ID: 386506
Sample Name: vEjGZyD0iN
Cookbook: default.jbs
Time: 11:42:13
Date: 14/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report vEjGZyD0iN 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
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
Contacted URLs 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 12
IPs 12
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18

Rich Headers 19
Data Directories 19
Sections 20
Imports 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 20
UDP Packets 21
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 23
Analysis Process: vEjGZyD0iN.exe PID: 5832 Parent PID: 5604 23
General 23
Analysis Process: vEjGZyD0iN.exe PID: 5720 Parent PID: 5832 23
General 23
File Activities 24
File Deleted 24
Analysis Process: svchost.exe PID: 6028 Parent PID: 568 24
General 24
File Activities 24
Analysis Process: appsys.exe PID: 4716 Parent PID: 568 24
General 24
Analysis Process: appsys.exe PID: 1020 Parent PID: 4716 25
General 25
File Activities 25
File Created 25
Analysis Process: svchost.exe PID: 5492 Parent PID: 568 26
General 26
File Activities 26
Registry Activities 27
Analysis Process: svchost.exe PID: 2436 Parent PID: 568 27
General 27
File Activities 27
Analysis Process: svchost.exe PID: 6404 Parent PID: 568 27
General 27
Analysis Process: svchost.exe PID: 6464 Parent PID: 568 27
General 27
File Activities 28
Analysis Process: svchost.exe PID: 6472 Parent PID: 568 28
General 28
File Activities 28
Analysis Process: svchost.exe PID: 6556 Parent PID: 568 28
General 28
Registry Activities 29
Analysis Process: svchost.exe PID: 6640 Parent PID: 568 29
General 29
Analysis Process: SgrmBroker.exe PID: 6696 Parent PID: 568 29
General 29
Analysis Process: svchost.exe PID: 6732 Parent PID: 568 29
General 29
Registry Activities 29
Analysis Process: svchost.exe PID: 6784 Parent PID: 568 30
General 30
File Activities 30
Analysis Process: MpCmdRun.exe PID: 5384 Parent PID: 6732 30
General 30
File Activities 30
File Written 30
Analysis Process: conhost.exe PID: 3596 Parent PID: 5384 32
General 32
Disassembly 32
Code Analysis 33

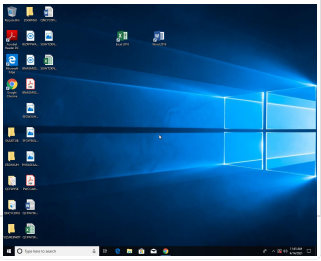
Analysis Report vEjGZyD0iN

Overview

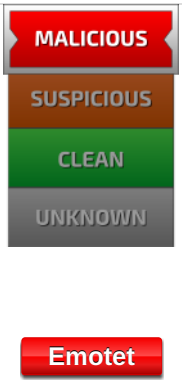
General Information

Sample Name:	vEjGZyD0iN (renamed file extension from none to exe)
Analysis ID:	386506
MD5:	ecbc4b40dcfec4e..
SHA1:	e08eb07c69d8fc8..
SHA256:	878d5137e0c9a0..
Infos:	

Most interesting Screenshot:



Detection

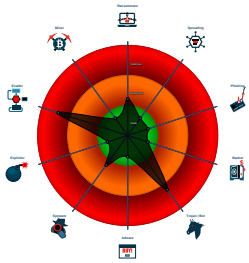


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- 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…
- Checks if Antivirus/Antispyware/Fire…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- vEjGZyD0iN.exe (PID: 5832 cmdline: 'C:\Users\user\Desktop\vEjGZyD0iN.exe' MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - vEjGZyD0iN.exe (PID: 5720 cmdline: C:\Users\user\Desktop\vEjGZyD0iN.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 6028 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- appsys.exe (PID: 4716 cmdline: C:\Windows\SysWOW64\appsys.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - appsys.exe (PID: 1020 cmdline: C:\Windows\SysWOW64\appsys.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 5492 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2436 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6404 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6464 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6472 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6556 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6640 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6696 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6732 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5384 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: 6784 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
vEjGZyD0iN.exe	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
vEjGZyD0iN.exe	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 40 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 40 00 85 C0

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.202803332.00000000013E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000000.203553485.00000000013E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000005.00000002.464331526.00000000013E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000000.197038659.00000000013E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.197424310.00000000013E1000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

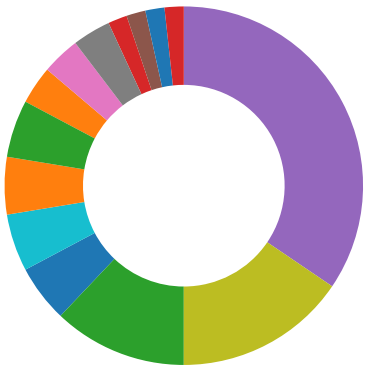
Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.appsys.exe.13e0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.0.appsys.exe.13e0000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 3E 01 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 3E 01 85 C0
1.0.vEjGZyD0iN.exe.13e0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.0.vEjGZyD0iN.exe.13e0000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 3E 01 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 3E 01 85 C0
4.0.appsys.exe.13e0000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

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:

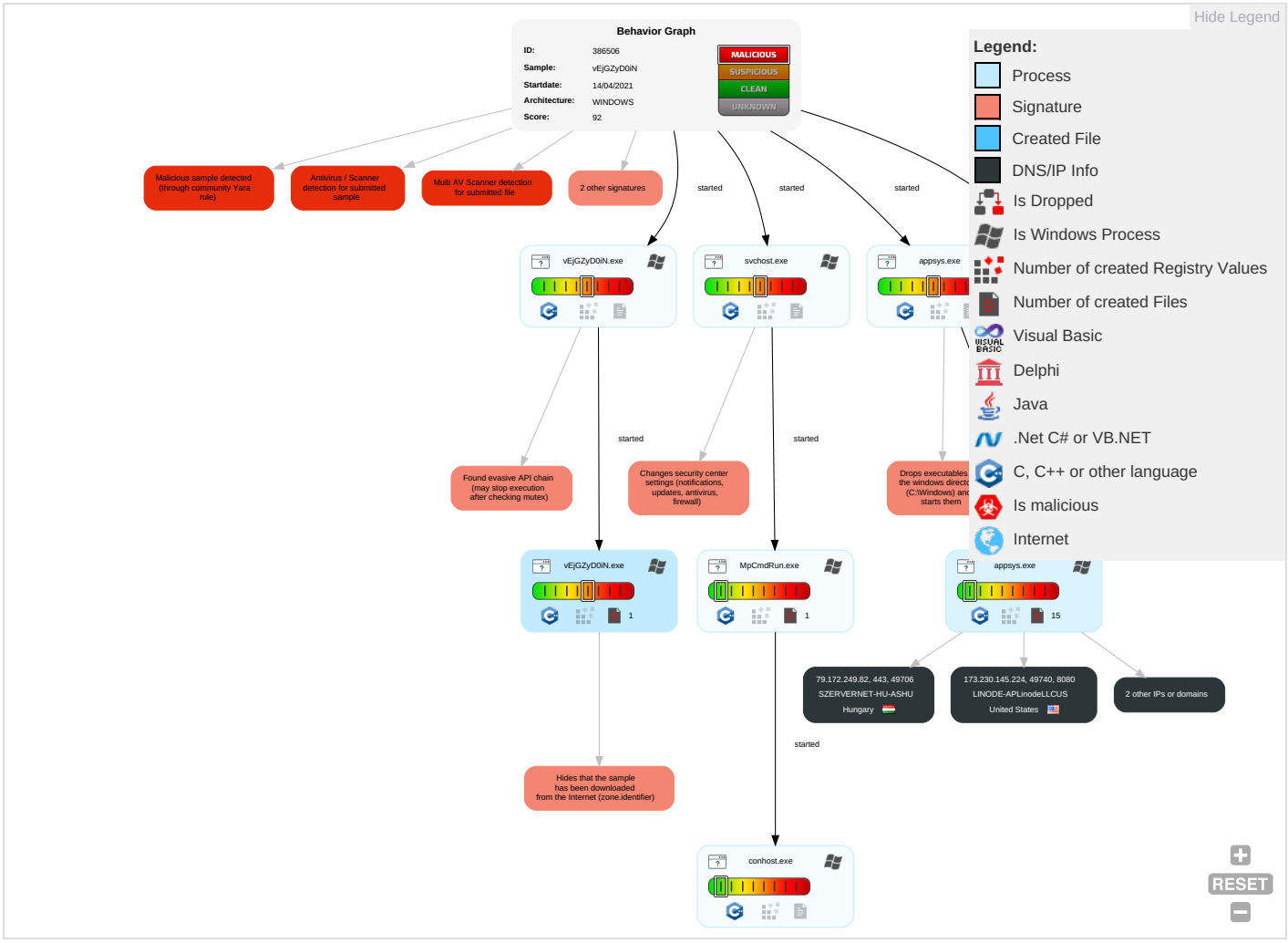
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Process Injection 2	Masquerading 1 2 1	OS Credential Dumping	Security Software Discovery 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

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
vEjGZyD0iN.exe	83%	Virustotal		Browse
vEjGZyD0iN.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
vEjGZyD0iN.exe	100%	Avira	TR/Crypt.XPACK.Gen	
vEjGZyD0iN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.appsys.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.vEjGZyD0iN.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.appsys.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.vEjGZyD0iN.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.vEjGZyD0iN.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.appsys.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.appsys.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.vEjGZyD0iN.exe.13e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://79.172.249.82:443/	3%	Virustotal		Browse
http://https://79.172.249.82:443/	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://%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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://79.172.249.82:443/	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000003.308982437.000001373AA56000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000010.00000002.309324516.000001373AA3C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000010.00000002.309324516.000001373AA3C000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000010.00000003.308939016.000001373AA47000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000010.00000002.309324516.000001373AA3C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000010.00000003.287205564.000001373AA30000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000003.308982437.000001373AA56000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp, svchost.exe, 00000010.00000003.308987811.000001373AA40000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000002.309305639.000001373AA24000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.309324516.000001373AA3C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000010.00000002.309331281.000001373AA42000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000D.00000002.463987902.00000208D3C2A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000003.287205564.000001373AA30000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000010.00000003.287205564.000001373AA30000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000008.00000002.470619802.00000282CCC70000.00000002.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000010.00000003.287205564.000001373AA30000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000010.00000002.309331281.000001373AA42000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000010.00000003.308920104.000001373AA62000.00000004.00000001.sdmp, svchost.exe, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000010.00000003.287205564.000001373AA30000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000D.00000002.463987902.00000208D3C2A000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000010.00000002.309305639.000001373AA24000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000010.00000003.308929719.000001373AA5F000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000002.309324516.000001373AA3C000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000D.00000002.463987902.00000208D3C2A000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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, 00000010.00000003.308958861.000001373AA5A000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.169.54.12	unknown	Germany		49464	ICFSYSTEMSDE	false
80.86.91.232	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
173.230.145.224	unknown	United States		63949	LINODE-APLinodeLLCUS	false
79.172.249.82	unknown	Hungary		43711	SZERVERNET-HU-ASHU	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	386506
Start date:	14.04.2021
Start time:	11:42:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vEjGZyD0iN (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:	28
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:	mal92.troj.evad.winEXE@20/8@0/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.3% (good quality ratio 38.7%) • Quality average: 79% • Quality standard deviation: 30.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 93.184.220.29, 92.122.145.220, 13.88.21.125, 104.42.151.234, 13.64.90.137, 20.50.102.62, 52.255.188.83, 104.76.200.56, 23.32.238.177, 23.32.238.234, 20.54.26.129, 52.147.198.201, 20.82.210.154, 104.43.193.48, 20.82.209.183 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:43:27	API Interceptor	2x Sleep call for process: svchost.exe modified
11:44:43	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
193.169.54.12	_01_.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	hEHN0WzBF.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://baseballpontedipiave.com/Sales-Invoice/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	emotet2.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://www.yourhabitchangecoach.co.uk/wp-content/Overdue-payment/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	RDuYHvb2jQ.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://okomekai.symphonic-net.com/Invoice-69070770/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	mail.rodolfogvalencia.com/Invoice/	Get hash	malicious	Browse	• 193.169.54.12:8080/
80.86.91.232	Invoice.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Overdue payment.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Emote.exe	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Question.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	960-27-621120-257 & 960-27-621120-969.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Rechnung.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Open invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 80.86.91.232:7080/
	Scan1782384.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	malware.exe	Get hash	malicious	Browse	• 80.86.91.232
	zeD11Fztx8.exe	Get hash	malicious	Browse	• 80.86.91.232
	TRS-11-0221-020.exe	Get hash	malicious	Browse	• 85.25.177.199
	Payment Advice.exe	Get hash	malicious	Browse	• 85.25.177.199
	VMtEguRH.exe	Get hash	malicious	Browse	• 85.25.177.199
	Reports-018315.xlsm	Get hash	malicious	Browse	• 185.21.102.197
	Reports-018315.xlsm	Get hash	malicious	Browse	• 185.21.102.197
	D12547698.VBS	Get hash	malicious	Browse	• 85.25.93.141
	sample.exe.exe	Get hash	malicious	Browse	• 80.86.91.232
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 217.172.179.54
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 217.172.179.54
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 80.86.91.232
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 85.25.43.31
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 217.172.179.54
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 217.172.179.54
	csrss.bin.exe	Get hash	malicious	Browse	• 188.138.33.233
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 92.51.129.66
	E00636067E.exe	Get hash	malicious	Browse	• 85.25.177.199
ICFSYSTEMSDE	malware.exe	Get hash	malicious	Browse	• 193.169.54.12
	zeD11Fztx8.exe	Get hash	malicious	Browse	• 193.169.54.12
	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 193.169.54.12
	sample.exe.exe	Get hash	malicious	Browse	• 193.169.54.12
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 193.169.54.12
	0HvIGwMmBV.exe	Get hash	malicious	Browse	• 193.169.54.12
	pitEBNziGR.exe	Get hash	malicious	Browse	• 193.169.54.12
	_01_.doc	Get hash	malicious	Browse	• 193.169.54.12
	hEHN0WzBF.exe	Get hash	malicious	Browse	• 193.169.54.12
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12
	http://baseballpontedipiave.com/Sales-Invoice/	Get hash	malicious	Browse	• 193.169.54.12
	emotet2.doc	Get hash	malicious	Browse	• 193.169.54.12
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 193.169.54.12
	http://www.yourhabitchangecoach.co.uk/wp-content/Overdue-payment/	Get hash	malicious	Browse	• 193.169.54.12
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 193.169.54.12
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12
LINODE-APLinodeLLCUS	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 139.162.60.124
	MTCC169.DLL	Get hash	malicious	Browse	• 176.58.123.25
	8ScpV1CK8c.exe	Get hash	malicious	Browse	• 104.200.22.130
	Swift copy.pdf.exe	Get hash	malicious	Browse	• 45.33.51.100
	malware.exe	Get hash	malicious	Browse	• 173.230.145.224
	zeD11Fztx8.exe	Get hash	malicious	Browse	• 173.230.145.224
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 45.56.127.45
	gunzipped.exe	Get hash	malicious	Browse	• 45.56.119.148

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	frox0cheats.exe	Get hash	malicious	Browse	• 176.58.123.25
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 172.104.164.58
	OfficeConsultPlugin.exe	Get hash	malicious	Browse	• 109.237.24.104
	RFQ#798606.exe	Get hash	malicious	Browse	• 45.56.119.148
	Private doc.docm	Get hash	malicious	Browse	• 109.237.24.104
	lK8vF3n2e7.exe	Get hash	malicious	Browse	• 172.104.23 3.225
	newordermx.exe	Get hash	malicious	Browse	• 45.33.2.79
	sample.exe	Get hash	malicious	Browse	• 66.228.32.51
	BnJvVt951o.exe	Get hash	malicious	Browse	• 45.33.54.74
	BnJvVt951o.exe	Get hash	malicious	Browse	• 45.33.54.74
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 45.33.54.74
	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 173.230.14 5.224

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):	0.5966085702512959
Encrypted:	false
SSDEEP:	6:0FIZ/llEk1GaD0JOCEfMuaaD0JOCEfMKQmD7Zb6Al/gz2cE0fMbhEZolrRSQ2hyy:0G7GaD0JcaaD0JwQQtb6Ag/0bjSQJ
MD5:	094363BE8F908743B9D630552596106A
SHA1:	7E42A69E811A96BD4433FA423CC9EB4FAF9E4B53
SHA-256:	E1B998036F4B81B95C07C1B9730C0975BEA65731925461784D574642640019F5
SHA-512:	95099CF3E65FC881C664630DA80B16EC635530374F2CF240313B70A42ABD4B0F9758830A316D5B3A6CC8B1F8EC77613F9E1390E16CEEBD6E16EB8BD192E1331
Malicious:	false
Preview:	.....:{..(.....+...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....+...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 0x7b4ae7aa, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09639948417965119
Encrypted:	false
SSDEEP:	12:A0+yPH+1O4bl4tUKu0+yPH+1O4bl4tUK:PR/XBR/X
MD5:	0EAC01569376E2645F4DF8DF2340B3A4
SHA1:	02EF7D1D5F5CB405DC5D2CD2202AC7025E3CF1DA
SHA-256:	BFC5636B87657FD87EE10F7A5D1C4E8AF12806F63646B537D765905BA7933FB1
SHA-512:	EEBBF117D9EC5847120A0E00B71B60F5B64AB13AB73136FFC53E3ABFD0DFA932541B4E105FEB29E960CAFEF73E382DA49F23CB25BC412D834CF26EFC931F83F4
Malicious:	false
Preview:	{J... .....e.f.3...w.....&.....w...+...y..h.(.....3...w.....B.....@..... ....3...w..... .....+...y.k.....gk...+...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11110880985443841
Encrypted:	false
SSDEEP:	3:fR/ll1Ev+OZAtjXl/bJdAtiy3rd/l/all:hY+OZI7t4d/lG
MD5:	1617F66803D745B33716215C9A171B8D
SHA1:	62518C2EB960F696A9345D2950A019666AB55373
SHA-256:	9D3ED0A872131F89ABC473795470ECF569E152EBF33EF2672DAF8994481CDCC4
SHA-512:	DD3BCBEE04D1538C574D868128B07838A8A2507FA4D954B01CB1C99754BE3B12DEAC79985F60207E02C38F0F027BB380FD9B9B08D597D2B95457F75E4C3DE01D
Malicious:	false
Preview:	A3.<.....3...w...+...y.....w.....w.....w....:O.....w.....gk...+...y..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.10966965674189857
Encrypted:	false
SSDEEP:	12:263nVXm/Ey6q9995ylo7q3qQ10nMCldimE8eawHjcr9d:26Il68cumLyMCldzE9BHjc7
MD5:	367176D1B03EDA499635A77652992C62
SHA1:	F21C3F0B53E19BD7F855AE028F8F083F7906F685
SHA-256:	F7428C6ED81FFD47F823ADE137CED1A883106E941FFE719BE4F90B9A332FC8BE
SHA-512:	DA1628222D4559E0E25C16BB9166ABDD02DB57E5803943B78DDCB071507A6670C4774AE8FCA09A6F78067B6046F97E02FE2AF4C114BF89CD4B4EF4C5DECD432
Malicious:	false
Preview:	.....t...H.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....D.,..... .....8.r.^1.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.t...H..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11229874950717302
Encrypted:	false
SSDEEP:	12:MjXm/Ey6q9995ylmg1miM3qQ10nMCldimE8eawHza1miIUP:pl68cIg1tMLyMCldzE9BHza1tIE
MD5:	6AC46745BD263853EDFB44184D077B8C
SHA1:	B336058F9A066FF4568CC0AA3FE7CBBAF1B62AE3
SHA-256:	D808089BB5EDCD104089D914F4EBAB58760D2AA77C538CE9685634028B962E49
SHA-512:	04B40D1F60F12EFB37D387C64C8285569304EF72658E5EA2E3C1BCC609F1B2D9F549C276F9D253C584DE45FAD1CF06BBAAE28207F6AC722804883720F753633E
Malicious:	false
Preview:	.....t...H.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....D.,..... .....%\k.^1.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.t...H..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11221285522965302
Encrypted:	false
SSDEEP:	12:RXm/Ey6q9995ylWw1mK2P3qQ10nMCldimE8eawHza1mKQ3:8l68csw1iPLyMCldzE9BHza1M3
MD5:	C33A8B92D82C1AB19C77E4FDA91D4E4E

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
SHA1:	EA6B58BDA7213552E6E498485BFA5037CEB6A313
SHA-256:	D3D74C5F92335FED1FB0CDA58AFCA7037EBE8D79AD5193C0506FBA814E900738
SHA-512:	DEDDD80E121A8F5CEAA4015D545F3F976BF44A9CA3660B91C156095E99CBF95CB19B677E65C54FD332DC905216F7DC4C0BEF3655A190C3CC608D1627C20DE3 E
Malicious:	false
Preview:	....t...H....1......................B.............Zb...@.t.z.r.e.s...d.l.l.,.-.2.1.2... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1..D..,..... ....].^1.........U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.......P.P.t...H....=.. ....

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):	3.1400697254635244
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rlsEyDk9+MlWlLehB4yAq7ejCEsEyO:OaqdmuF3rlf+kWReH4yJ7MNF
MD5:	BC98B2BC99B1D5F7CCF1335AF993C93B
SHA1:	1FA3E74D1407EE96634F598B0BDD372612BE2EA1
SHA-256:	7AF2E620931016CAD14F887BB12CCDAD0B8EB15D0B278772C459C23F6B29B50C
SHA-512:	2FA1ADF6FA1F277C01B72E6B29C964B5F56A1AD75421F3539604D3412A819F514EDBB4AE1B3AFCD4B450D0E83B53B94A61F8BCF4323FB8379D6FE71AC1C43B1 9
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.:. .. W.e.d. .. A.p.r. .. 1.4. .. 2.0.2.1. .1.1.:.4.4.:.4. 3.........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.:. .. W.e.d. .. A.p.r. .. 1.4. .. 2.0.2.1. .1.1.:.4.4.:.4.3.....- .-.....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.436116781781946
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:	vEjGZyD0iN.exe
File size:	45568
MD5:	ecbc4b40dcfec4ed1b2647b217da0441
SHA1:	e08eb07c69d8fc8e75927597767288a21d6ed7f6
SHA256:	878d5137e0c9a072c83c596b4e80f2aa52a8580ef214e5b a0d59daa5036a92f8

General

SHA512:	3ec4de3f35e10c874916a6402004e3b9fc60b5a026d2010ede992b592fe396db2bee0b225ab5f2fb85561f687a8abf0c9e7c8b3cf0344c384c80297278be7b5
SSDEEP:	768:uhBY2Tumxi0mv/LWT3uBoGMUslwORSSrUBqvWzNQRC1s:ABxT6jW7uBgyOvWS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..h...h...h.....h...i...h.....h.....h.Rich..h.....PE..L...7.]Z.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x409ee0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A5DA737 [Tue Jan 16 07:18:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	4cfe8bbfb0ca5b84bbad08b043ea0c87

Entrypoint Preview

Instruction
push esi
push 0040C1F0h
push 3966646Ch
push 00000009h
mov ecx, D22E2014h
call 00007FAE90D0A53Eh
mov edx, 004011F0h
mov ecx, eax
call 00007FAE90D0A462h
add esp, 0Ch
mov ecx, 8F7EE672h
push 0040C0D0h
push 6677A1D2h
push 00000048h
call 00007FAE90D0A519h
mov edx, 004010D0h
mov ecx, eax
call 00007FAE90D0A43Dh
add esp, 0Ch
push 08000000h
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C10Ch]
mov esi, eax

Instruction
test esi, esi
je 00007FAE90D12878h
push 08000000h
push 00000000h
push esi
call dword ptr [0040C1F8h]
add esp, 0Ch
push esi
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C1E8h]
call 00007FAE90D09E9Ah
push 00000000h
call dword ptr [0040C1ACh]
pop esi
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
push edi
mov edi, edx
mov dword ptr [ebp-0Ch], ecx
mov esi, 00000001h
mov dword ptr [ebp-08h], esi
mov eax, dword ptr [edi]
cmp eax, 7Fh
jbe 00007FAE90D12861h
lea ecx, dword ptr [ecx+00h]
shr eax, 07h
inc esi
cmp eax, 7Fh

Rich Headers

Programming Language:	• [LNK] VS2013 UPD4 build 31101 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbad0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd000	0x5cc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb000	0x8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

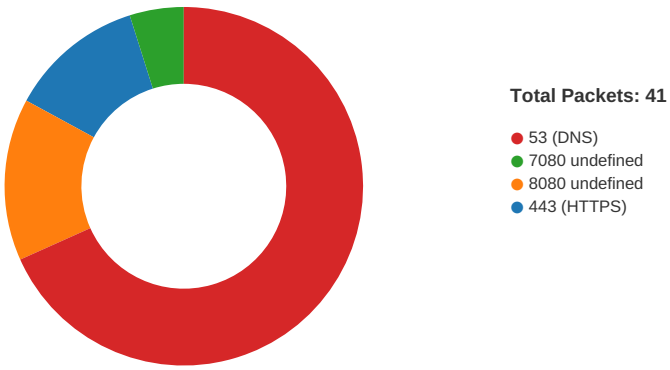
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x9883	0x9a00	False	0.503297483766	data	6.45508103349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0xb2e	0xc00	False	0.160807291667	data	4.23495809712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0xbd8	0x200	False	0.123046875	data	0.91267432928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xd000	0x5cc	0x600	False	0.8671875	data	6.49434732961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	WTSGetActiveConsoleSessionId

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 11:43:07.785733938 CEST	49706	443	192.168.2.3	79.172.249.82
Apr 14, 2021 11:43:07.839173079 CEST	443	49706	79.172.249.82	192.168.2.3
Apr 14, 2021 11:43:07.839747906 CEST	49706	443	192.168.2.3	79.172.249.82
Apr 14, 2021 11:43:07.839804888 CEST	49706	443	192.168.2.3	79.172.249.82
Apr 14, 2021 11:43:07.892940044 CEST	443	49706	79.172.249.82	192.168.2.3
Apr 14, 2021 11:43:07.893347979 CEST	443	49706	79.172.249.82	192.168.2.3
Apr 14, 2021 11:43:07.893378019 CEST	443	49706	79.172.249.82	192.168.2.3
Apr 14, 2021 11:43:07.893603086 CEST	49706	443	192.168.2.3	79.172.249.82
Apr 14, 2021 11:43:07.894906998 CEST	49706	443	192.168.2.3	79.172.249.82
Apr 14, 2021 11:43:07.949728012 CEST	443	49706	79.172.249.82	192.168.2.3
Apr 14, 2021 11:43:38.908854008 CEST	49720	8080	192.168.2.3	193.169.54.12
Apr 14, 2021 11:43:42.083831072 CEST	49720	8080	192.168.2.3	193.169.54.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 11:43:48.084366083 CEST	49720	8080	192.168.2.3	193.169.54.12
Apr 14, 2021 11:44:30.863162994 CEST	49740	8080	192.168.2.3	173.230.145.224
Apr 14, 2021 11:44:31.059032917 CEST	8080	49740	173.230.145.224	192.168.2.3
Apr 14, 2021 11:44:31.572434902 CEST	49740	8080	192.168.2.3	173.230.145.224
Apr 14, 2021 11:44:31.769329071 CEST	8080	49740	173.230.145.224	192.168.2.3
Apr 14, 2021 11:44:32.275563955 CEST	49740	8080	192.168.2.3	173.230.145.224
Apr 14, 2021 11:44:32.472771883 CEST	8080	49740	173.230.145.224	192.168.2.3
Apr 14, 2021 11:45:02.894905090 CEST	49743	7080	192.168.2.3	80.86.91.232
Apr 14, 2021 11:45:05.903651953 CEST	49743	7080	192.168.2.3	80.86.91.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 11:42:52.107168913 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:42:52.156163931 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 14, 2021 11:42:53.281032085 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:42:53.341649055 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 14, 2021 11:42:53.391813993 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:42:53.440597057 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:24.655630112 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:24.707287073 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:25.817858934 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:25.866787910 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:27.487283945 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:27.571316004 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:28.965804100 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:29.014842987 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:29.741539001 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:29.801790953 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:30.604532957 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:30.653295994 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:30.984755039 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:31.045522928 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:31.737567902 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:31.788723946 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:33.589778900 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:33.638511896 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:34.357992887 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:34.409686089 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:41.996906042 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:42.071863890 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:50.746473074 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:50.814496040 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 14, 2021 11:43:58.917186975 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:43:58.967308998 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:00.192394018 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:00.252368927 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:01.377516031 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:01.429486990 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:02.467273951 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:02.517357111 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:03.600243092 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:03.648941994 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:06.855969906 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:06.914968014 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:14.115796089 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:14.164699078 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:26.567142963 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:26.615823984 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:27.805074930 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:27.854285002 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:28.926460028 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:28.978002071 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:29.776983023 CEST	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 14, 2021 11:44:29.837472916 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:38.847352028 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:38.932538033 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 14, 2021 11:44:40.200555086 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 14, 2021 11:44:40.265592098 CEST	53	50713	8.8.8.8	192.168.2.3

HTTP Request Dependency Graph

- 79.172.249.82:443

HTTP Packets

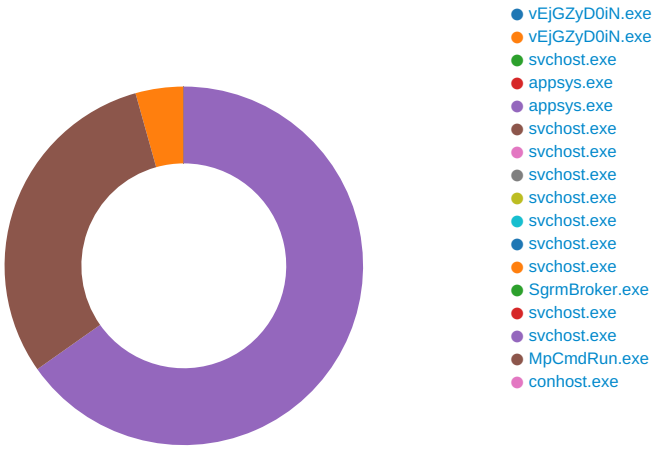
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49706	79.172.249.82	443	C:\Windows\SysWOW64\appsys.exe

Timestamp	kBytes transferred	Direction	Data
Apr 14, 2021 11:43:07.839804888 CEST	968	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.172.249.82:443 Content-Length: 436 Connection: Keep-Alive Cache-Control: no-cache Data Raw: a2 3d 2a 49 b9 06 f3 21 6b a7 b6 8a 8f 13 67 18 b4 45 8e 65 f4 38 7f d7 a5 3d cd ab a1 27 8c 63 f6 ea 88 f0 50 6d 06 50 e5 4c 75 d6 0a 63 35 73 9f 1d fe b9 13 80 5e 54 f6 ae a8 aa a1 74 de fe 36 4f f9 ab a3 2a d8 a9 13 19 28 a2 a3 b2 b3 d2 17 b1 dd 7b b8 f0 69 55 0b 48 87 ea bc 76 3d 6b 0c fb d2 a6 0d 94 e4 f7 c2 b5 2a b5 55 82 90 ed f8 3a 96 5c 5d 0f 1f ec f4 e5 ac a1 9b eb b7 b8 bf 03 38 45 fd 2d 14 c7 fa b6 ac 7f 03 d3 a2 9a ac e1 8d 8f 16 b2 73 52 ea 05 2c 1a f6 93 85 0a 6f a1 8f 51 fe d4 2b c2 82 e0 1e eb 8e 51 b3 a7 70 c8 fb 67 df 00 b9 4f 95 58 e4 25 3e ce c8 03 fe 14 b2 0d 82 4b 46 de 52 24 10 83 89 06 e4 b8 a9 d0 14 cd aa 9a c7 8f 0d 1a 7e e0 0f 48 07 19 53 9a 0c 7e 0e 42 ab 2f f6 d0 6c ff 07 cc 87 bb d6 66 33 78 7e 09 54 cb 81 ab 18 22 d2 cd a9 c9 92 d2 43 2c a0 83 09 68 f8 55 d3 e1 0e 97 05 ea 28 8d b8 56 f8 c4 91 13 3a 99 f0 fc 67 99 ca 7c 5e 1f c8 7e b1 ac bd cb 80 69 42 d4 f4 c2 cf ed 15 66 ba 9d 5a e0 b8 eb fc 99 f2 15 8e f2 5b 66 fd 0e 37 6d 6b c5 65 6d f6 7c c3 d3 1f 9a 53 d5 69 8a 69 db b4 a5 77 b9 27 7c a6 e9 8e 4e aa 33 6b d9 9b ab 10 f6 10 39 67 ab 8e 59 4e 6e f4 c1 fd c3 88 be fb 83 bf 44 14 f0 e0 2e 71 58 bb 8e 29 0c 57 34 c2 c2 f0 71 3b 26 df 3a d3 4a a8 7c da b4 c6 69 91 bb c6 4a b1 3b da 3b 24 31 a2 bb ce 00 16 68 10 45 e1 2b 5c 9b e9 96 c3 b3 8d 3f f7 f1 c0 34 Data Ascii: =*!!kgEe8='cPmPLuc5s^Tt6O*({iUHv=k*U:\]8E-sR,oQ+QpgOX%>KFR$~HS~B/lf3x~T"C,hU(V:g|^~iBfZ[f7mkem|Siiw'|N3k9gYNnD.qX)W4q;&:J|iJ;;$1hE+\?4
Apr 14, 2021 11:43:07.893347979 CEST	969	IN	HTTP/1.1 400 Bad Request Date: Wed, 14 Apr 2021 09:43:07 GMT Server: Apache/2.4.25 (Debian) Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 20 72 65 71 75 65 73 74 20 74 68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 75 6e 64 65 72 73 74 61 6e 64 2e 3c 62 72 20 2f 3e 0a 52 65 61 73 6f 6e 3a 20 59 6f 75 27 72 65 20 73 70 65 61 6b 69 6e 67 20 70 6c 61 69 6e 20 48 54 54 50 20 74 6f 20 61 6e 20 53 53 4c 2d 65 6e 61 62 6c 65 64 20 73 65 72 76 65 72 20 70 6f 72 74 2e 3c 62 72 20 2f 3e 0a 20 49 6e 73 74 65 61 64 20 75 73 65 20 74 68 65 20 48 54 54 50 53 20 73 63 68 65 6d 65 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 55 52 4c 2c 20 70 6c 65 61 73 65 2e 3c 62 72 20 2f 3e 0a 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>400 Bad Request</title> </head><body> Bad Request Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, please. </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: vEjGZyD0iN.exe PID: 5832 Parent PID: 5604

General

Start time:	11:42:58
Start date:	14/04/2021
Path:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\vEjGZyD0iN.exe'
Imagebase:	0x13e0000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000001.00000002.197424310.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.196126268.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: vEjGZyD0iN.exe PID: 5720 Parent PID: 5832

General

Start time:	11:42:58
Start date:	14/04/2021
Path:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vEjGZyD0iN.exe
Imagebase:	0x13e0000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000000.197038659.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.204289645.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\appsys.exe:Zone.Identifier	success or wait	1	13E19CE	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6028 Parent PID: 568

General

Start time:	11:43:00
Start date:	14/04/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: appsys.exe PID: 4716 Parent PID: 568

General

Start time:	11:43:01
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\appsys.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\appsys.exe
Imagebase:	0x13e0000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
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: 00000004.00000000.202803332.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.203947277.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: appsys.exe PID: 1020 Parent PID: 4716

General

Start time:	11:43:01
Start date:	14/04/2021
Path:	C:\Windows\SysWOW64\appsys.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\appsys.exe
Imagebase:	0x13e0000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000000.203553485.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.464331526.00000000013E1000.00000020.00020000.sdmp, Author: Joe Security
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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	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	13E1E04	HttpSendRequestW

Analysis Process: svchost.exe PID: 5492 Parent PID: 568

General

Start time:	11:43:27
Start date:	14/04/2021
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

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: 2436 Parent PID: 568

General

Start time:	11:43:27
Start date:	14/04/2021
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6404 Parent PID: 568

General

Start time:	11:43:38
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6464 Parent PID: 568

General

Start time:	11:43:39
Start date:	14/04/2021
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6472 Parent PID: 568

General

Start time:	11:43:39
Start date:	14/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6556 Parent PID: 568

General

Start time:	11:43:40
Start date:	14/04/2021
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

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

Analysis Process: svchost.exe PID: 6640 Parent PID: 568

General

Start time:	11:43:40
Start date:	14/04/2021
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: 6696 Parent PID: 568

General

Start time:	11:43:41
Start date:	14/04/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7b8520000
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: 6732 Parent PID: 568

General

Start time:	11:43:41
Start date:	14/04/2021
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

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: 6784 Parent PID: 568

General

Start time:	11:43:42
Start date:	14/04/2021
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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 5384 Parent PID: 6732

General

Start time:	11:44:42
Start date:	14/04/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7302e0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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

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 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	7FF73030BC96	WriteFile
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 45 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 57 00 65 00 64 00 20 00 0e 20 41 00 70 00 72 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 34 00 34 00 3a 00 34 00 33 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.:. .. W.e.d. .. A.p.r. .. 1.4. .. 2.0.2.1. .1.1.:. 4.4.:.4.3......	success or wait	1	7FF73030BC96	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	7FF73030BC96	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	7FF73030BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	7FF73030BC96	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 57 00 65 00 64 00 20 00 0e 20 41 00 70 00 72 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 31 00 3a 00 34 00 34 00 3a 00 34 00 33 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. A.p.r. .. 1.4. .. 2.0.2.1. .1.1.:.4.4. :.4.3.....	success or wait	1	7FF73030BC96	WriteFile
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 0d 00 0a 00	-.....	success or wait	1	7FF73030BC96	WriteFile

Analysis Process: conhost.exe PID: 3596 Parent PID: 5384

General

Start time:	11:44:42
Start date:	14/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis