Zeus (Zbot) Banking Trojan - Malware Analysis

Report Overview

Resources

- https://samples.vx-underground.org/root/Papers/Malware Defense/Malware Analysis/2023-03-14 - The Zeus Trojan Malware - Definition and Prevention.pdf
- https://www.malwarebytes.com/blog/news/2021/07/the-life-and-death-of-the-zeus-trojan
- https://krebsonsecurity.com/2015/02/fbi-3m-bounty-for-zeus-trojan-author/
- https://zeusmuseum.com/actors/
- https://github.com/ytisf/theZoo/tree/master/malware/Binaries/ZeusBankingVersion_26Nov2013
- https://web.archive.org/web/20210416013527/https://pfarrside.com/zeus-malware-analysis-remnux/

Background Information

- Primarily created to be a financial banking trojan.
- First spotted in the wild in 2007 when Zeus Trojan was caught stealing sensitive information from systems owned by the US Department of Transportation.
  - Since then, there have been 573+ known versions with 36 known families of the Zeus Trojan, according to website https://zeusmuseum.com/.
- Malicious code become public in 2011 after a leak. The suspected malware author of is Evgeniy Mikhailovich Bogachev (source: https://krebsonsecurity.com/2015/02/fbi-3m-bounty-for-zeus-trojan-author/)

- Delivery Methods:
    - Drive-by downloads: Require a user to visit a website that has the backdoor trojan code on it. Modern web browsers block these downloads by default. Attack vector is mostly obsolete.
    - Phishing & Spam Campaigns: Main infection method.
- Primary Goals:
    - Steal people's financial information to exfiltrate financial information.
    - Add machines to a globally distributed P2P botnet (depends on the family).
- Crackdown History:
    - FBI cracked down on Gameover Zeus (which was a prolific variant of the Zeus Trojan) in 2014.
    - An estimated 25% of computers were infected in the United States.
    - $100+ million in financial damages due to Gameover Zeus.
    - Evgeniy Mikhailovich Bogachev had a $3 million dollar bounty from the FBI. Continues to be one of the most wanted hackers.
- Impact:
    - Inspired hundreds of additional variants which use parts of source code.
    - Millions of infected machines with associated costs in damages in the millions.

Lab

Malware Composition

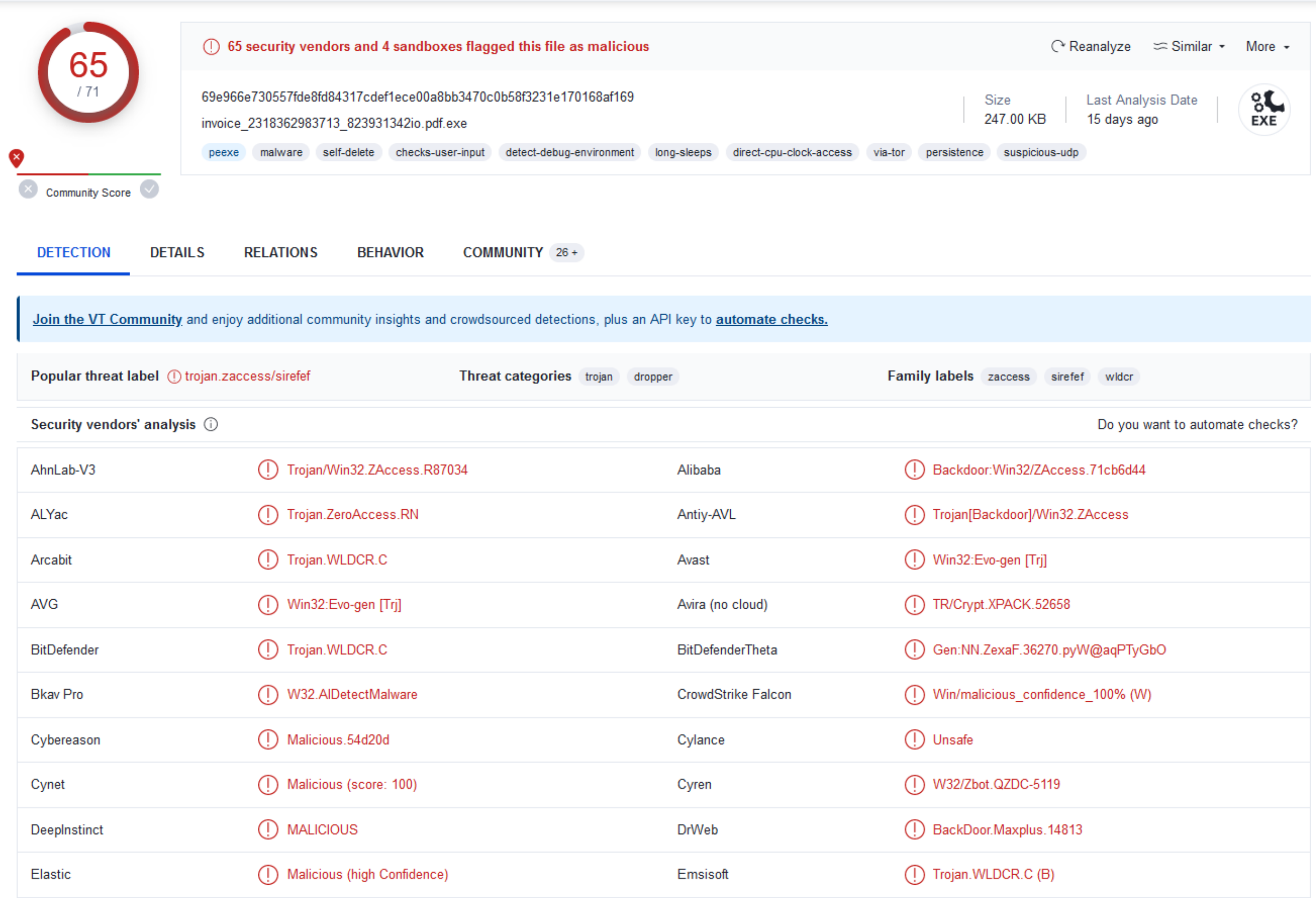
Filename: `invoice_2318362983713_823931342io.pdf.exe`

Hashes:

- md5: `EA039A854D20D7734C5ADD48F1A51C34`
- sha1: `9615DCA4C0E46B8A39DE5428AF7DB060399230B2`
- sha256: `69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169`

Basic Static Analysis

Virus Total



65 security vendors and 4 sandboxes flagged this file as malicious

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

invoice_2318362983713_823931342io.pdf.exe

Size 247.00 KB

Last Analysis Date 15 days ago

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

Popular threat label trojan.zaccess/sirefef Threat categories trojan dropper Family labels zaccess sirefef wldcr

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win32.ZAccess.R87034	Alibaba	Backdoor:Win32/ZAccess.71cb6d44
ALYac	Trojan.ZeroAccess.RN	Antiy-AVL	Trojan[Backdoor]/Win32.ZAccess
Arcabit	Trojan.WLDCR.C	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Crypt.XPACK.52658
BitDefender	Trojan.WLDCR.C	BitDefenderTheta	Gen:NN.ZexaF.36270.pyW@aqPTyGbO
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.54d20d	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Zbot.QZDC-5119
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Maxplus.14813
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.WLDCR.C (B)

65/71 security vendors flagged as malicious.

Strings

Tools Used: PeStudio, Floss.exe, & Capa

```
corect.com
```

```
AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyreroeno
KERNEL32.MulDiv
BagsSpicDollBikeAzonPoopHamsPyasmap
KERNEL32.SetCurrentDirectoryA
BardHolyawe
SHLWAPI.SHFreeShared
BathEftsDawnvilepughThroCymakohloverMitefuzerat
SHLWAPI.PathMakeSystemFolderW
BemaCadsPodsWavyCedeRadsbrioOustPerefenom
USER32.SetDlgItemTextW
BullbonyaweeWaitsnugTierDriblibye
KERNEL32.VirtualQuery
CameValeWauler
USER32.IsIconic
CedeSalsshulLimyThroliraValeDonabox
USER32.CreateCaret
```

```
CellrotoCrudUntohighCols
KERNEL32.CreateFileA
DenyLubeDunssawsOresvarut
SHLWAPI.PathRemoveFileSpecA
DragRoutflusCrowPeatmownNewsyaksSerfmare
USER32.DestroyIcon
Dumpcotsavo
USER32.SetDlgItemInt
DungBadebankBangGelthoboCocaBozotsksWheyVaryShoghoseNipsCadisi
USER32.EndPaint
ExitRollWoodGumsgamaSloerevsWussletssinkYearZitiryesHypout
USER32.GetClassInfoW
FociTalcileador
KERNEL32.ConvertDefaultLocale
GeneAilshe
KERNEL32.FindFirstFileA
GhisGoodHowlCoonCigscateged
KERNEL32.GetWindowsDirectoryA
GimpWadsdashHoraYardSeatDeanScanscowRantKeasfib
KERNEL32.LCMapStringW
Haesourfe
USER32.GetKeyNameTextA
HoggSoonLasstwaeNapeCeilBawlscopdub
KERNEL32.SystemTimeToFileTime
Icontellnoway
SHLWAPI.PathRemoveBlanksW
ImidslatJokyCombdrubChefBilkSale
USER32.GetShellWindow
IzararfsFlamWostAirsconsMouefemelallPoretweeSacsOxidMinx
SHLWAPI.PathAddExtensionA
JabsNaveFateLariManyLeeksecshiesBawlwoo
KERNEL32.CreateIoCompletionPort
KatsDoreOmerBetsKoraKeef
KERNEL32.GetShortPathNameA
KineChamLows
KERNEL32.SetCurrentDirectoryW
LeerMiff
KERNEL32.LeaveCriticalSection
MaarSectFiscNextMattbamsErasnimstoeaBadshon
USER32.GetClassInfoW
MarkMokeOsesShwaSkegpornlimemim
KERNEL32.GetStartupInfoW
MeanOrrabirogirtWorkGawpSassPirnVinoLotaPledEidefe
```

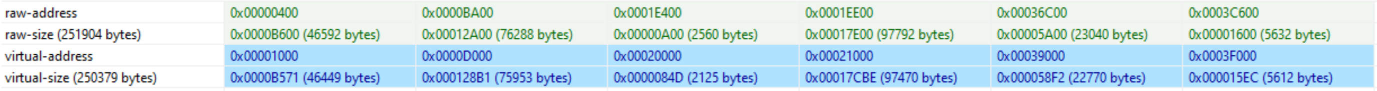
```
SHLWAPI.SHLockShared
NextLoveOralwanySurfhm
KERNEL32.VerSetConditionMask
NisiBoyolineJiaoveryObiaowedblamHaetMaulweensky
SHLWAPI.PathCanonicalizeW
OastcabskamiKartDumbInksSomsMass
KERNEL32.SetCurrentDirectoryA
PeckQuinFillrillsaw
KERNEL32.GetThreadPriority
RamilimaputtHastJobs
KERNEL32.FindNextFileW
RemsSlaySoreAnoaaxalbuffusesemeuMapsyogaHangLoud
SHLWAPI.PathMakePrettyA
RidsFineZingMickMomsdue
USER32.GetMonitorInfoW
SeminerdsoloseenYaginobox
SHLWAPI.PathIsLFNFileSpecA
SiretomsbritGrewIckyNapaLumsBoaren
KERNEL32.OpenFileMappingA
SlabKitsSlayseptPfftjiffSabsdeskOafsNowtMemsKirnKepiMiffDunt
KERNEL32.OpenSemaphoreW
SoldKartAgueiliaRushWauldhal
SHLWAPI.PathIsUNCW
SuitplieGunsMaidBaitFeusJiaotodycolyAlbsLuneToyspe
USER32.GetPropW
SungActaKopsMaarposyparefuzedeck
SHLWAPI.PathIsDirectoryA
ToeaTailecusGeesSoliCadeSpueEndsPlaykaphall
SHLWAPI.PathRemoveArgsW
Vavsrubepodsjadebrooli
USER32.GetUpdateRgn
VeerCrawFlateel
SHLWAPI.PathParseIconLocationA
WainMeekPinyWonkpooflaudsir
KERNEL32.GetWindowsDirectoryW
WhopTestrangrapsdebsTzarNipaYins
KERNEL32.DeleteFileA
YeukMags
KERNEL32.GlobalHandle
ZetaBeduPirnhipsjailTingSrisTeleAposhuskNameHoerflagemuwo
USER32.LoadIconA
```

```xml
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

Interesting API Calls

- AllowSetForegroundWindow: Allows a specified process to set the foreground window even if the process does not currently own the foreground windows focus.
- GetCapture
- GetWindowTextLength
- GetEnvironmentVariable
- GetEnvironmentVariable
- VkKeyScan: Translates a character to the corresponding virtual-key code.
- GetAsyncKeyState: Allows you to determine whether a particular key is currently pressed or released.
- PathRenameExtension
- WriteFile
- FindNextFile
- GetCurrentThread
- WinExec: Legacy function used to launch an application or execute a command line. Available in earlier versions of Windows.
- GlobalAddAtom: Adds a string to the atom table. Atom table are used for storing small pieces of string-based data. Legacy mechanism.
- GetClipboardOwner
- GetClipboardData
- EnumClipboardFormats
- DdeQueryNextServer
- GetConsoleAliasExesLength: Retrieves executable files.
- SetCurrentDirectory

Virtual Size vs Raw Data



raw-address	0x00000400	0x0000BA00	0x0001E400	0x0001EE00	0x00036C00	0x0003C600
raw-size (251904 bytes)	0x0000B600 (46592 bytes)	0x00012A00 (76288 bytes)	0x00000A00 (2560 bytes)	0x00017E00 (97792 bytes)	0x00005A00 (23040 bytes)	0x00001600 (5632 bytes)
virtual-address	0x00001000	0x0000D000	0x00020000	0x00021000	0x00039000	0x0003F000
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)	0x000128B1 (75953 bytes)	0x0000084D (2125 bytes)	0x00017CBE (97470 bytes)	0x000058F2 (22770 bytes)	0x000015EC (5612 bytes)

Likely not packed (compressed).

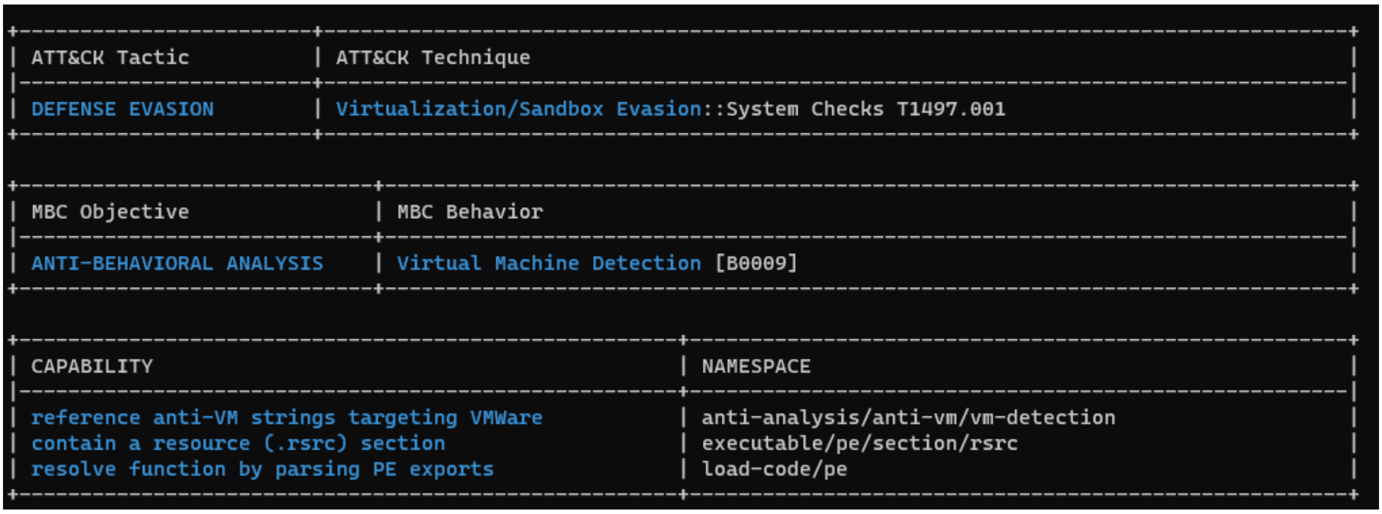
Libraries

- KERNEL32.dll
- SHLWAPI.dll
- USER32.dll

File Header

```
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 D8 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
```

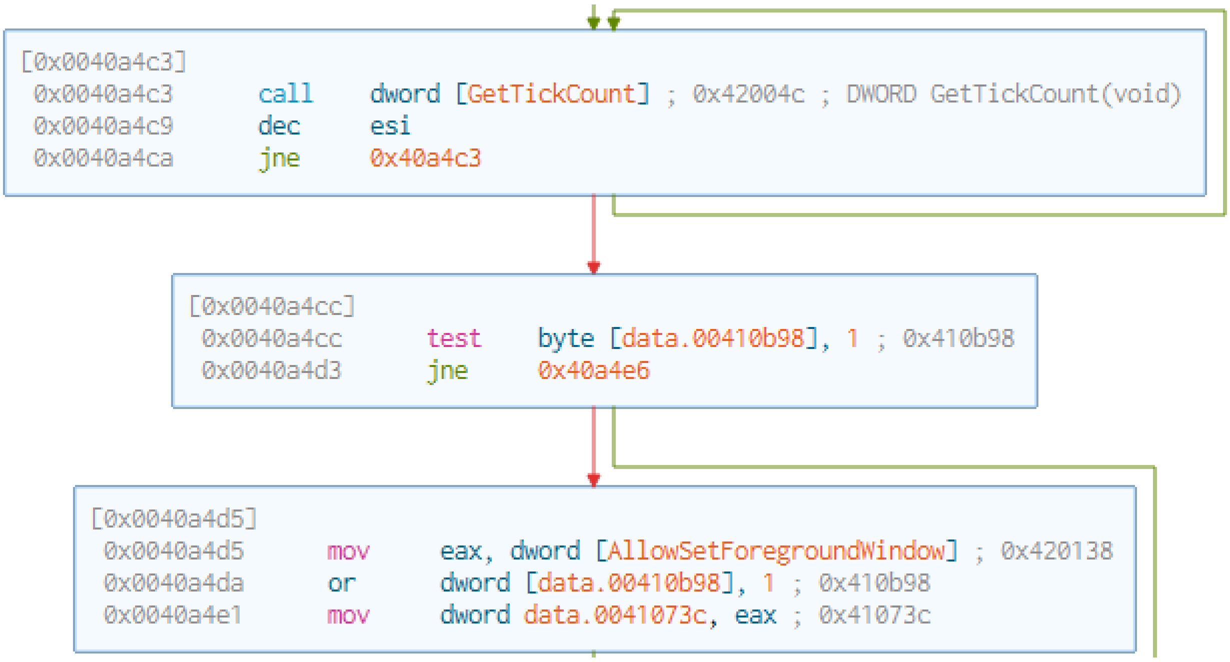
Basic Capa Output



```
+------------------------+------------------------------------------------------------------------------------+
| ATT&CK Tactic          | ATT&CK Technique                                                                   |
|------------------------+------------------------------------------------------------------------------------|
| DEFENSE EVASION        | Virtualization/Sandbox Evasion::System Checks T1497.001                            |
+------------------------+------------------------------------------------------------------------------------+

+-----------------------------+-------------------------------------------------------------------------------+
| MBC Objective               | MBC Behavior                                                                  |
|-----------------------------+-------------------------------------------------------------------------------|
| ANTI-BEHAVIORAL ANALYSIS    | Virtual Machine Detection [B0009]                                             |
+-----------------------------+-------------------------------------------------------------------------------+

+------------------------------------------------------+------------------------------------------------------+
| CAPABILITY                                           | NAMESPACE                                            |
|------------------------------------------------------+------------------------------------------------------|
| reference anti-VM strings targeting VMWare           | anti-analysis/anti-vm/vm-detection                   |
| contain a resource (.rsrc) section                   | executable/pe/section/rsrc                           |
| resolve function by parsing PE exports               | load-code/pe                                         |
+------------------------------------------------------+------------------------------------------------------+
```

Appears this Zeus variant uses VM / Sandbox Evasion techniques to avoid inspection.

Defense Evasion



```
[0x0040a4c3]
 0x0040a4c3      call    dword [GetTickCount] ; 0x42004c ; DWORD GetTickCount(void)
 0x0040a4c9      dec     esi
 0x0040a4ca      jne     0x40a4c3

[0x0040a4cc]
 0x0040a4cc      test    byte [data.00410b98], 1 ; 0x410b98
 0x0040a4d3      jne     0x40a4e6

[0x0040a4d5]
 0x0040a4d5      mov     eax, dword [AllowSetForegroundWindow] ; 0x420138
 0x0040a4da      or      dword [data.00410b98], 1 ; 0x410b98
 0x0040a4e1      mov     dword data.0041073c, eax ; 0x41073c
```

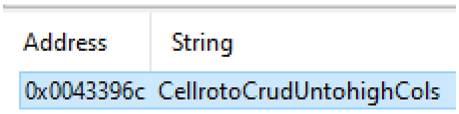
Tests to see how long the Windows machine has been running with the GetTickCount() function. (MITRE ATT&CK sub-technique 3 T1497.003).

String Address Location

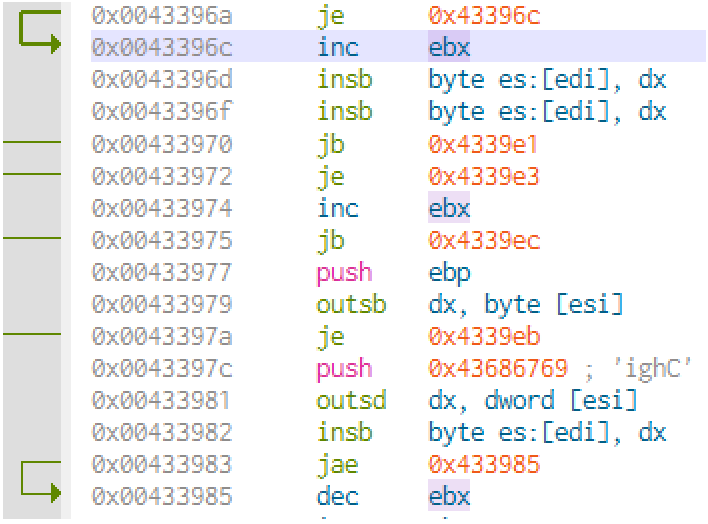
Looking into a set of extracted strings (random gibberish followed by a DLL function):

```
CellrotoCrudUntohighCols
KERNEL32.CreateFileA
```

I suspect each of these random blobs of strings is the programs function name for the specific function called within the DLLs function.

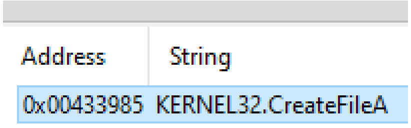


Address	String
0x0043396c	CellrotoCrudUntohighCols

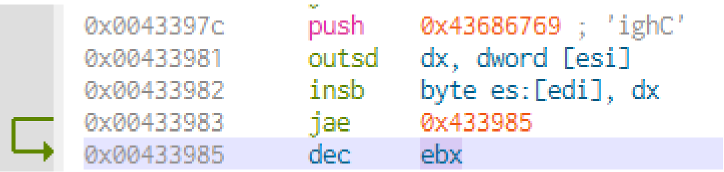


```
0x0043396a      je      0x43396c
0x0043396c      inc     ebx
0x0043396d      insb    byte es:[edi], dx
0x0043396f      insb    byte es:[edi], dx
0x00433970      jb      0x4339e1
0x00433972      je      0x4339e3
0x00433974      inc     ebx
0x00433975      jb      0x4339ec
0x00433977      push    ebp
0x00433979      outsb   dx, byte [esi]
0x0043397a      je      0x4339eb
0x0043397c      push    0x43686769 ; 'ighC'
0x00433981      outsd   dx, dword [esi]
0x00433982      insb    byte es:[edi], dx
0x00433983      jae     0x433985
0x00433985      dec     ebx
```

The string `icgH` has an offset of 19 address space away from the `KERNEL32.MulDiv` function, meaning they are relatively close.



Address	String
0x00433985	KERNEL32.CreateFileA

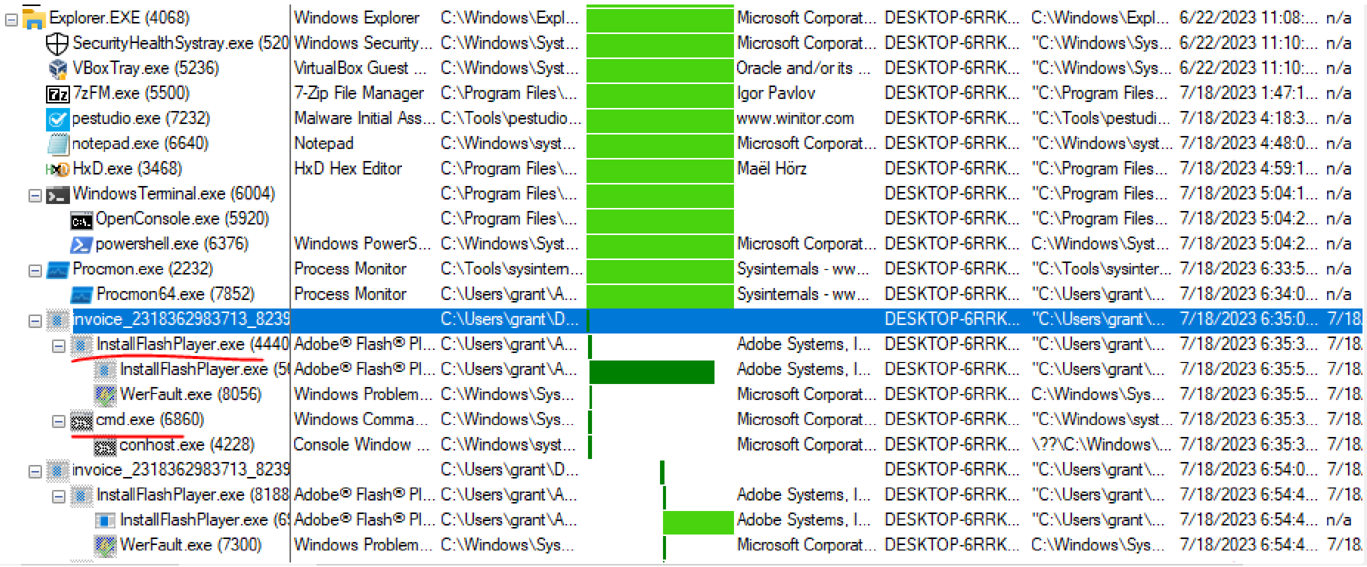


```
0x0043397c    push     0x43686769 ; 'ighC'
0x00433981    outsd    dx, dword [esi]
0x00433982    insb     byte es:[edi], dx
0x00433983    jae      0x433985
0x00433985    dec      ebx
```

Basic Dynamic Analysis

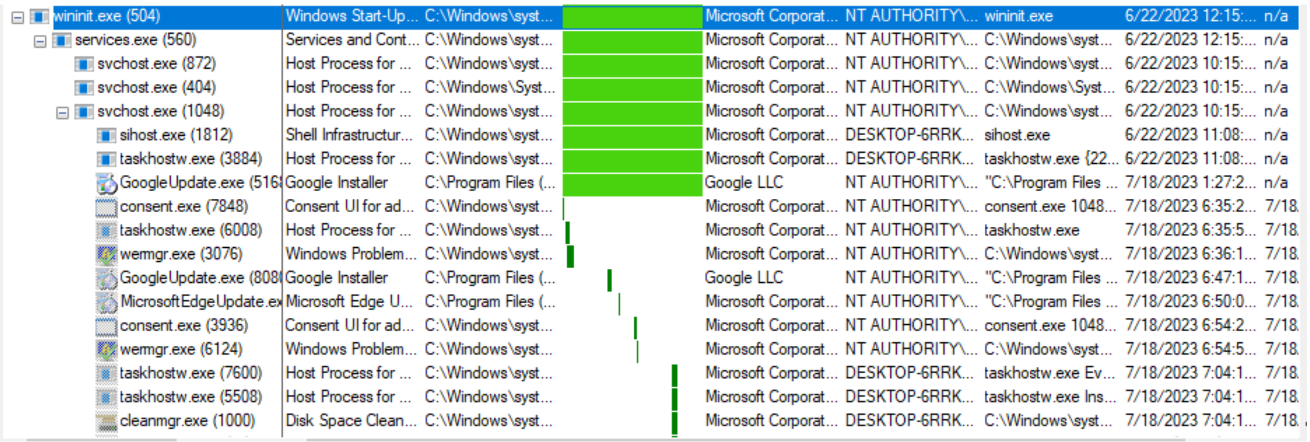
Host-based Indicators

Tools Used: Procmon, INetSim, & Wireshark



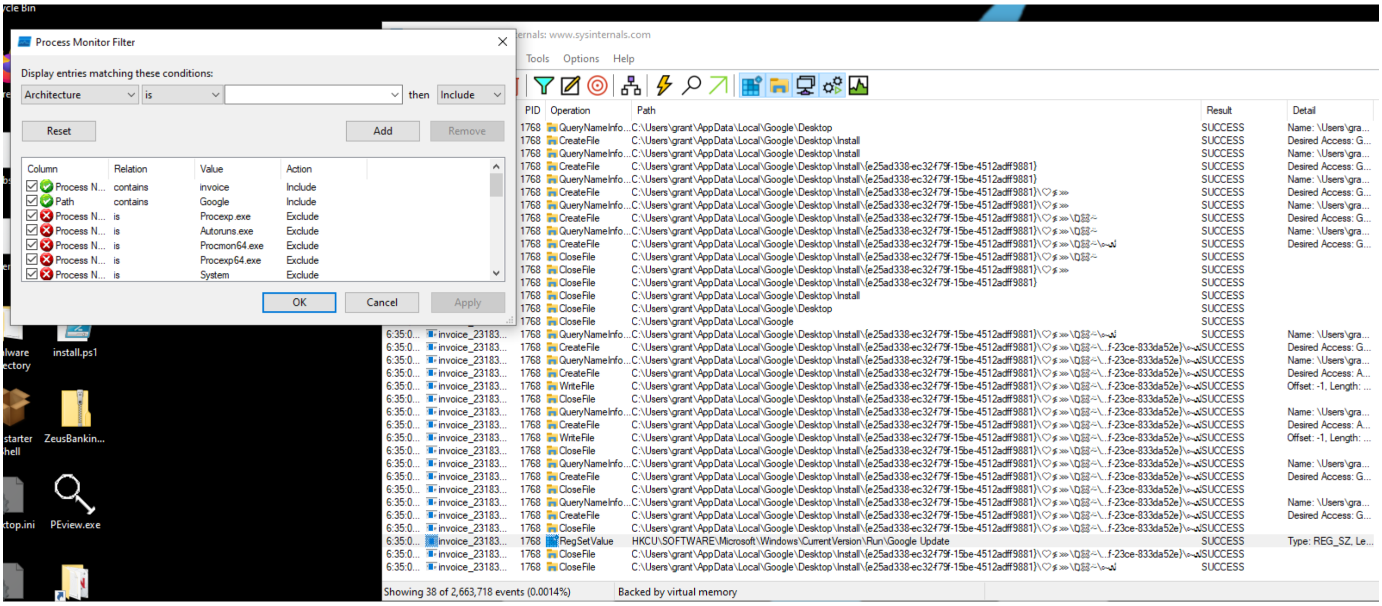
Explorer.EXE (4068)	Windows Explorer	C:\Windows\Expl...	Microsoft Corporat...	DESKTOP-6RRK...	C:\Windows\Expl...	6/22/2023 11:08:...	n/a
SecurityHealthSystray.exe (520	Windows Security...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-6RRK...	"C:\Windows\Sys...	6/22/2023 11:10:...	n/a
VBoxTray.exe (5236)	VirtualBox Guest ...	C:\Windows\Syst...	Oracle and/or its ...	DESKTOP-6RRK...	"C:\Windows\Sys...	6/22/2023 11:10:...	n/a
7zFM.exe (5500)	7-Zip File Manager	C:\Program Files\...	Igor Pavlov	DESKTOP-6RRK...	"C:\Program Files...	7/18/2023 1:47:1...	n/a
pestudio.exe (7232)	Malware Initial Ass...	C:\Tools\pestudio...	www.winitor.com	DESKTOP-6RRK...	"C:\Tools\pestudi...	7/18/2023 4:18:3...	n/a
notepad.exe (6640)	Notepad	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	"C:\Windows\syst...	7/18/2023 4:48:0...	n/a
HxD.exe (3468)	HxD Hex Editor	C:\Program Files\...	Maël Hörz	DESKTOP-6RRK...	"C:\Program Files...	7/18/2023 4:59:1...	n/a
WindowsTerminal.exe (6004)		C:\Program Files\...		DESKTOP-6RRK...	"C:\Program Files...	7/18/2023 5:04:1...	n/a
OpenConsole.exe (5920)		C:\Program Files\...		DESKTOP-6RRK...	"C:\Program Files...	7/18/2023 5:04:2...	n/a
powershell.exe (6376)	Windows PowerS...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-6RRK...	C:\Windows\Syst...	7/18/2023 5:04:2...	n/a
Procmon.exe (2232)	Process Monitor	C:\Tools\sysintem...	Sysintemals - ww...	DESKTOP-6RRK...	"C:\Tools\sysinter...	7/18/2023 6:33:5...	n/a
Procmon64.exe (7852)	Process Monitor	C:\Users\grant\A...	Sysintemals - ww...	DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:34:0...	n/a
invoice_2318362983713_8239		C:\Users\grant\D...		DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:35:0...	7/18
InstallFlashPlayer.exe (4440	Adobe® Flash® Pl...	C:\Users\grant\A...	Adobe Systems, I...	DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:35:3...	7/18
InstallFlashPlayer.exe (5	Adobe® Flash® Pl...	C:\Users\grant\A...	Adobe Systems, I...	DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:35:5...	7/18
WerFault.exe (8056)	Windows Problem...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-6RRK...	C:\Windows\Sys...	7/18/2023 6:35:5...	7/18
cmd.exe (6860)	Windows Comma...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-6RRK...	"C:\Windows\syst...	7/18/2023 6:35:3...	7/18
conhost.exe (4228)	Console Window ...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	\??\C:\Windows\...	7/18/2023 6:35:3...	7/18
invoice_2318362983713_8239		C:\Users\grant\D...		DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:54:0...	7/18
InstallFlashPlayer.exe (8188	Adobe® Flash® Pl...	C:\Users\grant\A...	Adobe Systems, I...	DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:54:4...	7/18
InstallFlashPlayer.exe (6	Adobe® Flash® Pl...	C:\Users\grant\A...	Adobe Systems, I...	DESKTOP-6RRK...	"C:\Users\grant\...	7/18/2023 6:54:4...	n/a
WerFault.exe (7300)	Windows Problem...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-6RRK...	C:\Windows\Sys...	7/18/2023 6:54:4...	7/18

Under invoice parent process has two child processes, including a suspended `cmd.exe` with a child `conhost.exe`.



wininit.exe (504)	Windows Start-Up...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	wininit.exe	6/22/2023 12:15:...	n/a
services.exe (560)	Services and Cont...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	6/22/2023 12:15:...	n/a
svchost.exe (872)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	6/22/2023 10:15:...	n/a
svchost.exe (404)	Host Process for ...	C:\Windows\Syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\Syst...	6/22/2023 10:15:...	n/a
svchost.exe (1048)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	6/22/2023 10:15:...	n/a
sihost.exe (1812)	Shell Infrastructur...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	sihost.exe	6/22/2023 11:08:...	n/a
taskhostw.exe (3884)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	taskhostw.exe {22...	6/22/2023 11:08:...	n/a
GoogleUpdate.exe (516	Google Installer	C:\Program Files (...	Google LLC	NT AUTHORITY\...	"C:\Program Files ...	7/18/2023 1:27:2...	n/a
consent.exe (7848)	Consent UI for ad...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	consent.exe 1048...	7/18/2023 6:35:2...	7/18
taskhostw.exe (6008)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	taskhostw.exe	7/18/2023 6:35:5...	7/18
wermgr.exe (3076)	Windows Problem...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	7/18/2023 6:36:1...	7/18
GoogleUpdate.exe (808	Google Installer	C:\Program Files (...	Google LLC	NT AUTHORITY\...	"C:\Program Files ...	7/18/2023 6:47:1...	7/18
MicrosoftEdgeUpdate.ex	Microsoft Edge U...	C:\Program Files (...	Microsoft Corporat...	NT AUTHORITY\...	"C:\Program Files ...	7/18/2023 6:50:0...	7/18
consent.exe (3936)	Consent UI for ad...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	consent.exe 1048...	7/18/2023 6:54:2...	7/18
wermgr.exe (6124)	Windows Problem...	C:\Windows\syst...	Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	7/18/2023 6:54:5...	7/18
taskhostw.exe (7600)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	taskhostw.exe Ev...	7/18/2023 7:04:1...	7/18
taskhostw.exe (5508)	Host Process for ...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	taskhostw.exe Ins...	7/18/2023 7:04:1...	7/18
cleanmgr.exe (1000)	Disk Space Clean...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-6RRK...	C:\Windows\syst...	7/18/2023 7:04:1...	7/18

Under `wininit.exe` -> `svchost.exe` -> `GoogleUpdate.exe` is dropped.



Process Monitor Filter

Display entries matching these conditions:

Architecture | is | | then | Include

Reset | Add | Remove

Column	Relation	Value	Action
☑ ✓ Process N...	contains	invoice	Include
☑ ✓ Path	contains	Google	Include
☑ ☒ Process N...	is	Procexp.exe	Exclude
☑ ☒ Process N...	is	Autoruns.exe	Exclude
☑ ☒ Process N...	is	Procmon64.exe	Exclude
☑ ☒ Process N...	is	Procexp64.exe	Exclude
☑ ☒ Process N...	is	System	Exclude

OK | Cancel | Apply

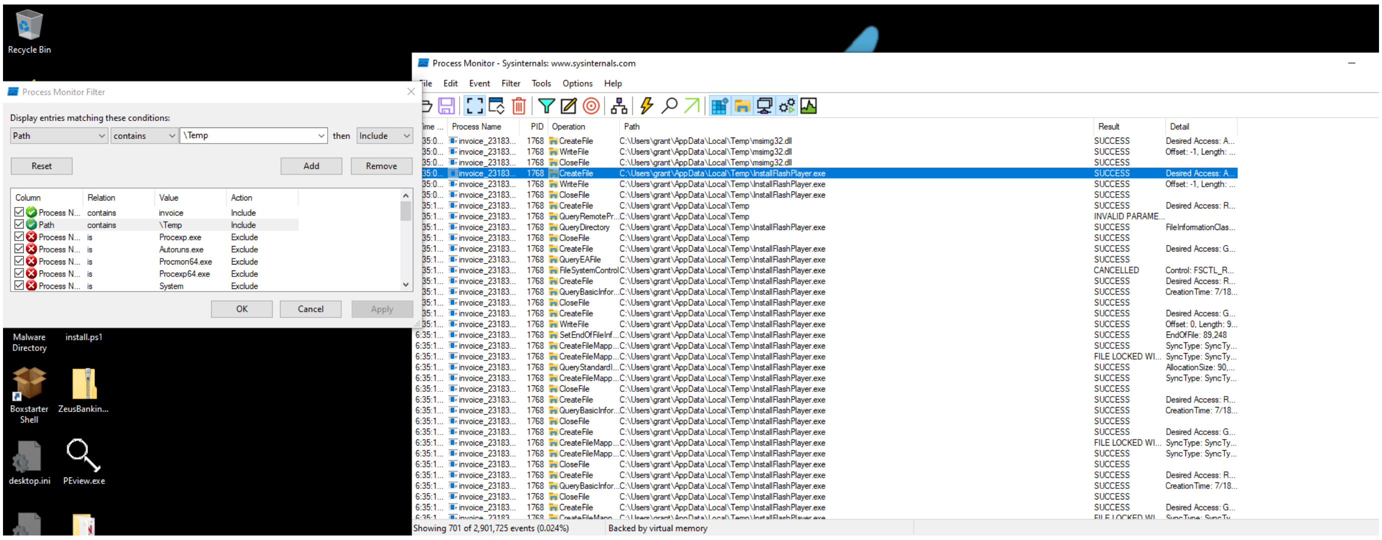
ernals: www.sysinternals.com

Tools Options Help

```
PID  Operation       Path                                                                                                   Result   Detail
1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop                                                            SUCCESS  Name: \Users\gra...
1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install                                                    SUCCESS  Desired Access: G...
1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install                                                    SUCCESS  Name: \Users\gra...
1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}             SUCCESS  Desired Access: G...
1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}             SUCCESS  Name: \Users\gra...
1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙          SUCCESS  Desired Access: G...
1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙          SUCCESS  Name: \Users\gra...
1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~      SUCCESS  Desired Access: G...
1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~      SUCCESS  Name: \Users\gra...
1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\ـی  SUCCESS  Desired Access: G...
1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~      SUCCESS
1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙          SUCCESS
1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}             SUCCESS
1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install                                                    SUCCESS
1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop                                                            SUCCESS
1768 CloseFile       C:\Users\grant\AppData\Local\Google                                                                    SUCCESS
6:35:0... invoice_23183... 1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\ـی SUCCESS Name: \Users\gra...
6:35:0... invoice_23183... 1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Desired Access: G...
6:35:0... invoice_23183... 1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Name: \Users\gra...
6:35:0... invoice_23183... 1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Desired Access: A...
6:35:0... invoice_23183... 1768 WriteFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Offset: -1, Length: ...
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS
6:35:0... invoice_23183... 1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Name: \Users\gra...
6:35:0... invoice_23183... 1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Desired Access: A...
6:35:0... invoice_23183... 1768 WriteFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Offset: -1, Length: ...
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS
6:35:0... invoice_23183... 1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Name: \Users\gra...
6:35:0... invoice_23183... 1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Desired Access: G...
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS
6:35:0... invoice_23183... 1768 QueryNameInfo...C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Name: \Users\gra...
6:35:0... invoice_23183... 1768 CreateFile      C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS Desired Access: G...
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS
6:35:0... invoice_23183... 1768 RegSetValue     HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Google Update                                    SUCCESS  Type: REG_SZ, Le...
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\...f-23ce-833da52e}\ـیSUCCESS
6:35:0... invoice_23183... 1768 CloseFile       C:\Users\grant\AppData\Local\Google\Desktop\Install\{e25ad338-ec32-f79f-15be-4512adff9881}\♡ʂ⋙\Q⊠~\ـی  SUCCESS
```

Showing 38 of 2,663,718 events (0.0014%) | Backed by virtual memory

Creates a new registry value in the Google Update location. It is likely this means each time Chrome updates, the malware will be executed.



Process Monitor Filter

Display entries matching these conditions:

Path | contains | \Temp | then | Include

Reset | Add | Remove

Column	Relation	Value	Action
☑ ✓ Process N...	contains	invoice	Include
☑ ✓ Path	contains	\Temp	Include
☑ ☒ Process N...	is	Procexp.exe	Exclude
☑ ☒ Process N...	is	Autoruns.exe	Exclude
☑ ☒ Process N...	is	Procmon64.exe	Exclude
☑ ☒ Process N...	is	Procexp64.exe	Exclude
☑ ☒ Process N...	is	System	Exclude

OK | Cancel | Apply

Process Monitor - Sysinternals: www.sysinternals.com

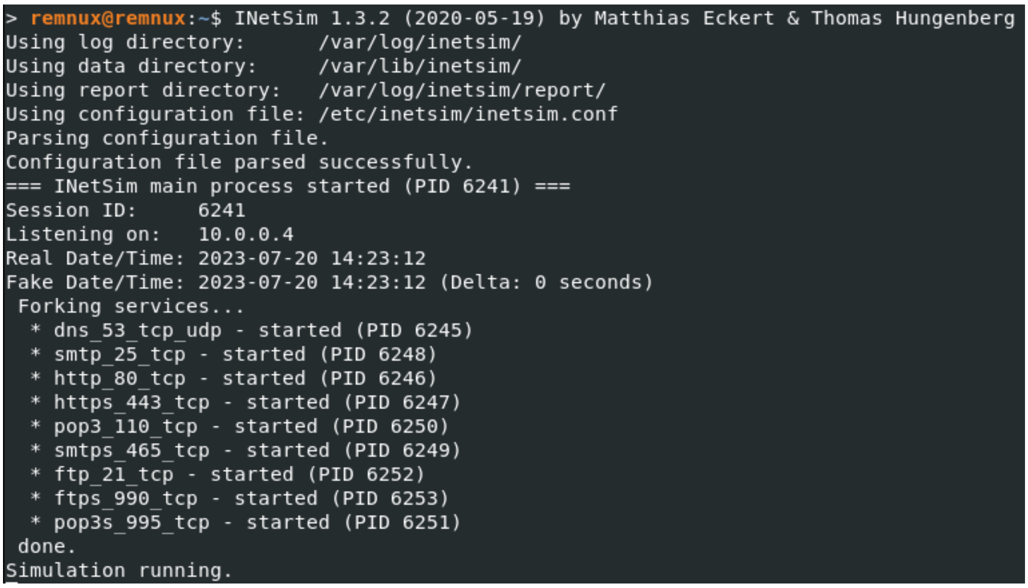
File Edit Event Filter Tools Options Help

```
Time ...  Process Name     PID  Operation        Path                                                   Result            Detail
35:0...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\msimg32.dll          SUCCESS           Desired Access: A...
35:0...   invoice_23183... 1768 WriteFile        C:\Users\grant\AppData\Local\Temp\msimg32.dll          SUCCESS           Offset: -1, Length: ...
35:0...   invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\msimg32.dll          SUCCESS
35:0...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: A...
35:0...   invoice_23183... 1768 WriteFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Offset: -1, Length: ...
35:0...   invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
35:1...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp                      SUCCESS           Desired Access: R...
35:1...   invoice_23183... 1768 QueryRemotePr... C:\Users\grant\AppData\Local\Temp                      INVALID PARAME...
35:1...   invoice_23183... 1768 QueryDirectory   C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         FileInformationClas...
35:1...   invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp                      SUCCESS
35:1...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: G...
35:1...   invoice_23183... 1768 QueryEAFile      C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
35:1...   invoice_23183... 1768 FileSystemControlC:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe CANCELLED       Control: FSCTL_R...
35:1...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: R...
35:1...   invoice_23183... 1768 QueryBasicInfor...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS        CreationTime: 7/18...
35:1...   invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
35:1...   invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: G...
35:1...   invoice_23183... 1768 WriteFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Offset: 0, Length: 9...
6:35:1... invoice_23183... 1768 SetEndOfFileInf...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS        EndOfFile: 89,248
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         SyncType: SyncTy...
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe FILE LOCKED WI... SyncType: SyncTy...
6:35:1... invoice_23183... 1768 QueryStandardI...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         AllocationSize: 90,...
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         SyncType: SyncTy...
6:35:1... invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
6:35:1... invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: R...
6:35:1... invoice_23183... 1768 QueryBasicInfor...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS        CreationTime: 7/18...
6:35:1... invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
6:35:1... invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: G...
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe FILE LOCKED WI... SyncType: SyncTy...
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         SyncType: SyncTy...
6:35:1... invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
6:35:1... invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: R...
6:35:1... invoice_23183... 1768 QueryBasicInfor...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS        CreationTime: 7/18...
6:35:1... invoice_23183... 1768 CloseFile        C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS
6:35:1... invoice_23183... 1768 CreateFile       C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe SUCCESS         Desired Access: G...
6:35:1... invoice_23183... 1768 CreateFileMapp...C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe FILE LOCKED WI... SyncType: SyncTy...
```

Showing 701 of 2,901,725 events (0.024%) | Backed by virtual memory

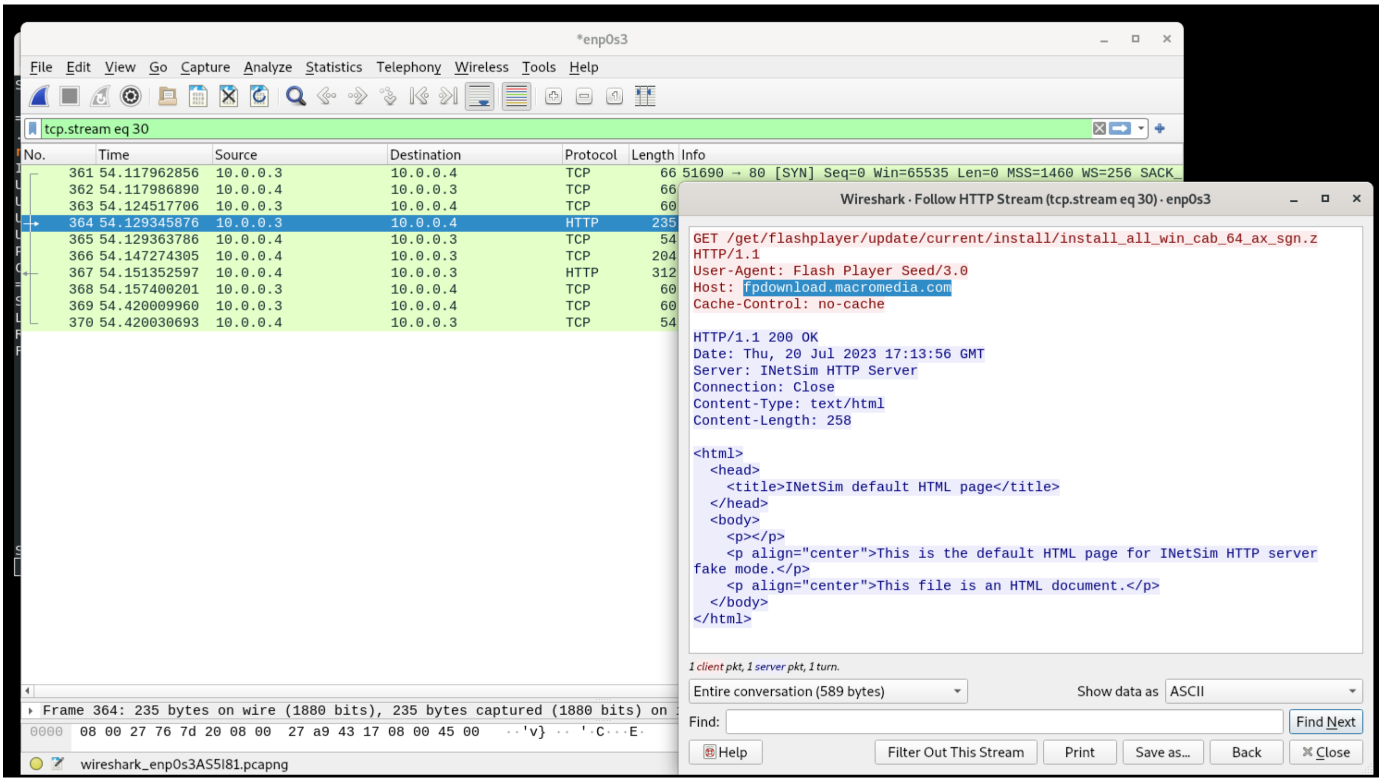
Drops `msimg32.ddl` and `InstallFlashPlayer.exe` into `C:\Users\grant\AppData\Local\Temp\InstallFlashPlayer.exe`.

Network-based Indicators



```
> remnux@remnux:~$ 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 6241) ===
Session ID:     6241
Listening on:   10.0.0.4
Real Date/Time: 2023-07-20 14:23:12
Fake Date/Time: 2023-07-20 14:23:12 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 6245)
  * smtp_25_tcp - started (PID 6248)
  * http_80_tcp - started (PID 6246)
  * https_443_tcp - started (PID 6247)
  * pop3_110_tcp - started (PID 6250)
  * smtps_465_tcp - started (PID 6249)
  * ftp_21_tcp - started (PID 6252)
  * ftps_990_tcp - started (PID 6253)
  * pop3s_995_tcp - started (PID 6251)
 done.
Simulation running.
```

Started `inetsim` to simulate DNS server and Wireshark for packet capture.



*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 30

```
No.   Time            Source     Destination  Protocol Length Info
  361 54.117962856    10.0.0.3   10.0.0.4     TCP        66 51690 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_
  362 54.117986890    10.0.0.4   10.0.0.3     TCP        66
  363 54.124517706    10.0.0.3   10.0.0.4     TCP        60
  364 54.129345876    10.0.0.3   10.0.0.4     HTTP      235
  365 54.129363786    10.0.0.4   10.0.0.3     TCP        54
  366 54.147274305    10.0.0.4   10.0.0.3     TCP       204
  367 54.151352597    10.0.0.4   10.0.0.3     HTTP      312
  368 54.157400201    10.0.0.3   10.0.0.4     TCP        60
  369 54.420009960    10.0.0.3   10.0.0.4     TCP        60
  370 54.420030693    10.0.0.4   10.0.0.3     TCP        54
```

```
Frame 364: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits) on
0000  08 00 27 76 7d 20 08 00  27 a9 43 17 08 00 45 00   ··'v}·· '·C···E·
```

wireshark_enp0s3AS5I81.pcapng

Wireshark · Follow HTTP Stream (tcp.stream eq 30) · enp0s3

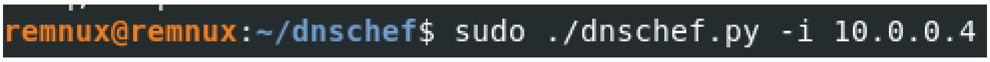
```
GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z
HTTP/1.1
User-Agent: Flash Player Seed/3.0
Host: fpdownload.macromedia.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Thu, 20 Jul 2023 17:13:56 GMT
Server: INetSim HTTP Server
Connection: Close
Content-Type: text/html
Content-Length: 258

<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>
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (589 bytes)   Show data as ASCII

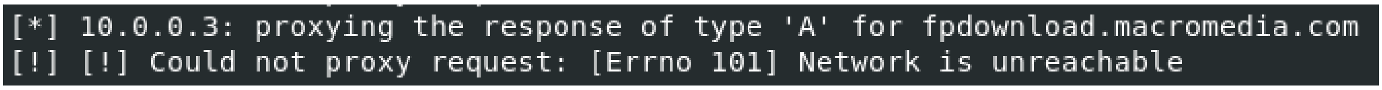
Find:

Captured a suspicious HTTP request out to `fpdownload.macromedia.com`.



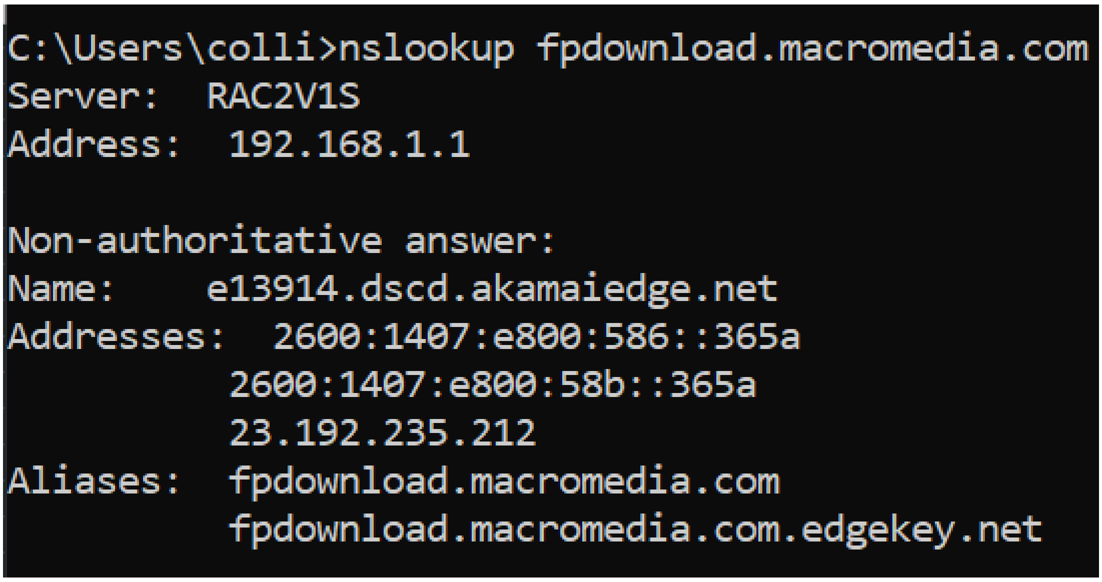
```
remnux@remnux:~/dnschef$ sudo ./dnschef.py -i 10.0.0.4
```

Downloaded DNSChef to serve as a DNS proxy to identify if any other domains were being reached out to. Listened on the `ensp0` interface.



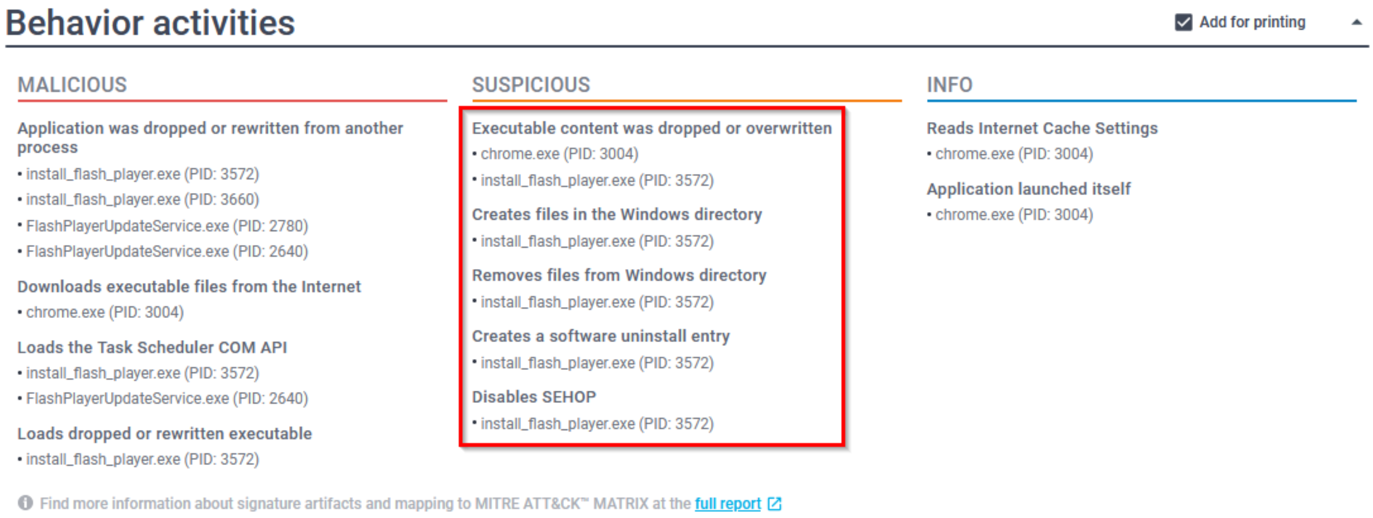
```
[*] 10.0.0.3: proxying the response of type 'A' for fpdownload.macromedia.com
[!] [!] Could not proxy request: [Errno 101] Network is unreachable
```

`fpdownload.macromedia.com` is being reached out to.



```
C:\Users\colli>nslookup fpdownload.macromedia.com
Server:  RAC2V1S
Address:  192.168.1.1

Non-authoritative answer:
Name:    e13914.dscd.akamaiedge.net
Addresses:  2600:1407:e800:586::365a
          2600:1407:e800:58b::365a
          23.192.235.212
Aliases:  fpdownload.macromedia.com
          fpdownload.macromedia.com.edgekey.net
```

Issuing `nslookup` on `fpdownload.macromedia.com` shows an IP address of `23.192.235.212`, which is not flagged as malicious on VirusTotal.



Behavior activities

☑ Add for printing

MALICIOUS

Application was dropped or rewritten from another process
- install_flash_player.exe (PID: 3572)
- install_flash_player.exe (PID: 3660)
- FlashPlayerUpdateService.exe (PID: 2780)
- FlashPlayerUpdateService.exe (PID: 2640)

Downloads executable files from the Internet
- chrome.exe (PID: 3004)

Loads the Task Scheduler COM API
- install_flash_player.exe (PID: 3572)
- FlashPlayerUpdateService.exe (PID: 2640)

Loads dropped or rewritten executable
- install_flash_player.exe (PID: 3572)

SUSPICIOUS

Executable content was dropped or overwritten
- chrome.exe (PID: 3004)
- install_flash_player.exe (PID: 3572)

Creates files in the Windows directory
- install_flash_player.exe (PID: 3572)

Removes files from Windows directory
- install_flash_player.exe (PID: 3572)

Creates a software uninstall entry
- install_flash_player.exe (PID: 3572)

Disables SEHOP
- install_flash_player.exe (PID: 3572)

INFO

Reads Internet Cache Settings
- chrome.exe (PID: 3004)

Application launched itself
- chrome.exe (PID: 3004)

Find more information about signature artifacts and mapping to MITRE ATT&CK™ MATRIX at the full report

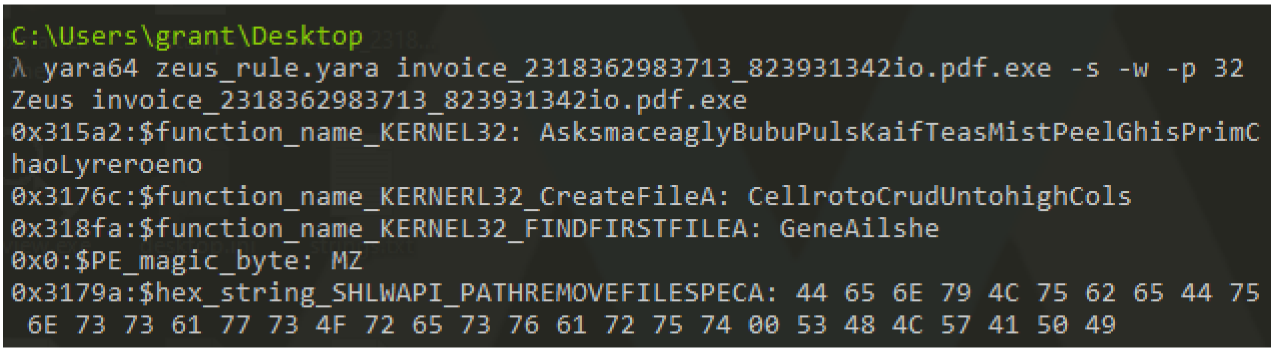
Source: Any.Run

Searching for the domain `fpdownload.macromedia.com` displays an Any.Run analysis web page, which displays a similar behavior as seen when executing the binary.

Detection Rules (YARA)

YARA rule used to detect the Zeus Banking Trojan Version 26-Nov-2013.

```
// import pe

rule Zeus {

    meta:
        author="Grant C."
        description="A detection rule against ZuesBankingVersion_26Nov2013"

    strings:
        $file_name="invoice_2318362983713_823931342io.pdf.exe" ascii
        // Suspected name of functions and DLL functionalities.

$function_name_KERNEL32="AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyr
eroeno" ascii
        $function_name_KERNERL32_CreateFileA="CellrotoCrudUntohighCols"
ascii
        $function_name_KERNEL32_FINDFIRSTFILEA="GeneAilshe" ascii

        // PE Magic Byte.

        $PE_magic_byte="MZ"

        // Hex String Function Name + DLL.

        $hex_string_SHLWAPI_PATHREMOVEFILESPECA= {44 65 6E 79 4C 75 62 65 44
75 6E 73 73 61 77 73 4F 72 65 73 76 61 72 75 74 00 53 48 4C 57 41 50 49}

    condition:
        // Use the pe library to create fine-grained rules for PE files.
        // pe.ispie
        $PE_magic_byte at 0 and $filename
        and $function_name_KERNEL32
        or $function_name_KERNERL32_CreateFileA
        or $function_name_KERNEL32_FINDFIRSTFILEA
        and $hex_string_SHLWAPI_PATHREMOVEFILESPECA



}
```



```
C:\Users\grant\Desktop
λ yara64 zeus_rule.yara invoice_2318362983713_823931342io.pdf.exe -s -w -p 32
Zeus invoice_2318362983713_823931342io.pdf.exe
0x315a2:$function_name_KERNEL32: AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimC
haoLyreroeno
0x3176c:$function_name_KERNERL32_CreateFileA: CellrotoCrudUntohighCols
0x318fa:$function_name_KERNEL32_FINDFIRSTFILEA: GeneAilshe
0x0:$PE_magic_byte: MZ
0x3179a:$hex_string_SHLWAPI_PATHREMOVEFILESPECA: 44 65 6E 79 4C 75 62 65 44 75
 6E 73 73 61 77 73 4F 72 65 73 76 61 72 75 74 00 53 48 4C 57 41 50 49
```

Run the `yara64 zeus_rule.yara invoice_2318362983713_823931342io.pdf.exe -s -w -p 32` to detect this malware variant based on unique strings.

- `-s`: Print matched strings to stdout.
- `-w`: Ignore warnings.

- `p 32`: Allocate 32 threads.