#....yqk.....M...#....yq.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10801090337418041
Encrypted:	false
SSDEEP:	3:kE17EvGZ0i0lcSXl/bJdAtizjlD/ill:kE1iGZ0hlc8t4U1G
MD5:	518B806DEB454B700E818B345A95C61C
SHA1:	53C2FB38B4AB68FC2414D36920212E45895260FB
SHA-256:	6F4DEAA5EDE225FB203717C88BAE62EB1EE0789B07C1548185C9338FE5A29C7A
SHA-512:	D17D2469510FA2AA3F080A8EF6C8D2657E0CB6AE65D5930FD08BB94A32CB5C2E0F7844FB991FDED7885E5D209269F718A76844CEA288CBBCBAC71EFA55C18F 27
Malicious:	false
Preview:	k.....3...w..#....yq.....w.....w.....w....:O....w.....M...#....yq.....

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):	0.11017776630826032

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Encrypted:	false
SSDEEP:	12:265Xm/Ey6q99954Klq3qQ10nMCldimE8eawHjcmj:26kl68wLyMCldzE9BHjc8
MD5:	D8C933C4D3562115CDA8EC19E4C40BAB
SHA1:	B56A16C4CCB98D25D5DFE0F211C87C28F6BAE8D5
SHA-256:	FAE8B7380E73264FFA75864B9F212C841A62D927153EC739D80DEDB876A482BB
SHA-512:	E75F13F453D4619F7722B799A8CAA47EF12184BFF7394309A12DEF148B5BA7DB20D6EA2A512B27B86B380BF6DE624F68B2AF8408D90F356517888C8524EAD3CA
Malicious:	false
Preview:	.....t.S.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....=.m.*..... .....-[...z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....S..... ....

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):	0.11280925407263487
Encrypted:	false
SSDEEP:	12:UrXm/Ey6q999549r1z1miM3qQ10nMCldimE8eawHza1miI5Z:/l684h1tMLyMCldzE9BHza1tln
MD5:	9D91B6F5D908F8FA9457289284D99D90
SHA1:	7FA4F2CC6A51660A2767B533B9629484DD209C00
SHA-256:	348FCA3B1B0151D5A3E0AB8F2EC51DD4404ABDB779CB3319255F5C4B7C7E77CF
SHA-512:	110A3DEE834FB3E03DA0152E809F2CD0A50294CFF62DB8CA2C9E96F9324729840EB44DCCC46D2815F50D14ED61A67CFBE06D5F2550A8FF48DEE6A0F43087CE 9
Malicious:	false
Preview:	.....nQ.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....=.m.*..... .....z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....<yQ..... ....

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):	0.11273590727037369
Encrypted:	false
SSDEEP:	12:U0Xm/Ey6q99954iH0z1mK2P3qQ10nMCldimE8eawHza1mKQe:Al68S1iPLyMCldzE9BHza13
MD5:	0573B48E6E823B072B981744C4EC755A
SHA1:	B0AC5879397474AF40AEE8E06E193A277A89D30C
SHA-256:	CAFED707C6D08E422CC295DD756129A2BDA528D830225142ABD5F4862CEAF3DC
SHA-512:	33F8D03E6DAC4E202ECAFE1D7491E131E8496D25FB8A0DF090EF7397B45350B9DEE82D286BA184EBD0DC319D92CC817AFFCB7CA5B3D1A42340A6156DC78C4 97
Malicious:	false
Preview:	.....P.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....=.m.*..... .....z.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....1P..... ....

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
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):	3.152601704217562
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rABD2iCk9+MlWlLehB4yAq7ejCpBD2iP:OaqdmuF3rg2iV+kWReH4yJ7M42iP
MD5:	2CA5726DE33B7191699EBFEEC4F7210C
SHA1:	0613DF20921345EFB902DFE198764AEF58BF6C9E
SHA-256:	00CFCED40E9C57E6C01FE432F6C4470A9330DE3DD47676C30294BB085A9EC9D5
SHA-512:	9D63083245C34A426097B74D9EF78CE8105CAA5B4CF4586F751C02774B91A2E79873A5B71F9C9694C22325031D6F97B4C617EF223DDC16884F18488E5F5A269A
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.:. .. F.r.i. .. J.u.l. .. 1.6. .. 2.0.2.1. .1.7.:.0.7.:.5. 1.........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.:. .. F.r.i. .. J.u.l. .. 1.6. .. 2.0.2.1. .1.7.:.0.7.:.5.1.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.359134894428257
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:	mormanti.exe
File size:	102912
MD5:	6c94edfea6e5ee001b00122c9d01bd8a
SHA1:	a8d0cc5088ee86c2be77afe157695d12e951f369
SHA256:	0154d1d06e755bda091168038f25c1dde101e3b77c66f88 b73c71be84ffdaf6e
SHA512:	8e4f44f2680feb8fa564a26b3f283ce360d966e01b158568 6e6eb23900f5e09d39e3b62b154604972091cc928f99f83 5ec2e042a5c06d7df29b8c225e3db447f
SSDEEP:	1536:jw9fHY8jOMiep0McpHa74EuSFGMpJ7q06VSE:sr OMiep0ZpeuQJmpSE
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.........$~..J-.. J-..J-:..-..J-...-..J-...-..J-...-..J-...-..J-.61-..J-..K-..J-...-..J-...- ..J-...-..J-Rich..J-......................

