ID: 450352
Sample Name:
methodsnetsh.exe
Cookbook: default.jbs
Time: 17:47:50
Date: 18/07/2021
Version: 33.0.0 White Diamond

Table of Contents

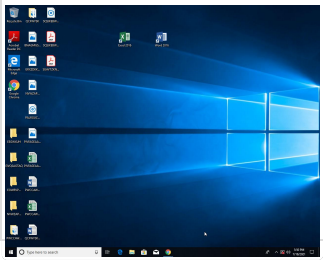
Windows Analysis Report methodsnetsh.exe

Overview

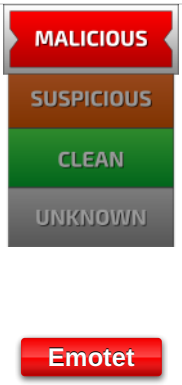
General Information

Sample Name:	methodsnetsh.exe
Analysis ID:	450352
MD5:	8e22080fe62e462.
SHA1:	8b58fd7bcd7083e.
SHA256:	d082395ca1ce0c…
Infos:	

Most interesting Screenshot:



Detection

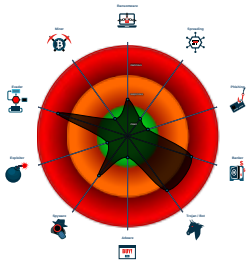


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Emotet e-Banking trojan
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- 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…
- Contains functionality to check if a w…

Classification



Process Tree

- **System is w10x64**
- methodsnetsh.exe (PID: 6032 cmdline: 'C:\Users\user\Desktop\methodsnetsh.exe' MD5: 8E22080FE62E462723D231FE5C8BA98A)
  - methodsnetsh.exe (PID: 5456 cmdline: --4a9ea48a MD5: 8E22080FE62E462723D231FE5C8BA98A)
- svchost.exe (PID: 3412 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- sensorias.exe (PID: 5564 cmdline: C:\Windows\SysWOW64\sensorias.exe MD5: 8E22080FE62E462723D231FE5C8BA98A)
  - sensorias.exe (PID: 6036 cmdline: --606904f7 MD5: 8E22080FE62E462723D231FE5C8BA98A)
- svchost.exe (PID: 6072 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5868 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5948 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5576 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2168 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 4168 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6096 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4880 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 496 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.204962255.0000000000620000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.204962255.0000000000620000.00000040.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x18ec:$snippet2: 6A 13 68 01 00 01 00 FF 15 D8 1B 41 00 85 C0 • 0x59a5:$snippet6: 33 C0 21 05 0C 3C 41 00 A3 08 3C 41 00 39 05 60 03 41 00 74 18 40 A3 08 3C 41 00 83 3C C5 60 03 ...

Source	Rule	Description	Author	Strings
00000000.00000002.204989867.00000000007D1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.204989867.00000000007D1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 D8 1B 7E 0 0 85 C0 • 0x5066:$snippet6: 33 C0 21 05 0C 3C 7E 00 A3 08 3C 7 E 00 39 05 60 03 7E 00 74 18 40 A3 08 3C 7E 00 83 3C C5 60 03 ...
00000006.00000002.224058115.0000000000AB0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.methodsnetsh.exe.6f053f.1.raw.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x3177:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x315d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
1.2.methodsnetsh.exe.6f053f.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.methodsnetsh.exe.6f053f.1.raw.unpack	Emotet	Emotet Payload	kevoreilly	• 0x13ad:$snippet2: 6A 13 68 01 00 01 00 FF 15 D8 1B 4 1 00 85 C0 • 0x5466:$snippet6: 33 C0 21 05 0C 3C 41 00 A3 08 3C 4 1 00 39 05 60 03 41 00 74 18 40 A3 08 3C 41 00 83 3C C5 60 03 ...
1.2.methodsnetsh.exe.6f053f.1.raw.unpack	Win32_Trojan_Emotet	unknown	ReversingLabs	• 0xe52:$decrypt_resource_v1: 55 8B EC 83 EC 18 53 8B D9 8B C2 56 57 89 45 F0 8B 3B 33 F8 8B C7 89 7D EC 83 E0 03 75 05 8D 77 ... • 0xcfbf:$generate_filename_v1: 56 57 33 C0 BF 28 41 41 00 57 50 50 6A 1C 50 FF 15 A8 2B 41 00 BA 7E BC E6 47 B9 60 0D 41 00 E8 ...
0.2.methodsnetsh.exe.62053f.1.raw.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x3177:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x315d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
Click to see the 23 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

Multi AV Scanner detection for submitted file

E-Banking Fraud:

Detected Emotet e-Banking trojan

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

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 checking mutex)

Lowering of HIPS / PFW / Operating System Security Settings:

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

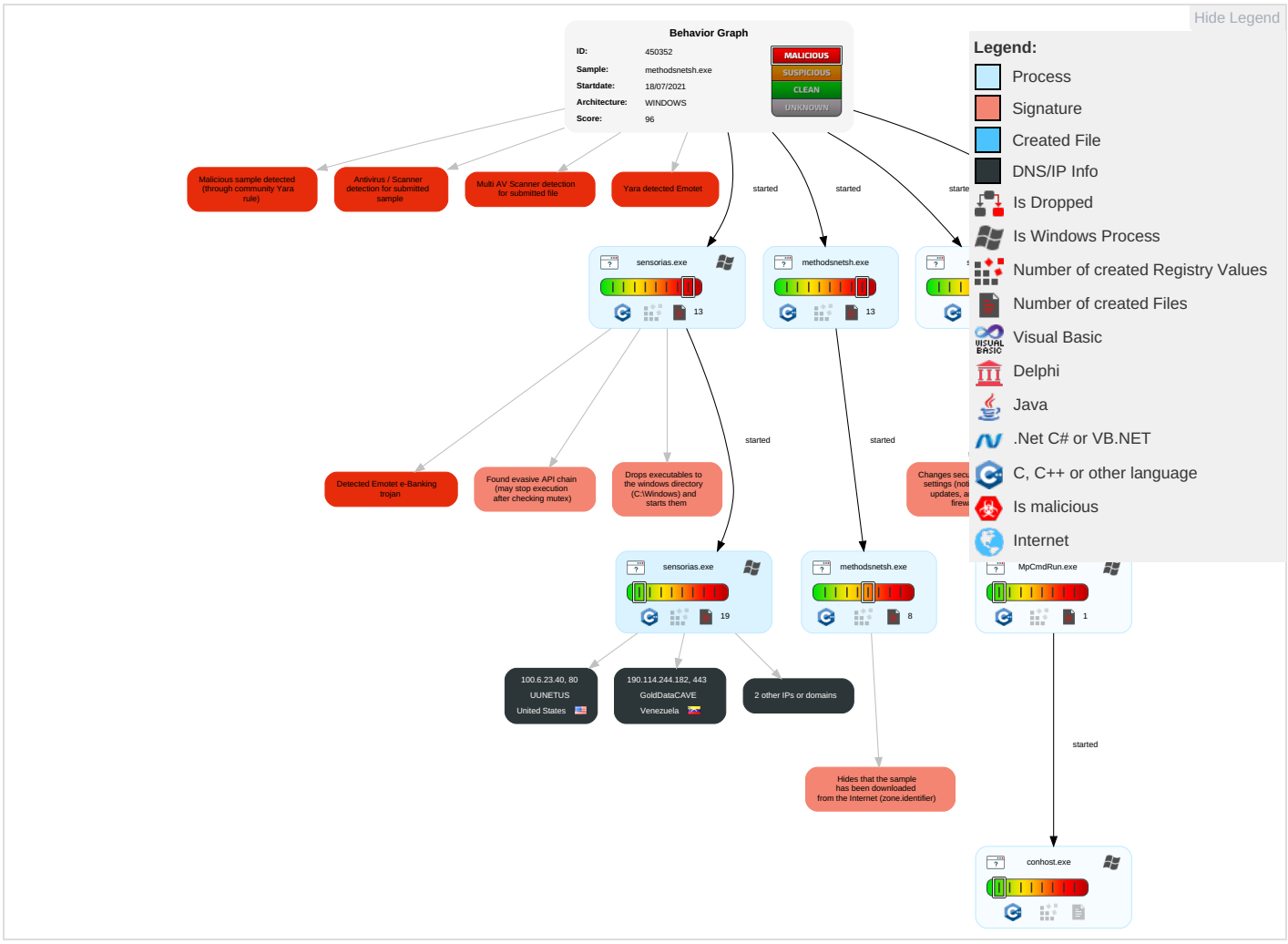
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 1 2 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 2	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 2	Windows Service 1 2	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	Service Execution 1 2	Logon Script (Mac)	Windows Service 1 2	DLL Side-Loading 1	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Process Injection 1	File Deletion 1	LSA Secrets	Security Software Discovery 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
methodsnetsh.exe	66%	Virustotal		Browse
methodsnetsh.exe	59%	Metadefender		Browse
methodsnetsh.exe	86%	ReversingLabs	Win32.Trojan.Emotet	
methodsnetsh.exe	100%	Avira	HEUR/AGEN.1123999	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.methodsnetsh.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
1.0.methodsnetsh.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
6.0.sensorias.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
0.2.methodsnetsh.exe.62053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.sensorias.exe.ea053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.0.sensorias.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
7.2.sensorias.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
6.2.sensorias.exe.ab053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.methodsnetsh.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.sensorias.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File
1.2.methodsnetsh.exe.6f053f.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.methodsnetsh.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123999		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://91.250.96.22/LhqjdNLOiM5Uy7n	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://%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://https://dynamic.t	0%	URL Reputation	safe	
http://https://fs.microsoft.cH	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	
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
91.250.96.22	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
100.6.23.40	unknown	United States		701	UUNETUS	false
190.114.244.182	unknown	Venezuela		28007	GoldDataCAVE	false
200.71.200.4	unknown	Chile		20015	FullComSACL	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	450352
Start date:	18.07.2021
Start time:	17:47:50
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	methodsnetsh.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.bank.troj.evad.winEXE@18/7@0/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
17:49:04	API Interceptor	2x Sleep call for process: svchost.exe modified
17:50:19	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
91.250.96.22	ipmimaker.exe	Get hash	malicious	Browse	
100.6.23.40	http://nofile.ir/wp-content/INC/hzv4v7-855-1188-y244-rxvi/	Get hash	malicious	Browse	• 100.6.23.40/DaV5
	http://https://sharevission.com/wp-content/statement/	Get hash	malicious	Browse	• 100.6.23.40/XXex1CeJN
	http://membros.rendaprevi.com.br/wp-content/OCT/yysn5-130737-9201067-melm80sxj-72bezyorg7	Get hash	malicious	Browse	• 100.6.23.40/tFCwNOMvoMKPyZws
	http://https://www.scriptmarket.cn/aspnet_client/payment/3gktoj3r/bild-72121-071870-9ebzsg4dasb-q8ak1kms1r/	Get hash	malicious	Browse	• 100.6.23.40/MMunsXz6R9eebVAh0z2
	http://https://istoselides.zerman.store/test/balance/vh8-20243-290351909-unq1qu11n-9xg9czfo1c	Get hash	malicious	Browse	• 100.6.23.40/143VIBS
	http://bellconsulting.co.in/fonts/balance/4jh-114249-3812-3getwfervju-3fw88reu/	Get hash	malicious	Browse	• 100.6.23.40/Vk87Wb1LgM3oF4zHE
	http://bellconsulting.co.in/fonts/balance/4jh-114249-3812-3getwfervju-3fw88reu	Get hash	malicious	Browse	• 100.6.23.40/cmA0qp
190.114.244.182	ipmimaker.exe	Get hash	malicious	Browse	
200.71.200.4	ipmimaker.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IWW-010120 NJO-011820.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	mormanti.exe	Get hash	malicious	Browse	• 83.169.21.32
	deepRats.exe	Get hash	malicious	Browse	• 85.25.213.211
	4zL5XaZ4kc.exe	Get hash	malicious	Browse	• 37.61.205.212
	Qbat1G0Mop.exe	Get hash	malicious	Browse	• 37.61.205.212
	NWMEaRqF7s.exe	Get hash	malicious	Browse	• 62.75.141.82
	rOFZ7NRC7X.exe	Get hash	malicious	Browse	• 188.93.8.132
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 87.230.93.218
	bol88C399w.exe	Get hash	malicious	Browse	• 62.75.141.82
	bol88C399w.exe	Get hash	malicious	Browse	• 62.75.141.82
	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 85.25.199.56
	wZtsCbg7ty.exe	Get hash	malicious	Browse	• 77.91.233.67
	u3O3kHV2IT.exe	Get hash	malicious	Browse	• 134.119.45.197
	SecuriteInfo.com.BackDoor.Rat.281.18292.exe	Get hash	malicious	Browse	• 85.25.185.17
	CIh8xCD9fi.exe	Get hash	malicious	Browse	• 188.138.33.41
	Shipping Doc578.exe	Get hash	malicious	Browse	• 92.204.54.9
	8mnXkjPdP0.exe	Get hash	malicious	Browse	• 188.138.33.41
	SecuriteInfo.com.VB.Trojan.Valyria.4515.27984.xls	Get hash	malicious	Browse	• 62.75.161.205
	CaUGJzgC.php.dll	Get hash	malicious	Browse	• 62.75.161.205
	CaUGJzgC.php.dll	Get hash	malicious	Browse	• 62.75.161.205
	inv062021.exe	Get hash	malicious	Browse	• 85.25.177.199
GoldDataCAVE	MkisahOBqH.dll	Get hash	malicious	Browse	• 190.52.102.57
UUNETUS	i	Get hash	malicious	Browse	• 100.49.120.210
	deepRats.exe	Get hash	malicious	Browse	• 96.253.78.108
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 98.117.195.74
	NWMEaRqF7s.exe	Get hash	malicious	Browse	• 173.62.217.22
	Remote Support-windows64-online.exe	Get hash	malicious	Browse	• 72.76.226.13
	segYCksCNt.exe	Get hash	malicious	Browse	• 96.231.136.12
	bol88C399w.exe	Get hash	malicious	Browse	• 173.63.222.65
	bol88C399w.exe	Get hash	malicious	Browse	• 173.63.222.65
	mjzvlwau	Get hash	malicious	Browse	• 65.253.41.93
	networkservice.exe	Get hash	malicious	Browse	• 206.112.13 9.168
	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 74.108.124.180
	8UsA.sh	Get hash	malicious	Browse	• 108.30.94.39
	Host Process For Windows Tasks.exe	Get hash	malicious	Browse	• 100.15.49.234
	nT7K5GG5km	Get hash	malicious	Browse	• 186.64.54.15
	KnAY2OIPI3	Get hash	malicious	Browse	• 100.58.97.165
	x86_unpacked	Get hash	malicious	Browse	• 203.102.4.9
	ppc_unpacked	Get hash	malicious	Browse	• 65.253.89.22
	JRyLnlTR1O	Get hash	malicious	Browse	• 108.27.92.79
	ldr.sh	Get hash	malicious	Browse	• 108.54.61.15
	rIbyGX66Op	Get hash	malicious	Browse	• 68.129.151.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\1942f959aae25ff5e177f0a0e912022f_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\SysWOW64\sensorias.exe
File Type:	data
Category:	dropped
Size (bytes):	57
Entropy (8bit):	2.062967662624547
Encrypted:	false
SSDEEP:	3:/lEltfgnwT:yvT
MD5:	B5D2B9D74D52DAC47A3F3CB1D065305F
SHA1:	41A4742BC23F3A6FF61C60884604DA6448FFF274
SHA-256:	6359A4FCB0DABE70B88913A6A03CC21385459B8A924A6B3688A2E185C54DAAFA
SHA-512:	01EA77C5972D33494C10D6ADB47CB3F30EAC1AA4B93D6BAAFB75299AA99FED818A6275801BAAE92C18AC5D3C64443BB631A63C2B39B1B88BCD774218BB2B9 0F
Malicious:	false
Preview:	.....computer$.

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5921564533653279
Encrypted:	false
SSDEEP:	6:0Fkcek1GaD0JOCEfMuaaD0JOCEfMKQmDpzh/tAl/gz2cE0fMbhEZolrRSQ2hyYI8:01GaD0JcaaD0JwQQRh/tAg/0bjSQJ
MD5:	113FD5F57C68BE1CD79EE5B4A4A94815
SHA1:	0B14D9A719D31D6CCB384C6B11913DA0E910D65A
SHA-256:	06C45184851B6B33F0D27C62282A411F3CFA3CE38284E5208C362C88EC2BB6C3
SHA-512:	337ADCB907F2EF5DBAF8D57A40C9BBAA21CFB07DCF9A55E5AA438E2AEFD365DD237E167C53000D97AAB5DB5FC3B249AAF38875FC17A887C3FC2232364C12E 6EA
Malicious:	false
Preview:	......:{..(.....1...y%..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....1...y%.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x99fb9f13, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09453052983328276
Encrypted:	false
SSDEEP:	6:mzwl/+9iRIE11Y8TRXcfWqKozwl/+9iRIE11Y8TRXcfWqK:m0+9iO4blcf1Ko0+9iO4blcf1K
MD5:	50E5B561598CBAB9303B7DBB607857B2
SHA1:	39B79BDD8D2BF8847C27C84646CD9E7F52F6E350
SHA-256:	16E60E7B0279AF13DDC3450FE9CB2E03BBDDC58BA68B153AEC313FB06B8BFDD9
SHA-512:	A16D50C436ABBE542AB9FAC12DF1D24AC33759EA4AF4779AF676539579BBC69E9FA719AFA525798941B52FA463D77B0474BC18E0C34BFBF7F23D7C9A16D216 D
Malicious:	false
Preview:	....e.f.3...w.....&.....w...1...y%.h.(.....3...w.....B.....@..... ....3...w..... .....1...y%m.....9.oa.1...y%..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10865628380359972
Encrypted:	false
SSDEEP:	3:ntTEvhnIp+/t+Al/bJdAtiufUcApllill:A9/t+At4/fWG

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
MD5:	0A4E1DE4FB960ADFE97339C432EB562B
SHA1:	81C02AB7F5B6D57A08200D88FB755918147AEC82
SHA-256:	58A57359E41D52C0F3BC7675DC538B45384BC7E536059E279904B092C369D4F2
SHA-512:	45E18DBEC85FADC44C6893E2A6DB3E4528E1540BC8002799F4F4926D8FCB4846B69F4A958F53E24A7C61424958D7E289803402B8A2DB536F6DD13CB57596712
Malicious:	false
Preview:	....3...w...1...y%......w...............w.......w....:O.....w..................9.oa.1...y%...

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\methodsnetsh.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5 DE
Malicious:	false
Preview:	....user.

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):	3.1549544060771617
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rZB2uD9Ck9+MlWlLehB4yAq7ejC4B2uD9P:OaqdmuF3rjf+kWReH4yJ7MrF
MD5:	1E366452F97A8482ECB9C00961CFB6CE
SHA1:	DD546B50184AB1398846B2497CACE845E7C068EB
SHA-256:	0975D17236669342BD464FE84038355F5335D7B36BDBAE20B578DDF57A8AC656
SHA-512:	D01A8C3B787F9BCD6646B8C50592F4E643D8CB6A515729BA2538C936B45E7DB08C773E7DAE3920B1F510857910EA6A42983FBC92AAD65DD93F5A53247114756
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.:. .. S.u.n. .. J.u.l. .. 1.8. .. 2.0.2.1. .1.7.:.5.0.:.1. 9.........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.:. .. S.u.n. .. J.u.l. .. 1.8. .. 2.0.2.1. .1.7.:.5.0.:.1.9.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.095719913394487
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	methodsnetsh.exe
File size:	352278
MD5:	8e22080fe62e462723d231fe5c8ba98a
SHA1:	8b58fd7bcd7083e5a326e7a04e10c0e0626ac4ca
SHA256:	d082395ca1ce0c118edbff1e5bf1b1d4ad2db5aefa5691cc4c15bd94208a3cc0
SHA512:	ad73acccf790f4962e8c67bfa4cdfc189b0e8bfb54af94902294f7b55c000a877cce7e22becd095133b701a5966a8b3809b850bcd5c24d30fe3c14584b09cbd7
SSDEEP:	6144:keeqOehy0o9z+dfMfpwZZZZw/zkF5+ZymSRln98x:nVjt8Pri5+ZIX9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._..._.. ._.....X...L...]...Z...C...Z.....t...V.....W.....N..._...G..... ^...Z...9.....^...Z...^...Rich_.....

File Icon

Icon Hash:	e0e2dbc5ddd1d9d9

Static PE Info

General

Entrypoint:	0x41d436
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5E21F7F3 [Fri Jan 17 18:07:47 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:	95079c0595744051842d53e9a3ed2db3

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x32664	0x33000	False	0.329182942708	data	5.2999185965	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x34000	0x73c8	0x8000	False	0.318481445312	data	4.70606194355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3c000	0x51d4	0x2000	False	0.29150390625	data	3.57086001659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0x17ed8	0x18000	False	0.79535929362	data	7.3193275368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
French	France	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: methodsnetsh.exe PID: 6032 Parent PID: 5632

General

Start time:	17:48:38
Start date:	18/07/2021
Path:	C:\Users\user\Desktop\methodsnetsh.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\methodsnetsh.exe'
Imagebase:	0x400000
File size:	352278 bytes
MD5 hash:	8E22080FE62E462723D231FE5C8BA98A
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: 00000000.00000002.204962255.0000000000620000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.204962255.0000000000620000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.204989867.00000000007D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.204989867.00000000007D1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: methodsnetsh.exe PID: 5456 Parent PID: 6032

General

Start time:	17:48:39
Start date:	18/07/2021
Path:	C:\Users\user\Desktop\methodsnetsh.exe
Wow64 process (32bit):	true
Commandline:	--4a9ea48a
Imagebase:	0x400000
File size:	352278 bytes
MD5 hash:	8E22080FE62E462723D231FE5C8BA98A
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: 00000001.00000002.224911448.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.224911448.00000000006F0000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.225065332.00000000009D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.225065332.00000000009D1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

File Deleted

Analysis Process: svchost.exe PID: 3412 Parent PID: 568

General

Start time:	17:48:46
Start date:	18/07/2021
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: sensorias.exe PID: 5564 Parent PID: 568

General

Start time:	17:48:47
Start date:	18/07/2021
Path:	C:\Windows\SysWOW64\sensorias.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sensorias.exe
Imagebase:	0x400000
File size:	352278 bytes
MD5 hash:	8E22080FE62E462723D231FE5C8BA98A
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: 00000006.00000002.224058115.0000000000AB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.224058115.0000000000AB0000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.224082773.0000000000F61000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.224082773.0000000000F61000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

Analysis Process: sensorias.exe PID: 6036 Parent PID: 5564

General

Start time:	17:48:48
Start date:	18/07/2021
Path:	C:\Windows\SysWOW64\sensorias.exe
Wow64 process (32bit):	true
Commandline:	--606904f7
Imagebase:	0x400000
File size:	352278 bytes
MD5 hash:	8E22080FE62E462723D231FE5C8BA98A
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: 00000007.00000002.469150686.0000000000EC1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000007.00000002.469150686.0000000000EC1000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000007.00000002.469102796.0000000000EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000007.00000002.469102796.0000000000EA0000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 6072 Parent PID: 568

General

Start time:	17:49:04
Start date:	18/07/2021
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: 5868 Parent PID: 568

General

Start time:	17:49:08
Start date:	18/07/2021
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: 5948 Parent PID: 568

General

Start time:	17:49:15
Start date:	18/07/2021
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: 5576 Parent PID: 568

General

Start time:	17:49:16
Start date:	18/07/2021
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: 2168 Parent PID: 568

General

Start time:	17:49:17
Start date:	18/07/2021
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: 4168 Parent PID: 568

General

Start time:	17:49:17

Start date:	18/07/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff675c40000
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: 6096 Parent PID: 568

General

Start time:	17:49:18
Start date:	18/07/2021
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: svchost.exe PID: 496 Parent PID: 568

General

Start time:	17:49:18
Start date:	18/07/2021
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: MpCmdRun.exe PID: 4880 Parent PID: 6096

General

Start time:	17:50:18
Start date:	18/07/2021

Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff653940000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 3596 Parent PID: 4880

General

Start time:	17:50:19
Start date:	18/07/2021
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
Reputation:	high

Disassembly

Code Analysis