ID: 405975
Sample Name: uIsv6VTOek
Cookbook: default.jbs
Time: 15:30:54
Date: 06/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

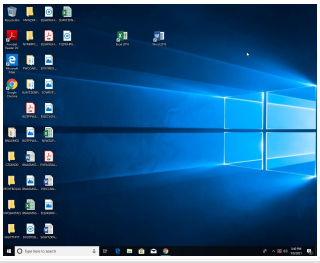
Analysis Report uIsv6VTOek

Overview

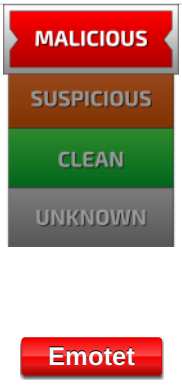
General Information

Sample Name:	uIsv6VTOek (renamed file extension from none to exe)
Analysis ID:	405975
MD5:	3ee16bbc971bce..
SHA1:	f20112dd192c7ec..
SHA256:	982a1c7af717a51..
Infos:	

Most interesting Screenshot:



Detection



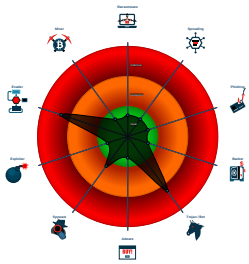
Emotet

Score:	88
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…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- AV process strings found (often use…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Connects to several IPs in different …
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- uIsv6VTOek.exe (PID: 5936 cmdline: 'C:\Users\user\Desktop\uIsv6VTOek.exe' MD5: 3EE16BBC971BCEB22C5EA3B79F8F711D)
  - uIsv6VTOek.exe (PID: 5980 cmdline: C:\Users\user\Desktop\uIsv6VTOek.exe MD5: 3EE16BBC971BCEB22C5EA3B79F8F711D)
- hyperlanes.exe (PID: 3040 cmdline: C:\Windows\SysWOW64\hyperlanes.exe MD5: 3EE16BBC971BCEB22C5EA3B79F8F711D)
  - hyperlanes.exe (PID: 3468 cmdline: C:\Windows\SysWOW64\hyperlanes.exe MD5: 3EE16BBC971BCEB22C5EA3B79F8F711D)
- svchost.exe (PID: 6024 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1268 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5844 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5656 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4088 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5344 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1740 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 484 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 3652 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5560 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 1004 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6504 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6596 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6904 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.1291468406.0000000000D11000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000006.00000002.1291468406.0000000000D11000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5990:$snippet4: 33 C0 C7 05 80 A8 D1 00 00 A0 D1 00 C7 05 84 A8 D1 00 00 A0 D1 00 A3 88 A8 D1 00 A3 8C A8 D1 00 ...
00000004.00000002.246701559.00000000005B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.246701559.00000000005B1000.00000020.00000001.sdmp	Emotet	Emotet Payload	kevoreilly	• 0x5990:$snippet4: 33 C0 C7 05 80 A8 5B 00 00 A0 5B 00 C7 05 84 A8 5B 00 00 A0 5B 00 A3 88 A8 5B 00 A3 8C A8 5B 00 ...
00000000.00000002.233356991.00000000005B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

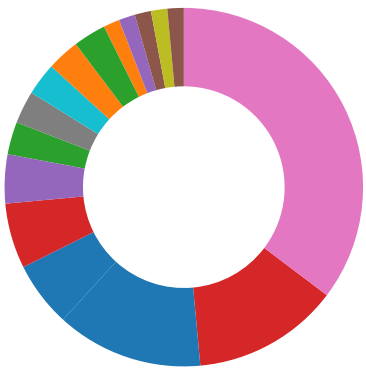
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.uIsv6VTOek.exe.5b0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.uIsv6VTOek.exe.5b0000.3.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5d90:$snippet4: 33 C0 C7 05 80 A8 5B 00 00 A0 5B 00 C7 05 84 A8 5B 00 00 A0 5B 00 A3 88 A8 5B 00 A3 8C A8 5B 00 ...
0.2.uIsv6VTOek.exe.5b0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
0.2.uIsv6VTOek.exe.5b0000.3.unpack	Emotet	Emotet Payload	kevoreilly	• 0x5d90:$snippet4: 33 C0 C7 05 80 A8 5B 00 00 A0 5B 00 C7 05 84 A8 5B 00 00 A0 5B 00 A3 88 A8 5B 00 A3 8C A8 5B 00 ...
6.2.hyperlanes.exe.d10000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Cryptography
- Compliance
- Networking
- E-Banking Fraud
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- 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

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)

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

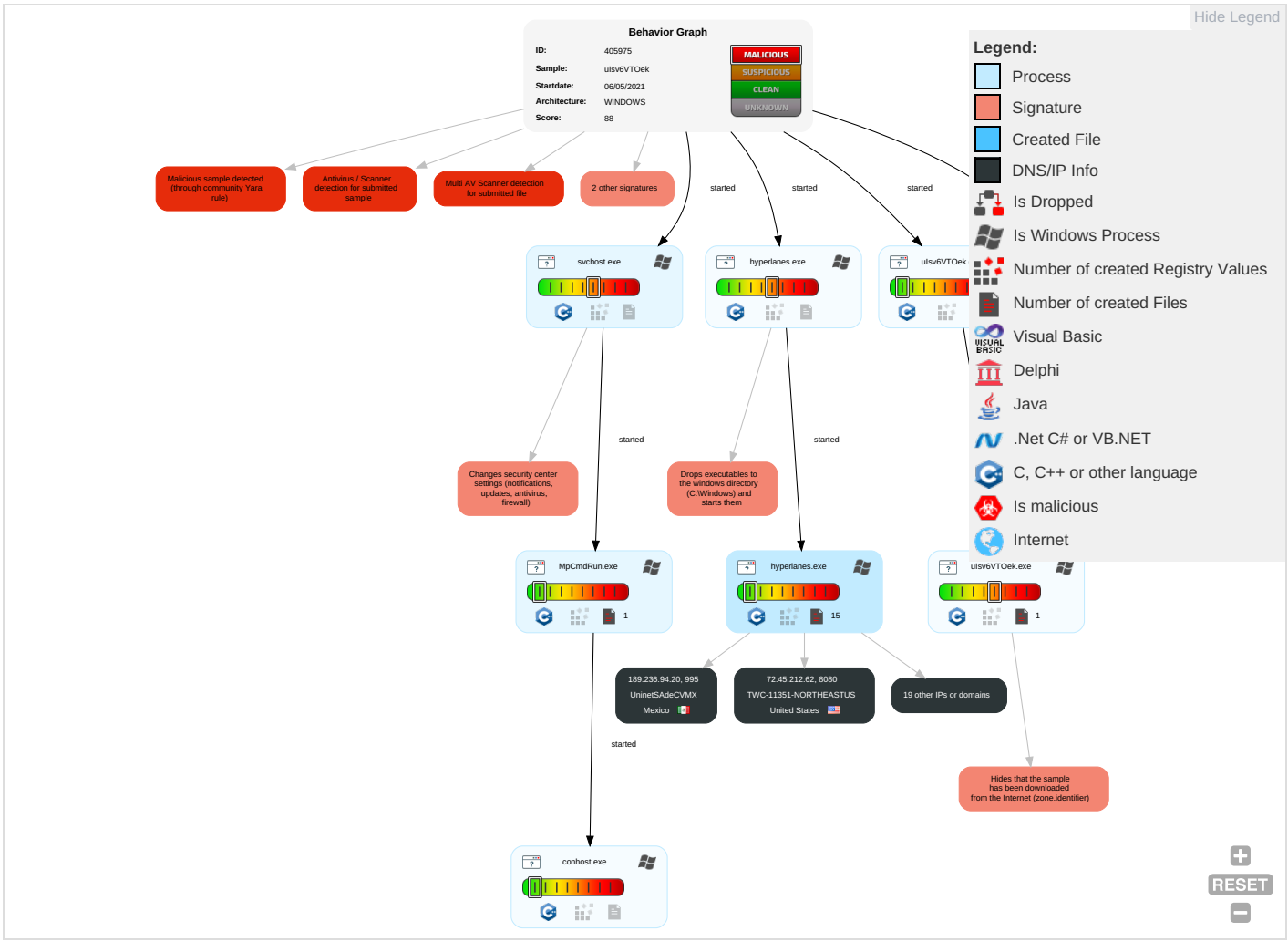
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Service Execution 1 2	Valid Accounts 1	Valid Accounts 1	Software Packing 1	LSASS Memory	System Service Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Windows Service 1 2	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Windows Service 1 2	File Deletion 1	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applicat Layer Protoco
Cloud Accounts	Cron	Network Logon Script	Process Injection 2	Masquerading 1 2 1	LSA Secrets	Security Software Discovery 5 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco

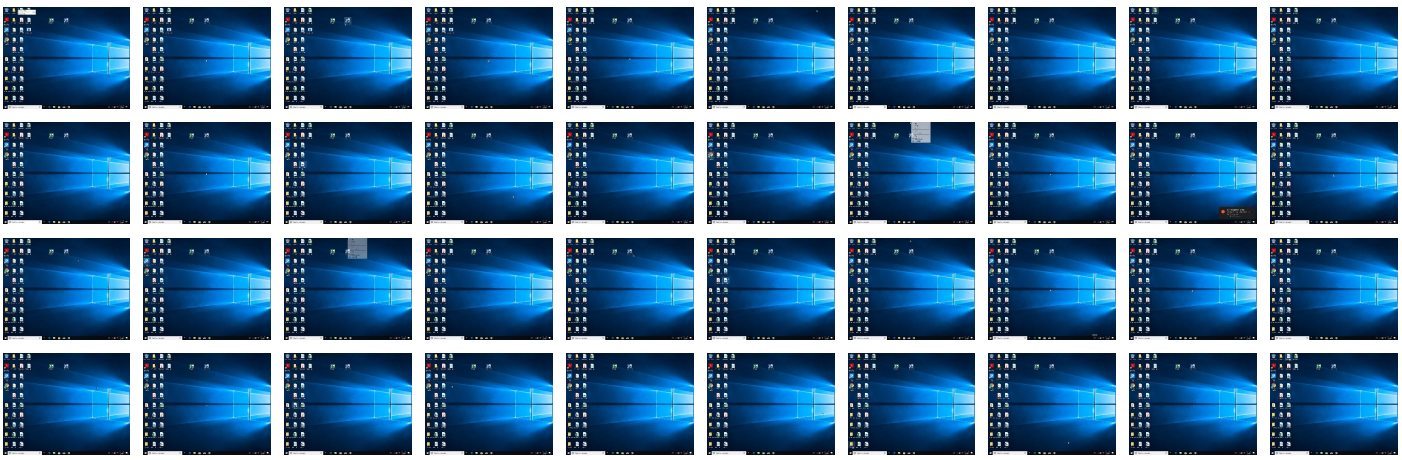
Behavior Graph



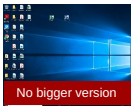
Screenshots

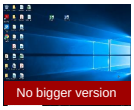
Thumbnails

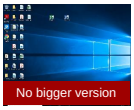
This section contains all screenshots as thumbnails, including those not shown in the slideshow.

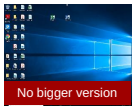


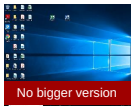


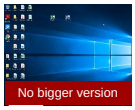












Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
uIsv6VTOek.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
uIsv6VTOek.exe	100%	Avira	TR/Crypt.EPACK.Gen8	
uIsv6VTOek.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
6.1.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
0.1.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.uIsv6VTOek.exe.5b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.hyperlanes.exe.d00000.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
6.2.hyperlanes.exe.d10000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.uIsv6VTOek.exe.5b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.hyperlanes.exe.5b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.uIsv6VTOek.exe.5a0000.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
5.0.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
6.2.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
4.1.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
4.2.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
5.2.hyperlanes.exe.5a0000.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
0.2.uIsv6VTOek.exe.5a0000.2.unpack	100%	Avira	HEUR/AGEN.1110377		Download File
0.0.uIsv6VTOek.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File
5.1.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.hyperlanes.exe.400000.0.unpack	100%	Avira	TR/Crypt.EPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://78.47.182.42:8080/	0%	Avira URL Cloud	safe	
http://72.45.212.62:8080/c(	0%	Avira URL Cloud	safe	
http://189.236.94.20:995/m#	0%	Avira URL Cloud	safe	
http://Passport.NET/tbpose	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/8j#	0%	Avira URL Cloud	safe	
http://72.45.212.62:8080/-	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/103.94:8080/	0%	Avira URL Cloud	safe	
http://194.88.246.242:443/.177.28:8080/m	0%	Avira URL Cloud	safe	
http://47.188.131.94:443/	0%	Avira URL Cloud	safe	
http://164.160.161.118:8080/	0%	Avira URL Cloud	safe	
http://passport.net/tb	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/M	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://70.182.77.184:8090/	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/N	0%	Avira URL Cloud	safe	
http://194.88.246.242:443/;(	0%	Avira URL Cloud	safe	
http://121.50.43.110:8080/	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://76.72.225.30:465//	0%	Avira URL Cloud	safe	
http://206.210.104.194/A	0%	Avira URL Cloud	safe	
http://71.244.60.231:4143/	0%	Avira URL Cloud	safe	
http://23.239.2.11:808/	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/%	0%	Avira URL Cloud	safe	
http://70.182.77.184:8090/sw	0%	Avira URL Cloud	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://70.184.125.132:8080/B	0%	Avira URL Cloud	safe	
http://194.88.246.242:443/	0%	Avira URL Cloud	safe	
http://184.180.177.28:8080/	0%	Avira URL Cloud	safe	
http://178.62.103.94:8080/	0%	Avira URL Cloud	safe	
http://164.160.161.118:8080/)Bo	0%	Avira URL Cloud	safe	
http://178.62.103.94:8080/I(s	0%	Avira URL Cloud	safe	
http://69.17.170.58/	0%	Avira URL Cloud	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.w3.o	0%	URL Reputation	safe	
http://76.72.225.30:465/0/u	0%	Avira URL Cloud	safe	
http://69.17.170.58/v	0%	Avira URL Cloud	safe	
http://70.182.77.184:8090/=#	0%	Avira URL Cloud	safe	
http://76.72.225.30:465/	0%	Avira URL Cloud	safe	
http://178.62.103.94:8080/60.231:4143/E	0%	Avira URL Cloud	safe	
http://69.17.170.58/E	0%	Avira URL Cloud	safe	
http://108.170.54.171:8080/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdng	svchost.exe, 00000026.00000003.825689349.0000024EB832A000.00000004.00000001.sdmp	false		high
http://78.47.182.42:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000010.00000002.312477867.000002A77143E000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 00000023.00000003.578478684.0000020499F6C000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.578518826.0000020499F88000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000010.00000002.312449752.000002A771424000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policyr	svchost.exe, 00000026.00000003.1148346365.0000024EB8381000.00000004.00000001.sdmp	false		high
http://72.45.212.62:8080/c(	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://189.236.94.20:995/m#	hyperlanes.exe, 00000006.00000003.481688344.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/Wizard/Password/Change?id=80601R	svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://Passport.NET/tbpose	svchost.exe, 00000026.00000003.1149031459.0000024EB8814000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://108.170.54.171:8080/8j#	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.311935000.000002A77144B000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdp://s	svchost.exe, 00000026.00000003.823424802.0000024EB832C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000010.00000003.312062878.000002A771441000.00000004.00000001.sdmp	false		high
http://72.45.212.62:8080/-	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

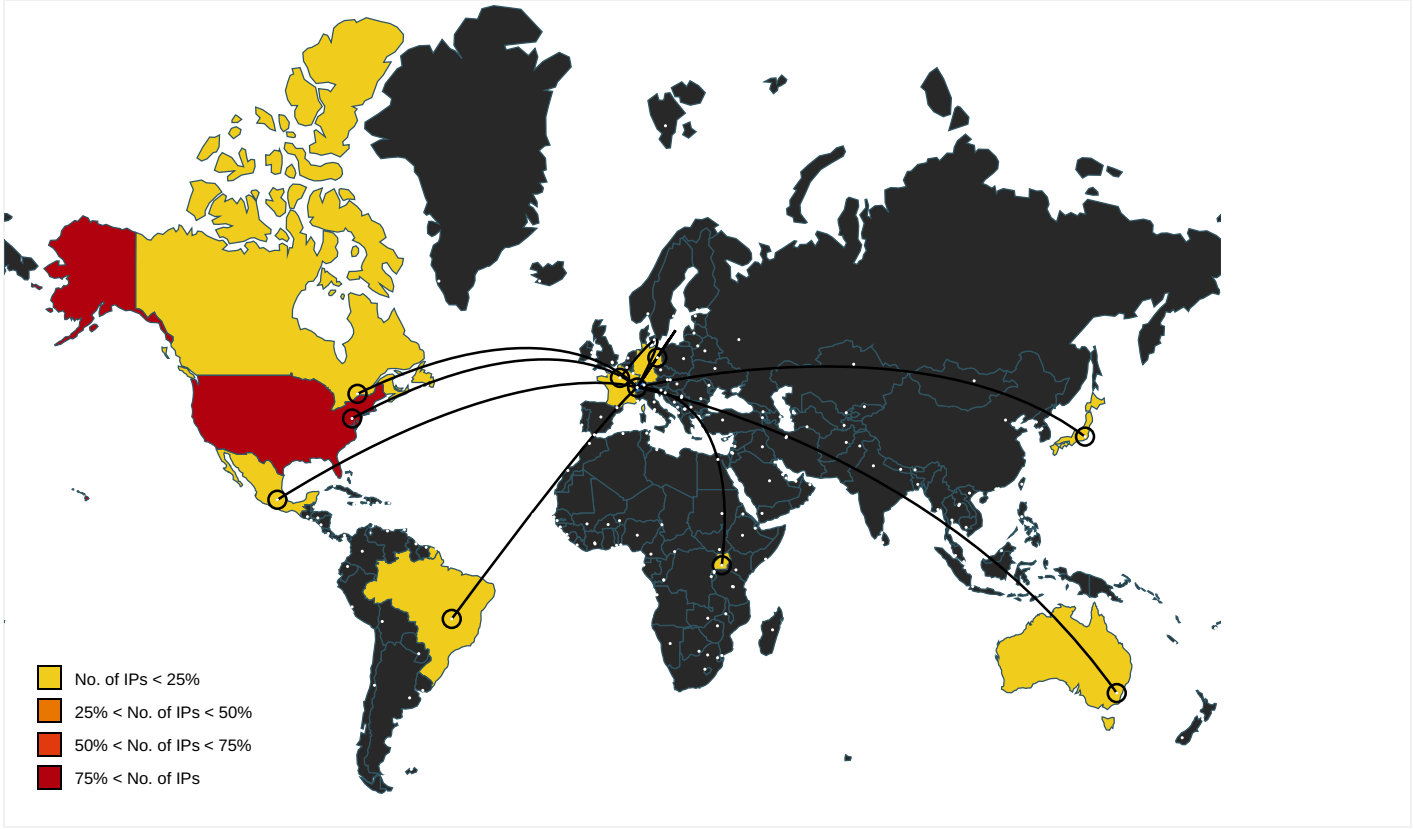
Name	Source	Malicious	Antivirus Detection	Reputation
http://108.170.54.171:8080/103.94:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdN	svchost.exe, 00000026.00000003.823424802.0000024EB832C000.00000004.00000001.sdmp	false		high
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 00000023.00000003.578478684.0000020499F6C000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.578518826.0000020499F88000.00000004.00000001.sdmp	false		high
http://https://account.live.com/InlineSignup.aspx?iww=1&id=80502	svchost.exe, 00000026.00000003.821431345.0000024EB8351000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000010.00000002.312434670.000002A771413000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://194.88.246.242:443/.177.28:8080/m	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://47.188.131.94:443/	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://164.160.161.118:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000003.312053370.000002A771445000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000010.00000002.312477867.000002A77143E000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/develop	svchost.exe, 00000023.00000003.578478684.0000020499F6C000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.578518826.0000020499F88000.00000004.00000001.sdmp	false		high
http://https://account.live.com/msangcwam	svchost.exe, 00000026.00000003.821214824.0000024EB8329000.00000004.00000001.sdmp, svchost.exe, 00000026.00000003.821478832.0000024EB832C000.00000004.00000001.sdmp, svchost.exe, 00000026.00000003.821469527.0000024EB8329000.00000004.00000001.sdmp, svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://passport.net/tb	svchost.exe, 00000026.00000002.1291561550.0000024EB7A7E000.00000004.00000001.sdmp, svchost.exe, 00000026.00000003.1148397347.0000024EB8819000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://corp.roblox.com/parents/	svchost.exe, 00000023.00000003.578478684.0000020499F6C000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.578518826.0000020499F88000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000002.312477867.000002A77143E000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.312434670.000002A771413000.00000004.00000001.sdmp	false		high
http://108.170.54.171:8080/M	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700 0.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 0000000E.00000002.1290004272.000002997EE3E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://70.182.77.184:8090/	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://108.170.54.171:8080/N	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsds	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603N	svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdptedD	svchost.exe, 00000026.00000003.825689349.0000024EB832A000.00000004.00000001.sdmp	false		high
http://194.88.246.242:443/;(	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://121.50.43.110:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000010.00000003.311901127.000002A77144D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000003.311935000.000002A77144B000.00000004.00000001.sdmp, svchost.exe, 00000010.00000003.312062878.000002A771441000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://76.72.225.30:465//	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp, svchost.exe, 00000026.00000003.827937050.000002 4EB7A8E000.00000004.00000001.sdmp	false		high
http://206.210.104.194/A	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdes	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issuessue	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000002.312490057.000002A771447000.00000004.00000001.sdmp	false		high
http://71.244.60.231:4143/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://23.239.2.11:808/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000003.311935000.000002A77144B000.00000004.00000001.sdmp	false		high
http://108.170.54.171:8080/%	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://70.182.77.184:8090/sw	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.mi	svchost.exe, 00000026.00000003.1148330747.0000024EB8307000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000010.00000002.312477867.000002A77143E000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80601y0	svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://70.184.125.132:8080/B	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://194.88.246.242:443/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000010.00000003.312062878.000002A771441000.00000004.00000001.sdmp	false		high
http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-saml-token-profile-1.0#SAMLAssertionID	svchost.exe, 00000026.00000003.827937050.0000024EB7A8E000.00000004.00000001.sdmp	false		high
http://184.180.177.28:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://178.62.103.94:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://164.160.161.118:8080/)Bo	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 00000023.00000003.569441527.000002049A402000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.569460119.0000020499F65000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.569472732.0000020499F54000.00000004.00000001.sdmp	false		high
http://178.62.103.94:8080/I(s	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://69.17.170.58/	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80600;	svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/schc=c	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://www.w3.o	svchost.exe, 00000026.00000003.826341450.0000024EB8358000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	svchost.exe, 00000026.00000003.827937050.0000024EB7A8E000.00000004.00000001.sdmp	false		high
http://76.72.225.30:465/0/u	hyperlanes.exe, 00000006.00000002.1290780450.000000000767000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsdxmldsi	svchost.exe, 00000026.00000003.1148330747.0000024EB8307000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://signup.live.com/signup.aspx	svchost.exe, 00000026.00000003.821469527.0000024EB8329000.00000004.00000001.sdmp, svchost.exe, 00000026.00000002.1291184647.0000024EB7A3D000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000002.312477867.000002A77143E000.00000004.00000001.sdmp, svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://69.17.170.58/v	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://70.182.77.184:8090/=#	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000010.00000003.311886865.000002A771460000.00000004.00000001.sdmp	false		high
http://76.72.225.30:465/	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80603	svchost.exe, 00000026.00000003.821478832.0000024EB832C000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 00000026.00000002.1292902175.0000024EB8337000.00000004.00000001.sdmp	false		high
http://178.62.103.94:8080/60.231:4143/E	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://69.17.170.58/E	hyperlanes.exe, 00000006.00000003.365988326.00000000007A1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80605	svchost.exe, 00000026.00000003.821214824.0000024EB8329000.00000004.00000001.sdmp, svchost.exe, 00000026.00000003.821478832.0000024EB832C000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000010.00000003.289950405.000002A771430000.00000004.00000001.sdmp	false		high
http://https://account.live.com/inlinesignup.aspx?iww=1&id=80604	svchost.exe, 00000026.00000003.821478832.0000024EB832C000.00000004.00000001.sdmp	false		high
http://108.170.54.171:8080/	hyperlanes.exe, 00000006.00000002.1290780450.000000000076700.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://instagram.com/hiddencity_	svchost.exe, 00000023.00000003.569441527.000002049A402000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.569460119.0000020499F65000.00000004.00000001.sdmp, svchost.exe, 00000023.00000003.569472732.0000020499F54000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000003.312053370.000002A771445000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.188.131.94	unknown	United States		5650	FRONTIER-FRTRUS	false
110.143.116.201	unknown	Australia		1221	ASN-TELSTRATelstraCorporation LtdAU	false
76.72.225.30	unknown	United States		53956	TOWNES-BROADBANDUS	false
164.160.161.118	unknown	Uganda		327717	SureTelecom-UG-ASUG	false
78.47.182.42	unknown	Germany		24940	HETZNER-ASDE	false
69.17.170.58	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
189.236.94.20	unknown	Mexico		8151	UninetSAdeCVMX	false
70.182.77.184	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
71.244.60.231	unknown	United States		5650	FRONTIER-FRTRUS	false
177.99.167.185	unknown	Brazil		18881	TELEFONICABRASILSABR	false
194.88.246.242	unknown	France		34177	CELESTE-ASCELESTE-InternetservicesproviderFR	false
23.239.2.11	unknown	United States		63949	LINODE-APLinodeLLCUS	false
184.180.177.28	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
206.210.104.194	unknown	Canada		33130	IASLCA	false
178.62.103.94	unknown	European Union		14061	DIGITALOCEAN-ASNUS	false
24.217.117.217	unknown	United States		20115	CHARTER-20115US	false
72.45.212.62	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
121.50.43.110	unknown	Japan		63997	TSUKAERUNETTsukaerunetWebHostingCompanyJapanJP	false
66.76.26.33	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
46.4.100.178	unknown	Germany		24940	HETZNER-ASDE	false
70.184.125.132	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	405975
Start date:	06.05.2021
Start time:	15:30:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uIsv6VTOek (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:	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:	mal88.troj.evad.winEXE@22/9@0/23
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 51.9% (good quality ratio 41.6%) • Quality average: 67.5% • Quality standard deviation: 38.7%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 92.122.145.220, 168.61.161.212, 13.64.90.137, 40.88.32.150, 184.30.24.56, 20.82.210.154, 8.238.85.254, 8.241.90.126, 8.238.29.126, 8.241.82.126, 8.238.27.126, 92.122.213.247, 92.122.213.194, 20.54.26.129, 20.82.209.183, 52.155.217.156, 20.190.160.132, 20.190.160.75, 20.190.160.134, 20.190.160.73, 20.190.160.71, 20.190.160.6, 20.190.160.2, 20.190.160.4, 51.104.136.2, 20.49.150.241, 40.126.31.6, 40.126.31.4, 40.126.31.139, 20.190.159.134, 20.190.159.138, 40.126.31.8, 20.190.159.132, 40.126.31.135 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, ams2.current.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/405975/sample/uIsv6VTOek.exe

Simulations

Behavior and APIs

Time	Type	Description
15:32:09	API Interceptor	13x Sleep call for process: svchost.exe modified
15:33:26	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
47.188.131.94	http://www.bilginerotoekspertiz.com/DOC/Order-35988251857/	Get hash	malicious	Browse	• 47.188.131.94:443/
	547815.exe	Get hash	malicious	Browse	• 47.188.131.94:443/
110.143.116.201	EMOTET.EXE	Get hash	malicious	Browse	• 110.143.116.201/
69.17.170.58	RFG-INV-44654524697988.doc	Get hash	malicious	Browse	• 69.17.170.58/
	Invoice-0159595.doc	Get hash	malicious	Browse	• 69.17.170.58/
	Invoice-0159595.doc	Get hash	malicious	Browse	• 69.17.170.58/
	Emotet.doc	Get hash	malicious	Browse	• 69.17.170.58/
	Zahlungserinnerung-vom-Juni.doc	Get hash	malicious	Browse	• 69.17.170.58/
	Rechnung-fur-Zahlung-080-438.doc	Get hash	malicious	Browse	• 69.17.170.58/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	43b5d336_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	FileZilla_3.53.1_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 49.12.121.47
	c46bd0ae_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	01dfc6c9_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	8007ff84_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	fd1dbef7_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	903930a7_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	zd1uT5UZFn1.dll	Get hash	malicious	Browse	• 188.40.137.206
	80f0e076_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	5af88031_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	db8e6a08_by_Libranalysis.exe	Get hash	malicious	Browse	• 95.216.186.40
	d4812def_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	viruss.xlsb	Get hash	malicious	Browse	• 95.216.186.40
	afbb944a_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	file.msg.exe	Get hash	malicious	Browse	• 138.201.223.6
	e24a2e43_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	4ee2bc17_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	6de01617_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	a7813732_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
	c8752ee0_by_Libranalysis.dll	Get hash	malicious	Browse	• 188.40.137.206
ASN-TELSTRATelstraCorporationLtdAU	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 101.187.197.33
	KnAY2OIPI3	Get hash	malicious	Browse	• 1.151.13.11
	x86_unpacked	Get hash	malicious	Browse	• 1.153.223.118
	ppc_unpacked	Get hash	malicious	Browse	• 1.126.33.34
	rIbyGX66Op	Get hash	malicious	Browse	• 203.49.228.158
	MGuvcs6Ocz	Get hash	malicious	Browse	• 139.130.197.234
	4JQil8gLKd	Get hash	malicious	Browse	• 124.177.182.198
	z3hir.x86	Get hash	malicious	Browse	• 1.150.156.5
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 110.145.101.66
	2ojdmC51As.exe	Get hash	malicious	Browse	• 110.142.236.207
	3kDM9S0iGA.exe	Get hash	malicious	Browse	• 124.182.146.41
	networkmanager	Get hash	malicious	Browse	• 203.46.154.161
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 110.142.236.207
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 144.139.47.206
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 101.184.48.99
	utox.exe	Get hash	malicious	Browse	• 1.132.105.157

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 101.187.176.67
	e5ad48f310b56ceb013a30be125d967e.exe	Get hash	malicious	Browse	• 139.130.242.43
	fIk5kbvEeK.exe	Get hash	malicious	Browse	• 139.130.242.43
	xESLg6TBHK.exe	Get hash	malicious	Browse	• 139.130.242.43
FRONTIER-FRTRUS	9cf2c56e_by_Libranalysis.exe	Get hash	malicious	Browse	• 47.148.241.179
	nT7K5GG5km	Get hash	malicious	Browse	• 72.87.194.121
	KnAY2OIPI3	Get hash	malicious	Browse	• 96.254.228.27
	JRyLnlTR1O	Get hash	malicious	Browse	• 47.207.20.144
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 47.144.21.37
	YPJ9DZYIpO	Get hash	malicious	Browse	• 47.206.88.151
	sample.exe.exe	Get hash	malicious	Browse	• 71.244.60.231
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 71.244.60.231
	PDFXCview.exe	Get hash	malicious	Browse	• 50.45.114.178
	#Ud83d#Udd04bvoneida- empirix.com iPhone 8 104 OKeep.htm	Get hash	malicious	Browse	• 184.24.29.126
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 47.146.169.85
	bin.sh	Get hash	malicious	Browse	• 172.95.177.246
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 50.121.246.26
	NormhjTcQb.exe	Get hash	malicious	Browse	• 47.148.117.234
	Astra.x86	Get hash	malicious	Browse	• 50.123.44.24
	4F58TLaSSt.exe	Get hash	malicious	Browse	• 184.24.28.12
	8uOajLllk2.exe	Get hash	malicious	Browse	• 47.146.32.175
	s4dz16MUhV.exe	Get hash	malicious	Browse	• 47.146.117.214
	IKp3ziFZtQ.exe	Get hash	malicious	Browse	• 47.146.32.175
	NCqZWgrjZ7.exe	Get hash	malicious	Browse	• 47.146.32.175

JA3 Fingerprints

No context

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):	0.2407788896284114
Encrypted:	false
SSDEEP:	12:0GlGaD0JcaaD0JwQQcFAg/0bjSQJT/4fsw/u1i/psw/u1i/:0GrgJctgJwE2rjSuTQfMYM

C:\ProgramData\Microsoft\Network\Downloader\edb.log

MD5:	59F29336D8CCDDB572055250699C7612
SHA1:	143F81BF34DA2DB957B08617121D228A24C035D2
SHA-256:	24D8E0D438DE0F84F38B40B8A10122B53DD03F3045A8623D09778B1AD74E763F
SHA-512:	6BE72B3CBF17EE77C9398A4CCFFFA7CB38E9023F1CEDF574531504377732209A98C8B8205460A46BA9F0BC9E9812CBFC63C59C96BCF099419BFDA17057AB354 1
Malicious:	false
Preview:	.....:{..(..... ...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@..... ...y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9c40291d, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.09680244578901817
Encrypted:	false
SSDEEP:	24:Botplx+1otplx+Woo+Woo+dPorL+dPorL+W1V1:U/vv3L3LbT
MD5:	46FB2F4EE273F10F4AA9BADBCAF8404F
SHA1:	4B2E3156300C476B026B757605CE1FD617EC07DD
SHA-256:	BE7C68A545D9A5FFE77295F090AD6F0B02499752C9E263818AE0C0E63FD876BC
SHA-512:	C774FE3988C205DCE428E6E2357BA5AABF80EF82DECA7745F82035E282B81F16690A51A3357960CFDC42817266A55ADC6F4AF257DEE9C1D4B01694A9F6BE89A 0
Malicious:	false
Preview:	.@).... .....e.f.3...w.....&.....w... ...y..h.(.....3...w.....B.....@..... ....3...w..... .....]... ...y.k.....y~.. ...y..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	SysEx File - SIEL
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.11527357190504775
Encrypted:	false
SSDEEP:	6:B/isS4MAt4fAzjGeDsS4MAPHQ+AFktKufktKFGxPXsS4MAtcxKwgtKuXbFGo9ZrQ:w8t4Y+084Diz82YPN8tZzJbqnzl8
MD5:	D6FC88F453AC93BEA35CDCE51D2A23FE
SHA1:	DE1372E1230912E563952F699AD65C8F1BB07EAF
SHA-256:	298D2A34DEF3F485107F758A34E1A8EA1B37CF6F219C2F028A024AA4D26F0A16
SHA-512:	42D18ECF68F3D74E9C42BDC1020C0862A7668EF2956F46A60C1B29867D484FA847597F8B3C7E107226FEC161744A9B76F78B522C2BC0FA7B287776E5F5F61611
Malicious:	false
Preview:	.!.f.....3...w... ...y.....w.....w.....w....:O.....w.....y~.. ...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):	0.10972430036902728
Encrypted:	false
SSDEEP:	12:26ZVXm/Ey6q9995UPNAlq3qQ10nMCldimE8eawHjchvd:26Z4l68CPBLyMCldzE9BHjchvd
MD5:	AB02BDAFBDD1AF497A3C7517EAA4D6C0
SHA1:	4501975BA9B4AA490A8F524D8B79B79E3D62E42E
SHA-256:	8EAA28439AF197B63F219FCF0701876A80DFD45D9C3606407BFC74B1EE0DD232
SHA-512:	C18359193860ED77E5C36FF146871972109CB6526994DBEB77462B93760B24E64DEC8F98DEDA59752493A6B1F8DC6A6F92A2BCF955DA13D69BE1B54CC9AA738
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Preview:	.....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.....M...1..... .....N..B.....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.....!..... ....

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):	0.1123908352906178
Encrypted:	false
SSDEEP:	12:cllzXm/Ey6q9995UPN4z1miM3qQ10nMCldimE8eawHza1miIu:Uwl68CPO1tMLyMCldzE9BHza1tIu
MD5:	335B52834DE3F6A97A92E6574E91EF0F
SHA1:	45471CA804AC819E13C84769CD1512A188DAC4D8
SHA-256:	03A3AB47E6C45C566856ABC663EFD7184B17D774F6CC47A6858CD4B5415F1576
SHA-512:	C0C8FBECE83F271D10B3D217446F3363A869BF773ABE2C67138CD38012BD35BA8BC01518AC569705F7BB14A4B173A4B1BD194B9820D9260F43BD016CBFEF3B4 5
Malicious:	false
Preview:	.....t.....CP .....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....M...1..... .....)..B.....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.....Y ....

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):	0.11220629493205327
Encrypted:	false
SSDEEP:	12:vFXm/Ey6q9995UPNM0z1mK2P3qQ10nMCldimE8eawHza1mKWn:Ql68CPb1iPLyMCldzE9BHza1Q
MD5:	2F98EEBBA7D8F12F08260881A89A76A1
SHA1:	525A7FE2D38794BFB7F405681458F80DC398F4BF
SHA-256:	BF1D755170FB80D875AD407EDDE97A362D30F62370DE27371A20B9F38EE47856
SHA-512:	E96188104FBEEADACEAAFECE62A69B872F19F6FDF813F9793DD5844EECD659F08208789E412469B72AAD16074FF9B87DAD9C6FF9BED7986AF9BC00B2723639 C
Malicious:	false
Preview:	.....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.....M...1..... .....B.....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.....L..... ....

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Size (bytes):	906
Entropy (8bit):	3.161054860519664
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rXxk9+MlWlLehB4yAq7ejCSQ:OaqdmuF3rG+kWReH4yJ7M4
MD5:	92028ECC4C8EAA2B257E7376C94A3D33
SHA1:	19A4A84D023301E8786F1092F04D0CD8AA5C7EB3
SHA-256:	5BFDE5226D832276F0DAD46A5D7963580A84C5370B0720C396CB844EFA43AB19
SHA-512:	B1984487375F80E340964733C1BD32F7B6874D94F47D51DD7C77B10FF837A832FC0D99C3F92E00C59B59411368DB40DAC49F442D0BE30451BEC3F2A985246E43
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.:. .. T.h.u. .. M.a.y. .. 0.6. .. 2.0.2.1. .1.5.:.3.3.:.2. 6.........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.:. .. T.h.u. .. M.a.y. .. 0.6. .. 2.0.2.1. .1.5.:.3.3.:.2.6.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.86734896093207
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:	uIsv6VTOek.exe
File size:	126976
MD5:	3ee16bbc971bceb22c5ea3b79f8f711d
SHA1:	f20112dd192c7ec6fbf1a3772769c833f60433b7
SHA256:	982a1c7af717a51a2b5a661b7e4d0e0d63565e80e9a74e76b33fe416076ee86b
SHA512:	b76b9408f50f34793a4b610dbaa19127f2f73238f7175700 57d1dc732800cb1707e1e8c9c82ccdf0287ece78310880 4dd7f7cbfa9ea7e9f560f198c57e5bc320
SSDEEP:	3072:VITbjGFrTPdoAfkIIxphNq7PfyEPpUWDzX:iTbid5IfPGPf
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......?..({..{{..{{..{r.G{j..{{..{f..{{..{z..{v..{z..{v..{z..{Rich{..{........PE..L.....+[.................`........................@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4014d1
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5B2BFACA [Thu Jun 21 19:21:46 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5

General	
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	edb14a960a2b14879d5a7c17f2162ccc

Entrypoint Preview

Instruction
push ebp
push ebx
mov eax, 00000056h
lea ecx, dword ptr [00415B22h]
mov dword ptr [ecx+eax], esi
mov eax, 001F56BEh
mov ecx, dword ptr [esp+04h]
lea edx, dword ptr [002204C6h]
mov dword ptr [edx+eax], ecx
mov ecx, esp
inc ecx
xchg eax, ecx
inc eax
lea edx, dword ptr [0040F7D5h]
add eax, 07h
xor ecx, ecx
add ecx, 000063B3h
dec eax
mov dword ptr [edx+ecx], eax
lea edx, dword ptr [00415B7Ch]
mov dword ptr [edx], edi
lea edx, dword ptr [00415B7Eh]
inc edx
pop ecx
inc edx
mov dword ptr [edx], ecx
pop eax
call 00007F0344B09323h
test eax, eax
call 00007F0344B093C6h
mov eax, 00000001h
ret
mov dword ptr [ebp-04h], eax
int3
push ebp
mov ebp, esp
push esi
and esp, FFFFFFF8h
sub esp, 28h
mov eax, dword ptr [ebp+08h]
mov dword ptr [esp+14h], 44134E68h
mov ecx, dword ptr [esp+18h]
mov edx, dword ptr [esp+1Ch]
mov esi, 01E48E3Ch
mov dword ptr [esp+0Ch], eax
mov eax, ecx
mov dword ptr [esp+08h], edx
mul esi
mov ecx, dword ptr [esp+08h]
imul ecx, ecx, 01E48E3Ch
add edx, ecx
mov dword ptr [esp+18h], eax
mov dword ptr [esp+1Ch], edx
mov dword ptr [esp+10h], 1BBA1F5Bh
mov eax, dword ptr [esp+10h]
mov ecx, dword ptr [esp+14h]

Instruction
mov edx, dword ptr [esp+0Ch]
mov esi, dword ptr [edx+3Ch]
xor ecx, 68E6DF45h
cmp eax, ecx

Rich Headers

Programming Language:	• [RES] VS2013 build 21005 • [LNK] VS2013 build 21005 • [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	0x4fec	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x8bf8	.pdata
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x40	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x40a0	0x38	.rdata
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	0x4000	0x94	.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	0x228c	0x3000	False	0.456787109375	data	5.14396711885	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x13d2	0x2000	False	0.155639648438	data	4.41665254462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x10b8c	0x10000	False	0.882965087891	data	7.87710670899	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x17000	0x8bf8	0x9000	False	0.331814236111	data	5.02661516801	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x17790	0x2028	data	French	France
RT_BITMAP	0x197b8	0x33d0	data	French	France
RT_BITMAP	0x1cb88	0xb8	data	English	United States
RT_BITMAP	0x1cc40	0x144	data	English	United States
RT_MENU	0x1cd88	0x19a	data	English	United States
RT_DIALOG	0x1cf28	0x1f2	data	English	United States
RT_DIALOG	0x1d120	0x286	data	French	France
RT_DIALOG	0x1d3a8	0xe8	data	English	United States
RT_DIALOG	0x1d490	0x34	data	English	United States
RT_STRING	0x1d4c8	0xe0	data	English	United States
RT_STRING	0x1d5a8	0x46	data	English	United States
RT_STRING	0x1d5f0	0x3c	data	English	United States
RT_STRING	0x1d630	0x166	data	English	United States
RT_STRING	0x1d798	0x260	data	English	United States
RT_STRING	0x1d9f8	0x328	data	English	United States
RT_STRING	0x1dd20	0x70	data	English	United States
RT_STRING	0x1dd90	0x106	data	English	United States
RT_STRING	0x1de98	0xda	data	English	United States
RT_STRING	0x1df78	0x46	data	English	United States
RT_STRING	0x1dfc0	0x78	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x1e038	0x1f8	data	English	United States
RT_STRING	0x1e230	0x86	data	English	United States
RT_STRING	0x1e2b8	0x82	data	English	United States
RT_STRING	0x1e340	0x2a	data	English	United States
RT_STRING	0x1e370	0x184	data	English	United States
RT_STRING	0x1e4f8	0x4e6	data	English	United States
RT_STRING	0x1e9e0	0x264	data	English	United States
RT_STRING	0x1ec48	0x2da	data	English	United States
RT_STRING	0x1ef28	0x8a	data	English	United States
RT_STRING	0x1efb8	0xac	data	English	United States
RT_STRING	0x1f068	0xde	data	English	United States
RT_STRING	0x1f148	0x4a8	data	English	United States
RT_STRING	0x1f5f0	0x228	data	English	United States
RT_STRING	0x1f818	0x2c	data	English	United States
RT_STRING	0x1f848	0x42	data	English	United States
RT_ACCELERATOR	0x1f890	0x68	data	English	United States
RT_VERSION	0x1f8f8	0x300	data	English	United States

Imports

DLL	Import
ole32.dll	CreateBindCtx
ADVAPI32.dll	GetPrivateObjectSecurity, AdjustTokenPrivileges, ReadEventLogA
MPRAPI.dll	MprInfoBlockRemove
USER32.dll	keybd_event, MonitorFromRect, DdeImpersonateClient, ArrangeIconicWindows, GetSystemMenu, GetSysColor, CountClipboardFormats, GetMenuInfo, GetScrollBarInfo, GetMessagePos, CharNextA, SetSystemCursor, IsZoomed
KERNEL32.dll	QueueUserWorkItem, CloseHandle, GetSystemTimeAsFileTime, GetHandleInformation, GetCommProperties, UnregisterApplicationRecoveryCallback, GetLogicalProcessorInformation, FreeUserPhysicalPages, InitializeCriticalSection, LocalReAlloc
SHLWAPI.dll	UrlUnescapeW
msvcrt.dll	fsetpos

Version Infos

Description	Data
LegalCopyright	(c)2008-2018 CPUID. All rights reserved.
InternalName	HWMonitor.exe
FileVersion	1, 3, 5, 0
CompanyName	CPUID
ProductName	CPUID Hardware Monitor
ProductVersion	1, 3, 5, 0
FileDescription	HWMonitor
OriginalFilename	HWMonitor.exe
Translation	0x0409 0x04e4

Possible Origin

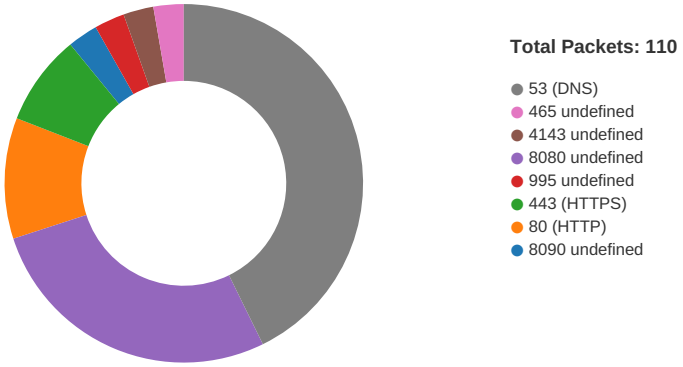
Language of compilation system	Country where language is spoken	Map
French	France	
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/06/21-15:33:57.561381	ICMP	399	ICMP Destination Unreachable Host Unreachable			173.219.152.57	192.168.2.3
05/06/21-15:37:49.216521	ICMP	399	ICMP Destination Unreachable Host Unreachable			83.118.200.66	192.168.2.3
05/06/21-15:37:52.735997	ICMP	399	ICMP Destination Unreachable Host Unreachable			83.118.200.66	192.168.2.3
05/06/21-15:37:59.536302	ICMP	399	ICMP Destination Unreachable Host Unreachable			83.118.200.66	192.168.2.3
05/06/21-15:39:10.098463	ICMP	449	ICMP Time-To-Live Exceeded in Transit			67.223.195.94	192.168.2.3
05/06/21-15:39:13.098340	ICMP	449	ICMP Time-To-Live Exceeded in Transit			67.223.195.94	192.168.2.3
05/06/21-15:39:19.099356	ICMP	449	ICMP Time-To-Live Exceeded in Transit			67.223.195.94	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 15:32:06.226484060 CEST	49713	8090	192.168.2.3	70.182.77.184
May 6, 2021 15:32:09.381048918 CEST	49713	8090	192.168.2.3	70.182.77.184
May 6, 2021 15:32:15.381580114 CEST	49713	8090	192.168.2.3	70.182.77.184
May 6, 2021 15:32:30.353677988 CEST	49724	80	192.168.2.3	69.17.170.58
May 6, 2021 15:32:33.390436888 CEST	49724	80	192.168.2.3	69.17.170.58
May 6, 2021 15:32:39.399202108 CEST	49724	80	192.168.2.3	69.17.170.58
May 6, 2021 15:33:00.394772053 CEST	49731	443	192.168.2.3	47.188.131.94
May 6, 2021 15:33:03.401187897 CEST	49731	443	192.168.2.3	47.188.131.94
May 6, 2021 15:33:09.401762009 CEST	49731	443	192.168.2.3	47.188.131.94
May 6, 2021 15:33:24.382530928 CEST	49737	995	192.168.2.3	189.236.94.20
May 6, 2021 15:33:27.387609005 CEST	49737	995	192.168.2.3	189.236.94.20
May 6, 2021 15:33:33.388103962 CEST	49737	995	192.168.2.3	189.236.94.20
May 6, 2021 15:33:54.378822088 CEST	49740	8080	192.168.2.3	66.76.26.33
May 6, 2021 15:33:57.390093088 CEST	49740	8080	192.168.2.3	66.76.26.33
May 6, 2021 15:34:03.390820980 CEST	49740	8080	192.168.2.3	66.76.26.33
May 6, 2021 15:34:18.375349045 CEST	49741	80	192.168.2.3	24.217.117.217
May 6, 2021 15:34:21.376645088 CEST	49741	80	192.168.2.3	24.217.117.217
May 6, 2021 15:34:27.377099037 CEST	49741	80	192.168.2.3	24.217.117.217
May 6, 2021 15:34:48.341793060 CEST	49752	80	192.168.2.3	110.143.116.201
May 6, 2021 15:34:51.343286037 CEST	49752	80	192.168.2.3	110.143.116.201
May 6, 2021 15:34:57.359481096 CEST	49752	80	192.168.2.3	110.143.116.201
May 6, 2021 15:35:12.282279968 CEST	49753	8080	192.168.2.3	46.4.100.178
May 6, 2021 15:35:12.355421066 CEST	8080	49753	46.4.100.178	192.168.2.3
May 6, 2021 15:35:12.860743999 CEST	49753	8080	192.168.2.3	46.4.100.178
May 6, 2021 15:35:12.933458090 CEST	8080	49753	46.4.100.178	192.168.2.3
May 6, 2021 15:35:13.438909054 CEST	49753	8080	192.168.2.3	46.4.100.178

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 15:35:13.512145042 CEST	8080	49753	46.4.100.178	192.168.2.3
May 6, 2021 15:35:20.568487883 CEST	49754	8080	192.168.2.3	23.239.2.11
May 6, 2021 15:35:20.767519951 CEST	8080	49754	23.239.2.11	192.168.2.3
May 6, 2021 15:35:21.283335924 CEST	49754	8080	192.168.2.3	23.239.2.11
May 6, 2021 15:35:21.482458115 CEST	8080	49754	23.239.2.11	192.168.2.3
May 6, 2021 15:35:21.986831903 CEST	49754	8080	192.168.2.3	23.239.2.11
May 6, 2021 15:35:22.185918093 CEST	8080	49754	23.239.2.11	192.168.2.3
May 6, 2021 15:35:28.955775023 CEST	49755	80	192.168.2.3	206.210.104.194
May 6, 2021 15:35:31.956150055 CEST	49755	80	192.168.2.3	206.210.104.194
May 6, 2021 15:35:37.956674099 CEST	49755	80	192.168.2.3	206.210.104.194
May 6, 2021 15:35:57.549324036 CEST	49756	8080	192.168.2.3	70.184.125.132
May 6, 2021 15:36:00.552290916 CEST	49756	8080	192.168.2.3	70.184.125.132
May 6, 2021 15:36:06.552738905 CEST	49756	8080	192.168.2.3	70.184.125.132
May 6, 2021 15:36:27.669280052 CEST	49757	443	192.168.2.3	177.99.167.185
May 6, 2021 15:36:30.679811001 CEST	49757	443	192.168.2.3	177.99.167.185
May 6, 2021 15:36:36.695914030 CEST	49757	443	192.168.2.3	177.99.167.185
May 6, 2021 15:36:51.982399940 CEST	49763	8080	192.168.2.3	184.180.177.28
May 6, 2021 15:36:54.994450092 CEST	49763	8080	192.168.2.3	184.180.177.28
May 6, 2021 15:37:00.995119095 CEST	49763	8080	192.168.2.3	184.180.177.28
May 6, 2021 15:37:22.571062088 CEST	49764	8080	192.168.2.3	164.160.161.118
May 6, 2021 15:37:25.575104952 CEST	49764	8080	192.168.2.3	164.160.161.118
May 6, 2021 15:37:31.575604916 CEST	49764	8080	192.168.2.3	164.160.161.118
May 6, 2021 15:37:47.713290930 CEST	49765	443	192.168.2.3	194.88.246.242
May 6, 2021 15:37:50.717812061 CEST	49765	443	192.168.2.3	194.88.246.242
May 6, 2021 15:37:56.734081030 CEST	49765	443	192.168.2.3	194.88.246.242
May 6, 2021 15:38:11.055357933 CEST	49766	4143	192.168.2.3	71.244.60.231
May 6, 2021 15:38:14.063576937 CEST	49766	4143	192.168.2.3	71.244.60.231
May 6, 2021 15:38:20.064596891 CEST	49766	4143	192.168.2.3	71.244.60.231
May 6, 2021 15:38:39.677284956 CEST	49767	8080	192.168.2.3	121.50.43.110
May 6, 2021 15:38:42.690911055 CEST	49767	8080	192.168.2.3	121.50.43.110
May 6, 2021 15:38:48.691518068 CEST	49767	8080	192.168.2.3	121.50.43.110
May 6, 2021 15:39:09.943407059 CEST	49770	465	192.168.2.3	76.72.225.30
May 6, 2021 15:39:12.943531036 CEST	49770	465	192.168.2.3	76.72.225.30
May 6, 2021 15:39:18.943975925 CEST	49770	465	192.168.2.3	76.72.225.30
May 6, 2021 15:39:34.473211050 CEST	49771	8080	192.168.2.3	78.47.182.42
May 6, 2021 15:39:34.541766882 CEST	8080	49771	78.47.182.42	192.168.2.3
May 6, 2021 15:39:35.060199022 CEST	49771	8080	192.168.2.3	78.47.182.42
May 6, 2021 15:39:35.131546974 CEST	8080	49771	78.47.182.42	192.168.2.3
May 6, 2021 15:39:35.632915974 CEST	49771	8080	192.168.2.3	78.47.182.42
May 6, 2021 15:39:35.701473951 CEST	8080	49771	78.47.182.42	192.168.2.3
May 6, 2021 15:39:43.959913969 CEST	49773	8080	192.168.2.3	72.45.212.62
May 6, 2021 15:39:46.962094069 CEST	49773	8080	192.168.2.3	72.45.212.62
May 6, 2021 15:39:52.963308096 CEST	49773	8080	192.168.2.3	72.45.212.62
May 6, 2021 15:40:06.485764980 CEST	49774	8080	192.168.2.3	178.62.103.94
May 6, 2021 15:40:06.544408083 CEST	8080	49774	178.62.103.94	192.168.2.3
May 6, 2021 15:40:07.057568073 CEST	49774	8080	192.168.2.3	178.62.103.94
May 6, 2021 15:40:07.115298033 CEST	8080	49774	178.62.103.94	192.168.2.3
May 6, 2021 15:40:07.620249987 CEST	49774	8080	192.168.2.3	178.62.103.94
May 6, 2021 15:40:07.679455996 CEST	8080	49774	178.62.103.94	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 15:31:38.084664106 CEST	51281	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:38.133375883 CEST	53	51281	8.8.8.8	192.168.2.3
May 6, 2021 15:31:38.875128031 CEST	49199	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:38.924026966 CEST	53	49199	8.8.8.8	192.168.2.3
May 6, 2021 15:31:40.135498047 CEST	50620	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:40.188798904 CEST	53	50620	8.8.8.8	192.168.2.3
May 6, 2021 15:31:40.734615088 CEST	64938	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:40.797544003 CEST	53	64938	8.8.8.8	192.168.2.3
May 6, 2021 15:31:41.047353983 CEST	60152	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:41.104626894 CEST	53	60152	8.8.8.8	192.168.2.3
May 6, 2021 15:31:42.999820948 CEST	57544	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 15:31:43.051486969 CEST	53	57544	8.8.8.8	192.168.2.3
May 6, 2021 15:31:43.890919924 CEST	55984	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:43.942557096 CEST	53	55984	8.8.8.8	192.168.2.3
May 6, 2021 15:31:44.992003918 CEST	64185	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:45.041794062 CEST	53	64185	8.8.8.8	192.168.2.3
May 6, 2021 15:31:51.530123949 CEST	65110	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:51.579452038 CEST	53	65110	8.8.8.8	192.168.2.3
May 6, 2021 15:31:52.418654919 CEST	58361	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:52.472273111 CEST	53	58361	8.8.8.8	192.168.2.3
May 6, 2021 15:31:53.620870113 CEST	63492	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:53.671596050 CEST	53	63492	8.8.8.8	192.168.2.3
May 6, 2021 15:31:54.686939001 CEST	60831	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:54.739104033 CEST	53	60831	8.8.8.8	192.168.2.3
May 6, 2021 15:31:56.001687050 CEST	60100	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:56.074513912 CEST	53	60100	8.8.8.8	192.168.2.3
May 6, 2021 15:31:57.433892012 CEST	53195	53	192.168.2.3	8.8.8.8
May 6, 2021 15:31:57.493952036 CEST	53	53195	8.8.8.8	192.168.2.3
May 6, 2021 15:32:05.116862059 CEST	50141	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:05.177787066 CEST	53	50141	8.8.8.8	192.168.2.3
May 6, 2021 15:32:06.224091053 CEST	53023	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:06.273238897 CEST	53	53023	8.8.8.8	192.168.2.3
May 6, 2021 15:32:07.007700920 CEST	49563	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:07.056502104 CEST	53	49563	8.8.8.8	192.168.2.3
May 6, 2021 15:32:08.144681931 CEST	51352	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:08.194434881 CEST	53	51352	8.8.8.8	192.168.2.3
May 6, 2021 15:32:09.481647015 CEST	59349	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:09.530811071 CEST	53	59349	8.8.8.8	192.168.2.3
May 6, 2021 15:32:10.925484896 CEST	57084	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:10.974401951 CEST	53	57084	8.8.8.8	192.168.2.3
May 6, 2021 15:32:12.965795994 CEST	58823	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:13.019792080 CEST	53	58823	8.8.8.8	192.168.2.3
May 6, 2021 15:32:18.144351959 CEST	57568	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:18.210285902 CEST	53	57568	8.8.8.8	192.168.2.3
May 6, 2021 15:32:32.761187077 CEST	50540	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:32.818281889 CEST	53	50540	8.8.8.8	192.168.2.3
May 6, 2021 15:32:38.214631081 CEST	54366	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:38.268451929 CEST	53	54366	8.8.8.8	192.168.2.3
May 6, 2021 15:32:48.135454893 CEST	53034	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:48.201159000 CEST	53	53034	8.8.8.8	192.168.2.3
May 6, 2021 15:32:58.309468031 CEST	57762	53	192.168.2.3	8.8.8.8
May 6, 2021 15:32:58.381560087 CEST	53	57762	8.8.8.8	192.168.2.3
May 6, 2021 15:33:02.390981913 CEST	55435	53	192.168.2.3	8.8.8.8
May 6, 2021 15:33:02.450048923 CEST	53	55435	8.8.8.8	192.168.2.3
May 6, 2021 15:33:33.531208038 CEST	50713	53	192.168.2.3	8.8.8.8
May 6, 2021 15:33:33.590696096 CEST	53	50713	8.8.8.8	192.168.2.3
May 6, 2021 15:33:35.228432894 CEST	56132	53	192.168.2.3	8.8.8.8
May 6, 2021 15:33:35.305547953 CEST	53	56132	8.8.8.8	192.168.2.3
May 6, 2021 15:34:31.326277018 CEST	58987	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:31.477597952 CEST	53	58987	8.8.8.8	192.168.2.3
May 6, 2021 15:34:32.444911003 CEST	56579	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:32.633549929 CEST	53	56579	8.8.8.8	192.168.2.3
May 6, 2021 15:34:34.232649088 CEST	60633	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:34.290153980 CEST	53	60633	8.8.8.8	192.168.2.3
May 6, 2021 15:34:34.798852921 CEST	61292	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:34.848334074 CEST	53	61292	8.8.8.8	192.168.2.3
May 6, 2021 15:34:35.427118063 CEST	63619	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:35.596689939 CEST	53	63619	8.8.8.8	192.168.2.3
May 6, 2021 15:34:36.228682995 CEST	64938	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:36.342725039 CEST	53	64938	8.8.8.8	192.168.2.3
May 6, 2021 15:34:36.853194952 CEST	61946	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:36.902080059 CEST	53	61946	8.8.8.8	192.168.2.3
May 6, 2021 15:34:37.736552000 CEST	64910	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:37.794832945 CEST	53	64910	8.8.8.8	192.168.2.3
May 6, 2021 15:34:39.016161919 CEST	52123	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 6, 2021 15:34:39.081379890 CEST	53	52123	8.8.8.8	192.168.2.3
May 6, 2021 15:34:39.661691904 CEST	56130	53	192.168.2.3	8.8.8.8
May 6, 2021 15:34:39.721920967 CEST	53	56130	8.8.8.8	192.168.2.3
May 6, 2021 15:36:33.250901937 CEST	56338	53	192.168.2.3	8.8.8.8
May 6, 2021 15:36:33.299753904 CEST	53	56338	8.8.8.8	192.168.2.3
May 6, 2021 15:36:33.873608112 CEST	59420	53	192.168.2.3	8.8.8.8
May 6, 2021 15:36:33.930630922 CEST	53	59420	8.8.8.8	192.168.2.3
May 6, 2021 15:36:35.239774942 CEST	58784	53	192.168.2.3	8.8.8.8
May 6, 2021 15:36:35.299114943 CEST	53	58784	8.8.8.8	192.168.2.3
May 6, 2021 15:36:36.385766029 CEST	63978	53	192.168.2.3	8.8.8.8
May 6, 2021 15:36:36.451849937 CEST	53	63978	8.8.8.8	192.168.2.3
May 6, 2021 15:36:36.698124886 CEST	62938	53	192.168.2.3	8.8.8.8
May 6, 2021 15:36:36.759447098 CEST	53	62938	8.8.8.8	192.168.2.3
May 6, 2021 15:39:04.807533026 CEST	55708	53	192.168.2.3	8.8.8.8
May 6, 2021 15:39:04.877876997 CEST	53	55708	8.8.8.8	192.168.2.3
May 6, 2021 15:39:05.537774086 CEST	56803	53	192.168.2.3	8.8.8.8
May 6, 2021 15:39:05.613012075 CEST	53	56803	8.8.8.8	192.168.2.3
May 6, 2021 15:39:38.364568949 CEST	57145	53	192.168.2.3	8.8.8.8
May 6, 2021 15:39:38.438050032 CEST	53	57145	8.8.8.8	192.168.2.3

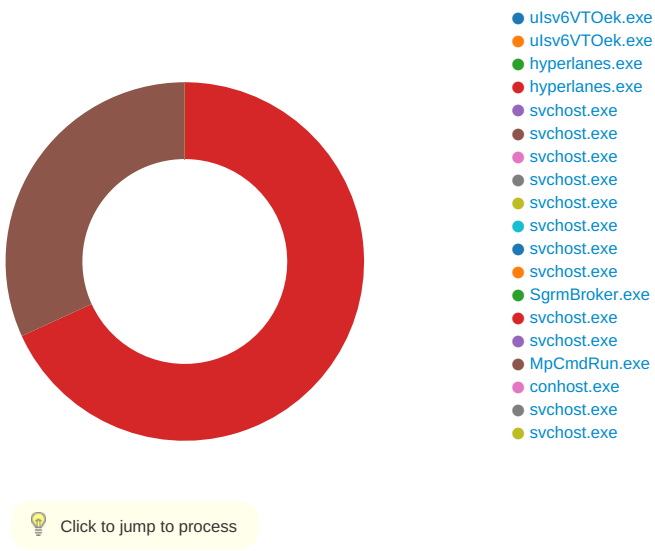
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 6, 2021 15:36:33.299753904 CEST	8.8.8.8	192.168.2.3	0x9c3c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 6, 2021 15:39:04.877876997 CEST	8.8.8.8	192.168.2.3	0xa2d8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: uIsv6VTOek.exe PID: 5936 Parent PID: 5692

General

Start time:	15:31:45
Start date:	06/05/2021
Path:	C:\Users\user\Desktop\uIsv6VTOek.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\uIsv6VTOek.exe'
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	3EE16BBC971BCEB22C5EA3B79F8F711D
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: 00000000.00000002.233356991.00000000005B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000000.00000002.233356991.00000000005B1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: uIsv6VTOek.exe PID: 5980 Parent PID: 5936

General

Start time:	15:31:56
Start date:	06/05/2021
Path:	C:\Users\user\Desktop\uIsv6VTOek.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\uIsv6VTOek.exe
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	3EE16BBC971BCEB22C5EA3B79F8F711D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.246701559.00000000005B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000004.00000002.246701559.00000000005B1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: hyperlanes.exe PID: 3040 Parent PID: 568

General

Start time:	15:31:58
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\hyperlanes.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\hyperlanes.exe
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	3EE16BBC971BCEB22C5EA3B79F8F711D
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: 00000005.00000002.245530482.00000000005B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000005.00000002.245530482.00000000005B1000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

Analysis Process: hyperlanes.exe PID: 3468 Parent PID: 3040

General

Start time:	15:31:59
Start date:	06/05/2021
Path:	C:\Windows\SysWOW64\hyperlanes.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\hyperlanes.exe
Imagebase:	0x400000
File size:	126976 bytes
MD5 hash:	3EE16BBC971BCEB22C5EA3B79F8F711D
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: 00000006.00000002.1291468406.0000000000D11000.00000020.00000001.sdmp, Author: Joe Security • Rule: Emotet, Description: Emotet Payload, Source: 00000006.00000002.1291468406.0000000000D11000.00000020.00000001.sdmp, Author: kevoreilly
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D11800	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	D11800	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	D11800	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	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	D11800	HttpSendRequestW

Analysis Process: svchost.exe PID: 6024 Parent PID: 568

General

Start time:	15:32:05

Start date:	06/05/2021
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: 1268 Parent PID: 568

General

Start time:	15:32:09
Start date:	06/05/2021
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: 5844 Parent PID: 568

General

Start time:	15:32:18
Start date:	06/05/2021
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: 5656 Parent PID: 568

General

Start time:	15:32:20
Start date:	06/05/2021
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: 4088 Parent PID: 568

General

Start time:	15:32:21
Start date:	06/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff63a9c0000
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: 5344 Parent PID: 568

General

Start time:	15:32:22
Start date:	06/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7ca4e0000
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: 1740 Parent PID: 568

General

Start time:	15:32:23
Start date:	06/05/2021
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: 484 Parent PID: 568

General

Start time:	15:32:23
Start date:	06/05/2021
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: 3652 Parent PID: 568

General

Start time:	15:32:24
Start date:	06/05/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff71c640000
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: 5560 Parent PID: 568

General

Start time:	15:32:25
Start date:	06/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: svchost.exe PID: 6504 Parent PID: 568

General

Start time:	15:32:38
Start date:	06/05/2021
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: 1004 Parent PID: 5560

General

Start time:	15:33:25
Start date:	06/05/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff705e40000
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 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	........-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.- .-.-.-.-.-.-.-.-.-.-.-.-.....	success or wait	1	7FF705E6BC96	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 54 00 68 00 75 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 30 00 36 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 35 00 3a 00 33 00 33 00 3a 00 32 00 36 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.:. .. T.h.u. .. M.a.y. .. 0.6. .. 2.0.2.1. .1.5.:. 3.3.:.2.6.....	success or wait	1	7FF705E6BC96	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	7FF705E6BC96	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	7FF705E6BC96	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	7FF705E6BC96	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 54 00 68 00 75 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 30 00 36 00 20 00 0e 20 32 00 30 00 32 00 31 00 20 00 31 00 35 00 3a 00 33 00 33 00 3a 00 32 00 36 00 0d 00 0a 00	M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. M.a.y. .. 0.6. .. 2.0.2.1. .1.5.:.3.3. :.2.6.....	success or wait	1	7FF705E6BC96	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 0d 00 0a 00	-.....	success or wait	1	7FF705E6BC96	WriteFile

Analysis Process: conhost.exe PID: 1000 Parent PID: 1004

General

Start time:	15:33:26
Start date:	06/05/2021
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: 6596 Parent PID: 568

General

Start time:	15:34:28
Start date:	06/05/2021
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: 6904 Parent PID: 568

General

Start time:	15:36:31
Start date:	06/05/2021
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	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

Disassembly

Code Analysis