File Icon

Icon Hash:	9a8a808292808000

Static PE Info

General

Entrypoint:	0x402b60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F325807 [Tue Aug 11 08:34:15 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	c75ae73417f3d8c7926ca2cc9989d6f5

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x243c	0x2600	False	0.655324835526	COM executable for DOS	6.36850956542	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x1702	0x1800	False	0.40625	data	5.1131105028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x648	0x200	False	0.232421875	data	2.09168969639	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7000	0x144c4	0x14600	False	0.486459930982	data	6.30306243713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c000	0x70c	0x800	False	0.49853515625	data	4.44276595657	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/16/21-17:07:12.259592	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			104.131.103.37	192.168.2.3
07/16/21-17:07:15.256691	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			104.131.103.37	192.168.2.3
07/16/21-17:07:21.273124	ICMP	486	ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited			104.131.103.37	192.168.2.3
07/16/21-17:07:42.618824	ICMP	399	ICMP Destination Unreachable Host Unreachable			72.10.63.118	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/16/21-17:07:45.806111	ICMP	399	ICMP Destination Unreachable Host Unreachable			72.10.63.118	192.168.2.3
07/16/21-17:07:51.997887	ICMP	399	ICMP Destination Unreachable Host Unreachable			72.10.63.118	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: mormanti.exe PID: 3412 Parent PID: 5572

General

Start time:	17:06:08
Start date:	16/07/2021
Path:	C:\Users\user\Desktop\mormanti.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mormanti.exe'
Imagebase:	0xc10000
File size:	102912 bytes
MD5 hash:	6C94EDFEA6E5EE001B00122C9D01BD8A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.203541228.0000000002DC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.203533038.0000000002DB0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Deleted

Analysis Process: eventvwr.exe PID: 2416 Parent PID: 3412

General

Start time:	17:06:09
Start date:	16/07/2021
Path:	C:\Windows\SysWOW64\msmpeg2vdec\eventvwr.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msmpeg2vdec\eventvwr.exe
Imagebase:	0xc10000
File size:	102912 bytes
MD5 hash:	6C94EDFEA6E5EE001B00122C9D01BD8A
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: 00000002.00000002.465228013.0000000001140000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.465253689.0000000001151000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3148 Parent PID: 568

General

Start time:	17:06:15
Start date:	16/07/2021
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: 384 Parent PID: 568

General

Start time:	17:06:35
Start date:	16/07/2021
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: 2168 Parent PID: 568

General

Start time:	17:06:37
Start date:	16/07/2021
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: 5924 Parent PID: 568

General

Start time:	17:06:45
Start date:	16/07/2021
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: 4744 Parent PID: 568

General

Start time:	17:06:46
Start date:	16/07/2021
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
Reputation:	high

Analysis Process: svchost.exe PID: 4880 Parent PID: 568

General

Start time:	17:06:47
Start date:	16/07/2021
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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 1276 Parent PID: 568

General

Start time:	17:06:47
Start date:	16/07/2021
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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4936 Parent PID: 568

General

Start time:	17:06:47
Start date:	16/07/2021
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

Reputation:	high

Registry Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 5588 Parent PID: 568

General

Start time:	17:06:48
Start date:	16/07/2021
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
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 3468 Parent PID: 568

General

Start time:	17:06:49
Start date:	16/07/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff641450000
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: 2648 Parent PID: 568

General

Start time:	17:06:49
Start date:	16/07/2021
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
Reputation:	high

Registry Activities — Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 4820 Parent PID: 2648

General

Start time:	17:07:50
Start date:	16/07/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff6922b0000
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: 5024 Parent PID: 4820

General

Start time:	17:07:50
Start date:	16/07/2021
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