

Analysis of Zeus Banking Trojan

Fingerprint:

VirusTotal output:

The screenshot shows the VirusTotal analysis interface for a file named 'invoice_2318362983713_823931342io.pdf.exe'. The main summary indicates 63 out of 72 security vendors flagged the file as malicious. The file is a PDF document (PDF) with a size of 247.00 KB, analyzed 1 month ago. The file type is identified as EXE. Threat categories listed include pexe, direct-cpu-clock-access, via-tor, malware, detect-debug-environment, suspicious-udp, checks-user-input, self-delete, persistence, and long-sleeps. A 'Community Score' of 63 is shown, with a total of 433 community members. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (29+). A green banner encourages joining the community for additional insights and automation. The 'Popular threat label' is trojan.zaccess/sirefef. Threat categories listed are trojan, dropper, pua. Family labels include zaccess, sirefef, wldcr. The 'Security vendors' analysis' section lists 15 vendors and their findings:

Vendor	Threat Label	Family Labels	
AhnLab-V3	Trojan/Win32.ZAccess.R87034	Alibaba	Backdoor.Win32.Obfuscator.71cb6d44
AliCloud	Backdoor:Win/ZAccess.emkb	ALYac	Trojan.ZeroAccess.RN
Arcabit	Trojan.WLDCR.C	Arctic Wolf	Unsafe
Avast	Win32:MalwareX-gen [Cryp]	AVG	Win32:MalwareX-gen [Cryp]
Avira (no cloud)	TR/Crypt.XPACK.52658	BitDefender	Trojan.WLDCR.C
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.zaccess	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Maxplus.14813
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.WLDCR.C (B)
eScan	Trojan.WLDCR.C	ESET-NOD32	Win32/Sirefef.FY.Trojan
Fortinet	W32/Generic.AC.3F8DF6ltr	GData	Win32.Trojan.Agent.TKFRZ8
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Gen.ccIs4
Ikarus	Trojan-Dropper.Win32.Sirefef	Jiangmin	Backdoor/ZAccess.psh

Hashes:

sha256:69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

md5:459E320C8A8F7E7049FF769CD123FD31

File Name: invoice_2318362983713_823931342io.pdf.exe

file > first 32 bytes (text),MZ.....@

Basic Static Analysis

Pestudio output:

The screenshot shows the Pestudio interface with the following details:

- File Path:** c:\users\cyber\Desktop\invoice_2318362983713_823931342io.pdf.exe (read-only)
- Properties:**
 - file**: sha256 - 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
 - file > sha256**: 69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169
 - file > first 32 bytes (hex)**: 4D 5A 90 00 03 00 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
 - file > first 32 bytes (text)**: MZ.....@.....
 - file > type**: executable, 32-bit, GUI
 - file > version**: n/a
 - file > description**: n/a
 - entry-point > first 32 bytes (hex)**: 55 BB EC 83 E4 F8 83 EC 7C A1 94 FC 40 00 8B 0D 9C FC 40 00 8B 15 98 FC 40 00 0F AF CA 53 56 35
 - entry-point > location**: 0x0000A3B6 (section[.text])
 - file > signature**: Microsoft Linker 10.0 | Visual Studio 2008
- Stamps:**
 - stamp > compiler**: Mon Nov 25 10:32:03 2013 (UTC)
 - stamp > debug**: n/a
 - stamp > resource**: n/a
 - stamp > import**: n/a
 - stamp > export**: Mon Nov 25 10:32:01 2013 (UTC)
- names:**
 - file > name**: c:\users\cyber\Desktop\invoice_2318362983713_823931342io.pdf.exe
 - debug > file**: n/a
 - export > original-file-name**: corect.com
 - version**: n/a
 - manifest**: n/a
 - .NET > module > name**: n/a
 - certificate > program-name**: n/a

names	
<u>file > name</u>	c:\users\cyber\Desktop\invoice_2318362983713_823931342io.pdf.exe
<u>debug > file</u>	n/a
<u>export > original-file-name</u>	corect.com
<u>version</u>	n/a
<u>manifest</u>	n/a
<u>.NET > module > name</u>	n/a
<u>certificate > program-name</u>	n/a

corect.com yielded no interesting results.

property	value
<u>section</u>	<u>section[0]</u>
<u>name</u>	.text
<u>section > sha256</u>	8309B5D320B3D392E25AFD5...
<u>entropy</u>	6.707
<u>file > ratio (99.60%)</u>	18.42 %
<u>raw-address (begin)</u>	0x000000400
<u>raw-address (end)</u>	0x0000BA00
<u>raw-size (251904 bytes)</u>	0x0000B600 (46592 bytes)
<u>virtual-address (begin)</u>	0x00001000
<u>virtual-address (end)</u>	0x0000C571
<u>virtual-size (250379 bytes)</u>	0x0000B571 (46449 bytes)

Capa output:

```
Windows PowerShell
FLARE-VM 01/18/2026 08:28:33
PS C:\Users\Cyber > capa
usage: capa.exe [-h] [--version] [-v] [-vv] [-d] [-q] [--color {auto,always,never}]
[-f {auto,pe,dotnet,elf,sc32,sc64,cape,drakvuf,vmray,freeze,binexport2,binja_data
base}]
[-b {auto,vivisect,ida,pefile,binja,dotnet,binexport2,freeze,cape,drakvuf,vmray}]
[--restrict-to-functions RESTRICT_TO_FUNCTIONS]
[--restrict-to-processes RESTRICT_TO_PROCESSES]
[--os {auto,linux,macos,windows}] [-r RULES] [-s SIGNATURES] [-t TAG] [-j]
input_file
capa.exe: error: the following arguments are required: input_file
FLARE-VM 01/18/2026 08:28:38
PS C:\Users\Cyber > cd Desktop
FLARE-VM 01/18/2026 08:29:04
PS C:\Users\Cyber\Desktop > capa .\invoice_2318362983713_823931342io.pdf.exe
md5          ea039a854d20d7734c5add48f1a51c34
sha1          9615dca4c0e46b8a39de5428af7db060399230b2
sha256        69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
analysis      static
os            windows
format        pe
arch           i386
path          C:/Users/cyber/Desktop/invoice_2318362983713_823931342io.pdf.exe



| ATT&CK Tactic   | ATT&CK Technique                                                                                     |
|-----------------|------------------------------------------------------------------------------------------------------|
| DEFENSE EVASION | Obfuscated Files or Information [T1027]<br>Virtualization/Sandbox Evasion::System Checks [T1497.001] |



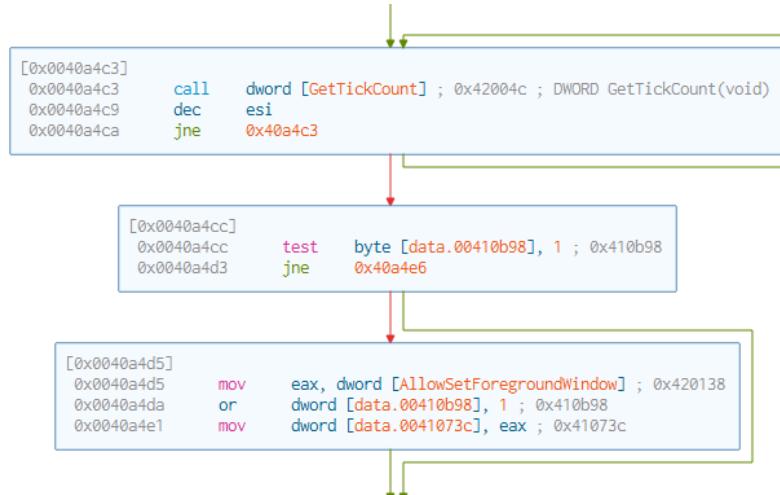
| MBC Objective                               | MBC Behavior                                                                                                    |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| ANTI-BEHAVIORAL ANALYSIS<br>DEFENSE EVASION | Virtual Machine Detection [B0009]<br>Obfuscated Files or Information::Encryption-Standard Algorithm [E1027.m05] |



| Capability                                                                                                                     | Namespace                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| reference anti-VM strings targeting VMWare<br>encrypt data using chaskey<br>resolve function by parsing PE exports (2 matches) | anti-analysis/anti-vm/vm-detection<br>data-manipulation/encryption/chaskey<br>load-code/pe |


FLARE-VM 01/18/2026 08:29:37
PS C:\Users\Cyber\Desktop >
```

Advanced Static Analysis:
this is an order of execution
Used cutter tool



gettickcount is an api call function that tells how long the machine is powered up

Basic Dynamic Analysis

Process Monitor procmon.

Process Tree								
<input type="checkbox"/> Only show processes still running at end of current trace	<input checked="" type="checkbox"/> Timelines cover displayed events only							
Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
msedge.exe (2668)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-354G5...	"C:\Program Files ...	19/01/2026 9:09...	19/01/2026 9:09
msedge.exe (2232)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-354G5...	"C:\Program Files ...	19/01/2026 9:09...	19/01/2026 9:09
Procmon64.exe (4524)	Process Monitor	C:\Tools\sysintern...		Sysinternals - ww...	DESKTOP-354G5...	"C:\Tools\sysinter...	19/01/2026 8:44...	n/a
invoice_2318362983713_8239		C:\Users\Cyber\D...			DESKTOP-354G5...	"C:\Users\Cyber\...	19/01/2026 8:44...	19/01/2026 8:45
InstallFlashPlayer.exe (4172)	Adobe® Flash® Pl...	C:\Users\Cyber\A...		Adobe Systems, I...	DESKTOP-354G5...	"C:\Users\Cyber\...	19/01/2026 8:45...	19/01/2026 8:45
InstallFlashPlayer.exe (1)	Adobe® Flash® Pl...	C:\Users\Cyber\A...		Adobe Systems, I...	DESKTOP-354G5...	"C:\Users\Cyber\...	19/01/2026 8:45...	n/a
WerFault.exe (4528)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\Sys...	19/01/2026 8:45...	19/01/2026 8:45
cmd.exe (1708)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-354G5...	"C:\Windows\syst...	19/01/2026 8:45...	19/01/2026 8:45
Conhost.exe (112)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	"??C:\Windows\...\\?C:\Windows\...	19/01/2026 8:45...	19/01/2026 8:45
Idle (0)	Idle	Custom		NT AUTHORITY\...			20/01/2026 9:07...	n/a
System (0)	System	Custom					20/01/2026 9:07...	n/a

Process Tree

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
msedge.exe (2668)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-354G5...	"C:\Program Files ...	19/01/2026 9:09...	19/01/2026 9:19 19 pm
msedge.exe (2232)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	DESKTOP-354G5...	"C:\Program Files ...	19/01/2026 9:09...	19/01/2026 9:09
Procmn64.exe (4524)	Process Monitor	C:\Tools\sysintern...		Sysinternals - ww...	DESKTOP-354G5...	"C:\Tools\sysinter...	19/01/2026 8:44...	n/a
invoice_2318362983713_8239		C:\Users\Cyber\.../			DESKTOP-354G5...	"C:\Users\Cyber\.../	19/01/2026 8:44...	19/01/2026 8:45
InstallFlashPlayer.exe (4172)	Adobe® Flash® Pl...	C:\Users\Cyber\A...		Adobe Systems, I...	DESKTOP-354G5...	"C:\Users\Cyber\.../	19/01/2026 8:45...	19/01/2026 8:45
InstallFlashPlayer.exe (1)	Adobe® Flash® Pl...	C:\Users\Cyber\A...		Adobe Systems, I...	DESKTOP-354G5...	"C:\Users\Cyber\.../	19/01/2026 8:45...	n/a
WerFault.exe (4528)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\Sys...	19/01/2026 8:45...	19/01/2026 8:45
cmd.exe (1708)	Windows Comma...	C:\Windows\Sys...		Microsoft Corporat...	DESKTOP-354G5...	"C:\Windows\Syst...	19/01/2026 8:45...	19/01/2026 8:45
Conhost.exe (112)	Console Window ...	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	\??C:\Windows\.../	19/01/2026 8:45...	19/01/2026 8:45
Idle (0)	Idle						20/01/2026 9:07...	n/a
System (4)	System				NT AUTHORITY\...		20/01/2026 9:07...	n/a
Registry (92)	Registry				NT AUTHORITY\...		20/01/2026 9:07...	n/a
smss.exe (312)	Windows Session ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\SystemRoot\System...		20/01/2026 9:07...	n/a
csrss.exe (416)	Client Server Runt...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\%SystemRoot%\s...		20/01/2026 9:07...	n/a
wininit.exe (492)	Windows Start-Up...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\wininit.exe		20/01/2026 9:07...	n/a
services.exe (632)	Services and Cont...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		20/01/2026 9:07...	n/a
svchost.exe (1584)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
AUDIODG.EXE (5720)	Windows Audio D...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:44...	19/01/2026 8:50
svchost.exe (1632)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
svchost.exe (1644)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
svchost.exe (1768)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
svchost.exe (1860)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
svchost.exe (1868)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a
spoolsv.exe (1876)	Spooler SubSyst...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...\C:\Windows\Syst...		19/01/2026 8:07...	n/a

Description: Adobe® Flash® Player Installer/Uninstaller 11.0 r1

Company: Adobe Systems, Inc.

Path: C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe

Command: "C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe"

User: DESKTOP-354G5UF\Cyber

PID: 1700 Started: 19/01/2026 8:45:22 pm

[Go To Event](#) [Include Process](#) [Include Subtree](#) [Close](#)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path Result Detail

Time ...	Process Name	PID	Operation	Path	Result	Detail
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\msimg32.dll	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	WriteFile	C:\Users\Cyber\AppData\Local\Temp\msimg32.dll	SUCCESS	Offset: -1, L
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\msimg32.dll	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	WriteFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Offset: -1, L
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	QueryRemotePr...	C:\Users\Cyber\AppData\Local\Temp	INVALID PARAM...	
8:44:5...	invoice_23183...	1896	QueryDirectory	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	FileInformat
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	FileSystemControl	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	CANCELLED	Control: FS*
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	QueryBasicInfor...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	CreationTim
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	WriteFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Offset: 0, L
8:44:5...	invoice_23183...	1896	SetEndOfFileIn...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	EndOfFile: I
8:44:5...	invoice_23183...	1896	CreateFileMapp...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	SyncType:
8:44:5...	invoice_23183...	1896	CreateFileMapp...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	FILE LOCKED WI...	SyncType:
8:44:5...	invoice_23183...	1896	QueryStandardI...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	AllocationSi
8:44:5...	invoice_23183...	1896	CreateFileMapp...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	SyncType:
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	CreateFileMapp...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	FILE LOCKED WI...	SyncType:
8:44:5...	invoice_23183...	1896	CreateFileMapp...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	SyncType:
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc
8:44:5...	invoice_23183...	1896	QueryBasicInfor...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	CreationTim
8:44:5...	invoice_23183...	1896	CloseFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Desired Acc

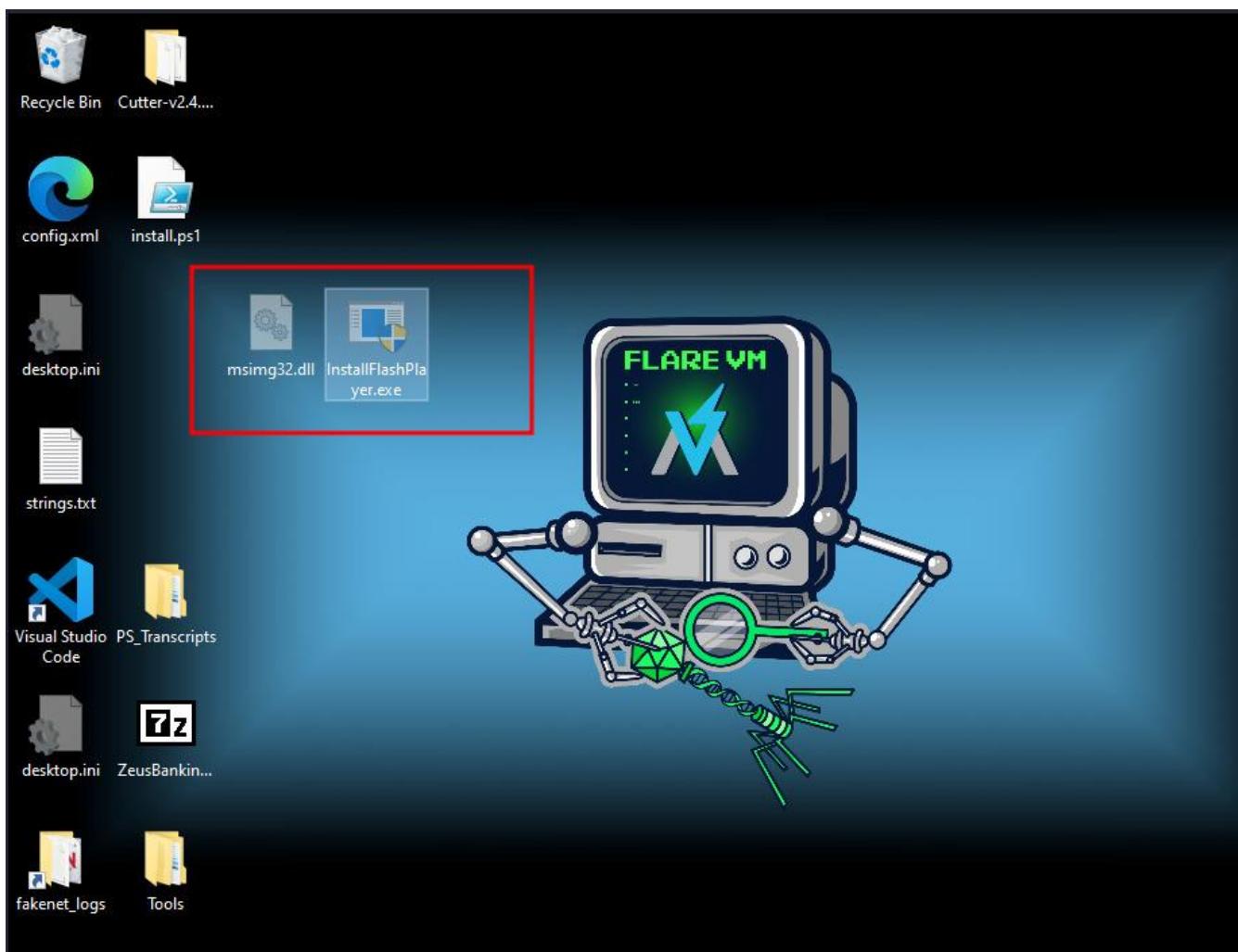
Showing 370 of 2,779,799 events (0.013%)

Backed by virtual memory

File		Home	Share	View	Manage	C:\Users\Cyber\AppData\Local\Temp	—	□	X
					Application Tools				
< AppData > Local > Temp >					Search Temp				
Name					Date modified	Type		Size	
cv_aebug.log					19/01/2020 9:09 pm	Text Document		/ KB	
db667c2d-ffb0-42a9-9268-4ff7011f2f55.t...					18/01/2026 2:41 am	TMP File		0 KB	
dd_MofCompiler_20260117132927.log					17/01/2026 1:29 pm	Text Document		1 KB	
DESKTOP-354G5UF-20260119-0707.log					19/01/2026 7:07 am	Text Document		156 KB	
e5ea5419-1902-40e3-a1c4-cdba2b28b891...					18/01/2026 10:19 am	TMP File		0 KB	
eccfd51c-828b-4960-8993-15c289257366....					18/01/2026 9:39 am	TMP File		0 KB	
fe3f1b68-c45c-4cdc-8856-942a249e94ce.t...					18/01/2026 9:38 am	TMP File		0 KB	
git_version.txt					19/01/2026 6:09 am	Text Document		1 KB	
InstallFlashPlayer.exe					19/01/2026 8:44 pm	Application		88 KB	
Microsoft Visual C++ 2010 x64 Redistrib...					17/01/2026 1:42 pm	Chrome HTML Do...		78 KB	
Microsoft Visual C++ 2010 x64 Redistrib...					17/01/2026 1:42 pm	Text Document		262 KB	
Microsoft Visual C++ 2010 x64 Redistrib...					17/01/2026 4:03 pm	Chrome HTML Do...		87 KB	
Microsoft Visual C++ 2010 x64 Redistrib...					17/01/2026 4:03 pm	Text Document		677 KB	
Microsoft Visual C++ 2010 x86 Redistrib...					17/01/2026 4:03 pm	Chrome HTML Do...		82 KB	
Microsoft Visual C++ 2010 x86 Redistrib...					17/01/2026 4:03 pm	Text Document		396 KB	
msedge_installer.log					17/01/2026 12:27 pm	Text Document		10 KB	
msimg32.dll					19/01/2026 8:44 pm	Application exten...		247 KB	
offline					17/01/2026 10:53 pm	File		24 KB	
offline.session64					17/01/2026 10:53 pm	SESSION64 File		65 KB	
Procmon64.exe					19/01/2026 6:52 am	Application		2,093 KB	
StructuredQuery.log					18/01/2026 2:45 am	Text Document		10 KB	

Invoice is downloading some different programs .
Specifically install adobe flashplayer





Process Tree

Only show processes still running at end of current trace
 Timelines cover displayed events only

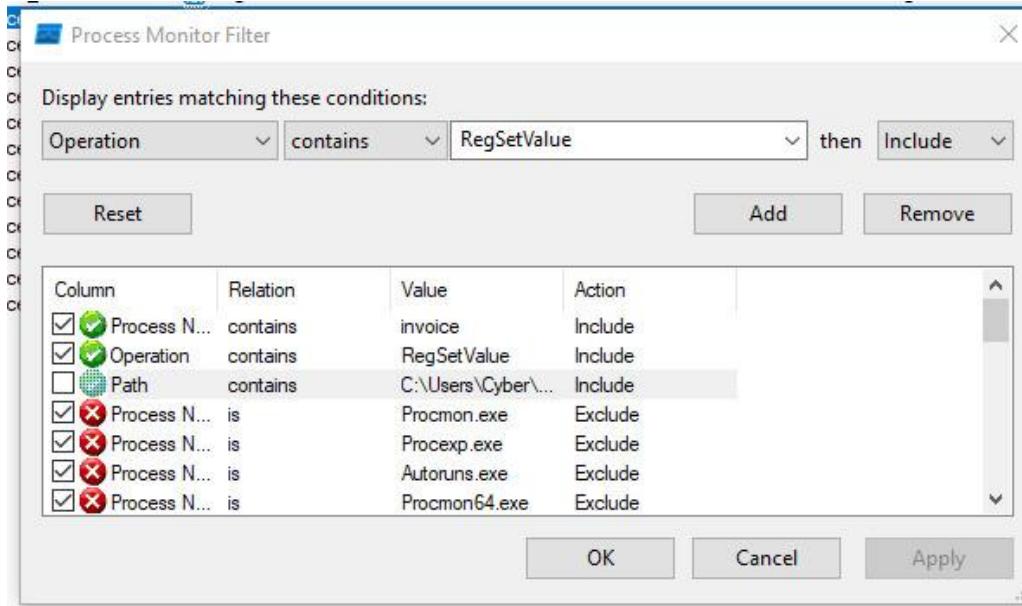
Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
svchost.exe (3640)	Host Process for ...	C:\Windows\system32\svchost.exe	19/01/2026 8:43... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	19/01/2026 8:43...	19/01/2026
svchost.exe (4724)	Host Process for ...	C:\Windows\System32\svchost.exe	19/01/2026 8:45... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	19/01/2026 8:45...	19/01/2026
WerFault.exe (4856)	Windows Problem... Host Process for ...	C:\Windows\System32\WerFault.exe	19/01/2026 8:45... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\System32\WerFault.exe	19/01/2026 8:45...	19/01/2026
sppsvc.exe (3136)	Microsoft Softwar...	C:\Windows\system32\sppsvc.exe	19/01/2026 8:50... n/a	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\sppsvc.exe	19/01/2026 8:50...	n/a
svchost.exe (5560)	Host Process for ...	C:\Windows\system32\svchost.exe	19/01/2026 8:57... n/a	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	19/01/2026 8:57...	n/a
MicrosoftEdgeUpdate.exe (4592)	Microsoft Edge U...	C:\Program Files\Microsoft\Edge\MicrosoftEdgeUpdate.exe	19/01/2026 8:57... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	"C:\Program Files\Microsoft\Edge\MicrosoftEdgeUpdate.exe"	19/01/2026 8:57...	19/01/2026
Microsoft Edge Update.exe (59)	Microsoft Edge U...	C:\Program Files\Microsoft\Edge\Microsoft Edge Update.exe	19/01/2026 8:57... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	"C:\Program Files\Microsoft\Edge\Microsoft Edge Update.exe"	19/01/2026 8:57...	19/01/2026
Updater.exe (1764)	Google Updater (x86)	C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe	19/01/2026 8:58... 19/01/2026	Google LLC	NT AUTHORITY\SYSTEM	"C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe" --system --window		
updater.exe (712)	Google Updater (x86)	C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe	19/01/2026 8:58... 19/01/2026	Google LLC	NT AUTHORITY\SYSTEM	"C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe" --system --window	19/01/2026 8:58...	19/01/2026
updater.exe (4588)	Google Updater (x86)	C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe	19/01/2026 8:58... 19/01/2026	Google LLC	NT AUTHORITY\SYSTEM	"C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe" --system --window	19/01/2026 8:58...	19/01/2026
updater.exe (3032)	Google Updater (x86)	C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe	19/01/2026 8:58... 19/01/2026	Google LLC	NT AUTHORITY\SYSTEM	"C:\Program Files\Google\Google Updater\144.0.7547.0\updater.exe" --system --window	19/01/2026 8:58...	19/01/2026
svchost.exe (320)	Host Process for ...	C:\Windows\system32\svchost.exe	19/01/2026 9:02... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	19/01/2026 9:02...	19/01/2026
svchost.exe (2552)	Host Process for ...	C:\Windows\system32\svchost.exe	19/01/2026 9:08... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	19/01/2026 9:08...	19/01/2026
elevation_service.exe (1208)	Microsoft Edge	C:\Program Files\Microsoft\Edge\MicrosoftEdge.exe	19/01/2026 9:08... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	"C:\Program Files\Microsoft\Edge\MicrosoftEdge.exe"	19/01/2026 9:08...	19/01/2026
elevation_service.exe (3892)	Microsoft Edge	C:\Program Files\Microsoft\Edge\MicrosoftEdge.exe	19/01/2026 9:08... 19/01/2026	Microsoft Corporat...	NT AUTHORITY\SYSTEM	"C:\Program Files\Microsoft\Edge\MicrosoftEdge.exe"	19/01/2026 9:08...	19/01/2026
svchost.exe (768)	Host Process for ...	C:\Windows\system32\svchost.exe	20/01/2026 9:07... n/a	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	20/01/2026 9:07...	n/a
DllHost.exe (2584)	COM Surrogate	C:\Windows\system32\dllhost.exe	19/01/2026 8:08... n/a	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Windows\system32\dllhost.exe	19/01/2026 8:08...	n/a
StartMenuExperienceHost.exe		C:\Windows\System32\StartMenuExperienceHost.exe	DESKTOP-354G5\... 19/01/2026 8:08... n/a	DESKTOP-354G5\...	DESKTOP-354G5\...	"C:\Windows\System32\StartMenuExperienceHost.exe"	19/01/2026 8:08...	n/a
RuntimeBroker.exe (4472)	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe	19/01/2026 8:08... n/a	Microsoft Corporat...	DESKTOP-354G5\...	C:\Windows\System32\RuntimeBroker.exe	19/01/2026 8:08...	n/a
SearchApp.exe (5388)	Search application	C:\Windows\System32\SearchApp.exe	19/01/2026 8:08... n/a	Microsoft Corporat...	DESKTOP-354G5\...	"C:\Windows\System32\SearchApp.exe"	19/01/2026 8:08...	n/a
RuntimeBroker.exe (5752)	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe	19/01/2026 8:08... n/a	Microsoft Corporat...	DESKTOP-354G5\...	C:\Windows\System32\RuntimeBroker.exe	19/01/2026 8:08...	n/a
RuntimeBroker.exe (2652)	Runtime Broker	C:\Windows\System32\RuntimeBroker.exe	19/01/2026 8:08... n/a	Microsoft Corporat...	DESKTOP-354G5\...	"C:\Windows\System32\RuntimeBroker.exe"	19/01/2026 8:08...	n/a
TextInputHost.exe (3712)	COM Surrogate	C:\Windows\System32\TextInputHost.exe	19/01/2026 8:43... n/a	Microsoft Corporat...	DESKTOP-354G5\...	"C:\Windows\System32\TextInputHost.exe"	19/01/2026 8:43...	n/a
DllHost.exe (5924)	COM Surrogate	C:\Windows\System32\dllhost.exe	19/01/2026 8:43... n/a	Microsoft Corporat...	DESKTOP-354G5\...	C:\Windows\System32\dllhost.exe	19/01/2026 8:43...	n/a

Description: Google Updater (x86)
 Company: Google LLC
 Path: C:\Program Files (x86)\Google\GoogleUpdater\144.0.7547.0\updater.exe
 Command: "C:\Program Files (x86)\Google\GoogleUpdater\144.0.7547.0\updater.exe" --system --window
 User: NT AUTHORITY\SYSTEM
 PID: 1764 Started: 19/01/2026 8:58:37 pm
 Exited: 19/01/2026 8:58:51 pm

[Go To Event](#) [Include Process](#) [Include Subtree](#) [Close](#)

every time the google chrome is updated the binary executable will be executed.

Registry Keys:

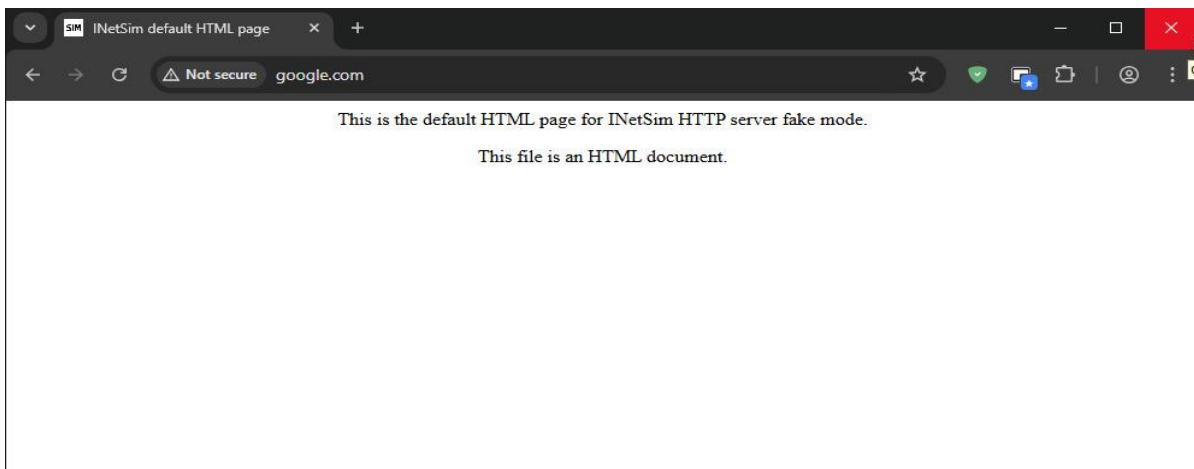


The screenshot shows the main Process Monitor window displaying a list of registry operations. The columns are: Time, Process Name, Operation, Path, Result, and Detail. The 'Operation' column for all rows shows 'RegSetValue'. The 'Path' column shows various registry keys under 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Google Update'. The 'Result' column shows 'SUCCESS' for all entries. The 'Detail' column provides specific details for each entry, such as type (REG_SZ, REG_BINARY, REG_DWORD), length, and data values.

Time	Process Name	Operation	Path	Result	Detail
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Google Update	SUCCESS	Type: REG_SZ, Length: 326, Data: "C:\Users\ Cyber\A..."
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuE...	SUCCESS	Type: REG_BINARY, Length: 100, Data: 60 24 B2 21 ...
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuE...	SUCCESS	Type: REG_BINARY, Length: 100, Data: 60 24 B2 21 ...
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuE...	SUCCESS	Type: REG_BINARY, Length: 100, Data: 60 24 B2 21 ...
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\U...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\U...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:44...	invoice_2318...18...	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\U...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
8:45...	invoice_2318...18...	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A0...	SUCCESS	Type: REG_BINARY, Length: 648, Data: 71 04 00 00 0...

Remnux as a DNS Server:

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
==== INetSim main process started (PID 1374) ====
Session ID:      1374
Listening on:    10.0.0.4
Real Date/Time: 2026-01-19 23:40:57
Fake Date/Time: 2026-01-19 23:40:57 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1378)
* smtps_465_tcp - started (PID 1382)
* http_80_tcp - started (PID 1379)
* ftp_21_tcp - started (PID 1385)
* smtp_25_tcp - started (PID 1381)
* pop3_110_tcp - started (PID 1383)
* pop3s_995_tcp - started (PID 1384)
* https_443_tcp - started (PID 1380)
* ftps_990_tcp - started (PID 1386)
done.
Simulation running.
```



Network Based Indicators

Wireshark:

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::a00:27ff:fe23... ff02::2		ICMPv6	70	Router Solicitation from 08:00:27:23:e4:d2
2	11.892677	10.0.0.3	10.0.0.4	DNS	85	Standard query 0x882a A fpdownload.macromedia.com
3	11.898649	10.0.0.4	10.0.0.3	DNS	101	Standard query response 0x882a A fpdownload.macromedia.com A ...
4	11.908286	10.0.0.3	10.0.0.4	TCP	66	49781 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_P...
5	11.908665	10.0.0.4	10.0.0.3	TCP	66	80 → 49781 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA...
6	11.908704	10.0.0.3	10.0.0.4	TCP	54	49781 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
7	11.909240	10.0.0.3	10.0.0.4	HTTP	235	GET /get/flashplayer/update/current/install/install_all_win_c...
8	11.909486	10.0.0.4	10.0.0.3	TCP	60	80 → 49781 [ACK] Seq=1 Ack=182 Win=64128 Len=0
9	11.918525	10.0.0.4	10.0.0.3	TCP	204	80 → 49781 [PSH, ACK] Seq=1 Ack=182 Win=64128 Len=150 [TCP PD...
10	11.918562	10.0.0.3	10.0.0.4	TCP	54	49781 → 80 [ACK] Seq=182 Ack=151 Win=261888 Len=0
11	11.918818	10.0.0.4	10.0.0.3	HTTP	312	HTTP/1.1 200 OK (text/html)
12	11.918834	10.0.0.3	10.0.0.4	TCP	54	49781 → 80 [ACK] Seq=182 Ack=409 Win=261632 Len=0
13	11.920199	10.0.0.4	10.0.0.3	TCP	60	80 → 49781 [FIN, ACK] Seq=409 Ack=182 Win=64128 Len=0
14	11.920239	10.0.0.3	10.0.0.4	TCP	54	49781 → 80 [ACK] Seq=182 Ack=410 Win=261632 Len=0
15	11.920929	10.0.0.3	10.0.0.4	TCP	54	49781 → 80 [FIN, ACK] Seq=182 Ack=410 Win=261632 Len=0

```
> Frame 7: Packet, 235 bytes on wire (1880 bits), 235 bytes captured (1
> Ethernet II, Src: PCSSystemtec_5e:8e:16 (08:00:27:5e:8e:16), Dst: PCS
> Internet Protocol Version 4, Src: 10.0.0.3, Dst: 10.0.0.4
> Transmission Control Protocol, Src Port: 49781, Dst Port: 80, Seq: 1,
> Hypertext Transfer Protocol
08 00 27 23 e4 d2 08 00 27 5e 8e 16 08 00 45 00  ...#....'^....E-
00 dd af 76 40 00 00 06 00 00 0a 00 00 03 0a 00  ...@.....
00 04 c2 75 00 50 91 04 81 09 d8 86 fb e7 50 18  ...u.P....P-
04 00 14 d6 00 00 47 45 54 20 2f 67 65 74 2f 66  .....GE T /get/f
0c 61 73 68 70 6c 61 79 65 72 2f 75 70 64 61 74  lashplay er/updat
05 2f 63 75 72 72 65 6e 74 2f 69 6e 73 74 61 6c  e/curren t/instal
0c 2f 69 6e 73 74 61 6c 6c 5f 61 6c 6c 5f 77 69  l/install_l_all_wi
0e 5f 63 61 62 5f 36 34 5f 61 78 5f 73 67 6e 2e  n_cab_64 _ax_sgn.
07 a0 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72  z HTTP/1.1 User
02 d4 41 67 65 6e 74 3a 20 46 6c 61 73 68 20 50 6c -Agent: Flash Pl
00 61 79 65 72 20 53 65 64 2f 33 2e 30 0d 0a 48 ayer See d/3.0.H
00 6f 73 74 3a 20 66 70 64 6f 77 6e 6c 6f 61 64 2e ost: fdp download.
00 6d 61 63 72 6f 6d 65 64 69 61 2e 63 6f 6d 0d 0a macromed ia.com.
00 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e Cache-Co ntrol: n
00 6f 2d 63 61 63 68 65 0d 0a 0d 0a o-cache: ...

```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · Ethernet



```
GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
User-Agent: Flash Player Seed/3.0
Host: fpdownload.macromedia.com
Cache-Control: no-cache
```

```
HTTP/1.1 200 OK
Date: Tue, 20 Jan 2026 05:49:25 GMT
Server: INetSim HTTP Server
Connection: Close
Content-Length: 258
Content-Type: text/html
```

```
<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```