ID: 383847
Sample Name: lfQuSBwdSf.exe
Cookbook: default.jbs
Time: 11:00:51
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

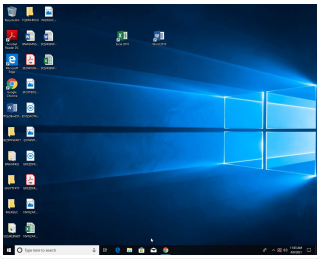
Analysis Report lfQuSBwdSf.exe

Overview

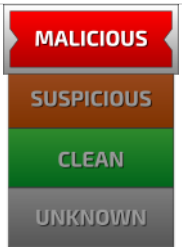
General Information

Sample Name:	lfQuSBwdSf.exe
Analysis ID:	383847
MD5:	0802967c1d72de..
SHA1:	f8edbbed8318311.
SHA256:	201872c79f07606.
Tags:	exe SnakeKeylogger
Infos:	

Most interesting Screenshot:



Detection



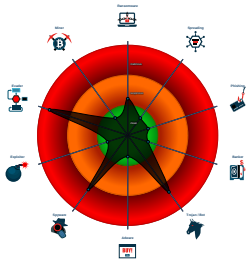
Snake Keylogger

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Adds a directory exclusion to Windo…
- Changes security center settings (no…
- Creates an autostart registry key po…
- Drops PE files with benign system n…
- Drops executables to the windows d…
- Hides threads from debuggers
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- May check the online IP address of …

Classification



Startup

- **System is w10x64**
- lfQuSBwdSf.exe (PID: 2788 cmdline: 'C:\Users\user\Desktop\lfQuSBwdSf.exe' MD5: 0802967C1D72DEEB4E1B79AF74FDB553)
  - powershell.exe (PID: 1004 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 720 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lfQuSBwdSf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1000 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3984 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6248 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - lfQuSBwdSf.exe (PID: 6864 cmdline: C:\Users\user\Desktop\lfQuSBwdSf.exe MD5: 0802967C1D72DEEB4E1B79AF74FDB553)
  - WerFault.exe (PID: 6164 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2788 -s 2300 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4908 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6216 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6528 cmdline: 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' MD5: 0802967C1D72DEEB4E1B79AF74FDB553)
- svchost.exe (PID: 6624 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6672 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6712 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6872 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6908 cmdline: 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' MD5: 0802967C1D72DEEB4E1B79AF74FDB553)
  - powershell.exe (PID: 4424 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5092 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3348 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6932 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7064 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7152 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1648 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5232 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": {
    "Port": "587",
    "SMTP Credential": "bal@nobettwo.xyzKvgnCIGBE8+Hnobettwo.xyz"
  }
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.485923538.000000000402000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000015.00000002.485923538.000000000402000.00000040.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000017.00000002.541864387.0000000004A72000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000017.00000002.541864387.0000000004A72000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000011.00000002.517681508.000000000496F000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	

Click to see the 1 entries

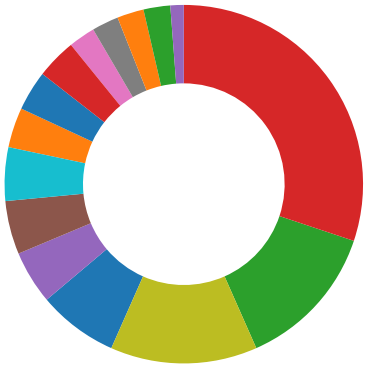
Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.svchost.exe.4a72390.5.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
23.2.svchost.exe.4a72390.5.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
23.2.svchost.exe.4ad53b0.6.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
23.2.svchost.exe.4ad53b0.6.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
23.2.svchost.exe.4ad53b0.6.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

May check the online IP address of the machine

Data Obfuscation:

Yara detected Beds Obfuscator

Persistence and Installation Behavior:

Drops PE files with benign system names

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

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Yara detected Beds Obfuscator

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

Yara detected Snake Keylogger

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

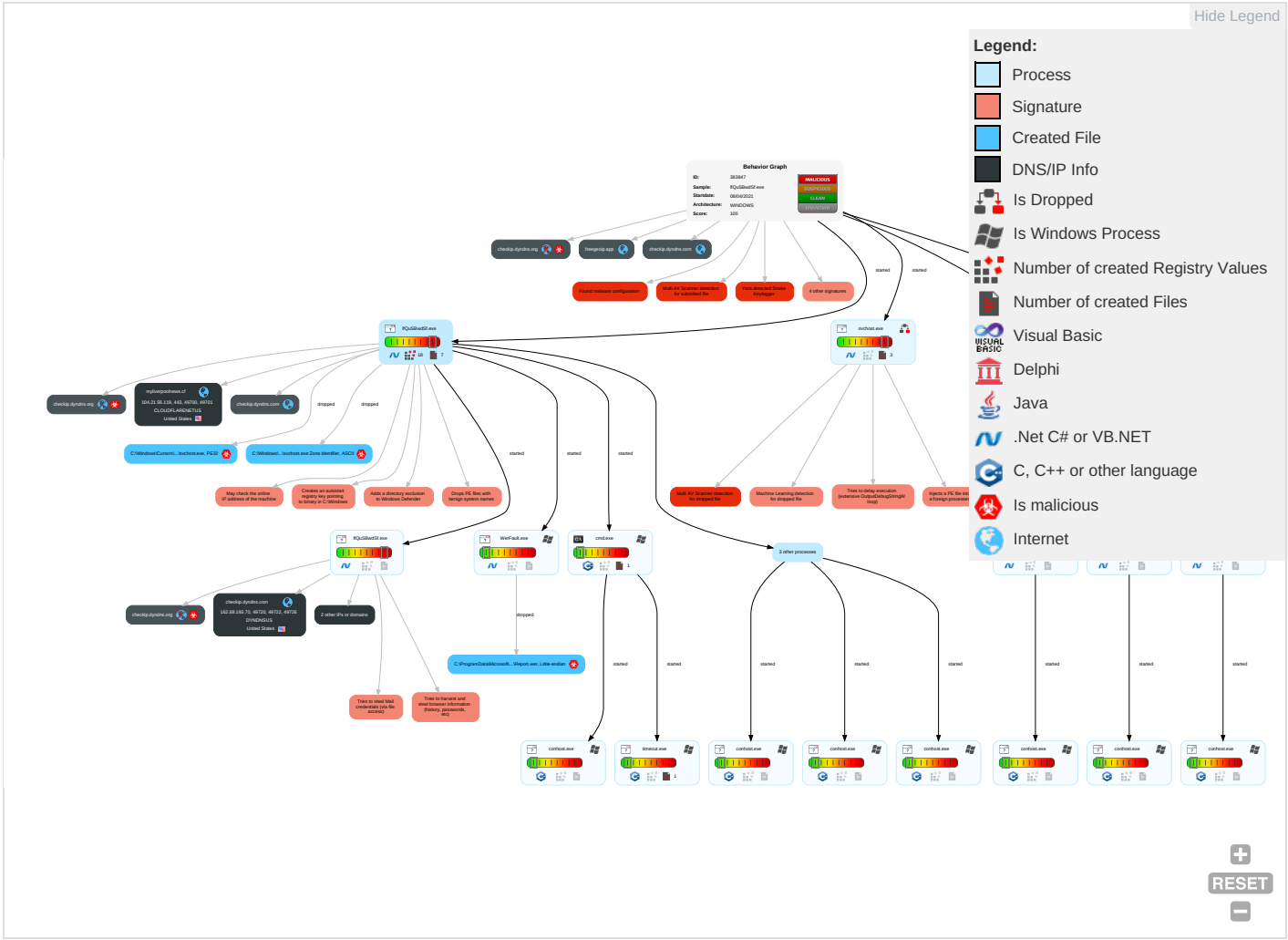
Yara detected Snake Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1	OS Credential Dumping 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E In N C
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 1	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 2 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	E R C
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 1	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 2	E Tr Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	Sl Sv
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 5 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	R A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D In Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	R Ba

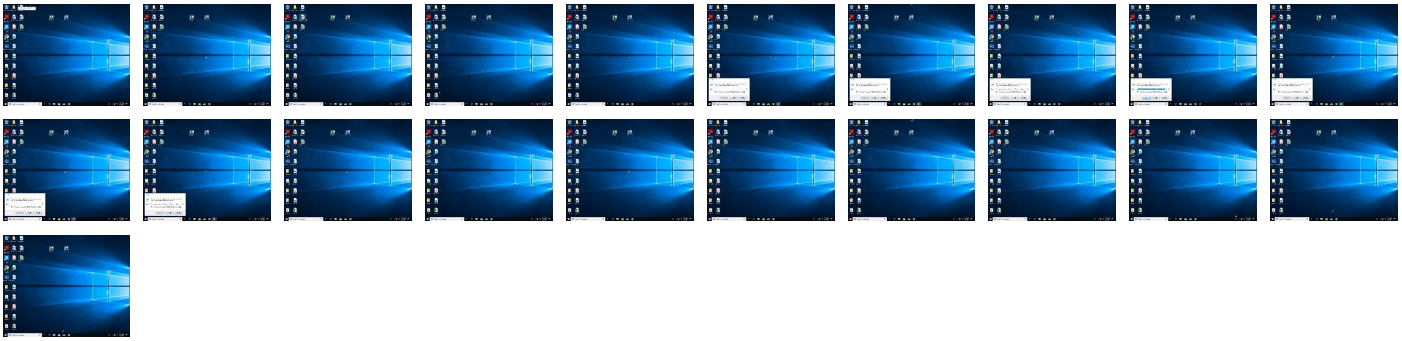
Behavior Graph



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
IfQuSBwdSf.exe	25%	Virustotal		Browse
IfQuSBwdSf.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
IfQuSBwdSf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.2.lfQuSBwdSf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
myliverpoolnews.cf	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7C92219C6C42B363C26A6A670922F074.html	0%	Avira URL Cloud	safe	
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-133B76AB9374D6781F41A2D553BC2BA3.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/featuresnC	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myliverpoolnews.cf	104.21.56.119	true	false	• 2%, Virustotal, Browse	unknown
freegeoip.app	172.67.188.154	true	false		unknown
checkip.dyndns.com	162.88.193.70	true	false		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7C92219C6C42B363C26A6A670922F074.html	false	• Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-133B76AB9374D6781F41A2D553BC2BA3.html	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C52937048F55BFE92995966F69D90F1.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nuget.org/nuget.exe	powershell.exe, 00000005.00000002.536067747.00000000058E2000.00000004.00000001.sdmp, powershell.exe, 00000007.00000002.535279406.0000000005E25000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.535629582.0000000005713000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	lfQuSBwdSf.exe, 00000000.00000002.344997356.00000000030C1000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.522995118.0000000004881000.00000004.00000001.sdmp, powershell.exe, 00000007.00000002.520364713.0000000004DC1000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/featuresnC	lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000007.00000002.524562534.0000000004EFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000005.00000002.526440831.00000000049BB000.00000004.00000001.sdmp, powershell.exe, 00000007.00000002.524562534.0000000004EFD000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000007.00000002.524562534.0000000004EFD000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000009.00000002.535629582.0000000005713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

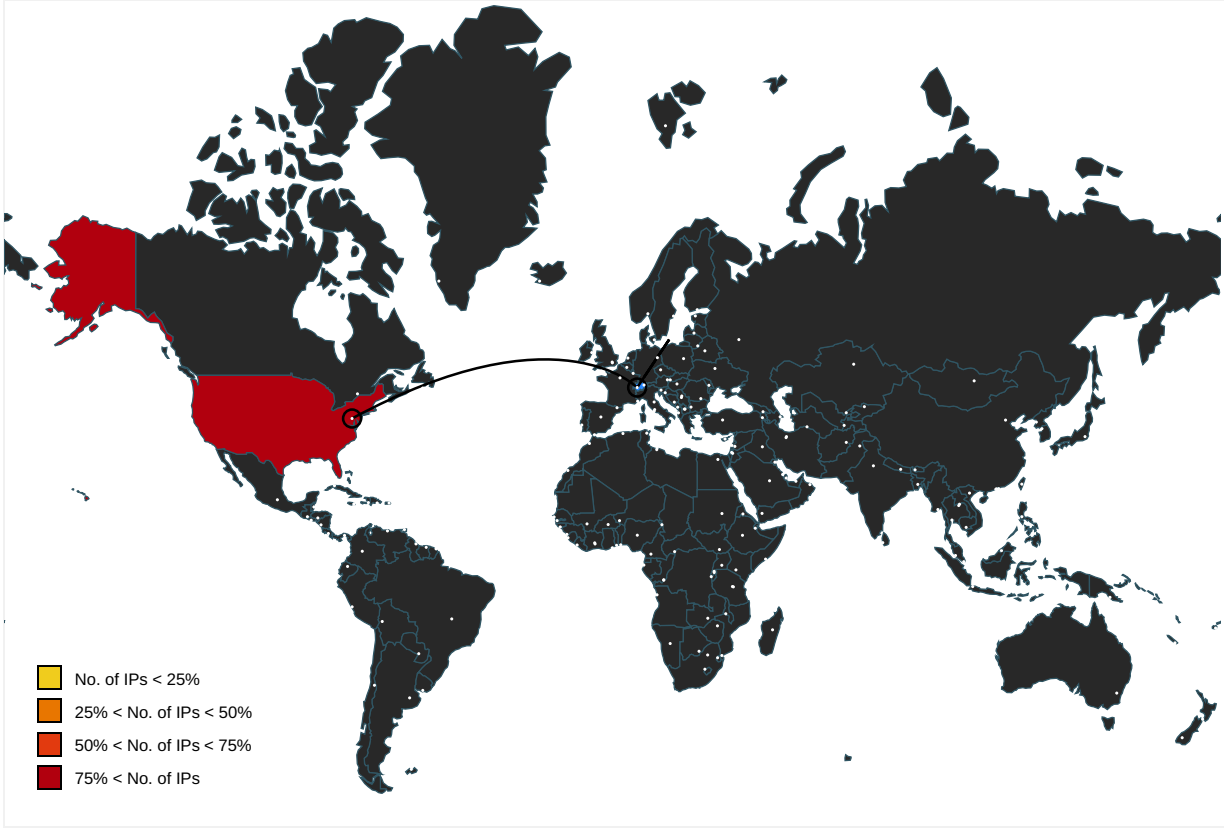
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://reachplc.hub.loginradius.com"	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com	lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 00000014.00000002.502117639.000001DDF383E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000007.00000002.524562534.0000000004EFD000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com	lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/ozan-kabak	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000005.00000002.526440831.00000000049BB000.00000004.00000001.sdmp, powershell.exe, 00000007.00000002.524562534.0000000004EFD000.00000004.00000001.sdmp	false		high
http://https://s2-prod.mirror.co.uk/	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-	lfQuSBwdSf.exe, 00000000.00000002.344997356.00000000030C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/curtis-jones	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features	lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/BreadcrumbList	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000009.00000002.535629582.0000000005713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com/	lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://myliverpoolnews.cf4&l	lfQuSBwdSf.exe, 00000000.00000002.345654171.00000000030F0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://felix.data.tm-awx.com/ampconfig.json"	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/ListItem	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/georginio-wijnaldum	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s180/0_GettyImages-1231353837.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com	lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000009.00000002.535629582.0000000005713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/andrew-robertson	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.225090354.0000000006081000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000002.346059518.000000000311E000.00000004.00000001.sdmp, lfQuSBwdSf.exe, 00000000.00000003.233038130.0000000003334000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article17166876.ece/ALTERNATES/s615/0_GettyImages-1175998874.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-gini-wijnaldum-rumours-fitness-199533	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s180/0_GettyImages-1304940818.	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf	lfQuSBwdSf.exe, 00000000.00000002.344997356.00000000030C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/transfers	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/rhian-brewster-liverpool-arsenal-team-17172763&	lfQuSBwdSf.exe, 00000000.00000003.228963232.00000000040EA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.88.193.70	checkip.dyndns.com	United States		33517	DYNDNSUS	false
104.21.56.119	myliverpoolnews.cf	United States		13335	CLOUDFLARENETUS	false
172.67.188.154	freegeoip.app	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383847
Start date:	08.04.2021
Start time:	11:00:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lfQuSBwdSf.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:	mal100.troj.spyw.evad.winEXE@49/25@11/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 1.4%) • Quality average: 11.3% • Quality standard deviation: 23.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.54.113.53, 52.255.188.83, 40.88.32.150, 104.43.193.48, 95.100.54.203, 168.61.161.212, 20.82.210.154, 13.64.90.137, 93.184.221.240, 23.10.249.26, 23.10.249.43, 13.88.21.125, 20.54.26.129, 20.50.102.62, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:02:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce wyreCRIln C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe
11:02:04	API Interceptor	2x Sleep call for process: svchost.exe modified
11:02:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce wyreCRIln C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe
11:02:38	API Interceptor	1x Sleep call for process: WerFault.exe modified
11:02:55	API Interceptor	130x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.88.193.70	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SER09090899.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	MUYR09080.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PURCHASE ORDER-34002174, pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order CG-210331-1004.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Invoice,PDF.exe.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	ej 9999999.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL FINAL REMINDER PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Statement For Month..exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	New Revised.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO_3351_60_20.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	SMA0908800.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.ArtemisCEDC6E147EF2.27473.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	NEW ORDER.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	INV0000075.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SWIFT COPY.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	tRuJwJgMos.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	RfTQP.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Payment advice IMG_417_302_680.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	A7aLfLs0oa.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myliverpoolnews.cf	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212
	kayo.exe	Get hash	malicious	Browse	• 172.67.150.212
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• 104.21.56.119
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 172.67.150.212
	items list.doc	Get hash	malicious	Browse	• 172.67.150.212
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• 104.21.56.119
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 104.21.56.119
	Krishna Gangaa Enviro System Pvt Ltd.exe	Get hash	malicious	Browse	• 172.67.150.212
	PO757739374758953 77.exe	Get hash	malicious	Browse	• 104.21.56.119
	New Order.exe	Get hash	malicious	Browse	• 104.21.56.119

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Artemis5C44BBDCCDFF.4370.exe	Get hash	malicious	Browse	• 172.67.150.212
	RFQ #46200058149.exe	Get hash	malicious	Browse	• 172.67.150.212
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• 104.21.56.119
	New Orders.exe	Get hash	malicious	Browse	• 172.67.150.212
freegeoip.app	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 172.67.188.154
	SER09090899.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	cricket.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 172.67.188.154
	EMPRESA SUMPEX TRADE.exe	Get hash	malicious	Browse	• 104.21.19.200
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Dringende RFQ_AP75887658_98788,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	MUYR09080.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER-34002174, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order CG-210331-1004.exe	Get hash	malicious	Browse	• 104.21.19.200
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice,PDF.exe.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• 172.67.188.154
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 104.21.19.200
	Confirmation_(#1422) DEKRA order,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	ATTACHED.exe	Get hash	malicious	Browse	• 172.67.188.154
	Urgent RFQ_AP65425652_040621,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 172.67.219.254
	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 172.67.150.212
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	kayo.exe	Get hash	malicious	Browse	• 172.67.150.212
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 104.16.18.94
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 172.67.164.131
	PO7321.exe	Get hash	malicious	Browse	• 172.67.154.93
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 172.67.188.154
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.25.233.53
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119
	invoice.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	new_order20210408_14.doc	Get hash	malicious	Browse	• 172.67.150.212
	PR_A1191-04052021.xlsx	Get hash	malicious	Browse	• 104.25.233.53
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 104.21.61.102
DYNDNSUS	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	PRICE_QUOTATION_RFQ_000988_PDF.exe	Get hash	malicious	Browse	• 131.186.113.70
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 162.88.193.70
	SER09090899.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	cricket.exe	Get hash	malicious	Browse	• 131.186.113.70
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 131.186.113.70
	EMPRESA SUMPEX TRADE.exe	Get hash	malicious	Browse	• 216.146.43.70
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	Dringende RFQ_AP75887658_98788,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	MUYR09080.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER-34002174, pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Order CG-210331-1004.exe	Get hash	malicious	Browse	• 162.88.193.70
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	Invoice,PDF.exe.exe	Get hash	malicious	Browse	• 216.146.43.70
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• 131.186.113.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 216.146.43.70
	Confirmation_(#1422) DEKRA order,pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	ATTACHED.exe	Get hash	malicious	Browse	• 216.146.43.71
	Urgent RFQ_AP65425652_040621,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	RFQ-034.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	ACdEbpiSYO.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	PURCHASE ORDER - XIFFA55,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	Invoice_ord00000009.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	kayo.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	new_order20210408_14.doc	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	BL01345678053567.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	SER09090899.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	PURCHASE ORDER-34002174,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	cricket.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	DHLdocument11022020680908911.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	20200804-8293847pdf.scr.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	234d9ec1757404f8fd9fbb1089b2e50c08c5119a2c0ab.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	SKMC25832100083932157.jar	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	SecuriteInfo.com.Artemis34DBCAD2CB5A.27289.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	EMPRESA SUMPEX TRADE.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	Yeni siparis _WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	Dringende RFQ_AP75887658_98788,pdf.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154
	MUYR09080.exe	Get hash	malicious	Browse	• 104.21.56.119 • 172.67.188.154

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5976804353698416
Encrypted:	false
SSDEEP:	6:bWlEk1GaD0JOCEfMuaaD0JOCEfMKQmDtAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bWNGaD0JcaaD0JwQQtAg/0bjSQJ
MD5:	0C2A0FB45AE1576A122F5656C2B87E6A
SHA1:	A93AA5CEE6A26BF623A545FC0DF2B9696165BFFA
SHA-256:	618F67B0C0755100E663919FFA287BCA588F800B638A2857067D393508FED4E3
SHA-512:	AC1D71B8B6DF42B7B63F6CB516338D21EEA2A59B6C9743243AE029A366D1D06C6C4EF48AE9649F8572BC966E4775C771800C2CCFBF08BB87D7B5C9D43511BF6

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Malicious:	false
Preview:	....E..h..(.....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 0xdc05173d, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09541840300770618
Encrypted:	false
SSDEEP:	6:RXzwl/+0XRIE11Y8TRXdyV6K7Xzwl/+0XRIE11Y8TRXdyV6K:50+0XO4bldzKL0+0XO4bldzK
MD5:	AA689052BE348C1ECC66B5E639E3234B
SHA1:	B9A6C6D0487A8165757361CDDC10811B65E8DE42
SHA-256:	25E1EA5E8E0F2468C89C39700FDAD0F8C204447B5B18D9B51D14049B4C22231F
SHA-512:	48BA3314A159441D4058A3BDEC38D70A0178A036D04127A4726A2A04AF7099DCC77CD79349BE0188E0EF7C20D287F27AD67B9C52C46F5D68958D2E1073D72B1
Malicious:	false
Preview:	...=... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....{.....y.e.....!.....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.1108664572894607
Encrypted:	false
SSDEEP:	3:JllTEvg3QUAl/bJdAtiVhVloll:xag3XAt4g2
MD5:	52FA11AC12F2144CC9C1D312B9B48211
SHA1:	3E9586A500E74302E80B17EE0F43721BC57440C9
SHA-256:	CCC3477C544B4A63479742AE688F25935EB4661AB7E56E16781EC03482F66AA2
SHA-512:	1A31B93FE26B4ECA6E389C1B1114B2732ACC27B3E18506A7C03EAF7CAA75F4FAC0048D113BAA092B305080424D7DB89552228B4D069E9BA8C74EA7C598566A0 1
Malicious:	false
Preview:	.Lt.....3...w.....y.....w.....w.....w....:O....w.....!.....y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_IfQuSBwdSf.exe_dbcf35fab953bf6b1a979b91e3aa6f6e971ce7_957fde8e_1840eb32\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17404
Entropy (8bit):	3.7598066063700224
Encrypted:	false
SSDEEP:	192:hZGB8e4mHBUZMXSaKQqueZitu/u7sQS274Itbx:O2eZBUZMXSaFmJ/u7sQX4Itbx
MD5:	79641D2E96E5F7DC6F51501B97E9CAAB
SHA1:	94CB1967BA3F74A848D81E33BC9A4EC849CD39A8
SHA-256:	CC51A3F9523D499F82ECEE27807107A7C707AF1E08C7FAC8C134760B130AEAE1
SHA-512:	CA78672F7C42C83E8CC208CBF7579689D26700C9B27C8D5B249DF1E2D408B471AF39B9DA9A62D555AF7B37432A681A335ED8DA6242D24435E27DD8D0B0A4FBC
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.3.7.8.5.4.6.7.1.3.2.2.0.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.3.7.8.5.5.5.1.0.3.8.2.6.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.6.1.c.b.d.3.0.-.7.e.c.3.-.4.b.f.5.-.b.b.c.4.-.f.8.e.d.a.b.c.f.9.c.f.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.4.d.f.c.b.0.3.-.b.3.a.c.-.4.0.7.e.-.8.4.b.8.-.6.4.7.e.6.3.1.c.0.e.f.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.f.Q.u.S.B.w.d.S.f...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.D.i.m.b.o.n.o...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.a.e.4.-.0.0.0.1.-.0.0.1.7.-.f.c.f.c.-.4.5.3.b.a.1.2.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.4.9.0.5.2.9.4.d.a.f.2.3.9.d.d.6.1.4.2.d.1.0.9.e.1.c.d.0.1.f.b.0.0.0.0.0.0.0.0.!.0.0.0.0.f.8.e.d.b.b.e.d.8.3.1.8.3.1.1.f.0.7.0.1.6.7.c.7.3.f.c.c.a.9.f.6.3.f.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBE46.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Apr 8 18:02:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	330441
Entropy (8bit):	3.629346303572354
Encrypted:	false
SSDEEP:	3072:DNa2o3eyzFdhx0nAyjd+pOD0QRUCgUeAw/9gIOgF59jVjZpXe:dQP0epW7Tj1k9RpD95jZle
MD5:	F80E8E853AC993B123EF2D189BC5D4A6
SHA1:	8C57934C587DBFBAA1236F1BF655CEB989EAB236
SHA-256:	5133BE65AFA86EB1B4F7906A86C113E06ECD13F42A839616DB99F290A5D6EB0C
SHA-512:	DA3BBCC9061439054BD4599DA2F56CADA8EA063B7296AC55D6158BCAB21BA18A5EF9A4C7CA9FC93168CCBBBE248C9039A9005A654F7D9752E5F43498A6835E29
Malicious:	false
Preview:	MDMP..... .....6Eo`.....U.....B.....l1.....GenuineIntelW.....T.....Eo`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD903.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8408
Entropy (8bit):	3.69539172946485
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiNB6K6YSKSUi6I3WegmfZOSUCprY89bTnEsf0zxm:RrlsNir6K6YPSUi6OWegmfcSpTn3fB
MD5:	0E16BAA073DA35DADE06031DE91DBB5E
SHA1:	27E52AD81E964E9EB4ECACE5528058776D7B9AF2
SHA-256:	D1F5C3BF879527D91027766168562B2E854AA6BF429B321A127A44916B30655C
SHA-512:	1205B8CA1F29160F6ED376E0CC13AED8037A91351E3846456074C45D758F640860CD7F36D76893501D23B34F3E2E1CA26FA941A5EA19CD9B72DF4BE139D6F512
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.7.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDB94.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4750
Entropy (8bit):	4.474044588371349
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9+Ay6WSC8BL8fm8M4J4FF037+q8vvrJEnJbCrcdd:uITfbYSSNeJz7KzJEnJGrcdd
MD5:	3E5B568551BEFAFC35E627281F8CDE65
SHA1:	CB3622DD78CB6F7F6C7CEA47F0DA87474D49E4B5
SHA-256:	C08106AF77EA9D1D5FB81C525BB443F9FA1C442D76381FAB26966B28217C57AD
SHA-512:	708FABFA888069A6F584666011EF9E2131A67FE902B53B2F42D92839BFD41842023434B26DA5EAD019C65B3818A94D82B8748BD4389F18E08BB363B04A3B067B
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="937633" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	698
Entropy (8bit):	5.049094101509586
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
SSDEEP:	12:reVGyMYx2Y5BYtmWNUc5AtYX5E4a2KryMYGH+ptsxptsOtw9O9S8:reUyMGF5ytmLcetYX5E2KryMb+zsxzsk
MD5:	B0CEEA53B3467F59FD8E87F80213BDE9
SHA1:	D9E6D1CBB480E7248658DF935648DFA733745602
SHA-256:	D9C93CB64E6F1F5BDC94581CEEA99F759EE1E35716EAF623C61962EA0152F9DD
SHA-512:	DDAA6C9FA3535B4926C60B692F8E202D10EB160D1F8BE7A9DE79239EF75AFD470403DF1D8F0CBF29A5F819E907D02E8E656BB9A52E71E30D9259987EAE88165 5
Malicious:	false
Preview:	PSMODULECACHE.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSourc e.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....I mport-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D..8.....C:\Program Files (x8 6)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation..... ..Invoke-OperationValidation.....

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):	0.11021535299334234
Encrypted:	false
SSDEEP:	12:26fEzXm/Ey6q9995cwuNq3qQ10nMCldimE8eawHjcIEv:26fBl689ugLyMCldzE9BHjcIE
MD5:	D8F8828F046E214C4F83197D79308E4E
SHA1:	0CE8ABF0F299AFA77651703664850B30F7205FF9
SHA-256:	298F7C2C58A35D3F9018C168A05CAB802CB908A32B5FE47325F050AD8222121C
SHA-512:	C263EE316960DC044520C7475A035D9E6F5BCE3064C025834AE468270C40C0A9CAB80905FA9A2C961AF55B5DAB1A47BB73A4F0EA6DEAF086DEA6D46C96908D 5
Malicious:	false
Preview:	.....(.....N.....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..... .....Y9Q.,.....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.(.....W..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11234695267431766
Encrypted:	false
SSDEEP:	12:BzXm/Ey6q9995cktL1miM3qQ10nMCldimE8eawHza1miluf:Ml68X1tMLyMCldzE9BHza1tlO
MD5:	25C45E2E80B645291BE51ED449ADF375
SHA1:	54C9935A5125550F947D32BF83AE7A5EFA57E0B8
SHA-256:	C5BFCFB1A1C6F430C88F820EBCD0B5DFEB66E1D504357C40BE1F11CCBA00ED0E
SHA-512:	E6CDC84A6D4AEFF20DD6E35D7EC45B3AA84E8BF310DD6B59F4F1FBD08A85AB71B355E2AD8AC6FF92AA7F041E2D2A7C4894B18A07ACCFE179D82D6DFA4DDI 49C9
Malicious:	false
Preview:	.....(.....F.....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..... .....x3.Q.,.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c. a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.(.....H..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11247201638927183
Encrypted:	false
SSDEEP:	12:kzXm/Ey6q9995c7x1mK2P3qQ10nMCldimE8eawHza1mKmf:hl68k1iPLyMCldzE9BHza1a
MD5:	B4833118DA36CBF8E6082C02364BBB4F
SHA1:	D5F49A356B1A273FA41B354F22F1642C726DA33C
SHA-256:	40F0F8C311F41D76B4599B105405CF2F7FA54A0D767DB3E5A43B0EEC2DDF66EC
SHA-512:	521010B548704EEDB1360549075BD5FBC7F2D7D725A1C632375BBB46FB731D25753242BF981EF48AC5BE32B93CDABD63AC2B4B1ADBBB655AB06952FF67B873 6
Malicious:	false

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Preview:	.....(.....s.+.....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..... .....t.P.,.....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.(.....-..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3unvo0at.i2z.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_afdwa5sz.ycm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bk34zenz.mnc.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cv5sw5e3.x0i.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cv5sw5e3.x0i.psm1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dkeuwky5.kyp.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wacrv0pl.app.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210408\PowerShell_transcript.216554.+ytC9MFS.20210408110204.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	862
Entropy (8bit):	5.356189201456313
Encrypted:	false
SSDEEP:	24:BxSA33yxvBndx2DOXUWeSuMG1OWbHjeTKKjX4CIym1ZJXDFuMG1C:BZuvhdoO+SqPbqDYB1Z3qg
MD5:	BCF1AA333B0E2685377E4D638341B518
SHA1:	D2D2DF3F261EBEDE89E39314B34FB153915B9A1F
SHA-256:	E69620958827E1C5ADABAB8EEBBE18350B0316BEFE2CE4852F496756E0B7F086
SHA-512:	E06DFFB20671B0DDB6AAAD522CF1BA442D7EA59334A235EDCE4C42E47E8F59FC7F9754FF0BA5DA2D9C6EEC58FCA81D60B13174E13B9DF6C8186D977786DB0 A38
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210408110234..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe -Force..Process ID: 1000..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210408110235..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe -Force..

C:\Users\user\Documents\20210408\PowerShell_transcript.216554.6CUcdU4H.20210408110202.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	843

C:\Users\user\Documents\20210408\PowerShell_transcript.216554.6CUcdU4H.20210408110202.txt	
Entropy (8bit):	5.329898122050224
Encrypted:	false
SSDEEP:	24:BxSAGxvBndx2DOXUWeSuWW9HjeTKKjX4CIym1ZJXVu6:BZyvhdoO+SI9qDYB1ZrR
MD5:	67C14436066F55A5F8035E0A8785E196
SHA1:	29F44AD56CD4E5515590510E3F20F3B71A73A2A2
SHA-256:	F5782A22B43FA86B0F2FE3AE18747CD303B4FCE8EC9B9405993BF4F7270EA14A
SHA-512:	567D1876B4FD16D28DDC5A820C28E08C56D6469DA5CB684F3D0BEFAE757D67940CF8791157DCA03B60F203C733E0D9DF21FDB4340386E13EFD149B422DEFC2 5
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210408110230..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\lfQuSBwdSf.exe -Force..Process ID: 720..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1. 0.1..**********************..**********************..Command start time: 20210408110231..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\ lfQuSBwdSf.exe -Force..

C:\Users\user\Documents\20210408\PowerShell_transcript.216554.Pgu86VMD.20210408110201.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	862
Entropy (8bit):	5.359412750263977
Encrypted:	false
SSDEEP:	24:BxSAYxvBndx2DOXUWeSuMG1OWXHjeTKKjX4CIym1ZJXZuMG1C:BZsvhdoO+SqPXqDYB1Zzqg
MD5:	668F65C7B522C96ACB85A8AAF637EF96
SHA1:	56D58F4E00C02FBC9E5356CB0F41AAC8F39AE683
SHA-256:	75FCC43B2DB59D46B2645D868015C09830BC71A423251C9DA05C6D45584528AB
SHA-512:	1369B9032D0A3840191BDB50068959A32E7142D3DE22AE44BAE0B5B287255E52BBF8EA2C147A753A4D4ED561C6C4C81C60EB19DCE1B164810D10DFF48AEAA0 B
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20210408110225..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe -Force..Process ID: 1004..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2 .0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVe rsion: 1.1.0.1..**********************..**********************..Command start time: 20210408110226..**********************..PS>Add-MpPreference -ExclusionPath C:\Windows\ Cursors\WQzhTjfBsYrOnkh\svchost.exe -Force..

C:\Users\user\WrdAHTtKmtDmuc	
Process:	C:\Users\user\Desktop\lfQuSBwdSf.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5832256
Entropy (8bit):	3.076288730928143
Encrypted:	false
SSDEEP:	12288:g/K5NquGjzowGM2Qn7QJi/7goLuPp393mcN6z03z9aLIG6ades08zoX4sm21Tgtk:Te8zlte8zld6StGZPve8zld6StGZPT
MD5:	41E25385DEA56C5FFE7F052EA7EC9865
SHA1:	B2B5504C508D07EC073718C953237A265F37B3A9
SHA-256:	C941110415F3819464D4A8D0A8EA8B7CA31FB22C576EBD850DD2F24AA55D118F
SHA-512:	76A0D7A15DF9595B82723D1A0696F57423683506FD40F73FB66974BE770BCD379908FB26D735E38547C5429B985A18130F52C997738D83EF274350BCBE95659B
Malicious:	false
Preview:	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 1 84 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116 32 98 101 32 114 117 110 32 105 110 32 68 79 83 32 109 111 100 101 46 13 13 10 36 0 0 0 0 0 0 0 80 69 0 0 76 1 3 0 76 142 41 180 0 0 0 0 0 0 0 0 224 0 34 0 11 1 80 0 0 114 13 0 0 6 0 0 0 0 0 0 110 144 13 0 0 32 0 0 0 160 13 0 0 0 0 128 0 32 0 0 0 2 0 0 4 0 0 0 0 0 0 0 4 0 0 0 0 0 0 0 0 224 13 0 0 2 0 0 0 0 0 0 2 0 64 133 0 0 16 0 0 16 0 0 0 0 16 0 0 16 0 0 0 0 0 0 16 0 0 0 0 0 0 0 0 0 0 0 32 144 13 0 75 0 0 0 0 160 13 0 212 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 192 13 0 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0 8 0 0 0 0 0 0 0 0 0 0 0 0 8 32 0 0 72 0 0 0 0 0 0 0 0 0 0 0 0 46 116 101 120 116 0 0 0 116 112 13 0 0 32 0 0 0 114 13 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 32 0 0

C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	
Process:	C:\Users\user\Desktop\lfQuSBwdSf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	46080
Entropy (8bit):	5.842547697365067
Encrypted:	false
SSDEEP:	384:GrrHzbTWuxdvMvNZeA7JLtNnE27w/yvej5VLUJflhAtRtkDo3mC05aESzAdG4caM:GrrHzbJx4so8yiGfluTcU
MD5:	0802967C1D72DEEB4E1B79AF74FDB553
SHA1:	F8EDBBED8318311F070167C73FCCA9F63F79C905

C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	
SHA-256:	201872C79F07606D9874BC471ACF1999E0EEF0703E73C71A4A297EB56C70BCFB
SHA-512:	7566FF29FD3D743AD92543540A42AEC7731B996D171A0197971812396B8221387495F8AC1606D647ABDB888B630D1273C4207A800FA886CCB1E59029D1B86153
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..h...J..... .....@.. ....@.....O.....dF.....r..... ....H.....text...$f... ...h..... ..`.rsrc...dF.....H...j.....@..@.relo c.....@..B.....H.....5...P.....*".(....*Vs....(....t.....*".(....*R.(.....s....}....*6.(....o,....*....0.....~.....+..*..0..9 .....r...p..((....r...p.(.....(.....,...(.....+..~.....+..*....0..#.....r...p..((....r...p.(.....(.....*..0..9.....s.....+.....o....o.....o...,...o.....o....o.....*....0.....(....o.....+.+.....*.0.. .....r#.. p.+.....s.....%r9..p .....%.r...p.%.r...p.%.r...p

C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\lfQuSBwdSf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.842547697365067
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	lfQuSBwdSf.exe
File size:	46080
MD5:	0802967c1d72deeb4e1b79af74fdb553
SHA1:	f8edbbed8318311f070167c73fcca9f63f79c905
SHA256:	201872c79f07606d9874bc471acf1999e0eef0703e73c71a4a297eb56c70bcfb

General

SHA512:	7566ff29fd3d743ad92543540a42aec7731b996d171a0197971812396b8221387495f8ac1606d647abdb888b630d1273c4207a800fa886ccb1e59029d1b86153
SSDEEP:	384:GrrHzbTWuxdvMvNZeA7JLtNnE27w/yvej5VLUJflhAtRtkDo3mC05aESzAdG4caM:GrrHzbJx4so8yiGfluTcU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....".....0..h...J..... .....@.. ....@.....

File Icon

Icon Hash:	30828a8c8c828010

Static PE Info

General

Entrypoint:	0x40861e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEDF52E0E [Wed Jul 4 19:25:02 2096 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x85cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x4664	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x7200	0x14e0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6624	0x6800	False	0.332594651442	data	6.27050186695	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x4664	0x4800	False	0.14892578125	data	4.10630489014	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa130	0x4028	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xe158	0x14	data		
RT_VERSION	0xe16c	0x30c	data		
RT_MANIFEST	0xe478	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

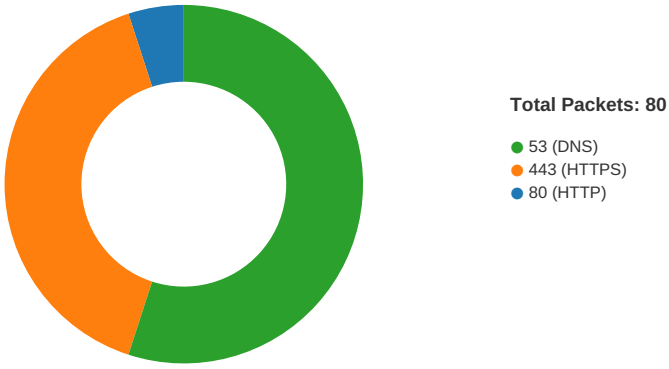
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	Dimbono.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Dimbono
ProductVersion	1.0.0.0
FileDescription	Dimbono
OriginalFilename	Dimbono.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:01:44.745105028 CEST	49700	80	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.763072014 CEST	80	49700	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.763185978 CEST	49700	80	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.763689041 CEST	49700	80	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.781486988 CEST	80	49700	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.789665937 CEST	80	49700	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.848814011 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.866358995 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.866476059 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.889404058 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.906951904 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.910037994 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.910068989 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.910156965 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.916479111 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.934339046 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.934370995 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:44.954818010 CEST	49700	80	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:44.987306118 CEST	49701	443	192.168.2.3	104.21.56.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:01:45.005022049 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206446886 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206482887 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206516981 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206542969 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206549883 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.206568956 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206583977 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.206603050 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206630945 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206648111 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.206655979 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206696033 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.206815004 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206837893 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.206882000 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.206965923 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.267350912 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.393932104 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.393970966 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.393992901 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394015074 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394033909 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394063950 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.394104958 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394110918 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.394150019 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.394181013 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394301891 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394324064 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394342899 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.394848108 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394895077 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.394906044 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.395047903 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395072937 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395092010 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.395802975 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395831108 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395853043 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395860910 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.395896912 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.395900965 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.396452904 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.396483898 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.396512032 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.396574974 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.396599054 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.396609068 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.397416115 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.397454023 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.397475004 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.397476912 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.397500038 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.397509098 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.398221016 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.398251057 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.398266077 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.398274899 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.398303032 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.398320913 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.399104118 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399136066 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399157047 CEST	49701	443	192.168.2.3	104.21.56.119

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:01:45.399213076 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399233103 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399250031 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.399724007 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399749994 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399769068 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.399821997 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.399857998 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.399858952 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.400578022 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.400609970 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.400633097 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.400635004 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.400672913 CEST	49701	443	192.168.2.3	104.21.56.119
Apr 8, 2021 11:01:45.412417889 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.412455082 CEST	443	49701	104.21.56.119	192.168.2.3
Apr 8, 2021 11:01:45.412477016 CEST	443	49701	104.21.56.119	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:01:38.755899906 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:38.775214911 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 11:01:40.972173929 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:40.984234095 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 11:01:41.679163933 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:41.692414045 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 11:01:44.681437016 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:44.724883080 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 11:01:44.803056002 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:44.847248077 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:01:56.968020916 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:01:56.980468035 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:02.752123117 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:02.764671087 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:03.696585894 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:03.709362984 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:05.024367094 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:05.036798000 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:09.424561977 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:09.451386929 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:11.972204924 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:11.984787941 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:13.304059029 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:13.316571951 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:15.070406914 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:15.082360983 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:16.156286955 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:16.168801069 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:24.921981096 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:24.934926033 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:27.071579933 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:27.085139990 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:28.164998055 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:28.176840067 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:29.803163052 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:29.815573931 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:30.633725882 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:30.646882057 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:30.671216965 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:30.683943987 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:34.746850014 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:34.758682013 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:34.833126068 CEST	58823	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:02:34.845623016 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:37.806899071 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:37.819520950 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:52.069416046 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:52.087430000 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 11:02:54.568016052 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:02:54.587409973 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:03.610271931 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:03.622721910 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:04.713150978 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:04.725918055 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:11.841286898 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:11.854012012 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:12.067235947 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:12.079967022 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:12.087239981 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:12.099225998 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:12.367260933 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:12.386113882 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:12.953145027 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:12.965672970 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:14.239921093 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:14.253173113 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:17.115955114 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:17.128592968 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:19.774718046 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:19.801333904 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:29.444453955 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:29.457216024 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:29.460191011 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:29.472771883 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:29.958946943 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:29.971657991 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:31.398861885 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:31.411643982 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:33.603425980 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:33.617084980 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 11:03:35.694166899 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:03:35.712686062 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 11:04:07.707721949 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:04:07.720654011 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 11:04:08.340862989 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:04:08.372174978 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 8, 2021 11:04:27.249521017 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:04:27.343425035 CEST	53	63978	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:01:44.681437016 CEST	192.168.2.3	8.8.8.8	0x9e2d	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:44.803056002 CEST	192.168.2.3	8.8.8.8	0x4547	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.746850014 CEST	192.168.2.3	8.8.8.8	0x4c9d	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.833126068 CEST	192.168.2.3	8.8.8.8	0xd4a3	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:54.568016052 CEST	192.168.2.3	8.8.8.8	0x8bcb	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.067235947 CEST	192.168.2.3	8.8.8.8	0x7afe	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.087239981 CEST	192.168.2.3	8.8.8.8	0xf800	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.367260933 CEST	192.168.2.3	8.8.8.8	0xc04	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.444453955 CEST	192.168.2.3	8.8.8.8	0x6506	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:03:29.460191011 CEST	192.168.2.3	8.8.8.8	0xca10	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.958946943 CEST	192.168.2.3	8.8.8.8	0xc9a5	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:01:44.724883080 CEST	8.8.8.8	192.168.2.3	0x9e2d	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:44.724883080 CEST	8.8.8.8	192.168.2.3	0x9e2d	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:44.847248077 CEST	8.8.8.8	192.168.2.3	0x4547	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:44.847248077 CEST	8.8.8.8	192.168.2.3	0x4547	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.758682013 CEST	8.8.8.8	192.168.2.3	0x4c9d	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.845623016 CEST	8.8.8.8	192.168.2.3	0xd4a3	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:54.587409973 CEST	8.8.8.8	192.168.2.3	0x8bcb	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:54.587409973 CEST	8.8.8.8	192.168.2.3	0x8bcb	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:03:12.079967022 CEST	8.8.8.8	192.168.2.3	0x7afe	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.099225998 CEST	8.8.8.8	192.168.2.3	0xf800	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.386113882 CEST	8.8.8.8	192.168.2.3	0xc04	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:12.386113882 CEST	8.8.8.8	192.168.2.3	0xc04	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.457216024 CEST	8.8.8.8	192.168.2.3	0x6506	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.472771883 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.971657991 CEST	8.8.8.8	192.168.2.3	0xc9a5	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:29.971657991 CEST	8.8.8.8	192.168.2.3	0xc9a5	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myliverpoolnews.cf
- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49700	104.21.56.119	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:01:44.763689041 CEST	1125	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7C92219C6C42B363C26A6A670922F074.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf Connection: Keep-Alive
Apr 8, 2021 11:01:44.789665937 CEST	1126	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:01:44 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 10:01:44 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-7C92219C6C42B363C26A6A670922F074.html cf-request-id: 0952505fc400002bd23ba83000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=XwmX5ySeaG4eevDa%2FP04VvipikZHPpRO%2FF3tIBV5NbuBA2RpBCIKkMorKYyO4EloOW3yiVGy%2BM7wNR%2FPg%2FysydqcyAkokNUfW2jqEcewsFpbnBQ%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63ca5012dfb72bd2-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 8, 2021 11:01:45.927328110 CEST	2428	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-133B76AB9374D6781F41A2D553BC2BA3.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf
Apr 8, 2021 11:01:45.947901011 CEST	2429	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:01:45 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 10:01:45 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-133B76AB9374D6781F41A2D553BC2BA3.html cf-request-id: 095250644f00002bd223b7d000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2FM5OpJ9ZNhUXYnGpSkNb%2FUtZPySDSsvajfeM4j8STf9GIOWR45sdkEsLIhpSSfqEN7XEGXfP8XhuLIkYDfbs2LuwkZfpRXsVYCZSjrNCUOzV2wU%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63ca501a1bb42bd2-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Apr 8, 2021 11:01:48.776110888 CEST	3738	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C52937048F55BFE92995966F69D90F1.html HTTP/1.1 UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: myliverpoolnews.cf

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:01:48.797709942 CEST	3739	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:01:48 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 10:01:48 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-5C5293704 8F55BFE92995966F69D90F1.html cf-request-id: 0952506f7100002bd2259ac000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ThxZPwViEomojqqL9TY KZl1FY0onC5hnScyCYl%2BZodngPBmYO9P1MTEK1lipzYJy0Mh8OBpGnFzpFVupNRQJ0RL8kyCbxJWmlX1LJu945sW b1Eo%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63ca502bea0c2bd2-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49720	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:02:35.342420101 CEST	4915	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Apr 8, 2021 11:02:35.450606108 CEST	4915	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49755	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:15.023585081 CEST	5053	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:15.128920078 CEST	5054	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49762	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:17.074606895 CEST	5064	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:17.180192947 CEST	5065	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49764	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:18.124327898 CEST	5077	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:18.229459047 CEST	5078	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49765	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:19.316049099 CEST	5078	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:19.421181917 CEST	5084	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49768	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:20.784250021 CEST	5106	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:20.889914036 CEST	5106	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49769	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:22.463843107 CEST	5119	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:22.569499016 CEST	5119	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49770	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:24.109728098 CEST	5120	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:24.214984894 CEST	5120	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49771	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:25.727107048 CEST	5121	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:25.835148096 CEST	5121	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49772	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:26.918950081 CEST	5122	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:27.026371956 CEST	5122	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49773	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:27.954987049 CEST	5123	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:28.061099052 CEST	5123	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49722	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:02:37.180475950 CEST	4940	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:02:37.285245895 CEST	4941	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49774	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:29.059497118 CEST	5124	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:29.167048931 CEST	5124	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49775	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:29.584446907 CEST	5125	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Apr 8, 2021 11:03:29.689801931 CEST	5126	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49776	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:29.802161932 CEST	5126	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:29.908320904 CEST	5127	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49778	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.080657959 CEST	5131	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:30.185421944 CEST	5133	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49779	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.261841059 CEST	5134	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.367794991 CEST	5134	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49780	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.485392094 CEST	5135	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:30.592964888 CEST	5135	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49781	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.704296112 CEST	5136	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:30.812805891 CEST	5136	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49782	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:30.921722889 CEST	5137	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:31.028373957 CEST	5137	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49784	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.139547110 CEST	5138	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:31.245043039 CEST	5138	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49783	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.139666080 CEST	5138	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:31.245871067 CEST	5139	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49726	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:03.263449907 CEST	4965	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:03.370083094 CEST	4966	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49785	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.359153986 CEST	5139	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.465229988 CEST	5140	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49787	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.574191093 CEST	5141	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:31.680071115 CEST	5142	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49788	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:31.793252945 CEST	5147	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:31.899229050 CEST	5149	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49789	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:32.138542891 CEST	5154	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:32.243829012 CEST	5154	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49790	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:32.355576038 CEST	5155	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:32.463823080 CEST	5155	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49791	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:32.597414017 CEST	5156	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:32.702333927 CEST	5156	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49792	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:32.810532093 CEST	5156	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:32.915160894 CEST	5157	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49793	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:33.327660084 CEST	5157	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:33.433768988 CEST	5158	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49794	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:33.553150892 CEST	5158	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:33.659982920 CEST	5159	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49796	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:34.491008043 CEST	5165	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:34.597080946 CEST	5165	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49729	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:05.745573044 CEST	4991	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:05.851958036 CEST	4991	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49799	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:34.765099049 CEST	5177	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:34.871043921 CEST	5181	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49800	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:34.983300924 CEST	5217	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:35.091293097 CEST	5218	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49801	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:35.199928999 CEST	5218	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:35.306433916 CEST	5219	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49802	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:35.417623043 CEST	5219	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:35.523013115 CEST	5220	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49803	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:35.631524086 CEST	5220	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:35.737811089 CEST	5221	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49730	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:08.507339954 CEST	4992	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:08.612941980 CEST	4992	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49731	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:09.783368111 CEST	4992	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:09.888408899 CEST	4993	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49732	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:11.054966927 CEST	4993	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:11.160370111 CEST	4994	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49733	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:11.827866077 CEST	4995	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:11.934300900 CEST	4996	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49742	162.88.193.70	80	C:\Users\user\Desktop\lfQuSBwdSf.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:03:13.074529886 CEST	5021	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Apr 8, 2021 11:03:13.179763079 CEST	5022	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 104 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 38 35 2e 33 32 2e 32 32 32 2e 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 185.32.222.8</body></html>

HTTPS Packets

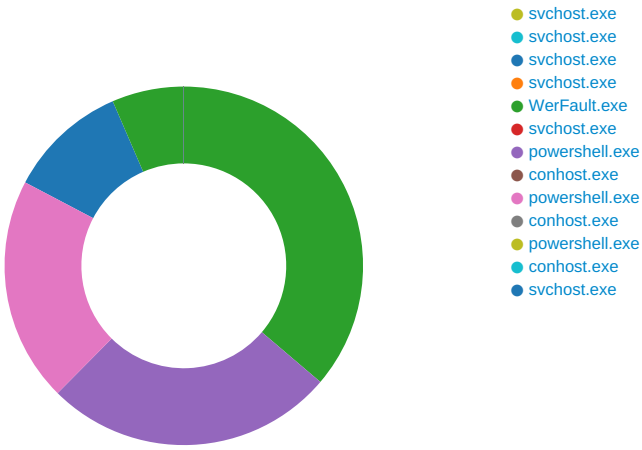
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 11:01:44.910068989 CEST	104.21.56.119	443	192.168.2.3	49701	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Mar 31 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Mar 31 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 11:02:55.378983021 CEST	172.67.188.154	443	192.168.2.3	49725	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 10 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 11:03:12.451477051 CEST	172.67.188.154	443	192.168.2.3	49737	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 10 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Apr 8, 2021 11:03:30.037919044 CEST	172.67.188.154	443	192.168.2.3	49777	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 10 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: lfQuSBwdSf.exe PID: 2788 Parent PID: 5552

General

Start time:	11:01:42
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\lfQuSBwdSf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\lfQuSBwdSf.exe'
Imagebase:	0xcb0000
File size:	46080 bytes
MD5 hash:	0802967C1D72DEEB4E1B79AF74FDB553
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\WrdAHTtKmtDmuc	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	3	6CE91E60	CreateFileW
C:\Windows\Cursors\WQzhTjfBsYrOnkh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE9BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CE9DD66	CopyFileW
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CE9DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32 20 39 39 20 39 37 20 31 31 30 20 31 31 30 20 31 31 31 20 31 31 36 20	77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32 99 97 110 110 111 116	success or wait	1422	6CE91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\WrdAHTtKmtDmuc	unknown	3496	34 20 34 20 31 31 38 20 31 31 38 20 31 30 39 20 31 30 39 20 31 35 34 20 36 35 20 34 36 20 34 36 20 33 39 20 33 39 20 32 31 35 20 32 31 34 20 36 35 20 32 30 35 20 32 35 33 20 32 35 33 20 31 33 37 20 31 33 37 20 31 30 31 20 31 30 31 20 31 36 37 20 37 38 20 33 32 20 33 32 20 39 31 20 39 31 20 34 31 20 34 30 20 39 30 20 32 33 30 20 32 31 32 20 32 31 32 20 32 32 38 20 32 32 38 20 32 35 30 20 32 35 30 20 32 38 20 31 39 35 20 31 37 39 20 31 37 39 20 32 33 33 20 32 33 33 20 38 39 20 38 38 20 31 34 35 20 32 39 20 34 35 20 34 35 20 33 31 20 33 31 20 31 35 33 20 31 35 33 20 31 32 36 20 33 37 20 38 34 20 38 34 20 34 34 20 34 34 20 31 20 30 20 31 32 34 20 38 20 35 38 20 35 38 20 31 30 20 31 30 20 31 36 32 20 31 36 32 20 33 32 20 31 39 39 20 31 37 36 20 31 37 36 20 32	4 4 118 118 109 109 154 65 46 46 39 39 215 214 65 205 253 253 137 137 101 101 167 78 32 32 91 91 41 40 90 230 212 212 228 228 250 250 28 195 179 179 233 233 89 88 145 29 45 45 31 31 153 153 126 37 84 84 44 44 1 0 124 8 58 58 10 10 162 162 32 199 176 176 2	success or wait	3	6CE91B4F	WriteFile
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	0	46080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0e 2e f5 ed 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 68 00 00 00 4a 00 00 00 00 00 00 1e 86 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 d7 c0 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................. "...0..h...J........... ....@.. ....@................	success or wait	1	6CE9DD66	CopyFileW
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CE9DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	success or wait	748	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	600	end of file	2	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	end of file	2	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	696	end of file	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6E00D72F	unknown
C:\Users\user\Desktop\lfQuSBwdSf.exe	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Users\user\Desktop\lfQuSBwdSf.exe	unknown	512	success or wait	1	6E00D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CE95F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CE95F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CE95F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	dword	0	success or wait	1	6CE9C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\lfQuSBwdSf.exe	dword	0	success or wait	1	6CE9C075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	wyreCRIln	unicode	C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	success or wait	1	6CE9646A	RegSetValueExW

Analysis Process: svchost.exe PID: 4908 Parent PID: 568

General

Start time:	11:01:50
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 1004 Parent PID: 2788

General

Start time:	11:01:55
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wacrv0pl.app.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3unvo0at.i2z.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\Documents\20210408	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE9BEFF	CreateDirectoryW
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.Pgu86VMD.20210408110201.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wacrv0pl.app.ps1	success or wait	1	6CE96A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3unvo0at.i2z.psm1	success or wait	1	6CE96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wacrv0pl.app.ps1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3unvo0at.i2z.psm1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.Pgu86VMD.20210408110201.txt	unknown	3	ef bb bf	...	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.Pgu86VMD.20210408110201.txt	unknown	685	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 34 30 38 31 31 30 32 32 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210408110225..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CE91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	2	6CE91B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0d 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CE91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CE91B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E02CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E031F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6E03203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	119	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CE91B4F	ReadFile

Analysis Process: conhost.exe PID: 4808 Parent PID: 1004

General

Start time:	11:01:56
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: powershell.exe PID: 720 Parent PID: 2788

General

Start time:	11:01:56
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\lfQuSBwdSf.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDF5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDF5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dkeuwky5.kyp.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bk34zenz.mnc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.6CUcdU4H.20210408110202.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dkeuwky5.kyp.ps1	success or wait	1	6CE96A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bk34zenz.mnc.psm1	success or wait	1	6CE96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dkeuwky5.kyp.ps1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bk34zenz.mnc.psm1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.6CUcdU4H.20210408110202.txt	unknown	3	ef bb bf	...	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.6CUcdU4H.20210408110202.txt	unknown	675	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 34 30 38 31 31 30 32 33 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210408110230..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CE91B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E02CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E031F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6E03203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	122	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile

Analysis Process: conhost.exe PID: 4456 Parent PID: 720

General

Start time:	11:01:57
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 1000 Parent PID: 2788

General

Start time:	11:01:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDF5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CDF5B28	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afdwa5sz.ycm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cv5sw5e3.x0i.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.+ytC9MFS.20210408110204.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE91E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afdwa5sz.ycm.ps1	success or wait	1	6CE96A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cv5sw5e3.x0i.psm1	success or wait	1	6CE96A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_afdwa5sz.ycm.ps1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cv5sw5e3.x0i.psm1	unknown	1	31	1	success or wait	1	6CE91B4F	WriteFile
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.+ytC9MFS.20210408110204.txt	unknown	3	ef bb bf	...	success or wait	1	6CE91B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210408\PowerShell_transcript.216554.+ytC9MFS.20210408110204.txt	unknown	685	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 34 30 38 31 31 30 32 33 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210408110234..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	5	6CE91B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	1	6CE91B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E02CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E031F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6E03203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	3	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CE91B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CE91B4F	ReadFile

Analysis Process: conhost.exe PID: 5988 Parent PID: 1000

General

Start time:	11:01:57
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 3984 Parent PID: 2788

General

Start time:	11:02:03
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: conhost.exe PID: 5816 Parent PID: 3984

General

Start time:	11:02:03
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6216 Parent PID: 568

General

Start time:	11:02:04
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: timeout.exe PID: 6248 Parent PID: 3984

General

Start time:	11:02:04
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xee0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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: 6528 Parent PID: 3388

General

Start time:	11:02:11
Start date:	08/04/2021
Path:	C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe'
Imagebase:	0xf50000
File size:	46080 bytes
MD5 hash:	0802967C1D72DEEB4E1B79AF74FDB553
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000011.00000002.517681508.0000000004965000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000011.00000002.517681508.0000000004965000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E04CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E025705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E02CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF803DE	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	success or wait	2	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	success or wait	1348	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	696	end of file	2	6CE91B4F	ReadFile
C:\Users\user\WrdAHTtKmtDmuc	unknown	4096	end of file	2	6CE91B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF803DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E025705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE91B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6E00D72F	unknown
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	unknown	4096	success or wait	1	6E00D72F	unknown
C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe	unknown	512	success or wait	1	6E00D72F	unknown

Analysis Process: svchost.exe PID: 6624 Parent PID: 568

General

Start time:	11:02:15
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6672 Parent PID: 568

General

Start time:	11:02:16
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6712 Parent PID: 568

General

Start time:	11:02:17
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: lfQuSBwdSf.exe PID: 6864 Parent PID: 2788

General

Start time:	11:02:19
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\lfQuSBwdSf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\lfQuSBwdSf.exe
Imagebase:	0x7d0000
File size:	46080 bytes
MD5 hash:	0802967C1D72DEEB4E1B79AF74FDB553
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000015.00000002.485923538.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000015.00000002.485923538.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6872 Parent PID: 568

General

Start time:	11:02:19
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6908 Parent PID: 3388

General

Start time:	11:02:20
Start date:	08/04/2021
Path:	C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe'
Imagebase:	0x640000
File size:	46080 bytes
MD5 hash:	0802967C1D72DEEB4E1B79AF74FDB553
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000017.00000002.541864387.0000000004A72000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000017.00000002.541864387.0000000004A72000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6932 Parent PID: 568

General

Start time:	11:02:20
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7064 Parent PID: 568

General

Start time:	11:02:21
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7152 Parent PID: 568

General

Start time:	11:02:22
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6164 Parent PID: 2788

General

Start time:	11:02:24
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2788 -s 2300
Imagebase:	0xa40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 1648 Parent PID: 568

General

Start time:	11:02:29
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 4424 Parent PID: 6908

General

Start time:	11:02:47
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 2120 Parent PID: 4424

General

Start time:	11:02:47
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5092 Parent PID: 6908

General

Start time:	11:02:48
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5136 Parent PID: 5092

General

Start time:	11:02:48
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3348 Parent PID: 6908

General

Start time:	11:02:49
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\WQzhTjfBsYrOnkh\svchost.exe' -Force
Imagebase:	0xb0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5224 Parent PID: 3348

General

Start time:	11:02:50
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5232 Parent PID: 568

General

Start time:	11:02:50
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis