ID: 376365
Sample Name: aEdlObiYav
Cookbook: default.jbs
Time: 12:14:01
Date: 26/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report aEdlObiYav 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
E-Banking Fraud: 6
System Summary: 6
Persistence and Installation Behavior: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
Lowering of HIPS / PFW / Operating System Security Settings: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 11
Public 11
Private 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Rich Headers 18
Data Directories 18

Sections 19
Resources 19
Imports 20
Exports 21
Possible Origin 21
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: aEdlObiYav.exe PID: 5064 Parent PID: 5764 24
General 24
File Activities 24
Analysis Process: aEdlObiYav.exe PID: 5528 Parent PID: 5064 24
General 24
File Activities 25
File Deleted 25
Analysis Process: picturerus.exe PID: 6084 Parent PID: 556 25
General 25
File Activities 25
Analysis Process: picturerus.exe PID: 4228 Parent PID: 6084 26
General 26
File Activities 26
File Created 26
Analysis Process: svchost.exe PID: 5536 Parent PID: 556 27
General 27
File Activities 27
Registry Activities 28
Analysis Process: svchost.exe PID: 2376 Parent PID: 556 28
General 28
File Activities 28
Analysis Process: svchost.exe PID: 4504 Parent PID: 556 28
General 28
Registry Activities 28
Analysis Process: svchost.exe PID: 804 Parent PID: 556 29
General 29
Analysis Process: SgrmBroker.exe PID: 1228 Parent PID: 556 29
General 29
Analysis Process: svchost.exe PID: 5540 Parent PID: 556 29
General 29
Registry Activities 29
Analysis Process: MpCmdRun.exe PID: 5048 Parent PID: 5540 30
General 30
File Activities 30
File Written 30
Analysis Process: conhost.exe PID: 3896 Parent PID: 5048 32
General 32
Disassembly 32
Code Analysis 32

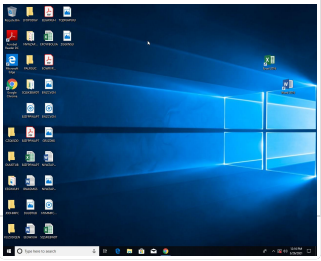
Analysis Report aEdlObiYav

Overview

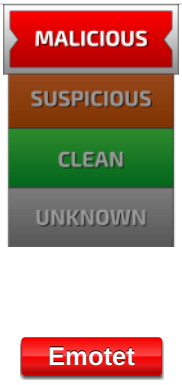
General Information

Sample Name:	aEdlObiYav (renamed file extension from none to exe)
Analysis ID:	376365
MD5:	ae03a6f8fb74d40..
SHA1:	6ee320cedc7749..
SHA256:	1ad1ff05930f27e…
Infos:	

Most interesting Screenshot:



Detection

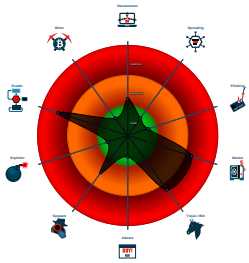


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Antivirus or Machine Learning detec…

Classification



Startup

- **System is w10x64**
- aEdlObiYav.exe (PID: 5064 cmdline: 'C:\Users\user\Desktop\aEdlObiYav.exe' MD5: AE03A6F8FB74D401B403647D28E21574)
  - aEdlObiYav.exe (PID: 5528 cmdline: --79fd8b32 MD5: AE03A6F8FB74D401B403647D28E21574)
- picturerus.exe (PID: 6084 cmdline: C:\Windows\SysWOW64\picturerus.exe MD5: AE03A6F8FB74D401B403647D28E21574)
  - picturerus.exe (PID: 4228 cmdline: --b743c2a4 MD5: AE03A6F8FB74D401B403647D28E21574)
- svchost.exe (PID: 5536 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2376 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4504 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 804 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1228 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5540 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5048 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.488250881.0000000000ED1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.488250881.0000000000ED1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA ED 0 0 85 C0 • 0x50d4:$snippet6: 33 C0 21 05 EC 10 EE 00 A3 E8 10 E E 00 39 05 A0 E3 ED 00 74 18 40 A3 E8 10 EE 00 83 3C C5 A0 E3 ...
00000003.00000002.240281211.0000000000E21000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.240281211.0000000000E21000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA E2 0 0 85 C0 • 0x50d4:$snippet6: 33 C0 21 05 EC 10 E3 00 A3 E8 10 E 3 00 39 05 A0 E3 E2 00 74 18 40 A3 E8 10 E3 00 83 3C C5 A0 E3 ...
00000001.00000002.241329316.0000000002180000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

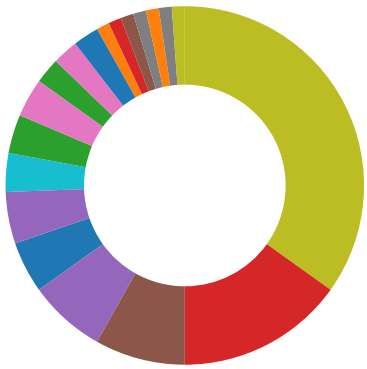
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.aEdlObiYav.exe.22c053f.2.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
0.2.aEdlObiYav.exe.22c053f.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.aEdlObiYav.exe.22c053f.2.unpack	Emotet	Emotet Payload	kevoreilly	• 0x7ad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x48d4:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 4 1 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...
3.2.picturerus.exe.e1053f.2.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
3.2.picturerus.exe.e1053f.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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:

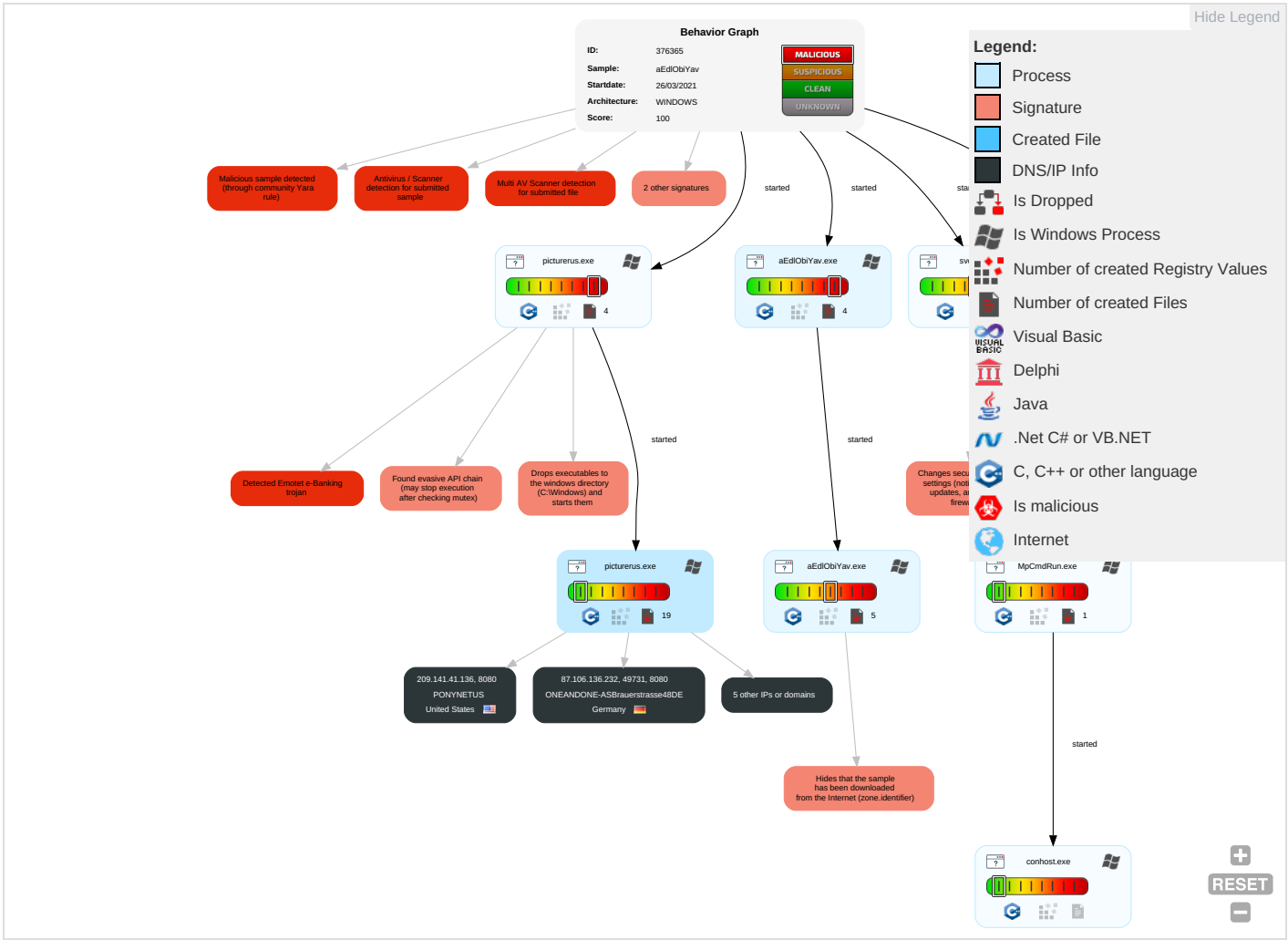
Yara detected Emotet

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 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 1 1 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 1	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-S Port 1
Local Accounts	Service Execution 1 2	Logon Script (Mac)	Windows Service 1 2	Software Packing 1	NTDS	System Information Discovery 4 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Process Injection 1	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 1	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)	Virtualization/Sandbox Evasion 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

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
aEdlObiYav.exe	96%	ReversingLabs	Win32.Trojan.Emotet	
aEdlObiYav.exe	100%	Avira	HEUR/AGEN.1111753	
aEdlObiYav.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.aEdlObiYav.exe.22c053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.picturerus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
0.2.aEdlObiYav.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
3.2.picturerus.exe.e1053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.aEdlObiYav.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
1.2.aEdlObiYav.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
4.2.picturerus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
3.0.picturerus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
1.0.aEdlObiYav.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
4.2.picturerus.exe.60053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.aEdlObiYav.exe.218053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.0.picturerus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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://178.210.51.222/attrib/glitch/add/merge/	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

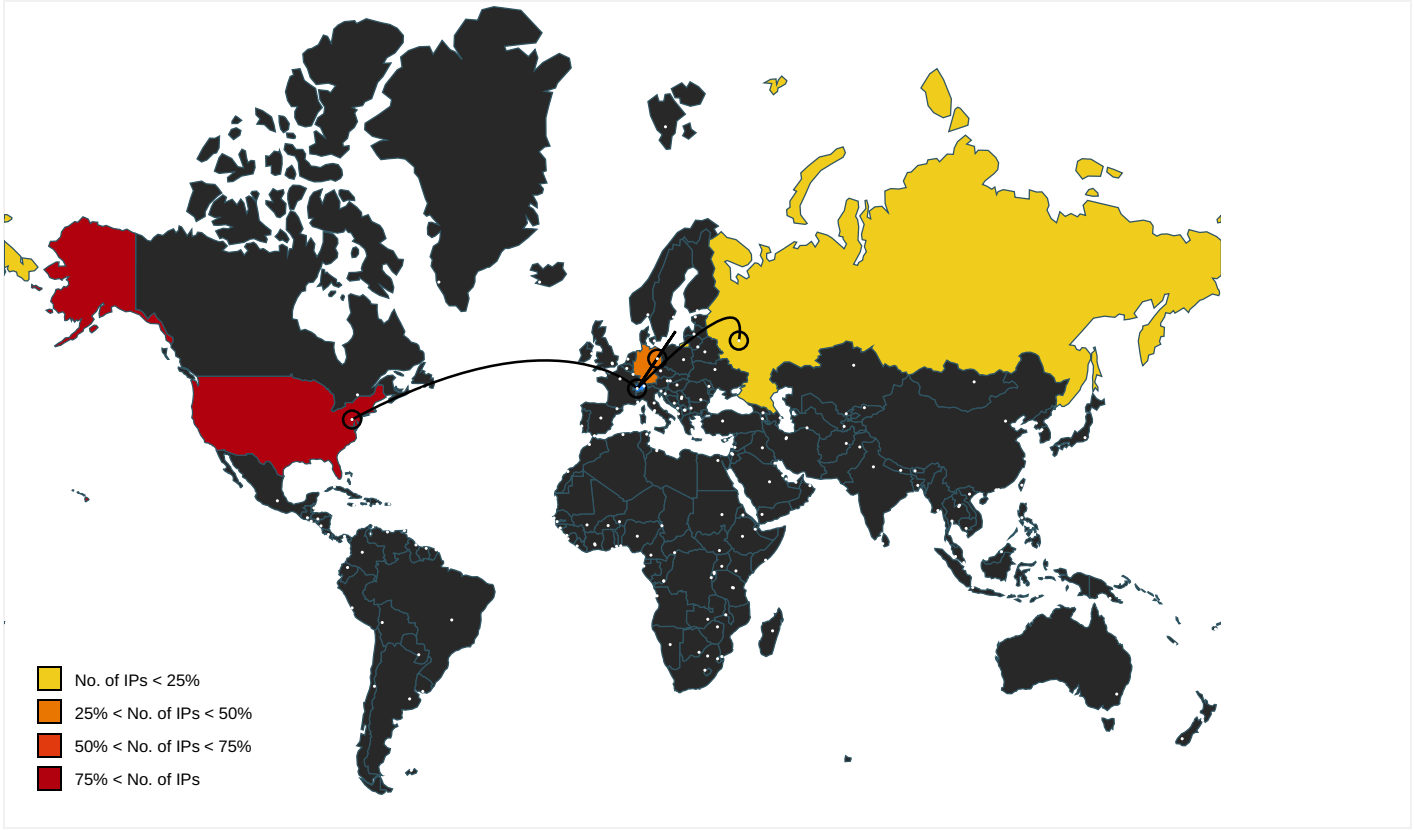
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000003.305027218.0000023F57C45000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000009.00000002.305319310.0000023F57C3D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000009.00000002.305319310.0000023F57C3D000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000009.00000002.305345104.0000023F57C4E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000009.00000002.305319310.0000023F57C3D000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000003.305027218.0000023F57C45000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000009.00000002.305351605.0000023F57C5C000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000002.305301146.0000023F57C13000.00000004.00000001.sdmp, svchost.exe, 00000009.00000002.305319310.0000023F57C3D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000009.00000002.305323775.0000023F57C42000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000007.00000002.488280885.000001D9ACE3E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000002.305345104.0000023F57C4E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000009.00000003.283224217.0000023F57C31000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000003.305003343.0000023F57C5A000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000009.00000003.283224217.0000023F57C31000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000009.00000002.305351605.0000023F57C5C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 00000005.00000002.491346023.000001F634C00000.00000002.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000009.00000002.305323775.0000023F57C42000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000009.00000002.305368398.0000023F57C64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000009.00000003.305042012.0000023F57C3A000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000009.00000002.305351605.0000023F57C5C000.00000004.00000001.sdmp	false		high
http://178.210.51.222/attrib/glitch/add/merge/	picturerus.exe, 00000004.00000002.487408684.0000000000199000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://activity.windows.com	svchost.exe, 00000007.00000002.488280885.000001D9ACE3E000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000009.00000002.305301146.0000023F57C13000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000009.00000003.304991002.0000023F57C5F000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000009.00000002.305319310.0000023F57C3D000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000007.00000002.488280885.000001D9ACE3E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000009.00000003.305003343.0000023F57C5A000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.89.236.214	unknown	Germany		31400	ACCELERATED-ITDE	false
198.199.114.69	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
104.236.246.93	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
178.210.51.222	unknown	Russian Federation		43727	KVANT-TELECOMRU	false
45.33.54.74	unknown	United States		63949	LINODE-APLinodeLLCUS	false
209.141.41.136	unknown	United States		53667	PONYNETUS	false
87.106.136.232	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	376365
Start date:	26.03.2021
Start time:	12:14:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aEdlObiYav (renamed file extension from none to exe)

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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.bank.troj.evad.winEXE@15/5@0/8
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 91.1% • Quality standard deviation: 6.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.82.210.154, 40.88.32.150, 13.64.90.137, 52.147.198.201, 13.88.21.125, 104.43.139.144, 95.100.54.203, 51.103.5.186, 20.50.102.62, 23.10.249.43, 23.10.249.26, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/376365/sample/aEdlObiYav.exe

Simulations

Behavior and APIs

Time	Type	Description
12:15:06	API Interceptor	2x Sleep call for process: svchost.exe modified

Time	Type	Description
12:16:21	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
198.199.114.69	VYHauUUCLr.exe	Get hash	malicious	Browse	• 198.199.114.69:8080/badge/report/xian/
	http://infraturkey.com/deletecomment/parts_service/daaMnHeDzR/	Get hash	malicious	Browse	• 198.199.114.69:8080/jit/
	http://https://newwell.studio/test/DOC/NtnDpOmWbTdPEdBxrLyy/	Get hash	malicious	Browse	• 198.199.114.69:8080/json/
104.236.246.93	form.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/hZhNeaDm/dcUDNcyqQW/niVKRU29uscA3Ju/
	UAr7Xz5JWr.exe	Get hash	malicious	Browse	• 104.236.246.93:8080/ZxZomdMT6G9XK/ghoypfynUN/
	invoice #865119.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/XzlcYaBSUK0cswU/pzKYcLCk/PbvwO3hXkaN7W/WM9ZNIP/
	XY8707573112TQ.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/att30xZ/YONUKbuNJ8lOQjL/G34JI8e3LEFl/jaWgrB/
	test-emotet.exe	Get hash	malicious	Browse	• 104.236.246.93/
45.33.54.74	FA_36802305641_Oct2019.doc	Get hash	malicious	Browse	• 45.33.54.74:443/loadan/stubs/
87.106.136.232	http://87.106.136.232	Get hash	malicious	Browse	• 87.106.136.232/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 185.245.99.134
	usb	Get hash	malicious	Browse	• 45.133.9.100
	bin.exe	Get hash	malicious	Browse	• 84.200.110.123
	run32dll.exe	Get hash	malicious	Browse	• 45.154.35.214
	Vidoe001mp4.scr signed FAT11 d.o.exe	Get hash	malicious	Browse	• 45.154.35.218
	OD29081792Y_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 185.245.99.2
	Fakt. - 19 okt., 2020.doc	Get hash	malicious	Browse	• 185.194.237.65
	liposnejk.exe	Get hash	malicious	Browse	• 84.200.209.11
	jackpot_http.exe	Get hash	malicious	Browse	• 213.190.30.57
	http://cumds.com/_vti_log/paclm/02d8rg/2jx860566807ll82z66y0b2bd/	Get hash	malicious	Browse	• 84.200.5.215
	mb10.exe	Get hash	malicious	Browse	• 185.245.99.134

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mb10.exe	Get hash	malicious	Browse	• 185.245.99.134
	http://https://withered-butterfly-9cd3.tkbizulvc.workers.dev/	Get hash	malicious	Browse	• 193.135.10.219
	5xcdJCRyWp.exe	Get hash	malicious	Browse	• 82.211.30.202
	emotet_11.doc	Get hash	malicious	Browse	• 82.211.30.202
	emotet_11.doc	Get hash	malicious	Browse	• 82.211.30.202
	emotet.doc	Get hash	malicious	Browse	• 82.211.30.202
	emotet.doc	Get hash	malicious	Browse	• 82.211.30.202
	RechnungRechnung.doc	Get hash	malicious	Browse	• 82.211.30.202
	RechnungRechnung.doc	Get hash	malicious	Browse	• 82.211.30.202
DIGITALOCEAN-ASNUS	ajESKclz8f.exe	Get hash	malicious	Browse	• 138.197.53.157
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 134.209.159.22
	rona.exe	Get hash	malicious	Browse	• 104.248.117.19
	fDFkIEBfpm.exe	Get hash	malicious	Browse	• 206.189.174.29
	JE74.vbs	Get hash	malicious	Browse	• 104.248.193.149
	4d86320858effdc2c8bf3fc2ae86080f0f6b449141991.dll	Get hash	malicious	Browse	• 167.172.240.248
	Rc93GKN1MJ.exe	Get hash	malicious	Browse	• 138.197.161.207
	tBU1h89Elf.dll	Get hash	malicious	Browse	• 167.172.240.248
	JbzAir8erB.dll	Get hash	malicious	Browse	• 167.172.240.248
	5sH546K9WX.dll	Get hash	malicious	Browse	• 167.172.240.248
	qcxuvc6i7S.dll	Get hash	malicious	Browse	• 167.172.240.248
	4itHMydujq.dll	Get hash	malicious	Browse	• 167.172.240.248
	LzYnwzj8zx.dll	Get hash	malicious	Browse	• 167.172.240.248
	si8zqjtdqI.dll	Get hash	malicious	Browse	• 167.172.240.248
	5aVrBcmCyl.dll	Get hash	malicious	Browse	• 167.172.240.248
	8z5iVMz39r.dll	Get hash	malicious	Browse	• 167.172.240.248
	fXNR9O8fGS.dll	Get hash	malicious	Browse	• 167.172.240.248
	wdPI7Jq0EV.dll	Get hash	malicious	Browse	• 167.172.240.248
	SHWUWeV5aB.dll	Get hash	malicious	Browse	• 167.172.240.248
	XG8kPPiEda.dll	Get hash	malicious	Browse	• 167.172.240.248
DIGITALOCEAN-ASNUS	ajESKclz8f.exe	Get hash	malicious	Browse	• 138.197.53.157
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 134.209.159.22
	rona.exe	Get hash	malicious	Browse	• 104.248.117.19
	fDFkIEBfpm.exe	Get hash	malicious	Browse	• 206.189.174.29
	JE74.vbs	Get hash	malicious	Browse	• 104.248.193.149
	4d86320858effdc2c8bf3fc2ae86080f0f6b449141991.dll	Get hash	malicious	Browse	• 167.172.240.248
	Rc93GKN1MJ.exe	Get hash	malicious	Browse	• 138.197.161.207
	tBU1h89Elf.dll	Get hash	malicious	Browse	• 167.172.240.248
	JbzAir8erB.dll	Get hash	malicious	Browse	• 167.172.240.248
	5sH546K9WX.dll	Get hash	malicious	Browse	• 167.172.240.248
	qcxuvc6i7S.dll	Get hash	malicious	Browse	• 167.172.240.248
	4itHMydujq.dll	Get hash	malicious	Browse	• 167.172.240.248
	LzYnwzj8zx.dll	Get hash	malicious	Browse	• 167.172.240.248
	si8zqjtdqI.dll	Get hash	malicious	Browse	• 167.172.240.248
	5aVrBcmCyl.dll	Get hash	malicious	Browse	• 167.172.240.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8z5iVMz39r.dll	Get hash	malicious	Browse	• 167.172.240.248
	fXNR9O8fGS.dll	Get hash	malicious	Browse	• 167.172.240.248
	wdPI7Jq0EV.dll	Get hash	malicious	Browse	• 167.172.240.248
	SHWUWeV5aB.dll	Get hash	malicious	Browse	• 167.172.240.248
	XG8kPPiEda.dll	Get hash	malicious	Browse	• 167.172.240.248

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):	0.597889115294713
Encrypted:	false
SSDEEP:	6:bVk1GaD0JOCEfMuaaD0JOCEfMKQmDF1Al/gz2cE0fMbhEZolrRSQ2hyYIIT:bCGaD0JcaaD0JwQQF1Ag/0bjSQJ
MD5:	4E33D805E2A479CEE4D175EDBAE59C11
SHA1:	1EAA684AA38277FA15E860035EB1BDEBCE587FAE
SHA-256:	C9040CEDCAA9BC5392C8A43422B685431F804EF7E2669F45A546DAFEE0512988
SHA-512:	D74D01C1C48F02E7E75DD5BFA2BA0849912165C532A8D62D47BD8D5E2DBC5CD9AD391DB420CDDCA382EB10CC55B0905E164A1739B2C89161DF89A74810230C7
Malicious:	false
Reputation:	low
Preview:	....E..h..(.....yY..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....yY.....&.....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 0x04dffe7c, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09636108144020473
Encrypted:	false
SSDEEP:	6:sEsAzwl/+KRIE11Y8TRXrrFlKGEsAzwl/+KRIE11Y8TRXrrFlK:sFA0+KO4blrrFlKGFA0+KO4blrrFlK
MD5:	CC2B342ACF2A0814B5BCAE5A58DBD2FC
SHA1:	C44E20AB2EA24C9EA9A4C381B6E01B832946E984
SHA-256:	F709D7EA01C60FA0756B3E170EC7FCE60EFD88499230B57C9064D38FC77C63A2
SHA-512:	AA06D2E349B13ADD0C70ADBE8268B0C03B39EC1AA4BDAD6E8CFD1A25F9CB898C9ED653364A1DA03814D8769D111E0DB33DDDFD38E172BD661537642363CDFE2
Malicious:	false
Reputation:	low
Preview:	...|.. .....e.f.3...w.....&.....w.....yY.h.(.....3...w.....B.....@..... ....3...w.....Z.....yY.....b.....yY.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11086134938174995
Encrypted:	false
SSDEEP:	3:DnSLEvjUOMjSXl/bJdAtixx/CYIl:OyPMj8t4O/
MD5:	F88FE82FEE638B48780BE86DCD42F59B
SHA1:	68CEFD6EF8B846506CCBD4615FF9BBE46281EA49
SHA-256:	3C0871C0DD8B3D2A331A974F01A144C665E3476291AB203118C257FEFBB3483D
SHA-512:	9105C803F7A75AFC6D3502A7BC89B9719A32AAB46909C010B3ACA2D408E29E534138946B62DD0EF0DD99EFD8306AE0BED2DFEA4964C5EBFE776098B98A6E1BE5
Malicious:	false
Reputation:	low
Preview:	.....3...w.....yY.....w.....w.....w....:O....w.....b.....yY.....

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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Reputation:	high, very likely benign file
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):	3.132534585600141
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rYyGljok9+MlWlLehB4yAq7ejCZyGljB:OaqdmuF3roljL+kWReH4yJ7MAljB
MD5:	565473E4D9B99CA298056458A32F5C4A
SHA1:	41B263FB8EF34508A270C1131E851F03AA21152C
SHA-256:	AB279EB907E7309130B86D1709ACA6F349EEDD5AC22FA34388685A2EAC32FDB2
SHA-512:	FC96109E8D6901953C225F7483A935CAF1068F4DD2A10CD8F645FFD84A0C74374D0124F09723001883DFAA86631F56D770301BC043A38515F880C64F3CC09839
Malicious:	false
Reputation:	low
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. .. M.a.r. .. 2.6. .. 2.0.2.1. .1.2.:.1.6.:.2.1.....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. .. M.a.r. .. 2.6. .. 2.0.2.1. .1.2.:.1.6.:.2.1.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.625638741868008

General

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:	aEdlObiYav.exe
File size:	516346
MD5:	ae03a6f8fb74d401b403647d28e21574
SHA1:	6ee320cedc77499f5df9ae9c93ef42c0d91f3ce8
SHA256:	1ad1ff05930f27ef4b349c7a612235d1632ef7ceaa1a17adf7c7b3a97b40ca4d
SHA512:	ab2a30d32722419c72808032ae01b9443bfb8ea80ec52426aeb42ac21a84f0a2b04dd6f311c13b06bcaa37b7874b4e311ff8dc0c94ccfa42cbf6dcac0e2facab
SSDEEP:	6144:PebeJq15KNVIjux9tE9dVyAhwoajYPNo4ahRFPhpxOtYS0xefNPf+R6axxVccVPo:W5KNgux9t0VyAShUPCRdUi8cVRPw17i
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*1..Db..Db..Dbd..b..Db..]b..Db...b..Db..Kb..Db...ba.Db..cb..Dbd..b..Db..Eb..Db..$b..Db...b..Db...b..Db...b..DbRich..Db.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x419b95
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:	0x5D9A0326 [Sun Oct 6 15:07:18 2019 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:	92bdfd5dfdc574760c27f87d6f10fe98

Entrypoint Preview

Instruction
push 00000060h
push 0045C7A8h
call 00007FD794FDE160h
mov edi, 00000094h
mov eax, edi
call 00007FD794FDE2B8h
mov dword ptr [ebp-18h], esp
mov esi, esp
mov dword ptr [esi], edi
push esi
call dword ptr [004552A0h]
mov ecx, dword ptr [esi+10h]

Instruction
mov dword ptr [0047B960h], ecx
mov eax, dword ptr [esi+04h]
mov dword ptr [0047B96Ch], eax
mov edx, dword ptr [esi+08h]
mov dword ptr [0047B970h], edx
mov esi, dword ptr [esi+0Ch]
and esi, 00007FFFh
mov dword ptr [0047B964h], esi
cmp ecx, 02h
je 00007FD794FDEACEh
or esi, 00008000h
mov dword ptr [0047B964h], esi
shl eax, 08h
add eax, edx
mov dword ptr [0047B968h], eax
xor esi, esi
push esi
mov edi, dword ptr [00455320h]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007FD794FDEAE1h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
cmp dword ptr [ecx], 00004550h
jne 00007FD794FDEAD4h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007FD794FDEAE1h
cmp eax, 0000020Bh
je 00007FD794FDEAC7h
mov dword ptr [ebp-1Ch], esi
jmp 00007FD794FDEAE9h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007FD794FDEAB4h
xor eax, eax
cmp dword ptr [ecx+000000F8h], esi
jmp 00007FD794FDEAD0h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007FD794FDEAA4h
xor eax, eax
cmp dword ptr [ecx+000000E8h], esi
setne al
mov dword ptr [ebp-1Ch], eax

Rich Headers

Programming Language:	• [ASM] VS2003 (.NET) build 3077 • [LNK] VS2003 (.NET) build 3077 • [RES] VS2003 (.NET) build 3077 • [EXP] VS2003 (.NET) build 3077 • [C++] VS2003 (.NET) build 3077 • [C] VS2003 (.NET) build 3077

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x68cf0	0x53	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x66224	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x3ebc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x55880	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x60ed0	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x55000	0x878	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x66174	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x53ee9	0x54000	False	0.505048479353	DOS executable (COM)	6.50788658927	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x55000	0x13d43	0x14000	False	0.315026855469	data	5.20395932053	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x69000	0x14234	0x11000	False	0.795568129596	data	7.54511629913	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x3ebc	0x4000	False	0.259643554688	data	3.45842321085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7eb68	0x134	data	English	United States
RT_CURSOR	0x7ec9c	0xb4	data	English	United States
RT_CURSOR	0x7ed50	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7ee84	0x134	data	English	United States
RT_CURSOR	0x7efb8	0x134	data	English	United States
RT_CURSOR	0x7f0ec	0x134	data	English	United States
RT_CURSOR	0x7f220	0x134	data	English	United States
RT_CURSOR	0x7f354	0x134	data	English	United States
RT_CURSOR	0x7f488	0x134	data	English	United States
RT_CURSOR	0x7f5bc	0x134	data	English	United States
RT_CURSOR	0x7f6f0	0x134	data	English	United States
RT_CURSOR	0x7f824	0x134	data	English	United States
RT_CURSOR	0x7f958	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7fa8c	0x134	data	English	United States
RT_CURSOR	0x7fbc0	0x134	data	English	United States
RT_CURSOR	0x7fcf4	0x134	data	English	United States
RT_BITMAP	0x7fe28	0xb8	data	English	United States
RT_BITMAP	0x7fee0	0x144	data	English	United States
RT_DIALOG	0x80024	0x184	data	English	United States
RT_DIALOG	0x801a8	0xf4	data	English	United States
RT_DIALOG	0x8029c	0x100	data	English	United States
RT_DIALOG	0x8039c	0xe8	data	English	United States
RT_STRING	0x80484	0x44	data	English	United States
RT_STRING	0x804c8	0x48	data	English	United States
RT_STRING	0x80510	0x2c	data	English	United States
RT_STRING	0x8053c	0x38	data	English	United States
RT_STRING	0x80574	0x48	data	English	United States
RT_STRING	0x805bc	0x64	data	English	United States
RT_STRING	0x80620	0x46	data	English	United States
RT_STRING	0x80668	0x82	data	English	United States
RT_STRING	0x806ec	0x2a	data	English	United States
RT_STRING	0x80718	0x192	data	English	United States
RT_STRING	0x808ac	0x4e2	data	English	United States
RT_STRING	0x80d90	0x31a	data	English	United States
RT_STRING	0x810ac	0x2dc	data	English	United States
RT_STRING	0x81388	0x8a	data	English	United States
RT_STRING	0x81414	0xac	data	English	United States
RT_STRING	0x814c0	0xde	data	English	United States
RT_STRING	0x815a0	0x4c4	data	English	United States
RT_STRING	0x81a64	0x264	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x81cc8	0x2c	data	English	United States
RT_STRING	0x81cf4	0x42	data	English	United States
RT_STRING	0x81d38	0x48	data	English	United States
RT_GROUP_CURSOR	0x81d80	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x81da4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81db8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81dcc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81de0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81df4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e08	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e1c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e30	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e44	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e58	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e6c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e80	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e94	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81ea8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States

Imports

DLL	Import
CRYPT32.dll	CertOpenStore
KERNEL32.dll	GetStartupInfoA, GetCommandLineA, ExitProcess, HeapReAlloc, TerminateProcess, ExitThread, CreateThread, HeapSize, FatalAppExitA, HeapDestroy, HeapCreate, VirtualFree, IsBadWritePtr, GetStdHandle, UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, IsValidCodePage, SetConsoleCtrlHandler, RtlUnwind, GetLocaleInfoW, SetEnvironmentVariableA, InterlockedExchange, GetACP, GetLocaleInfoA, GetThreadLocale, GetVersionExA, MultiByteToWideChar, WideCharToMultiByte, GetLastError, GetVersion, lstrcmpiA, lstrlenW, lstrcmpiW, lstrlenA, CompareStringA, CompareStringW, GetEnvironmentVariableA, GetEnvironmentVariableW, GetStringTypeExA, GetStringTypeExW, SizeofResource, LockResource, LoadResource, FindResourceA, FreeResource, GlobalFree, GlobalUnlock, GlobalLock, LocalFree, lstrcpynA, FormatMessageA, GlobalAlloc, GlobalSize, MulDiv, CopyFileA, SetLastError, GetProcAddress, GetModuleHandleA, lstrcmpW, VirtualQuery, GetSystemInfo, VirtualAlloc, VirtualProtect, HeapFree, HeapAlloc, GetDiskFreeSpaceA, GetTempFileNameA, LocalLock, LocalUnlock, GetFileTime, GetFileAttributesA, SetFileAttributesA, SetFileTime, LocalFileTimeToFileTime, FileTimeToLocalFileTime, SetErrorMode, GetShortPathNameA, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, DeleteFileA, MoveFileA, GetCurrentDirectoryA, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, SystemTimeToFileTime, FileTimeToSystemTime, GetOEMCP, GetCPInfo, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, InterlockedIncrement, GlobalFlags, DeleteCriticalSection, InitializeCriticalSection, RaiseException, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, lstrcmpA, GetModuleFileNameA, lstrcatA, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, InterlockedDecrement, GetCurrentThreadId, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, GlobalDeleteAtom, LoadLibraryA, FreeLibrary, SetStdHandle

DLL	Import
USER32.dll	IsClipboardFormatAvailable, MessageBeep, GetTabbedTextExtentA, GetDCEx, LockWindowUpdate, SetParent, InvalidateRect, InsertMenuItemA, CreatePopupMenu, SetRectEmpty, BringWindowToTop, SetMenu, TranslateAcceleratorA, DestroyIcon, DeleteMenu, wsprintfA, WaitMessage, GetWindowThreadProcessId, ReleaseCapture, WindowFromPoint, SetCapture, LoadCursorA, GetSysColorBrush, GetDialogBaseUnits, GetMessageA, TranslateMessage, GetCursorPos, ValidateRect, ShowOwnedPopups, SetCursor, PostQuitMessage, EndPaint, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, FillRect, DestroyMenu, GetMenuItemInfoA, InflateRect, SetMenuItemBitmaps, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, ScrollWindowEx, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, IsDlgButtonChecked, SetDlgItemInt, GetDlgItemTextA, GetDlgItemInt, CheckRadioButton, CheckDlgButton, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, SetWindowsHookExA, CallNextHookEx, KillTimer, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, GetFocus, SetFocus, IsChild, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, GetLastActivePopup, DispatchMessageA, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, PeekMessageA, MapWindowPoints, ScrollWindow, MessageBoxA, TrackPopupMenuEx, TrackPopupMenu, GetKeyState, SetScrollRange, SetDlgItemTextA, CharLowerA, CharLowerW, CharUpperA, CharUpperW, SendMessageA, EnableWindow, DrawIcon, AppendMenuA, GetSystemMenu, IsIconic, GetClientRect, SetActiveWindow, LoadIconA, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, IsWindowVisible, UpdateWindow, GetMenu, PostMessageA, GetSysColor, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, GetScrollInfo, SetScrollInfo, SetTimer, SetRect, UnionRect, IsRectEmpty, MapVirtualKeyA, GetClassInfoA, RegisterClassA, UnregisterClassA, SetWindowPlacement, GetDlgCtrlID, DefWindowProcA, SetWindowLongA, SetWindowPos, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetKeyNameTextA, LoadMenuA, UnpackDDElParam, ReuseDDElParam, GetClassLongA, LoadAcceleratorsA, CallWindowProcA, LoadStringW, GetSystemMetrics, EndDialog, GetNextDlgTabItem, GetParent, IsWindowEnabled, GetDlgItem, GetWindowLongA, IsWindow, DestroyWindow, CreateDialogIndirectParamA, GetActiveWindow, GetDesktopWindow, RemoveMenu, GetSubMenu, GetMenuItemCount, InsertMenuA, GetWindowRect, CopyRect, PtInRect, GetWindow, GetMenuState, GetMenuStringA, GetMenuItemID
GDI32.dll	SetMapperFlags, SetArcDirection, SetColorAdjustment, DeleteObject, SelectClipRgn, GetClipRgn, CreateRectRgn, SelectClipPath, GetViewportExtEx, GetWindowExtEx, GetPixel, StartDocA, PtVisible, RectVisible, TextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, OffsetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, GetCurrentPositionEx, ArcTo, PolyDraw, PolylineTo, PolyBezierTo, SetTextCharacterExtra, DeleteDC, CreateDIBPatternBrushPt, CreatePatternBrush, GetStockObject, SelectPalette, PlayMetaFileRecord, GetObjectType, EnumMetaFile, PlayMetaFile, CreatePen, ExtCreatePen, CreateSolidBrush, CreateHatchBrush, GetTextMetricsA, CreateRectRgnIndirect, SetRectRgn, CombineRgn, GetMapMode, PatBlt, DPtoLP, CreateCompatibleBitmap, StretchDIBits, GetCharWidthA, CreateFontA, GetBkColor, StartPage, EndPage, SetAbortProc, AbortDoc, EndDoc, SetTextJustification, SetTextAlign, MoveToEx, LineTo, OffsetClipRgn, IntersectClipRect, ExcludeClipRect, SetMapMode, SetStretchBltMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, GetTextExtentPoint32A, ExtTextOutA, BitBlt, CreateCompatibleDC, CreateFontIndirectA, CreateBitmap, GetObjectA, SetBkColor, SetTextColor, GetClipBox, GetDCOrgEx, CreateDCA, CopyMetaFileA, ExtSelectClipRgn, GetDeviceCaps
comdlg32.dll	PageSetupDlgA, FindTextA, ReplaceTextA, GetOpenFileNameA, CommDlgExtendedError, PrintDlgA, GetFileTitleA, GetSaveFileNameA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter, GetJobA
ADVAPI32.dll	GetFileSecurityA, RegCloseKey, RegSetValueA, RegOpenKeyA, RegQueryValueExA, RegOpenKeyExA, RegDeleteKeyA, RegEnumKeyA, RegQueryValueA, RegCreateKeyExA, RegSetValueExA, RegDeleteValueA, RegCreateKeyA, SetFileSecurityW, SetFileSecurityA
SHELL32.dll	SHGetFileInfoA, DragFinish, DragQueryFileA, ExtractIconA
COMCTL32.dll	ImageList_Draw, ImageList_GetImageInfo, ImageList_Read, ImageList_Write, ImageList_Destroy, ImageList_Create, ImageList_LoadImageA, ImageList_Merge
SHLWAPI.dll	PathRemoveExtensionA, PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
ole32.dll	WriteClassStg, OleRegGetUserType, SetConvertStg, CoTaskMemFree, ReadFmtUserTypeStg, ReadClassStg, StringFromCLSID, CoTreatAsClass, CreateBindCtx, CoTaskMemAlloc, ReleaseStgMedium, OleDuplicateData, CoDisconnectObject, CoCreateInstance, StringFromGUID2, CLSIDFromString, WriteFmtUserTypeStg
OLEAUT32.dll	VariantClear, VariantChangeType, VariantInit, SysAllocStringLen, SysFreeString, SysStringLen, SysAllocStringByteLen, SysStringByteLen, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayGetElemsize, SafeArrayGetDim, SafeArrayCreate, SafeArrayRedim, VariantCopy, SafeArrayAllocData, SafeArrayAllocDescriptor, SafeArrayCopy, SafeArrayGetElement, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayLock, SafeArrayUnlock, SafeArrayDestroy, SafeArrayDestroyData, SafeArrayDestroyDescriptor, VariantTimeToSystemTime, SystemTimeToVariantTime, SysAllocString, SysReAllocStringLen, VarDateFromStr, VarBstrFromDec, VarDecFromStr, VarCyFromStr, VarBstrFromCy, VarBstrFromDate

Exports

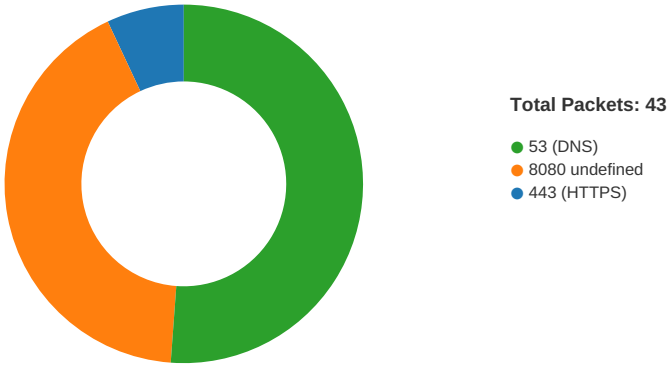
Name	Ordinal	Address
mcfGvgupamvngNBNmgO	1	0x401e04

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2021 12:15:13.856343985 CET	49714	443	192.168.2.5	45.33.54.74
Mar 26, 2021 12:15:14.022622108 CET	443	49714	45.33.54.74	192.168.2.5
Mar 26, 2021 12:15:14.533005953 CET	49714	443	192.168.2.5	45.33.54.74
Mar 26, 2021 12:15:14.699125051 CET	443	49714	45.33.54.74	192.168.2.5
Mar 26, 2021 12:15:15.204783916 CET	49714	443	192.168.2.5	45.33.54.74
Mar 26, 2021 12:15:15.372411013 CET	443	49714	45.33.54.74	192.168.2.5
Mar 26, 2021 12:15:19.258178949 CET	49717	8080	192.168.2.5	209.141.41.136
Mar 26, 2021 12:15:22.257272959 CET	49717	8080	192.168.2.5	209.141.41.136
Mar 26, 2021 12:15:28.364118099 CET	49717	8080	192.168.2.5	209.141.41.136
Mar 26, 2021 12:15:45.480190039 CET	49726	8080	192.168.2.5	104.236.246.93
Mar 26, 2021 12:15:48.662617922 CET	49726	8080	192.168.2.5	104.236.246.93
Mar 26, 2021 12:15:54.663077116 CET	49726	8080	192.168.2.5	104.236.246.93
Mar 26, 2021 12:16:10.887083054 CET	49727	8080	192.168.2.5	198.199.114.69
Mar 26, 2021 12:16:13.883450985 CET	49727	8080	192.168.2.5	198.199.114.69
Mar 26, 2021 12:16:19.883981943 CET	49727	8080	192.168.2.5	198.199.114.69
Mar 26, 2021 12:16:37.280674934 CET	49730	8080	192.168.2.5	152.89.236.214
Mar 26, 2021 12:16:37.298701048 CET	8080	49730	152.89.236.214	192.168.2.5
Mar 26, 2021 12:16:37.808387041 CET	49730	8080	192.168.2.5	152.89.236.214
Mar 26, 2021 12:16:37.826337099 CET	8080	49730	152.89.236.214	192.168.2.5
Mar 26, 2021 12:16:38.338735104 CET	49730	8080	192.168.2.5	152.89.236.214
Mar 26, 2021 12:16:38.357024908 CET	8080	49730	152.89.236.214	192.168.2.5
Mar 26, 2021 12:16:44.243448973 CET	49731	8080	192.168.2.5	87.106.136.232
Mar 26, 2021 12:16:44.263411045 CET	8080	49731	87.106.136.232	192.168.2.5
Mar 26, 2021 12:16:44.776601076 CET	49731	8080	192.168.2.5	87.106.136.232
Mar 26, 2021 12:16:44.796765089 CET	8080	49731	87.106.136.232	192.168.2.5
Mar 26, 2021 12:16:45.307971954 CET	49731	8080	192.168.2.5	87.106.136.232
Mar 26, 2021 12:16:45.328773975 CET	8080	49731	87.106.136.232	192.168.2.5
Mar 26, 2021 12:16:49.226500034 CET	49732	8080	192.168.2.5	178.210.51.222
Mar 26, 2021 12:16:52.230490923 CET	49732	8080	192.168.2.5	178.210.51.222
Mar 26, 2021 12:16:58.230922937 CET	49732	8080	192.168.2.5	178.210.51.222

UDP Packets

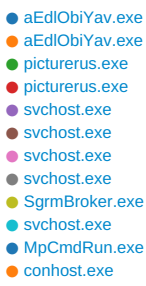
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2021 12:14:41.512866974 CET	54302	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:41.525654078 CET	53	54302	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:41.585858107 CET	53784	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:41.598005056 CET	53	53784	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:41.610990047 CET	65307	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:41.615739107 CET	64344	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 26, 2021 12:14:41.623008013 CET	53	65307	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:41.627897024 CET	53	64344	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:42.167435884 CET	62060	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:42.180625916 CET	53	62060	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:43.448725939 CET	61805	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:43.461241007 CET	53	61805	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:44.423804998 CET	54795	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:44.436858892 CET	53	54795	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:45.104419947 CET	49557	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:45.117428064 CET	53	49557	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:46.996332884 CET	61733	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:47.010894060 CET	53	61733	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:48.214711905 CET	65447	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:48.228995085 CET	53	65447	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:49.268984079 CET	52441	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:49.283057928 CET	53	52441	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:50.040528059 CET	62176	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:50.053486109 CET	53	62176	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:51.121691942 CET	59596	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:51.135163069 CET	53	59596	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:51.804497004 CET	65296	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:51.819228888 CET	53	65296	8.8.8.8	192.168.2.5
Mar 26, 2021 12:14:53.942034006 CET	63183	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:14:53.955611944 CET	53	63183	8.8.8.8	192.168.2.5
Mar 26, 2021 12:15:09.783927917 CET	60151	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:15:09.802167892 CET	53	60151	8.8.8.8	192.168.2.5
Mar 26, 2021 12:15:17.823621988 CET	56969	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:15:17.836400986 CET	53	56969	8.8.8.8	192.168.2.5
Mar 26, 2021 12:15:37.598907948 CET	55161	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:15:37.611623049 CET	53	55161	8.8.8.8	192.168.2.5
Mar 26, 2021 12:15:39.159313917 CET	54757	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:15:39.192080975 CET	53	54757	8.8.8.8	192.168.2.5
Mar 26, 2021 12:15:44.632929087 CET	49992	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:15:44.651496887 CET	53	49992	8.8.8.8	192.168.2.5
Mar 26, 2021 12:16:18.667603016 CET	60075	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:16:18.680677891 CET	53	60075	8.8.8.8	192.168.2.5
Mar 26, 2021 12:16:18.968331099 CET	55016	53	192.168.2.5	8.8.8.8
Mar 26, 2021 12:16:19.002011061 CET	53	55016	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: aEdlObiYav.exe PID: 5064 Parent PID: 5764

General

Start time:	12:14:48
Start date:	26/03/2021
Path:	C:\Users\user\Desktop\aEdlObiYav.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\aEdlObiYav.exe'
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
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: 00000000.00000002.221393603.00000000022C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.221393603.00000000022C0000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.221405204.00000000022D1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.221405204.00000000022D1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: aEdlObiYav.exe PID: 5528 Parent PID: 5064

General

Start time:	12:14:48
Start date:	26/03/2021
Path:	C:\Users\user\Desktop\aEdlObiYav.exe
Wow64 process (32bit):	true

Commandline:	--79fd8b32
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
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: 00000001.00000002.241329316.0000000002180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.241329316.0000000002180000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.241344979.0000000002191000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.241344979.0000000002191000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\picturerus.exe:Zone.Identifier	success or wait	1	2191126	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: picturerus.exe PID: 6084 Parent PID: 556

General

Start time:	12:14:57
Start date:	26/03/2021
Path:	C:\Windows\SysWOW64\picturerus.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\picturerus.exe
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.240281211.0000000000E21000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.240281211.0000000000E21000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.240268046.0000000000E10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000003.00000002.240268046.0000000000E10000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: picturerus.exe PID: 4228 Parent PID: 6084

General

Start time:	12:14:57
Start date:	26/03/2021
Path:	C:\Windows\SysWOW64\picturerus.exe
Wow64 process (32bit):	true
Commandline:	--b743c2a4
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
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: 00000004.00000002.488250881.0000000000ED1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000004.00000002.488250881.0000000000ED1000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.487903177.0000000000600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000004.00000002.487903177.0000000000600000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	ED14A5	HttpSendRequestW

Analysis Process: svchost.exe PID: 5536 Parent PID: 556

General

Start time:	12:15:06
Start date:	26/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2376 Parent PID: 556

General

Start time:	12:15:16
Start date:	26/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4504 Parent PID: 556

General

Start time:	12:15:17
Start date:	26/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 804 Parent PID: 556

General

Start time:	12:15:17
Start date:	26/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 1228 Parent PID: 556

General

Start time:	12:15:18
Start date:	26/03/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff744c80000
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: 5540 Parent PID: 556

General

Start time:	12:15:18
Start date:	26/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: MpCmdRun.exe PID: 5048 Parent PID: 5540

General

Start time:	12:16:20
Start date:	26/03/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff668430000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF66845BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 4d 00 61 00 72 00 20 00 0e 20 32 00 36 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 32 00 3a 00 31 00 36 00 3a 00 32 00 31 00 0d 00 0a 00 0d	M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. ."C.:\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m. p.c.m.d.r.u.n...e.x.e.". .-.w. d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. F.r.i. .. M.a.r. .. 2.6. .. 2.0.2.1. .1.2.:. 1.6.:.2.1.....	success or wait	1	7FF66845BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....	success or wait	1	7FF66845BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	W.D.E.n.a.b.l.e.....	success or wait	1	7FF66845BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e. (.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....	success or wait	1	7FF66845BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 46 00 72 00 69 00 20 00 0e 20 4d 00 61 00 72 00 20 00 0e 20 32 00 36 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 32 00 3a 00 31 00 36 00 3a 00 32 00 31 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. F.r.i. .. M.a.r. .. 2.6. .. 2.0.2.1. .1.2.:.1.6. :.2.1.....	success or wait	1	7FF66845BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.....	success or wait	1	7FF66845BC96	WriteFile

Analysis Process: conhost.exe PID: 3896 Parent PID: 5048

General

Start time:	12:16:21
Start date:	26/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis