ID: 381863
Sample Name: SMtbg7yHyR
Cookbook: default.jbs
Time: 09:15:39
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

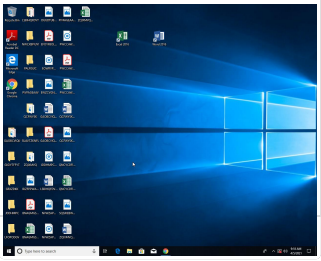
Analysis Report SMtbg7yHyR

Overview

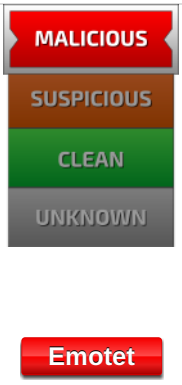
General Information

Sample Name:	SMtbg7yHyR (renamed file extension from none to exe)
Analysis ID:	381863
MD5:	ae03a6f8fb74d40..
SHA1:	6ee320cedc7749..
SHA256:	1ad1ff05930f27e…
Infos:	

Most interesting Screenshot:



Detection

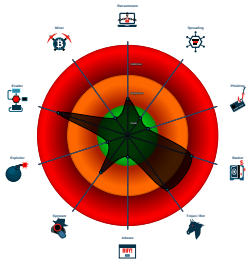


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Emotet e-Banking trojan
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Changes security center settings (no…
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Antivirus or Machine Learning detec…

Classification



Startup

- **System is w10x64**
- SMtbg7yHyR.exe (PID: 5880 cmdline: 'C:\Users\user\Desktop\SMtbg7yHyR.exe' MD5: AE03A6F8FB74D401B403647D28E21574)
  - SMtbg7yHyR.exe (PID: 5412 cmdline: --a1310dca MD5: AE03A6F8FB74D401B403647D28E21574)
- ijpnenglish.exe (PID: 3864 cmdline: C:\Windows\SysWOW64\ijpnenglish.exe MD5: AE03A6F8FB74D401B403647D28E21574)
  - ijpnenglish.exe (PID: 68 cmdline: --23cc28c7 MD5: AE03A6F8FB74D401B403647D28E21574)
- svchost.exe (PID: 5560 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 488 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3636 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4816 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6088 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1140 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2628 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5972 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 2000 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6192 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5172 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6336 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.194305007.0000000002240000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.194305007.0000000002240000.00000040.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x18ec:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x5a13:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 41 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...
00000006.00000002.461305550.0000000000F41000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.461305550.0000000000F41000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0xfad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA F4 0 0 85 C0 • 0x50d4:$snippet6: 33 C0 21 05 EC 10 F5 00 A3 E8 10 F 5 00 39 05 A0 E3 F4 00 74 18 40 A3 E8 10 F5 00 83 3C C5 A0 E3 ...
00000000.00000002.194323919.0000000002281000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.ijpnenglish.exe.e0053f.2.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x2577:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x255d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
5.2.ijpnenglish.exe.e0053f.2.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
5.2.ijpnenglish.exe.e0053f.2.unpack	Emotet	Emotet Payload	kevoreilly	• 0x7ad:$snippet2: 6A 13 68 01 00 01 00 FF 15 48 FA 40 00 85 C0 • 0x48d4:$snippet6: 33 C0 21 05 EC 10 41 00 A3 E8 10 4 1 00 39 05 A0 E3 40 00 74 18 40 A3 E8 10 41 00 83 3C C5 A0 E3 ...
5.2.ijpnenglish.exe.e0053f.2.raw.unpack	MAL_Emotet_Jan20_1	Detects Emotet malware	Florian Roth	• 0x3177:$op1: 03 FE 66 39 07 0F 85 2A FF FF FF 8B 4D F0 6A 20 • 0x315d:$op2: 8B 7D FC 0F 85 49 FF FF FF 85 DB 0F 8 4 D1
5.2.ijpnenglish.exe.e0053f.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Detected Emotet e-Banking trojan

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

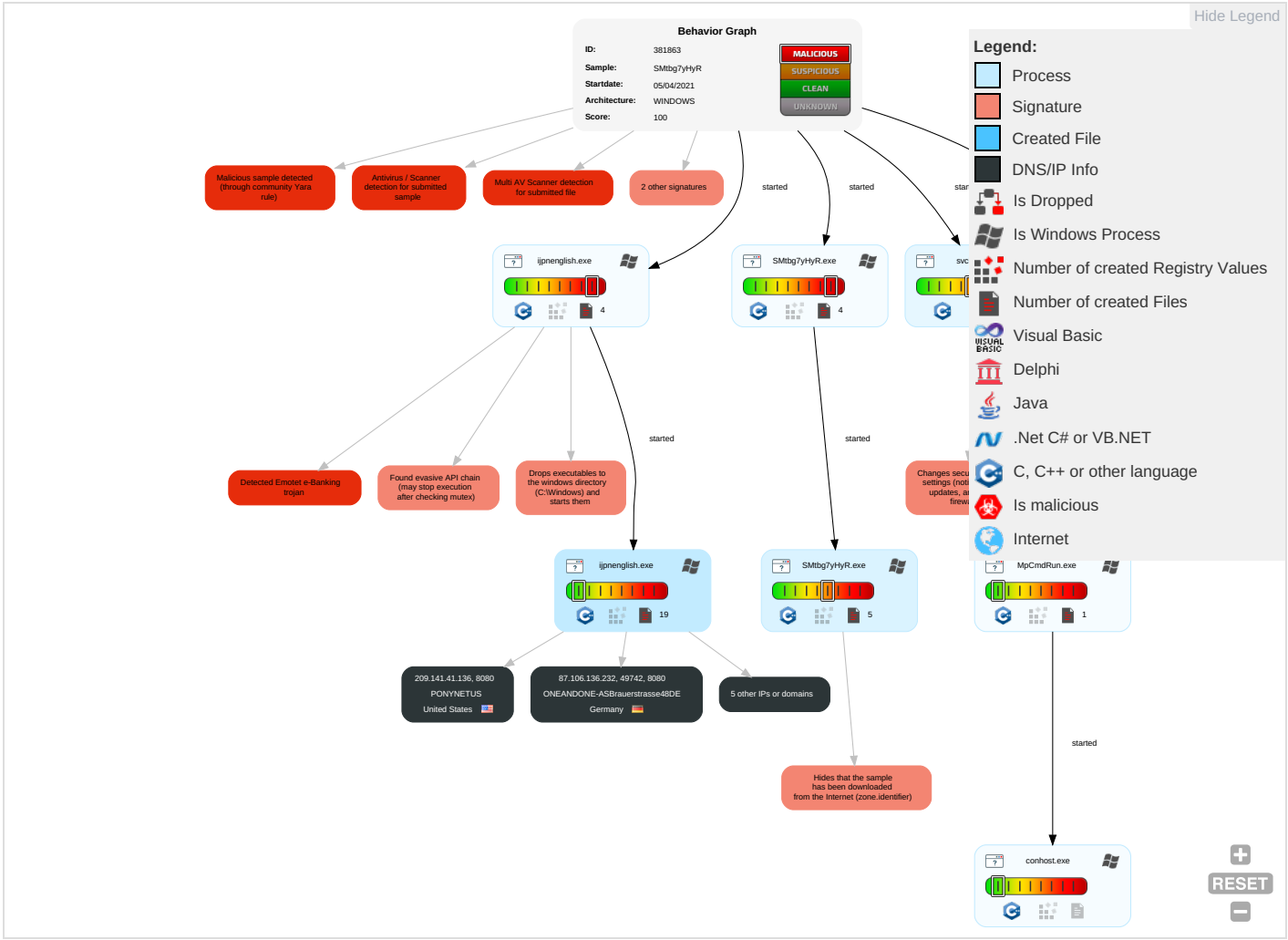
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 1 1 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 2	Windows Service 1 2	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-S Port 1
Local Accounts	Service Execution 1 2	Logon Script (Mac)	Windows Service 1 2	Software Packing 1	NTDS	System Information Discovery 4 7	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Process Injection 2	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

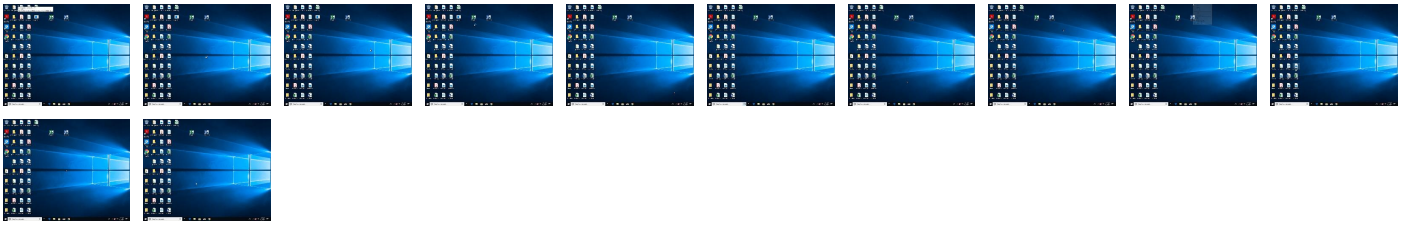
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SMtbg7yHyR.exe	80%	Virustotal		Browse
SMtbg7yHyR.exe	96%	ReversingLabs	Win32.Trojan.Emotet	
SMtbg7yHyR.exe	100%	Avira	HEUR/AGEN.1111753	
SMtbg7yHyR.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.ijpnenglish.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
6.2.ijpnenglish.exe.f3053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.ijpnenglish.exe.e0053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.SMtbg7yHyR.exe.224053f.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.SMtbg7yHyR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
6.2.ijpnenglish.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
1.2.SMtbg7yHyR.exe.217053f.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.SMtbg7yHyR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
0.0.SMtbg7yHyR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
5.2.ijpnenglish.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
1.0.SMtbg7yHyR.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File
6.0.ijpnenglish.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1111753		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://209.141.41.136:8080/entries/ringin/pdf/X	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/psec/window/pdf/T;	0%	Avira URL Cloud	safe	
http://209.141.41.136:8080/entries/ringin/pdf/Q	0%	Avira URL Cloud	safe	
http://104.236.246.93:8080/glitch/prov/pdf/b	0%	Avira URL Cloud	safe	
http://178.210.51.222:8080/glitch/	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/psec/window/pdf/J	0%	Avira URL Cloud	safe	
http://178.210.51.222:8080/glitch/iYq	0%	Avira URL Cloud	safe	
http://104.236.246.93:8080/glitch/prov/pdf/	0%	Avira URL Cloud	safe	
http://152.89.236.214:8080/codec/raster/pdf/merge/	0%	Avira URL Cloud	safe	
http://209.141.41.136:8080/entries/ringin/pdf/G	0%	Avira URL Cloud	safe	
http://45.33.54.74:443/enable/add/	0%	Avira URL Cloud	safe	
http://178.210.51.222/glitch/~	0%	Avira URL Cloud	safe	
http://178.210.51.222/glitch/	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/psec/window/pdf/	0%	Avira URL Cloud	safe	
http://87.106.136.232:8080/psec/window/pdf/.	0%	Avira URL Cloud	safe	
http://152.89.236.214/codec/raster/pdf/merge/	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://87.106.136.232:8080/psec/window/pdf/#	0%	Avira URL Cloud	safe	
http://87.106.136.232/psec/window/pdf/	0%	Avira URL Cloud	safe	
http://104.236.246.93:8080/glitch/prov/pdf/2	0%	Avira URL Cloud	safe	
http://209.141.41.136:8080/entries/ringin/pdf/	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://104.236.246.93:8080/glitch/prov/pdf/hF	0%	Avira URL Cloud	safe	
http://45.33.54.74:443/enable/add/F	0%	Avira URL Cloud	safe	
http://198.199.114.69:8080/between/balloon/pdf/merge/	0%	Avira URL Cloud	safe	
http://152.89.236.214:8080/psec/window/pdf/	0%	Avira URL Cloud	safe	
http://152.89.236.214/codec/raster/pdf/merge/E	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

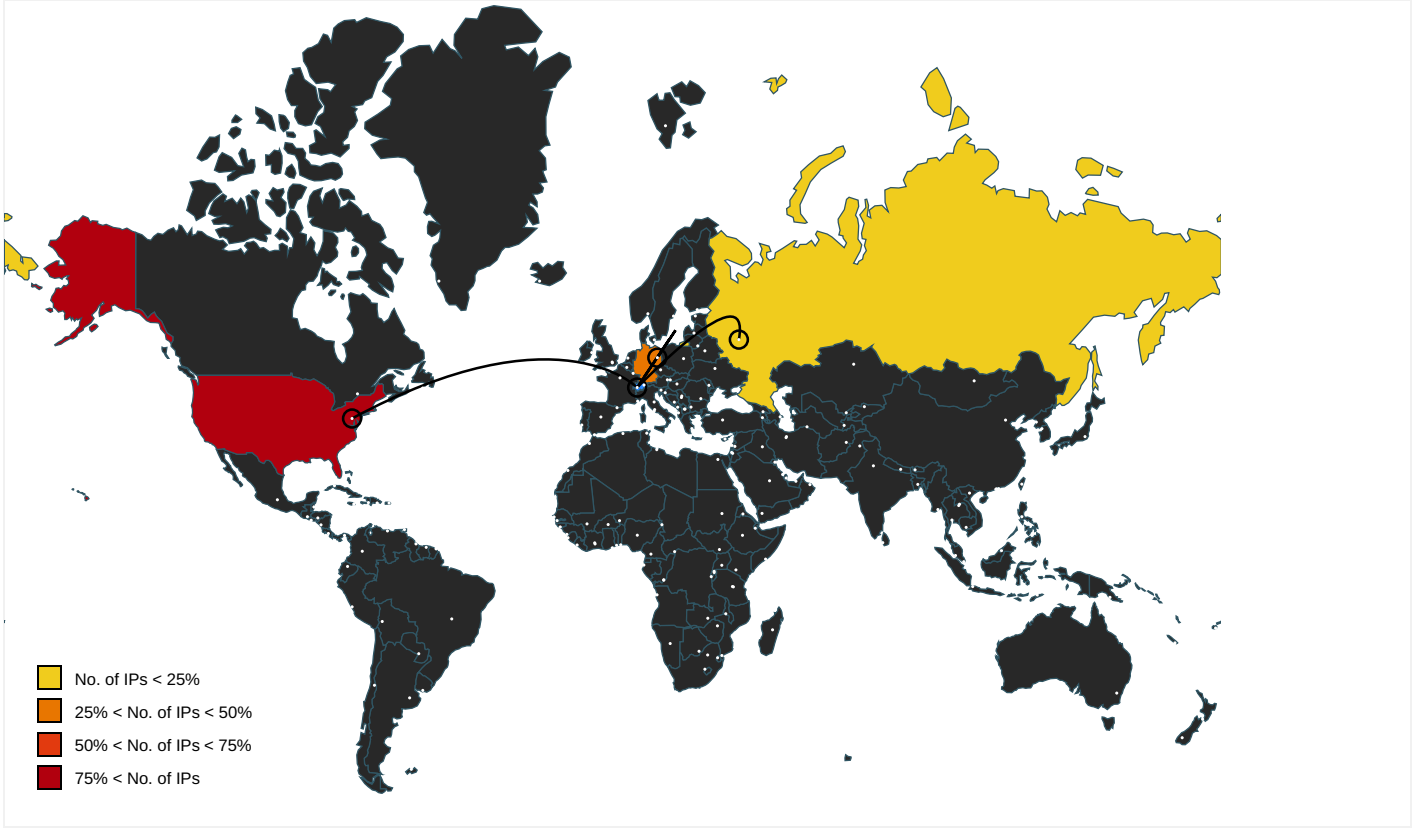
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://209.141.41.136:8080/entries/ringin/pdf/X	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://87.106.136.232:8080/psec/window/pdf/T;	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C00.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000012.00000002.309086422.000001D91F23D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000012.00000002.309086422.000001D91F23D000.00000004.00000001.sdmp	false		high
http://209.141.41.136:8080/entries/ringin/pdf/Q	ijpnenglish.exe, 00000006.00000003.370686900.000000000075D00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000012.00000002.309055802.000001D91F213000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://104.236.246.93:8080/glitch/prov/pdf/b	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000012.00000003.308872767.000001D91F241000.00000004.00000001.sdmp	false		high
http://178.210.51.222:8080/glitch/	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C00.00000004.00000020.sdmp, ijpnenglish.exe, 00000006.00000002.460967488.0000000000735000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000003.308833849.000001D91F249000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000012.00000003.287040478.000001D91F231000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/psec/window/pdf/J	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000012.00000003.308872767.000001D91F241000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/enumeration	svchost.exe, 0000000A.00000002.461539415.00000205F78AC000.00000004.00000001.sdmp	false		high
http://178.210.51.222:8080/glitch/iYq	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://104.236.246.93:8080/glitch/prov/pdf/	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D00.00000004.00000001.sdmp, ijpnenglish.exe, 00000006.00000002.460967488.0000000000735000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://152.89.236.214:8080/codec/raster/pdf/merge/	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://209.141.41.136:8080/entries/ringin/pdf/G	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.33.54.74:443/enable/add/	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://178.210.51.222/glitch/~	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://178.210.51.222/glitch/	ijpnenglish.exe, 00000006.00000002.460302376.000000000019900.00000004.00000001.sdmp, ijpnenglish.exe, 00000006.00000002.461064542.000000000075C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 00000012.00000002.309055802.000001D91F213000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000002.309086422.000001D91F23D000.00000004.00000001.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/psec/window/pdf/	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.308862731.000001D91F245000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/psec/window/pdf/.	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://152.89.236.214/codec/raster/pdf/merge/	ijpnenglish.exe, 00000006.00000002.460890944.000000000071000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000012.00000002.309086422.000001D91F23D000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000003.287040478.000001D91F231000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000002.309086422.000001D91F23D000.00000004.00000001.sdmp, svchost.exe, 00000012.00000002.309055802.000001D91F213000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000E.00000002.461113527.000001F9F663E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000003.287040478.000001D91F231000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://87.106.136.232:8080/psec/window/pdf/#	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://87.106.136.232/psec/window/pdf/	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://104.236.246.93:8080/glitch/prov/pdf/2	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 0000000A.00000002.465219518.00000205FD100000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://209.141.41.136:8080/entries/ringin/pdf/	ijpnenglish.exe, 00000006.00000003.370686900.000000000075D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 00000012.00000003.308815349.000001D91F24C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000012.00000003.287040478.000001D91F231000.00000004.00000001.sdmp	false		high
http://104.236.246.93:8080/glitch/prov/pdf/hF	ijpnenglish.exe, 00000006.00000002.460910977.000000000071700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.33.54.74:443/enable/add/F	ijpnenglish.exe, 00000006.00000002.460910977.000000000071700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://198.199.114.69:8080/between/balloon/pdf/merge/	ijpnenglish.exe, 00000006.00000002.460967488.000000000073500.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://activity.windows.com	svchost.exe, 0000000E.00000002.461113527.000001F9F663E000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000012.00000003.308798345.000001D91F261000.00000004.00000001.sdmp	false		high
http://152.89.236.214:8080/psec/window/pdf/	ijpnenglish.exe, 00000006.00000002.461064542.000000000075C00.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://152.89.236.214/codec/raster/pdf/merge/E	ijpnenglish.exe, 00000006.00000003.440734870.000000000075D00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000E.00000002.461113527.000001F9F663E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000002.309114905.000001D91F25C000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000003.308833849.000001D91F249000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381863
Start date:	05.04.2021
Start time:	09:15:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SMtbg7yHyR (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winEXE@20/8@0/8
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 90.9% • Quality standard deviation: 6.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, wermgr.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.88.21.125, 20.82.210.154, 52.147.198.201, 92.122.145.220, 23.218.208.56, 104.42.151.234, 92.122.213.194, 92.122.213.247, 8.238.29.126, 8.238.85.126, 8.238.32.126, 8.241.80.126, 8.241.90.126, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:16:52	API Interceptor	2x Sleep call for process: svchost.exe modified
09:18:07	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.199.114.69	VYHauUUCLr.exe	Get hash	malicious	Browse	• 198.199.114.69:8080/badge/report/xian/
	http://infraturkey.com/deletecomment/parts_service/daaMnHeDzR/	Get hash	malicious	Browse	• 198.199.114.69:8080/jit/
	http://https://newwell.studio/test/DOC/NtnDpOmWbTdPEdBxrLyy/	Get hash	malicious	Browse	• 198.199.114.69:8080/json/
104.236.246.93	form.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/hZhNeaDm/dcUDNcyqQW/niVKRU29uscA3Ju/
	UAr7Xz5JWr.exe	Get hash	malicious	Browse	• 104.236.246.93:8080/ZxZomdMT6G9XK/ghoypfynUN/
	invoice #865119.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/XzlcYaBSUK0cswU/pzKYcLCk/PbvwO3hXkaN7W/WM9ZNIP/
	XY8707573112TQ.doc	Get hash	malicious	Browse	• 104.236.246.93:8080/att30xZ/YONUKbuNJ8lOQjL/G34JI8e3LEFl/jaWgrB/
	test-emotet.exe	Get hash	malicious	Browse	• 104.236.246.93/
178.210.51.222	aEdlObiYav.exe	Get hash	malicious	Browse	
45.33.54.74	FA_36802305641_Oct2019.doc	Get hash	malicious	Browse	• 45.33.54.74:443/loadan/stubs/
209.141.41.136	aEdlObiYav.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1590815978.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-66411652.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-415601328.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69633738.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-779106205.xls	Get hash	malicious	Browse	• 185.243.114.196
DIGITALOCEAN-ASNUS	TW#9898748948-TZE.exe	Get hash	malicious	Browse	• 162.243.129.169
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 159.89.4.33
	5AKljISD4v.exe	Get hash	malicious	Browse	• 206.189.80.59
	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 104.248.119.44
	documents-575751901.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	MIpyc881Ka.dll	Get hash	malicious	Browse	• 138.197.197.35
	278.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1449.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	documents-1987093434.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1737.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	492.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3205.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1984.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	2503.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3032.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	937.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	FB3gRiNQNX.dll	Get hash	malicious	Browse	• 138.197.197.35
	documents-760030714.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	883fc57b5494b71116dc0f7e3988a4a695adaa4528186.dll	Get hash	malicious	Browse	• 167.172.240.248
	XRLR7xvyRQ.dll	Get hash	malicious	Browse	• 138.197.197.35
DIGITALOCEAN-ASNUS	TW#9898748948-TZE.exe	Get hash	malicious	Browse	• 162.243.129.169
	xqtEOiEeHh.exe	Get hash	malicious	Browse	• 159.89.4.33
	5AKljISD4v.exe	Get hash	malicious	Browse	• 206.189.80.59
	nnrlOwKZlc.exe	Get hash	malicious	Browse	• 104.248.119.44
	documents-575751901.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	MIpyc881Ka.dll	Get hash	malicious	Browse	• 138.197.197.35
	278.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1449.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	documents-1987093434.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1737.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	492.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3205.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	1984.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	2503.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	3032.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	937.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	FB3gRiNQNX.dll	Get hash	malicious	Browse	• 138.197.197.35
	documents-760030714.xlsm	Get hash	malicious	Browse	• 138.197.197.35
	883fc57b5494b71116dc0f7e3988a4a695adaa4528186.dll	Get hash	malicious	Browse	• 167.172.240.248
	XRLR7xvyRQ.dll	Get hash	malicious	Browse	• 138.197.197.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5963998903264245
Encrypted:	false
SSDEEP:	6:0FOqHMk1GaD0JOCEfMuaaD0JOCEfMKQmDGz6Al/gz2cE0fMbhEZolrRSQ2hyYIIT:04+TGaD0JcaaD0JwQQdAg/0bjSQJ
MD5:	F87DAFE2EA18A8F165A852D633CD3DC5
SHA1:	FA5A31CA201D798DA202B03857C69A2ED633CF61
SHA-256:	02DD798ECFF085F3764373E20818004A012BFA8355287927CA0E267443B4ED88
SHA-512:	1FC69B93FB932DE10B7F02C27F1592B0076954051A75C22849C014A6B9C0A3F38CA8A55EA23023DA0D127F9289401F3154CEEE2AE05C85A4ED0D29E708EAC61
Malicious:	false
Preview:	......:{..(.....4....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....4....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 0x98e00ff8, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09625516484514189
Encrypted:	false
SSDEEP:	6:qVczwl/+MtRIE11Y8TRXk9l/lnUK4Vczwl/+MtRIE11Y8TRXk9l/lnUK:q+0+UO4blk9XnUK4+0+UO4blk9XnUK
MD5:	8D1531E395C0577D235FF6FC1AC1E40E
SHA1:	F6E3AD5722F4F851A9401838C2F017359BA1331D
SHA-256:	EDDBF87CA8DCBB8B30C052A41E9237CE8D008E3F625493FD5F5A7F45779BC737
SHA-512:	6AB97ADC54B26FBE9F4932DF7897F59174B2141B14D8C51097261BD8DDA190E962CB5DA972295A53FBDE0FD214FDC40DC8A8131FBE0178C4DFD38717FBF485A
Malicious:	false
Preview:	....e.f.3...w.....&.....w..4....y..h.(.....3...w.....B.....@..... ....3...w..... .....3uD.4....y.k.....^.4....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11178317787104357
Encrypted:	false
SSDEEP:	3:gm//l7EvRohcJxXl/bJdAtim6tall:btiecnt4yl
MD5:	A20D0D568C57E607C423468F1D2AB916
SHA1:	90177E65ACF309BAC84D770506C267CD8B11572F
SHA-256:	86F06FB35837A4404CC269C540A5E90C5FBDBAF0F82AE1AC3E0A1EE99BB90C9D
SHA-512:	FE58D0C1B2F9F8E7E86172ACBFFC107FCBFB089F42AE7E04035118454C0D9EDE00D93397A47DA7FA4146442EA18AAF8F1E7B40275BC0B0AAD0DCA1C86D9BA68
Malicious:	false
Preview:	.'(6.....3...w..4....y.....w.....w.....w....:O....w.....^.4....y..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.10959478611349435

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Encrypted:	false
SSDEEP:	12:264FXm/Ey6q9995TGNGf3q3qQ10nMCldimE8eawHjcb:264ol68j6LyMCldzE9BHjcb
MD5:	E2D4D0365D629474CD3E8568B6F64044
SHA1:	4D1892A728A2255FDA7FE501D996130C4C250AEC
SHA-256:	999DE7568E7D2293B60E94095E7AE47E8CE0881F5844B2777F85BF72E154A635
SHA-512:	D787331D7928CFA68A570A2F96EA4AF9AFD96476729336A93912FD78BACFA79871E16D7AC7ECEE8A102E2DA113F85648F998610894E28541D43BEDA760CEAF3
Malicious:	false
Preview:	.....t...t....O.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....+..... .....U r.7*.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.t...t....W..... ....

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):	0.11241375944530693
Encrypted:	false
SSDEEP:	12:jCjXm/Ey6q9995TGNN1miM3qQ10nMCldimE8eawHza1miIcS/6P:jnl6861tMLyMCldzE9BHza1tIcia
MD5:	534BDB616F9F0A0783FF881037101EC6
SHA1:	EABD345F7C83E4FB9DCCB1271ACDD871B09C68FA
SHA-256:	774562DD46E0A8C526F10AC1E525B94C8C8DE261000BBC08B5B56A3E5F546C87
SHA-512:	7FEBC301FF51C10B3857F675079731289EED261886BA2E901525F327205A02B8ECEDDDCD74DACB4D034878E4F8EB94FA42B4EB2EA9FD7904229397461B850FC
Malicious:	false
Preview:	.....t...t.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....+..... .....h.7*.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.t...t..... ....

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):	0.11190841963544637
Encrypted:	false
SSDEEP:	12:ljXm/Ey6q9995TGNbw1mK2P3qQ10nMCldimE8eawHza1mKV8P:ol68D1iPLyMCldzE9BHza1a
MD5:	E60F4332A6D57FCAEBB7E25C7F494232
SHA1:	290DA489E9505E50CC7B34B6460BF612D5436A5C
SHA-256:	0AB05C4AF97312CAD419BEC4F403A145B920C74D5A966BEC35756FF4CC1C767B
SHA-512:	0417835FD1481B9946AE5640F9C0576D8723B20B9D957732AD083BD983DDC931B4E3CF847EBB49348255F929C2BAE4E92A701F55692F2C8AEFC91E3C81AE6C0
Malicious:	false
Preview:	.....t...t.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....+..... .....oa.7*.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c. k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.t...t..'..... ....

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
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):	3.147616716367721
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3r88eowZk9+MlWlLehB4yAq7ejC18eoQI:OaqdmuF3rWW+kWReH4yJ7M+w
MD5:	2D5B5BBF958129129EF4E1D7C614AF63
SHA1:	1FC63EF43ECC3B86CACA008DE458C09577E7A28E
SHA-256:	F4263BA982973DB39573F123A72BA49335C0BB2AE93B391390518562067F6C94
SHA-512:	970236C9F9E80C0C2D70AEBA5A5F827D5946A939746BEC7A97D47546010E6368F71C52FED25508EE85244393D33D8C5320ADCFA24B1BAB7AD7CC11B4DCD6221
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.:. .. M.o.n. .. A.p.r. .. 0.5. .. 2.0.2.1. .0.9.:.1.8.:.0. 7.........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.:. .. M.o.n. .. A.p.r. .. 0.5. .. 2.0.2.1. .0.9.:.1.8.:.0.7.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.625638741868008
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:	SMtbg7yHyR.exe
File size:	516346
MD5:	ae03a6f8fb74d401b403647d28e21574
SHA1:	6ee320cedc77499f5df9ae9c93ef42c0d91f3ce8
SHA256:	1ad1ff05930f27ef4b349c7a612235d1632ef7ceaa1a17ad f7c7b3a97b40ca4d
SHA512:	ab2a30d32722419c72808032ae01b9443bfb8ea80ec524 26aeb42ac21a84f0a2b04dd6f311c13b06bcaa37b7874b4 e311ff8dc0c94ccfa42cbf6dcac0e2facab
SSDEEP:	6144:PebeJq15KNVIjux9tE9dVyAhwoajYPNo4ahRFPh pxOtYS0xefNPf+R6axxVccVPo:W5KNgux9t0VyAShUP CRdUi8cVRPw17i
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.........*1..Db. .Db..Dbd..b..Db..]b..Db...b..Db..Kb..Db...ba.Db..cb..Dbd. .b..Db..Eb..Db..$b..Db...b..Db...b..Db...b..DbRich..Db..... ..

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x419b95
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5D9A0326 [Sun Oct 6 15:07:18 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	92bdfd5dfdc574760c27f87d6f10fe98

Entrypoint Preview

Instruction
push 00000060h
push 0045C7A8h
call 00007FCC5502E270h
mov edi, 00000094h
mov eax, edi
call 00007FCC5502E3C8h
mov dword ptr [ebp-18h], esp
mov esi, esp
mov dword ptr [esi], edi
push esi
call dword ptr [004552A0h]
mov ecx, dword ptr [esi+10h]
mov dword ptr [0047B960h], ecx
mov eax, dword ptr [esi+04h]
mov dword ptr [0047B96Ch], eax
mov edx, dword ptr [esi+08h]
mov dword ptr [0047B970h], edx
mov esi, dword ptr [esi+0Ch]
and esi, 00007FFFh
mov dword ptr [0047B964h], esi
cmp ecx, 02h
je 00007FCC5502EBDEh
or esi, 00008000h
mov dword ptr [0047B964h], esi
shl eax, 08h
add eax, edx
mov dword ptr [0047B968h], eax
xor esi, esi
push esi
mov edi, dword ptr [00455320h]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007FCC5502EBF1h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
cmp dword ptr [ecx], 00004550h
jne 00007FCC5502EBE4h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007FCC5502EBF1h
cmp eax, 0000020Bh
je 00007FCC5502EBD7h
mov dword ptr [ebp-1Ch], esi
jmp 00007FCC5502EBF9h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007FCC5502EBC4h
xor eax, eax

Instruction
cmp dword ptr [ecx+000000F8h], esi
jmp 00007FCC5502EBE0h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007FCC5502EBB4h
xor eax, eax
cmp dword ptr [ecx+000000E8h], esi
setne al
mov dword ptr [ebp-1Ch], eax

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x68cf0	0x53	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x66224	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x3ebc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x55880	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x60ed0	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x55000	0x878	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x66174	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7eb68	0x134	data	English	United States
RT_CURSOR	0x7ec9c	0xb4	data	English	United States
RT_CURSOR	0x7ed50	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7ee84	0x134	data	English	United States
RT_CURSOR	0x7efb8	0x134	data	English	United States
RT_CURSOR	0x7f0ec	0x134	data	English	United States
RT_CURSOR	0x7f220	0x134	data	English	United States
RT_CURSOR	0x7f354	0x134	data	English	United States
RT_CURSOR	0x7f488	0x134	data	English	United States
RT_CURSOR	0x7f5bc	0x134	data	English	United States
RT_CURSOR	0x7f6f0	0x134	data	English	United States
RT_CURSOR	0x7f824	0x134	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7f958	0x134	AmigaOS bitmap font	English	United States
RT_CURSOR	0x7fa8c	0x134	data	English	United States
RT_CURSOR	0x7fbc0	0x134	data	English	United States
RT_CURSOR	0x7fcf4	0x134	data	English	United States
RT_BITMAP	0x7fe28	0xb8	data	English	United States
RT_BITMAP	0x7fee0	0x144	data	English	United States
RT_DIALOG	0x80024	0x184	data	English	United States
RT_DIALOG	0x801a8	0xf4	data	English	United States
RT_DIALOG	0x8029c	0x100	data	English	United States
RT_DIALOG	0x8039c	0xe8	data	English	United States
RT_STRING	0x80484	0x44	data	English	United States
RT_STRING	0x804c8	0x48	data	English	United States
RT_STRING	0x80510	0x2c	data	English	United States
RT_STRING	0x8053c	0x38	data	English	United States
RT_STRING	0x80574	0x48	data	English	United States
RT_STRING	0x805bc	0x64	data	English	United States
RT_STRING	0x80620	0x46	data	English	United States
RT_STRING	0x80668	0x82	data	English	United States
RT_STRING	0x806ec	0x2a	data	English	United States
RT_STRING	0x80718	0x192	data	English	United States
RT_STRING	0x808ac	0x4e2	data	English	United States
RT_STRING	0x80d90	0x31a	data	English	United States
RT_STRING	0x810ac	0x2dc	data	English	United States
RT_STRING	0x81388	0x8a	data	English	United States
RT_STRING	0x81414	0xac	data	English	United States
RT_STRING	0x814c0	0xde	data	English	United States
RT_STRING	0x815a0	0x4c4	data	English	United States
RT_STRING	0x81a64	0x264	data	English	United States
RT_STRING	0x81cc8	0x2c	data	English	United States
RT_STRING	0x81cf4	0x42	data	English	United States
RT_STRING	0x81d38	0x48	data	English	United States
RT_GROUP_CURSOR	0x81d80	0x22	Lotus unknown worksheet or configuration, revision 0x2	English	United States
RT_GROUP_CURSOR	0x81da4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81db8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81dcc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81de0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81df4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e08	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e1c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e30	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e44	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e58	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e6c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e80	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81e94	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x81ea8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States

Imports

DLL	Import
CRYPT32.dll	CertOpenStore

DLL	Import
KERNEL32.dll	GetStartupInfoA, GetCommandLineA, ExitProcess, HeapReAlloc, TerminateProcess, ExitThread, CreateThread, HeapSize, FatalAppExitA, HeapDestroy, HeapCreate, VirtualFree, IsBadWritePtr, GetStdHandle, UnhandledExceptionFilter, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetFileType, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetUnhandledExceptionFilter, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetTimeZoneInformation, IsBadReadPtr, IsBadCodePtr, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, EnumSystemLocalesA, IsValidLocale, IsValidCodePage, SetConsoleCtrlHandler, RtlUnwind, GetLocaleInfoW, SetEnvironmentVariableA, InterlockedExchange, GetACP, GetLocaleInfoA, GetThreadLocale, GetVersionExA, MultiByteToWideChar, WideCharToMultiByte, GetLastError, GetVersion, lstrcmpiA, lstrlenW, lstrcmpiW, lstrlenA, CompareStringA, CompareStringW, GetEnvironmentVariableA, GetEnvironmentVariableW, GetStringTypeExA, GetStringTypeExW, SizeofResource, LockResource, LoadResource, FindResourceA, FreeResource, GlobalFree, GlobalUnlock, GlobalLock, LocalFree, lstrcpynA, FormatMessageA, GlobalAlloc, GlobalSize, MulDiv, CopyFileA, SetLastError, GetProcAddress, GetModuleHandleA, lstrcmpW, VirtualQuery, GetSystemInfo, VirtualAlloc, VirtualProtect, HeapFree, HeapAlloc, GetDiskFreeSpaceA, GetTempFileNameA, LocalLock, LocalUnlock, GetFileTime, GetFileAttributesA, SetFileAttributesA, SetFileTime, LocalFileTimeToFileTime, FileTimeToLocalFileTime, SetErrorMode, GetShortPathNameA, CreateFileA, GetFullPathNameA, GetVolumeInformationA, FindFirstFileA, FindClose, GetCurrentProcess, DuplicateHandle, GetFileSize, SetEndOfFile, UnlockFile, LockFile, FlushFileBuffers, SetFilePointer, WriteFile, ReadFile, DeleteFileA, MoveFileA, GetCurrentDirectoryA, GetPrivateProfileStringA, WritePrivateProfileStringA, GetPrivateProfileIntA, SystemTimeToFileTime, FileTimeToSystemTime, GetOEMCP, GetCPInfo, TlsFree, LocalReAlloc, TlsSetValue, TlsAlloc, TlsGetValue, EnterCriticalSection, GlobalHandle, GlobalReAlloc, LeaveCriticalSection, LocalAlloc, InterlockedIncrement, GlobalFlags, DeleteCriticalSection, InitializeCriticalSection, RaiseException, CreateEventA, SuspendThread, SetEvent, WaitForSingleObject, ResumeThread, SetThreadPriority, CloseHandle, GetCurrentThread, lstrcmpA, GetModuleFileNameA, lstrcatA, ConvertDefaultLocale, EnumResourceLanguagesA, lstrcpyA, InterlockedDecrement, GetCurrentThreadId, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, GlobalDeleteAtom, LoadLibraryA, FreeLibrary, SetStdHandle
USER32.dll	IsClipboardFormatAvailable, MessageBeep, GetTabbedTextExtentA, GetDCEx, LockWindowUpdate, SetParent, InvalidateRect, InsertMenuItemA, CreatePopupMenu, SetRectEmpty, BringWindowToTop, SetMenu, TranslateAcceleratorA, DestroyIcon, DeleteMenu, wsprintfA, WaitMessage, GetWindowThreadProcessId, ReleaseCapture, WindowFromPoint, SetCapture, LoadCursorA, GetSysColorBrush, GetDialogBaseUnits, GetMessageA, TranslateMessage, GetCursorPos, ValidateRect, ShowOwnedPopups, SetCursor, PostQuitMessage, EndPaint, BeginPaint, GetWindowDC, ReleaseDC, GetDC, ClientToScreen, GrayStringA, DrawTextExA, DrawTextA, TabbedTextOutA, FillRect, DestroyMenu, GetMenuItemInfoA, InflateRect, SetMenuItemBitmaps, ModifyMenuA, EnableMenuItem, CheckMenuItem, GetMenuCheckMarkDimensions, LoadBitmapA, ScrollWindowEx, ShowWindow, MoveWindow, SetWindowTextA, IsDialogMessageA, IsDlgButtonChecked, SetDlgItemInt, GetDlgItemTextA, GetDlgItemInt, CheckRadioButton, CheckDlgButton, RegisterWindowMessageA, WinHelpA, GetCapture, CreateWindowExA, SetWindowsHookExA, CallNextHookEx, KillTimer, GetClassInfoExA, GetClassNameA, SetPropA, GetPropA, RemovePropA, SendDlgItemMessageA, GetFocus, SetFocus, IsChild, GetWindowTextLengthA, GetWindowTextA, GetForegroundWindow, GetLastActivePopup, DispatchMessageA, BeginDeferWindowPos, EndDeferWindowPos, GetTopWindow, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, PeekMessageA, MapWindowPoints, ScrollWindow, MessageBoxA, TrackPopupMenuEx, TrackPopupMenu, GetKeyState, SetScrollRange, SetDlgItemTextA, CharLowerA, CharLowerW, CharUpperA, CharUpperW, SendMessageA, EnableWindow, DrawIcon, AppendMenuA, GetSystemMenu, IsIconic, GetClientRect, SetActiveWindow, LoadIconA, GetScrollRange, SetScrollPos, GetScrollPos, SetForegroundWindow, ShowScrollBar, IsWindowVisible, UpdateWindow, GetMenu, PostMessageA, GetSysColor, AdjustWindowRectEx, ScreenToClient, EqualRect, DeferWindowPos, GetScrollInfo, SetScrollInfo, SetTimer, SetRect, UnionRect, IsRectEmpty, MapVirtualKeyA, GetClassInfoA, RegisterClassA, UnregisterClassA, SetWindowPlacement, GetDlgCtrlID, DefWindowProcA, SetWindowLongA, SetWindowPos, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetKeyNameTextA, LoadMenuA, UnpackDDElParam, ReuseDDElParam, GetClassLongA, LoadAcceleratorsA, CallWindowProcA, LoadStringW, GetSystemMetrics, EndDialog, GetNextDlgTabItem, GetParent, IsWindowEnabled, GetDlgItem, GetWindowLongA, IsWindow, DestroyWindow, CreateDialogIndirectParamA, GetActiveWindow, GetDesktopWindow, RemoveMenu, GetSubMenu, GetMenuItemCount, InsertMenuA, GetWindowRect, CopyRect, PtInRect, GetWindow, GetMenuState, GetMenuStringA, GetMenuItemID
GDI32.dll	SetMapperFlags, SetArcDirection, SetColorAdjustment, DeleteObject, SelectClipRgn, GetClipRgn, CreateRectRgn, SelectClipPath, GetViewportExtEx, GetWindowExtEx, GetPixel, StartDocA, PtVisible, RectVisible, TextOutA, Escape, SelectObject, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowOrgEx, OffsetWindowOrgEx, SetWindowExtEx, ScaleWindowExtEx, GetCurrentPositionEx, ArcTo, PolyDraw, PolylineTo, PolyBezierTo, SetTextCharacterExtra, DeleteDC, CreateDIBPatternBrushPt, CreatePatternBrush, GetStockObject, SelectPalette, PlayMetaFileRecord, GetObjectType, EnumMetaFile, PlayMetaFile, CreatePen, ExtCreatePen, CreateSolidBrush, CreateHatchBrush, GetTextMetricsA, CreateRectRgnIndirect, SetRectRgn, CombineRgn, GetMapMode, PatBlt, DPtoLP, CreateCompatibleBitmap, StretchDIBits, GetCharWidthA, CreateFontA, GetBkColor, StartPage, EndPage, SetAbortProc, AbortDoc, EndDoc, SetTextJustification, SetTextAlign, MoveToEx, LineTo, OffsetClipRgn, IntersectClipRect, ExcludeClipRect, SetMapMode, SetStretchBltMode, SetROP2, SetPolyFillMode, SetBkMode, RestoreDC, SaveDC, GetTextExtentPoint32A, ExtTextOutA, BitBlt, CreateCompatibleDC, CreateFontIndirectA, CreateBitmap, GetObjectA, SetBkColor, SetTextColor, GetClipBox, GetDCOrgEx, CreateDCA, CopyMetaFileA, ExtSelectClipRgn, GetDeviceCaps
comdlg32.dll	PageSetupDlgA, FindTextA, ReplaceTextA, GetOpenFileNameA, CommDlgExtendedError, PrintDlgA, GetFileTitleA, GetSaveFileNameA
WINSPOOL.DRV	OpenPrinterA, DocumentPropertiesA, ClosePrinter, GetJobA
ADVAPI32.dll	GetFileSecurityA, RegCloseKey, RegSetValueA, RegOpenKeyA, RegQueryValueExA, RegOpenKeyExA, RegDeleteKeyA, RegEnumKeyA, RegQueryValueA, RegCreateKeyExA, RegSetValueExA, RegDeleteValueA, RegCreateKeyA, SetFileSecurityW, SetFileSecurityA
SHELL32.dll	SHGetFileInfoA, DragFinish, DragQueryFileA, ExtractIconA
COMCTL32.dll	ImageList_Draw, ImageList_GetImageInfo, ImageList_Read, ImageList_Write, ImageList_Destroy, ImageList_Create, ImageList_LoadImageA, ImageList_Merge
SHLWAPI.dll	PathRemoveExtensionA, PathFindFileNameA, PathStripToRootA, PathFindExtensionA, PathIsUNCA
ole32.dll	WriteClassStg, OleRegGetUserType, SetConvertStg, CoTaskMemFree, ReadFmtUserTypeStg, ReadClassStg, StringFromCLSID, CoTreatAsClass, CreateBindCtx, CoTaskMemAlloc, ReleaseStgMedium, OleDuplicateData, CoDisconnectObject, CoCreateInstance, StringFromGUID2, CLSIDFromString, WriteFmtUserTypeStg

DLL	Import
OLEAUT32.dll	VariantClear, VariantChangeType, VariantInit, SysAllocStringLen, SysFreeString, SysStringLen, SysAllocStringByteLen, SysStringByteLen, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayGetElemsize, SafeArrayGetDim, SafeArrayCreate, SafeArrayRedim, VariantCopy, SafeArrayAllocData, SafeArrayAllocDescriptor, SafeArrayCopy, SafeArrayGetElement, SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayLock, SafeArrayUnlock, SafeArrayDestroy, SafeArrayDestroyData, SafeArrayDestroyDescriptor, VariantTimeToSystemTime, SystemTimeToVariantTime, SysAllocString, SysReAllocStringLen, VarDateFromStr, VarBstrFromDec, VarDecFromStr, VarCyFromStr, VarBstrFromCy, VarBstrFromDate

Exports

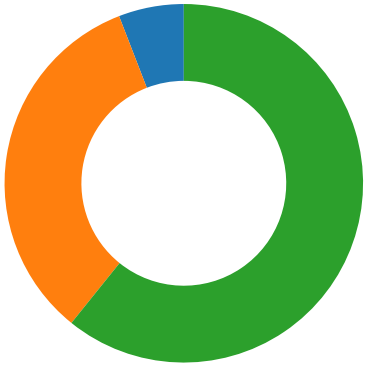
Name	Ordinal	Address
mcfGvgupamvngNBNmgO	1	0x401e04

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 09:16:49.634516001 CEST	49710	443	192.168.2.3	45.33.54.74
Apr 5, 2021 09:16:49.831779003 CEST	443	49710	45.33.54.74	192.168.2.3
Apr 5, 2021 09:16:50.346028090 CEST	49710	443	192.168.2.3	45.33.54.74
Apr 5, 2021 09:16:50.540414095 CEST	443	49710	45.33.54.74	192.168.2.3
Apr 5, 2021 09:16:51.049235106 CEST	49710	443	192.168.2.3	45.33.54.74
Apr 5, 2021 09:16:51.243505955 CEST	443	49710	45.33.54.74	192.168.2.3
Apr 5, 2021 09:16:56.071508884 CEST	49716	8080	192.168.2.3	209.141.41.136
Apr 5, 2021 09:16:59.143676043 CEST	49716	8080	192.168.2.3	209.141.41.136
Apr 5, 2021 09:17:05.144263983 CEST	49716	8080	192.168.2.3	209.141.41.136
Apr 5, 2021 09:17:20.559530020 CEST	49729	8080	192.168.2.3	104.236.246.93
Apr 5, 2021 09:17:23.567615032 CEST	49729	8080	192.168.2.3	104.236.246.93
Apr 5, 2021 09:17:29.568475962 CEST	49729	8080	192.168.2.3	104.236.246.93
Apr 5, 2021 09:17:45.896600962 CEST	49738	8080	192.168.2.3	198.199.114.69
Apr 5, 2021 09:17:48.897833109 CEST	49738	8080	192.168.2.3	198.199.114.69
Apr 5, 2021 09:17:54.898366928 CEST	49738	8080	192.168.2.3	198.199.114.69
Apr 5, 2021 09:18:12.034565926 CEST	49741	8080	192.168.2.3	152.89.236.214
Apr 5, 2021 09:18:12.074902058 CEST	8080	49741	152.89.236.214	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 09:18:12.587445974 CEST	49741	8080	192.168.2.3	152.89.236.214
Apr 5, 2021 09:18:12.625788927 CEST	8080	49741	152.89.236.214	192.168.2.3
Apr 5, 2021 09:18:13.134372950 CEST	49741	8080	192.168.2.3	152.89.236.214
Apr 5, 2021 09:18:13.173031092 CEST	8080	49741	152.89.236.214	192.168.2.3
Apr 5, 2021 09:18:18.581378937 CEST	49742	8080	192.168.2.3	87.106.136.232
Apr 5, 2021 09:18:18.623788118 CEST	8080	49742	87.106.136.232	192.168.2.3
Apr 5, 2021 09:18:19.134790897 CEST	49742	8080	192.168.2.3	87.106.136.232
Apr 5, 2021 09:18:19.178415060 CEST	8080	49742	87.106.136.232	192.168.2.3
Apr 5, 2021 09:18:19.681596041 CEST	49742	8080	192.168.2.3	87.106.136.232
Apr 5, 2021 09:18:19.725167036 CEST	8080	49742	87.106.136.232	192.168.2.3
Apr 5, 2021 09:18:25.664623976 CEST	49743	8080	192.168.2.3	178.210.51.222
Apr 5, 2021 09:18:28.666738033 CEST	49743	8080	192.168.2.3	178.210.51.222

UDP Packets

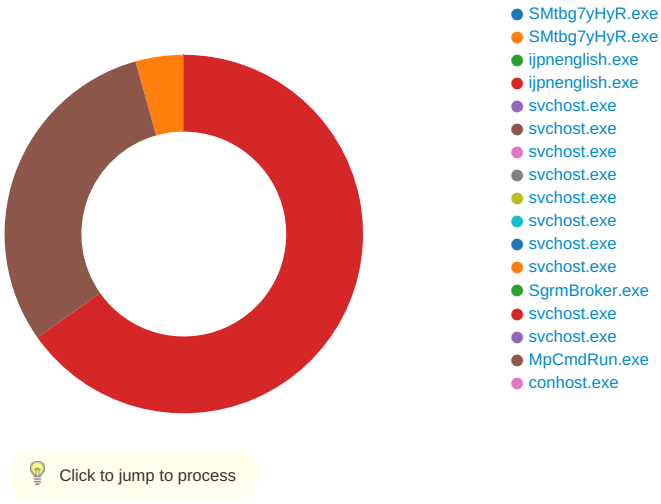
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 09:16:15.974296093 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:16.033528090 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:16.694695950 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:16.743758917 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:16.805288076 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:16.855740070 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:18.029567957 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:18.083921909 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:18.773416996 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:18.830735922 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:18.878134012 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:18.938483000 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:19.677510977 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:19.725665092 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:20.743665934 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:20.792572975 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:21.679435968 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:21.736130953 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:22.751379013 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:22.807127953 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:23.667259932 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:23.713251114 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:24.520864010 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:24.566847086 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:25.278831005 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:25.327621937 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:54.191589117 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:54.240457058 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:55.605709076 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:55.654757977 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:56.269715071 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:56.331041098 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:57.717669964 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:57.766590118 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:58.851695061 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:58.906142950 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 5, 2021 09:16:59.650053024 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:16:59.698878050 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:00.457350969 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:00.505016088 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:01.740768909 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:01.786746025 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:02.519961119 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:02.577811003 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:03.297364950 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:03.345118999 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:09.059760094 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:09.115963936 CEST	53	50540	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 09:17:09.891547918 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:09.940416098 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:11.613806963 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:11.668544054 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:16.856203079 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:16.918642044 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:32.670361996 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:32.717812061 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 5, 2021 09:17:35.707624912 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:17:35.763530016 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 5, 2021 09:18:07.607659101 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:18:07.653599024 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 5, 2021 09:18:09.381201982 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 5, 2021 09:18:09.445626020 CEST	53	58987	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SMtbg7yHyR.exe PID: 5880 Parent PID: 5616

General

Start time:	09:16:21
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\SMtbg7yHyR.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SMtbg7yHyR.exe'
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.194305007.0000000002240000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.194305007.0000000002240000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.194323919.0000000002281000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.194323919.0000000002281000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: SMtbg7yHyR.exe PID: 5412 Parent PID: 5880

General

Start time:	09:16:22
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\SMtbg7yHyR.exe
Wow64 process (32bit):	true
Commandline:	--a1310dca
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.207769804.0000000002181000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.207769804.0000000002181000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.207750477.0000000002170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000001.00000002.207750477.0000000002170000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ijpnenglish.exe:Zone.Identifier	success or wait	1	2181126	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ijpnenglish.exe PID: 3864 Parent PID: 568

General

Start time:	09:16:27
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\ijpnenglish.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ijpnenglish.exe
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.206978674.0000000000E00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000005.00000002.206978674.0000000000E00000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000005.00000002.206996427.0000000000E21000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000005.00000002.206996427.0000000000E21000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: ijpnenglish.exe PID: 68 Parent PID: 3864

General

Start time:	09:16:28
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\ijpnenglish.exe
Wow64 process (32bit):	true
Commandline:	--23cc28c7
Imagebase:	0x400000
File size:	516346 bytes
MD5 hash:	AE03A6F8FB74D401B403647D28E21574
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.461305550.0000000000F41000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.461305550.0000000000F41000.00000020.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000006.00000002.461230272.0000000000F30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.461230272.0000000000F30000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	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	F414A5	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F414A5	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	F414A5	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	F414A5	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	F414A5	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	F414A5	HttpSendRequestW

Analysis Process: svchost.exe PID: 5560 Parent PID: 568

General

Start time:	09:16:30
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 488 Parent PID: 568

General

Start time:	09:16:52
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 3636 Parent PID: 568

General

Start time:	09:16:53
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4816 Parent PID: 568

General

Start time:	09:17:03
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6088 Parent PID: 568

General

Start time:	09:17:04
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 1140 Parent PID: 568

General

Start time:	09:17:04
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2628 Parent PID: 568

General

Start time:	09:17:04
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 5972 Parent PID: 568

General

Start time:	09:17:05
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 2000 Parent PID: 568

General

Start time:	09:17:06
Start date:	05/04/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff612f20000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6192 Parent PID: 568

General

Start time:	09:17:06
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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: 6336 Parent PID: 568

General

Start time:	09:17:07
Start date:	05/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: 5172 Parent PID: 6192

General

Start time:	09:18:07
Start date:	05/04/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff7e8ce0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	.......-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF7E8D0BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 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 4d 00 6f 00 6e 00 20 00 0e 20 41 00 70 00 72 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 30 00 39 00 3a 00 31 00 38 00 3a 00 30 00 37 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.:. .. M.o.n. .. A.p.r. .. 0.5. .. 2.0.2.1. .0.9.:. 1.8.:.0.7......	success or wait	1	7FF7E8D0BC96	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	7FF7E8D0BC96	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	7FF7E8D0BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e. (.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....	success or wait	1	7FF7E8D0BC96	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 4d 00 6f 00 6e 00 20 00 0e 20 41 00 70 00 72 00 20 00 0e 20 30 00 35 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 30 00 39 00 3a 00 31 00 38 00 3a 00 30 00 37 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. M.o.n. .. A.p.r. .. 0.5. .. 2.0.2.1. .0.9.:.1.8. :.0.7.....	success or wait	1	7FF7E8D0BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	unknown	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	-.....	success or wait	1	7FF7E8D0BC96	WriteFile

Analysis Process: conhost.exe PID: 5180 Parent PID: 5172

General

Start time:	09:18:07
Start date:	05/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis