

Analysis of Zeus Banking Trojan

Fingerprint: VirusTotal output:

63
/ 72

Community Score -433

63/72 security vendors flagged this file as malicious

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

invoice_2318362983713_823931342io.pdf.exe

Size 247.00 KB

Last Analysis Date 1 month ago

EXE

peexe direct-cpu-clock-access via-tor malware detect-debug-environment suspicious-udp checks-user-input self-delete persistence long-sleeps

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 29+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label 1 trojan.zaccess/sirefef

Threat categories trojan dropper pua

Family labels zaccess sirefef wldcr

Security vendors' analysis 1

Do you want to automate checks?

AhnLab-V3	1 Trojan.Win32.ZAccess.R87034	Alibaba	1 Backdoor.Win32/Obfuscator.71cb6d44
AliCloud	1 Backdoor.Win/ZAccess.emkb	ALYac	1 Trojan.ZeroAccess.RN
Arcabit	1 Trojan.WLDCR.C	Arctic Wolf	1 Unsafe
Avast	1 Win32-MalwareX-gen [Cryp]	AVG	1 Win32-MalwareX-gen [Cryp]
Avira (no cloud)	1 TR/Crypt.XPACK.52658	BitDefender	1 Trojan.WLDCR.C
Bkav Pro	1 W32.AIDetectMalware	CrowdStrike Falcon	1 Win/malicious_confidence_100% (W)
CTX	1 Exe.trojan.zaccess	Cynet	1 Malicious (score: 99)
DeepInstinct	1 MALICIOUS	DrWeb	1 BackDoor.Maxplus.14813
Elastic	1 Malicious (high Confidence)	Emsisoft	1 Trojan.WLDCR.C (B)
eScan	1 Trojan.WLDCR.C	ESET-NOD32	1 Win32/Sirefef.FY Trojan
Fortinet	1 W32/Generic.AC.3F8DF61tr	GData	1 Win32.Trojan.Agent.TKFR28
Google	1 Detected	Gridinsoft (no cloud)	1 Trojan.Win32.Gen.cc1s4
Ikarus	1 Trojan-Dropper.Win32.Sirefef	Jiangmin	1 Backdoor/ZAccess.osh

Hashes:

sha256:69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

md5:459E320C8A8F7E7049FF769CD123FD31

File Name:invoice_2318362983713_823931342io.pdf.exe

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

Basic Static Analysis

Pestudio output:

pestudio 9.61 - Malware Initial Assessment - www.winitor.com c:\users\cyber\desktop\invoice_2318362983713_823931342io.pdf.exe (read-only)		
file settings about		
c:\users\cyber\desktop\invoice_2318362983713_823931342io.pdf.exe	property	value
	file	
indicators (sections > self-modifying)	file > sha256	69E966E730557FDE8FD84317CDEF1EC00A8BB3470C0B58F3231E170168AF169
footprints (type > sha256)	file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 04 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
virustotal (offline)	file > first 32 bytes (text)	MZ.....@.....
dos-header (size > 64 bytes)	file > info	size: 252928 bytes, entropy: 6.982
dos-stub (size > 152 bytes)	file > type	executable, 32-bit, GUI
rich-header (tooling > Visual Studio 2008)	file > version	n/a
file-header (executable > 32-bit)	file > description	n/a
optional-header (subsystem > GUI)	entry-point > first 32 bytes (hex)	55 8B 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
directories (count > 4)	entry-point > location	0x0000A3B6 (section[.text])
sections (characteristics > self-modifying)	file > signature	Microsoft Linker 10.0 Visual Studio 2008
libraries (count > 3)	stamps	
imports (flag > 17)	stamp > compiler	Mon Nov 25 10:32:03 2013 (UTC)
exports (n/a)	stamp > debug	n/a
thread-local-storage (n/a)	stamp > resource	n/a
.NET (n/a)	stamp > import	n/a
resources (count > 11)	stamp > export	Mon Nov 25 10:32:01 2013 (UTC)
strings (count > 1416)	names	
debug (n/a)	file > name	c:\users\cyber\desktop\invoice_2318362983713_823931342io.pdf.exe
manifest (level > aslnvoker)	debug > file	n/a
version (n/a)	export > original-file-name	corect.com
certificate (n/a)	version	n/a
overlay (n/a)	manifest	n/a
	.NET > module > name	n/a
	certificate > program-name	n/a
sha256 > 69E966E730557FDE8FD84317CDEF1EC00A8BB3470C0B58F3231E170168AF169 cpu > 32-bit file > type > executable subsystem > GUI entry-point > 0x0000A3B6		

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

corect.com yielded no interesting results.

property	value
section	section[0]
name	.text
section > sha256	8309B5D320B3D392E25AFD5...
entropy	6.707
file > ratio (99.60%)	18.42 %
raw-address (begin)	0x00000400
raw-address (end)	0x0000BA00
raw-size (251904 bytes)	0x0000B600 (46592 bytes)
virtual-address (begin)	0x00001000
virtual-address (end)	0x0000C571
virtual-size (250379 bytes)	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] Virtualization/Sandbox Evasion::System Checks [T1497.001]

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

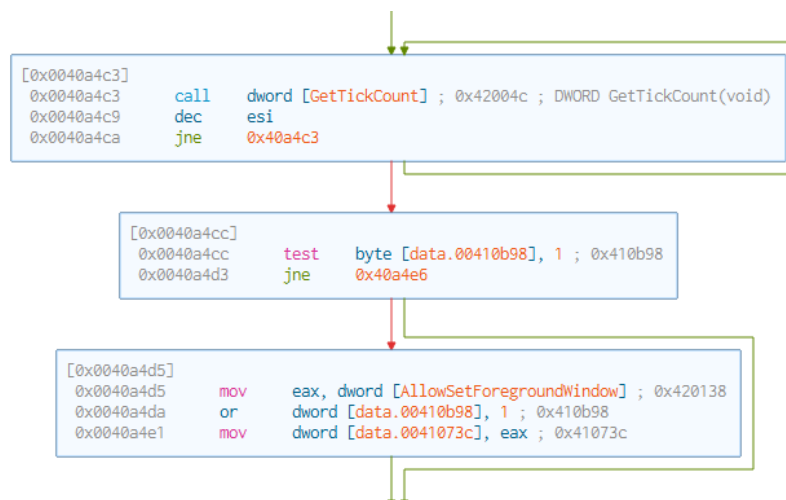
Capability	Namespace
reference anti-VM strings targeting VMWare encrypt data using chaskey resolve function by parsing PE exports (2 matches)	anti-analysis/anti-vm/vm-detection data-manipulation/encryption/chaskey load-code/pe

```
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\sysinter...		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\...	19/01/2026 8:45:...	19/01/2026 8:45	
Idle (0)	Idle						20/01/2026 9:07:...	n/a	
System (4)	System	System			NT AUTHORITY\...		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 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
Procmon64.exe (4524)	Process Monitor	C:\Tools\sysintem...		Sysintemals - ww...	DESKTOP-354G5...	"C:\Tools\sysinter...	19/01/2026 8:44:...	n/a
invoice_2318362983713_8239		C:\Users\Cyber\A...			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 (1708)	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 Comm...	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\Syst...	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 SubSyste...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	19/01/2026 8:07:...	n/a

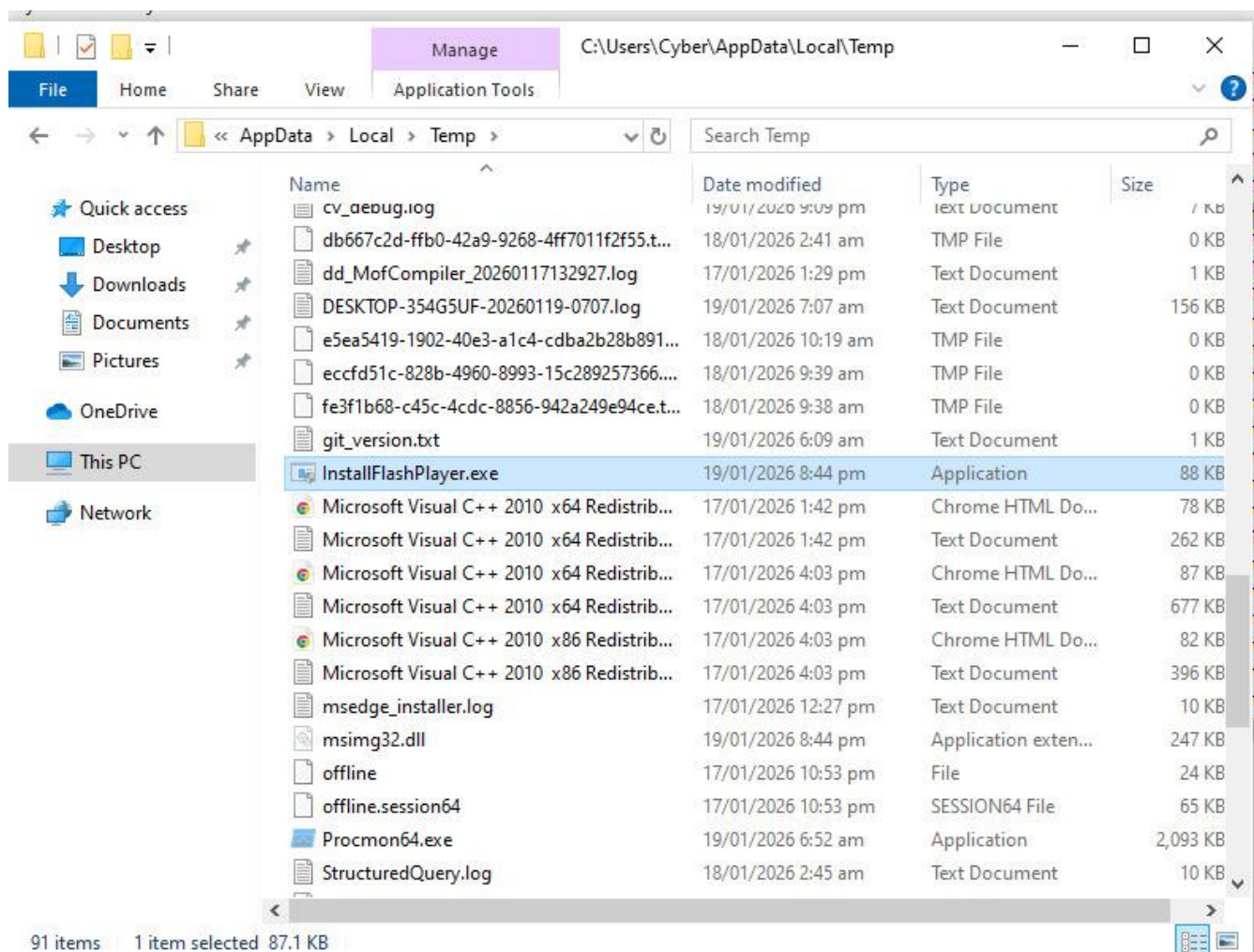
Description: Adobe® Flash® Player Installer/Uninstaller 11.0 r1
Company: Adobe Systems, Inc.
Path: C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe
Command: "C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe"
User: DESKTOP-354G5UF\Cyber
PID: 1700 Started: 19/01/2026 8:45:22 pm

Go To Event Include Process Include Subtree Close

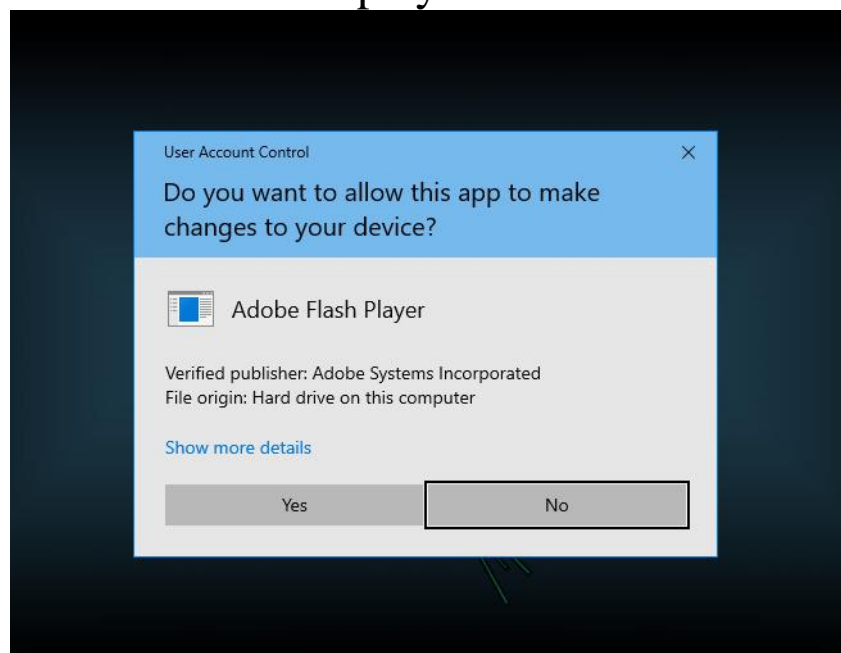
Process Monitor - Sysinternals: www.sysinternals.com									
File Edit Event Filter Tools Options Help									
Time ...	Process Name	PID	Operation	Path	Result	Detail			
8:44:5...	invoice_23183...	1896	CreateFile	C:\Users\Cyber\AppData\Local\Temp\msimg32.dll	SUCCESS	Desired Acc			
8:44:5...	invoice_23183...	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	Creation Tim			
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	SetEndOfFileInf...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	EndOfFile: 1			
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	QueryBasicInfor...	C:\Users\Cyber\AppData\Local\Temp\InstallFlashPlayer.exe	SUCCESS	Creation Tim			
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	Creation Tim			
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			

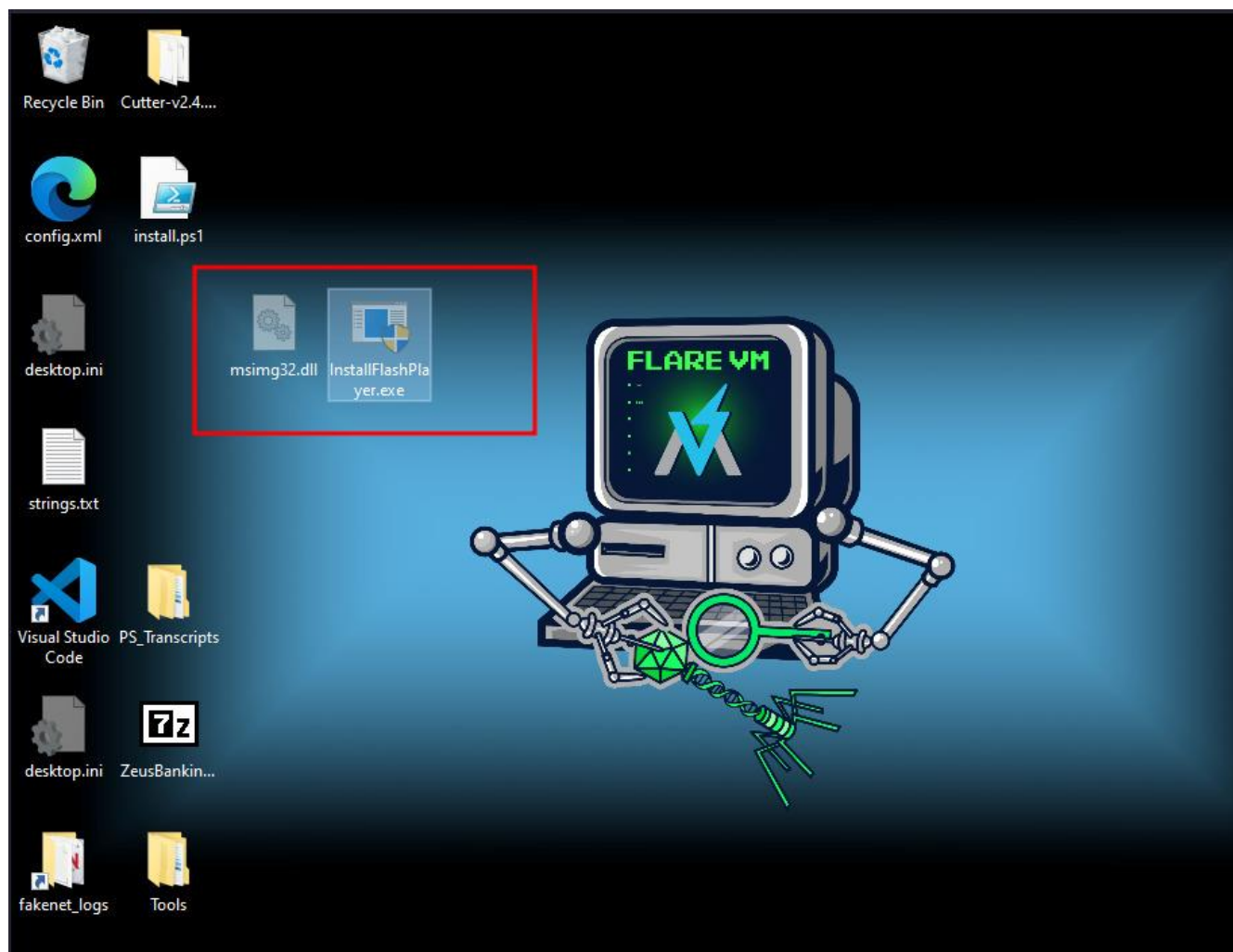
Showing 370 of 2,779,799 events (0.013%)

Backed by virtual memory



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\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	19/01/2026 8:43:...	19/01/2026
svchost.exe (4724)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	19/01/2026 8:45:...	19/01/2026
WerFault.exe (4856)	Windows Problem...	C:\Windows\Sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Sys...	19/01/2026 8:45:...	19/01/2026
spsvc.exe (3136)	Microsoft Softwar...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	19/01/2026 8:50:...	19/01/2026
svchost.exe (5560)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	19/01/2026 8:50:...	n/a
MicrosoftEdgeUpdate.exe (4592)	Microsoft Edge U...	C:\Program Files (...)		Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 8:57:...	19/01/2026
Updater.exe (1764)	Google Updater (x...	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 8:58:...	19/01/2026
updater.exe (712)	Google Updater (x...	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 8:58:...	19/01/2026
updater.exe (4588)	Google Updater (x...	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 8:58:...	19/01/2026
updater.exe (3032)	Google Updater (x...	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 8:58:...	19/01/2026
svchost.exe (320)	Host Process for ...	C:\Windows\Syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	19/01/2026 9:02:...	19/01/2026
svchost.exe (2552)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	19/01/2026 9:08:...	19/01/2026
elevation_service.exe (1208)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 9:08:...	19/01/2026
elevation_service.exe (3892)	Microsoft Edge	C:\Program Files (...)		Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	19/01/2026 9:08:...	19/01/2026
svchost.exe (768)	Host Process for ...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	20/01/2026 9:07:...	n/a
DllHost.exe (2584)	COM Surrogate	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	19/01/2026 8:08:...	n/a
StartMenuExperienceHost.exe		C:\Windows\Syst...			DESKTOP-354G5...	C:\Windows\Sys...	19/01/2026 8:08:...	n/a
RuntimeBroker.exe (4472)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\Syst...	19/01/2026 8:08:...	n/a
SearchApp.exe (5388)	Search application	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	"C:\Windows\Sys...	19/01/2026 8:08:...	n/a
RuntimeBroker.exe (5752)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\Syst...	19/01/2026 8:08:...	n/a
RuntimeBroker.exe (2652)	Runtime Broker	C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\Syst...	19/01/2026 8:08:...	n/a
TextInputHost.exe (3712)		C:\Windows\Syst...		Microsoft Corporat...	DESKTOP-354G5...	"C:\Windows\Sys...	19/01/2026 8:43:...	n/a
DllHost.exe (5924)	COM Surrogate	C:\Windows\syst...		Microsoft Corporat...	DESKTOP-354G5...	C:\Windows\syst...	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

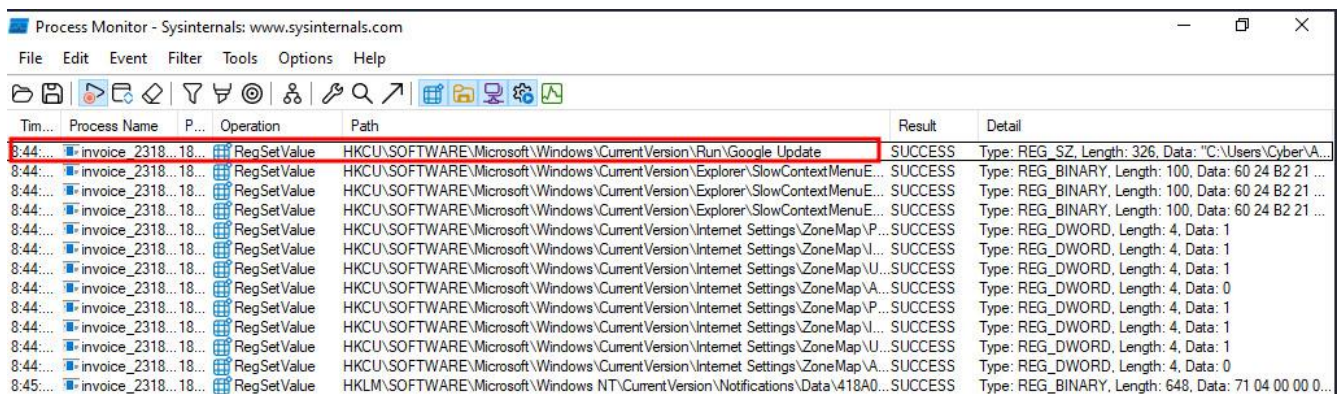
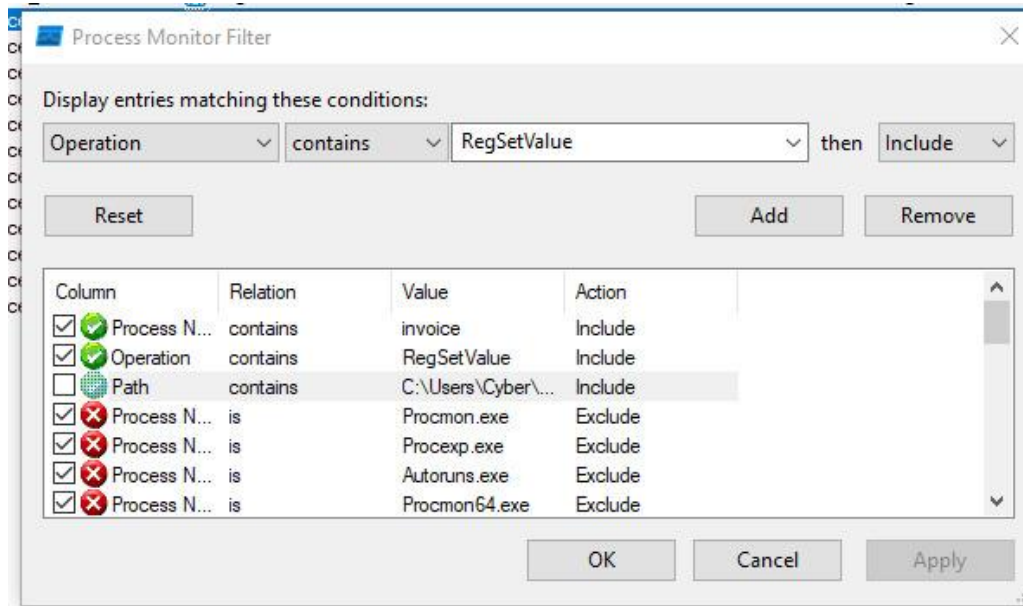
User: NT AUTHORITY\SYSTEM

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

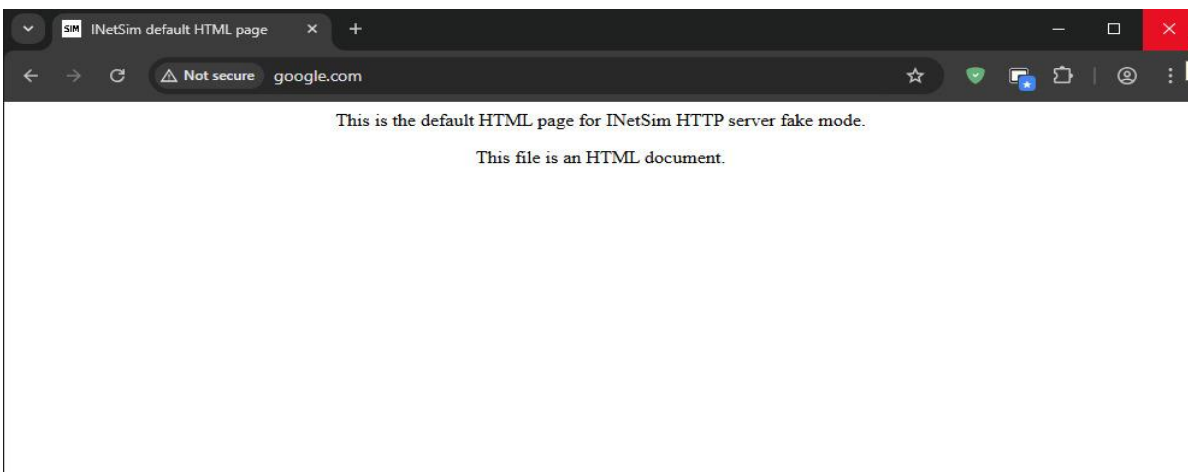
every time the google chrome is updated the binary executable will be executed.

Registry Keys:



Remnux as a DNS Server:

```
remnux@remnux: ~  
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:

The image shows a Wireshark network traffic capture. The top bar indicates 'Capturing from Ethernet'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The display filter is set to 'Apply a display filter ... <Ctrl-/>'. The packet list shows 15 packets. Packet 7 is selected, showing an HTTP GET request. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

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 (1880 bits) on interface 0

Ethernet II, Src: PCSSystemtec_5e:8e:16 (08:00:27:5e:8e:16), Dst: PCSSystemtec_5e:8e:16 (08:00:27:5e:8e:16)

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, Len: 235

Hypertext Transfer Protocol

0 08 00 27 23 e4 d2 08 00 27 5e 8e 16 08 00 45 00 ...'#....'A....E..

0 00 dd af 76 40 00 80 06 00 00 0a 00 00 03 0a 00 ...v@.....

0 00 04 c2 75 00 50 91 04 81 09 d8 86 fb e7 50 18 ...u-P.....P..

0 04 00 14 d6 00 00 47 45 54 20 2f 67 65 74 2f 66GET /get/f

0 6c 61 73 68 70 6c 61 79 65 72 2f 75 70 64 61 74 ..lashplay er/updat

0 65 2f 63 75 72 72 65 6e 74 2f 69 6e 73 74 61 6c ..e/curren t/install

0 6c 2f 69 6e 73 74 61 6c 6c 5f 61 6c 6c 5f 77 69 ..l/install_l_all_wi

0 6e 5f 63 61 62 5f 36 34 5f 61 78 5f 73 67 6e 2e ..n_cab_64_ax_sgn.

0 7a 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72 ..z HTTP/1.1..User

0 2d 41 67 65 6e 74 3a 20 46 6c 61 73 68 20 50 6c ..-Agent: Flash Pl

0 61 79 65 72 20 53 65 65 64 2f 33 2e 30 0d 0a 48 ..ayer See d/3.0..

0 6f 73 74 3a 20 66 70 64 6f 77 6e 6c 6f 61 64 2e ..ost: fpd ownload.

0 6d 61 63 72 6f 6d 65 64 69 61 2e 63 6f 6d 0d 0a ..macromed ia.com..

0 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e ..Cache-Co ntrol: n

0 6f 2d 63 61 63 68 65 0d 0a 0d 0a ..o-cache: ...


```
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>
```