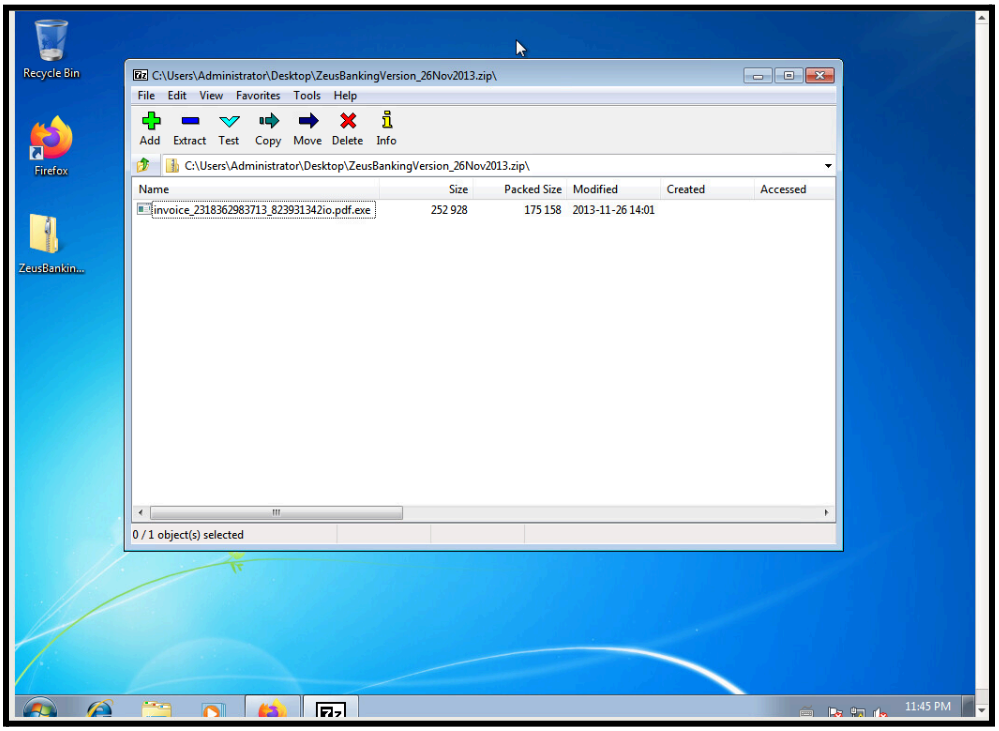
Zeus Banking Trojan - Analysis

John Tolomay

Static Analysis


Recycle Bin
Firefox
ZeusBankin...
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
11:45 PM

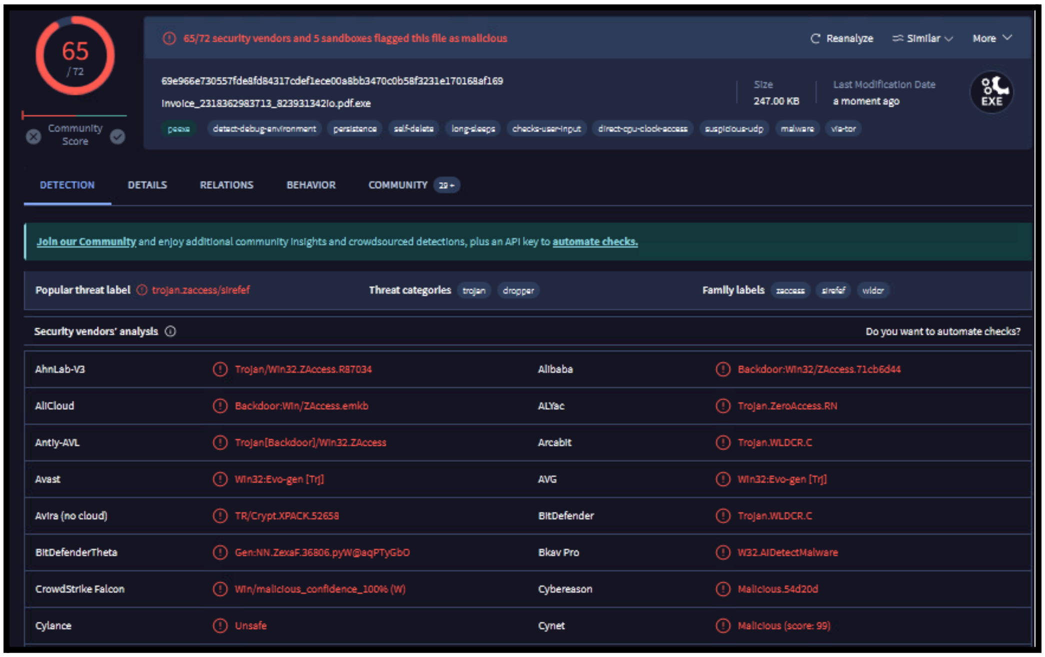
C:\Users\Administrator\Desktop\ZeusBankingVersion_26Nov2013.zip\

Name	Size	Packed Size	Modified	Created	Accessed
invoice_2318362983713_823931342io.pdf.exe	252 928	175 158	2013-11-26 14:01		

0 / 1 object(s) selected

Used 7-Zip to unfold the zip file and it contains a suspicious file disguised as a pdf named invoice_2318362983713_823931342io.pdf.exe.

VirusTotal



65/72 security vendors and 5 sandboxes flagged this file as malicious

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
invoice_2318362983713_823931342io.pdf.exe

Size
247.00 KB

Last Modification Date
a moment ago

Join our 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

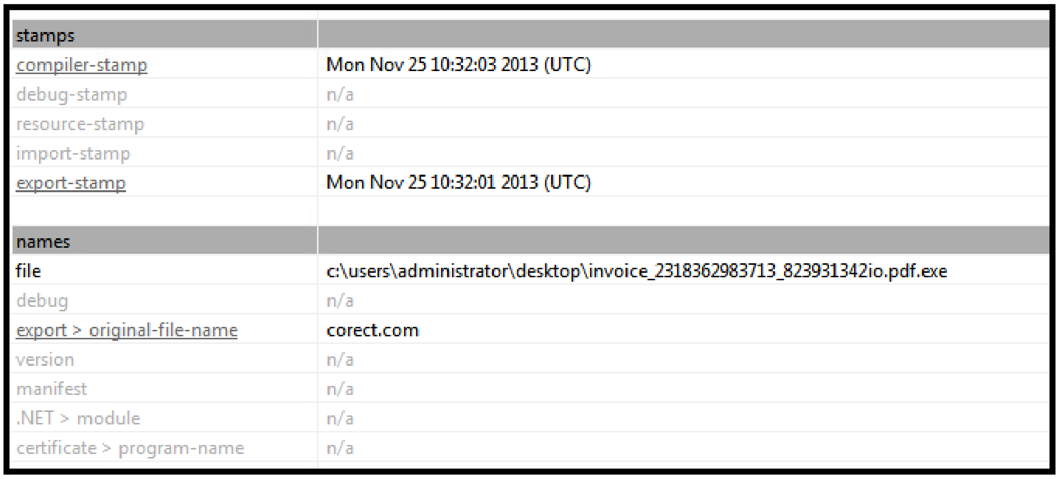
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.ZAccess.R87034	Alibaba	Backdoor:Win32/ZAccess.71cb6d44
AliCloud	Backdoor:Win/ZAccess.emkb	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.36806.pyW@aqPTyGbO	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.54d20d
Cylance	Unsafe	Cynet	Malicious (score: 99)

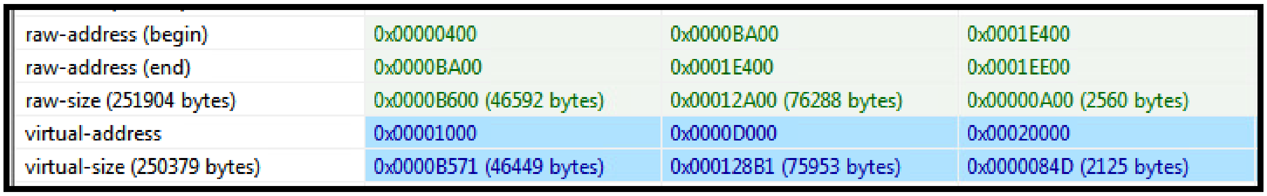
Submitting the sample to VirusTotal shows that it has been flagged as malicious by 65/72 vendors. This displays the category they flagged it as and also how they named the sample.

PeStudio



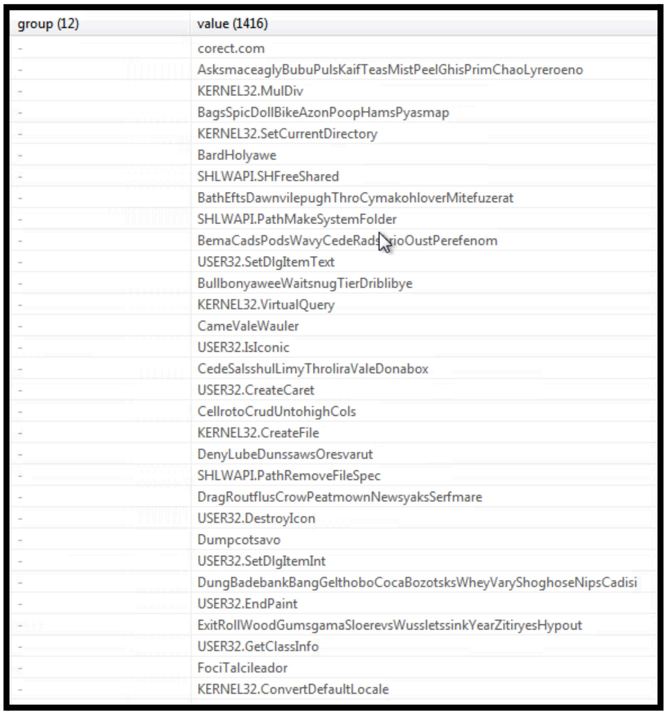
stamps	
compiler-stamp	Mon Nov 25 10:32:03 2013 (UTC)
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	Mon Nov 25 10:32:01 2013 (UTC)
names	
file	c:\users\administrator\desktop\invoice_2318362983713_823931342io.pdf.exe
debug	n/a
export > original-file-name	corect.com
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

Submitting the file to PeStudio shows that the malware was compiled in November of 2013. This screenshot also displays an interesting URL, corect.com. corect.com is a Romanian website, but otherwise gave no interesting results.



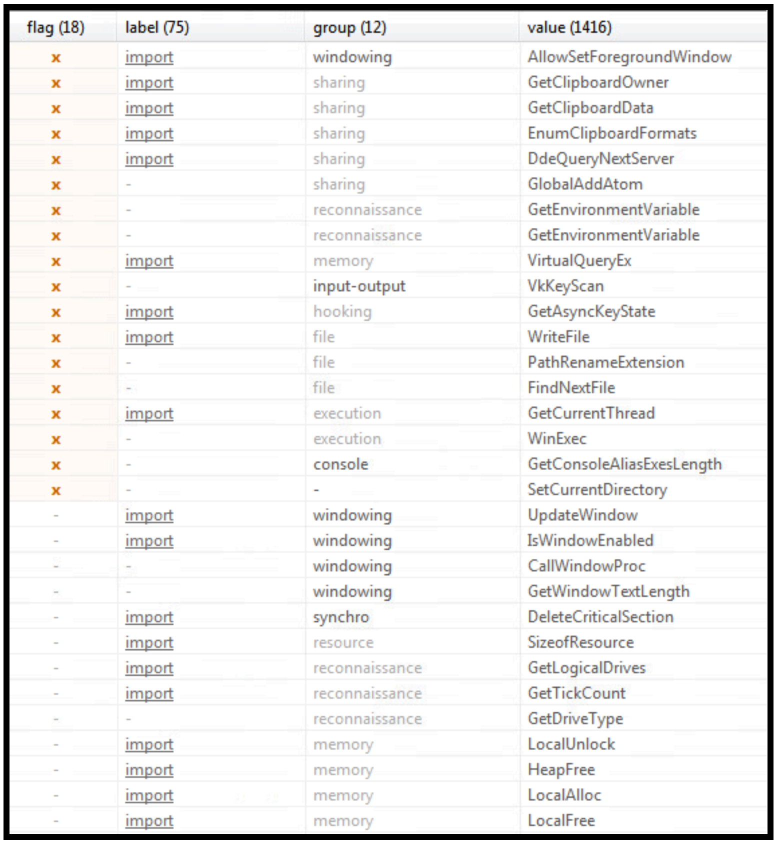
raw-address (begin)	0x00000400	0x0000BA00	0x0001E400
raw-address (end)	0x0000BA00	0x0001E400	0x0001EE00
raw-size (251904 bytes)	0x0000B600 (46592 bytes)	0x00012A00 (76288 bytes)	0x00000A00 (2560 bytes)
virtual-address	0x00001000	0x0000D000	0x00020000
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)	0x000128B1 (75953 bytes)	0x0000084D (2125 bytes)

The file has about the same raw-size and virtual-size, meaning there is no compression or “packing” to obfuscate the malware.



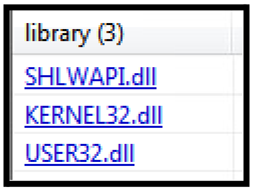
group (12)	value (1416)
-	corect.com
-	AsksmaceaglyBubuPulsKaifTeasMistPeelGhisPrimChaoLyreroeno
-	KERNEL32.MulDiv
-	BagsSpicDollBikeAzonPoopHamsPyasmap
-	KERNEL32.SetCurrentDirectory
-	BardHolyawe
-	SHLWAPI.SHFreeShared
-	BathEftsDawnvilepughThroCymakohloverMitefuzerat
-	SHLWAPI.PathMakeSystemFolder
-	BemaCadsPodsWavyCedeRadsrioOustPerefenom
-	USER32.SetDlgItemText
-	BullbonyaweeWaitsnugTierDriblibye
-	KERNEL32.VirtualQuery
-	CameValeWauler
-	USER32.IsIconic
-	CedeSalsshulLimyThroliraValeDonabox
-	USER32.CreateCaret
-	CellrotoCrudUntohighCols
-	KERNEL32.CreateFile
-	DenyLubeDunssawsOresvarut
-	SHLWAPI.PathRemoveFileSpec
-	DragRoutflusCrowPeatmownNewsyaksSerfmare
-	USER32.DestroyIcon
-	Dumpcotsavo
-	USER32.SetDlgItemInt
-	DungBadebankBangGelthoboCocaBozotsksWheyVaryShoghoseNipsCadisi
-	USER32.EndPaint
-	ExitRollWoodGumsgamaSloerevsWussletssinkYearZitiryesHypout
-	USER32.GetClassInfo
-	FociTalcileador
-	KERNEL32.ConvertDefaultLocale

This is a small portion of the list of strings used by the sample, which includes URLs, file paths, API calls, etc. In this screenshot, there are legit KERNEL32 function calls surrounded by gibberish strings.



flag (18)	label (75)	group (12)	value (1416)
x	import	windowing	AllowSetForegroundWindow
x	import	sharing	GetClipboardOwner
x	import	sharing	GetClipboardData
x	import	sharing	EnumClipboardFormats
x	import	sharing	DdeQueryNextServer
x	-	sharing	GlobalAddAtom
x	-	reconnaissance	GetEnvironmentVariable
x	-	reconnaissance	GetEnvironmentVariable
x	import	memory	VirtualQueryEx
x	-	input-output	VkKeyScan
x	import	hooking	GetAsyncKeyState
x	import	file	WriteFile
x	-	file	PathRenameExtension
x	-	file	FindNextFile
x	import	execution	GetCurrentThread
x	-	execution	WinExec
x	-	console	GetConsoleAliasExesLength
x	-	-	SetCurrentDirectory
-	import	windowing	UpdateWindow
-	import	windowing	IsWindowEnabled
-	-	windowing	CallWindowProc
-	-	windowing	GetWindowTextLength
-	import	synchro	DeleteCriticalSection
-	import	resource	SizeofResource
-	import	reconnaissance	GetLogicalDrives
-	import	reconnaissance	GetTickCount
-	-	reconnaissance	GetDriveType
-	import	memory	LocalUnlock
-	import	memory	HeapFree
-	import	memory	LocalAlloc
-	import	memory	LocalFree

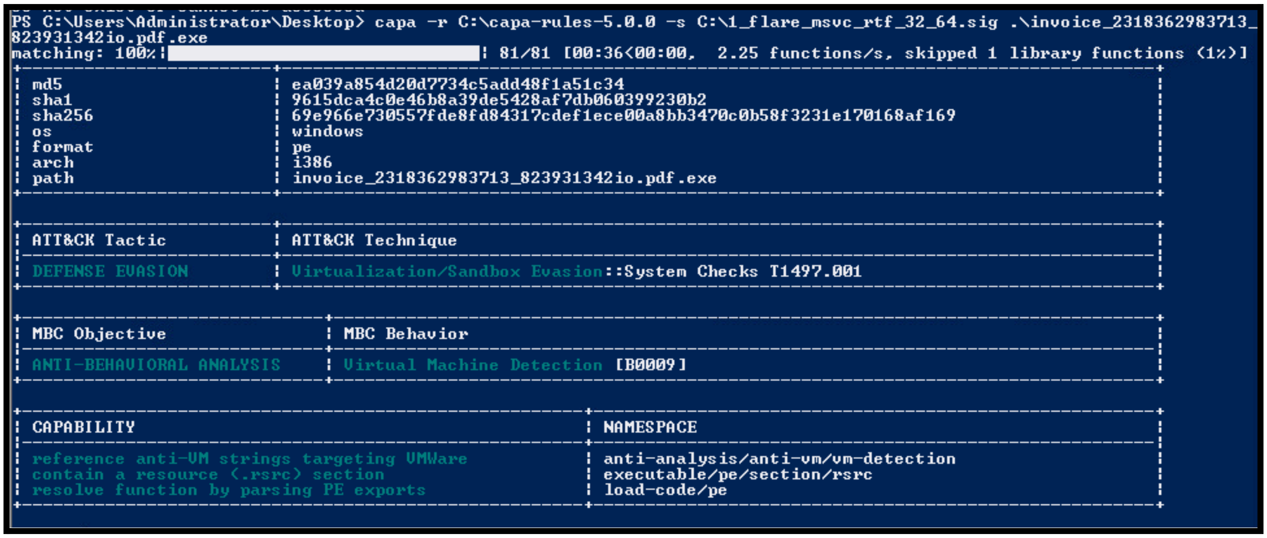
List of API calls from the sample, with the “x” flagging it as possibly malicious.



library (3)
SHLWAPI.dll
KERNEL32.dll
USER32.dll

Libraries the malware uses.

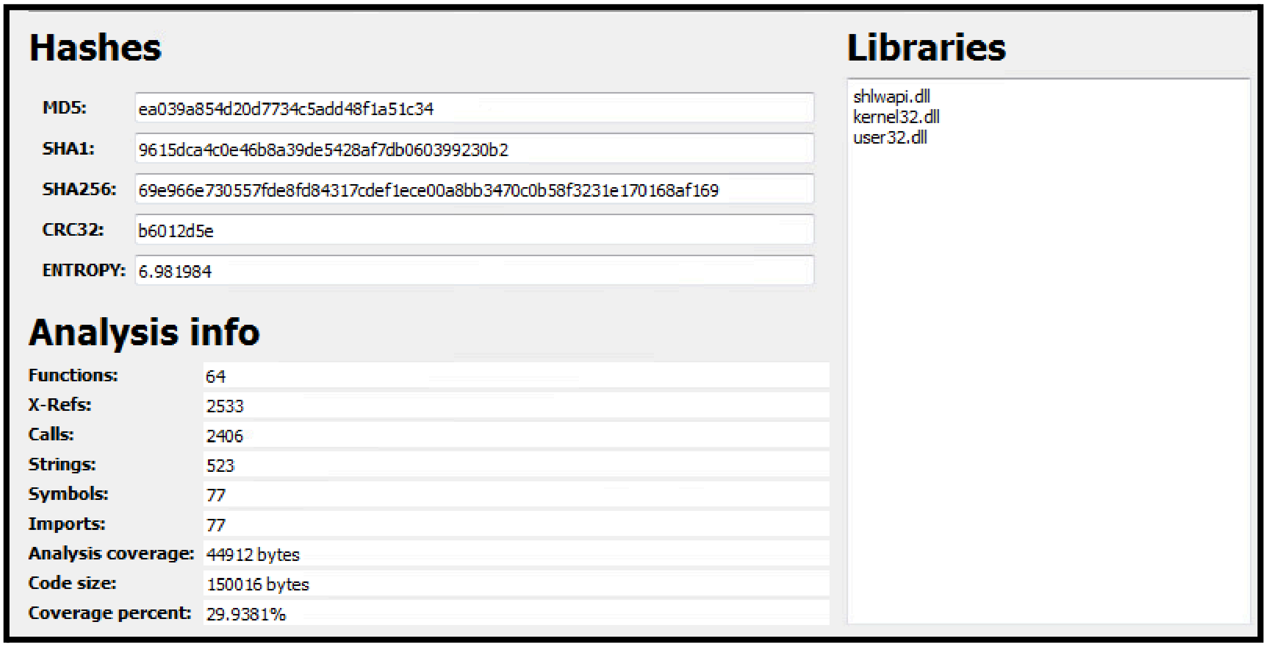
Capa



```
PS C:\Users\Administrator\Desktop> capa -r C:\capa-rules-5.0.0 -s C:\1_flare_msvc_rtf_32_64.sig .\invoice_2318362983713_
823931342io.pdf.exe
matching: 100%|██████████████████████| 81/81 [00:36<00:00,  2.25 functions/s, skipped 1 library functions (1%)]
+--------------------------+--------------------------------------------------------------------------+
| md5                      | ea039a854d20d7734c5add48f1a51c34                                         |
| sha1                     | 9615dca4c0e46b8a39de5428af7db060399230b2                                 |
| sha256                   | 69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169         |
| os                       | windows                                                                  |
| format                   | pe                                                                       |
| arch                     | i386                                                                     |
| path                     | invoice_2318362983713_823931342io.pdf.exe                                |
+--------------------------+--------------------------------------------------------------------------+

+--------------------------+--------------------------------------------------------------------------+
| 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                                |
+-------------------------------------------------------+---------------------------------------------+
```

Capa references the MITRE ATT&CK framework and claims the malware's objective is to avoid detection by virtualized/sandboxed environments.

Cutter



Hashes

MD5:	ea039a854d20d7734c5add48f1a51c34
SHA1:	9615dca4c0e46b8a39de5428af7db060399230b2
SHA256:	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
CRC32:	b6012d5e
ENTROPY:	6.981984

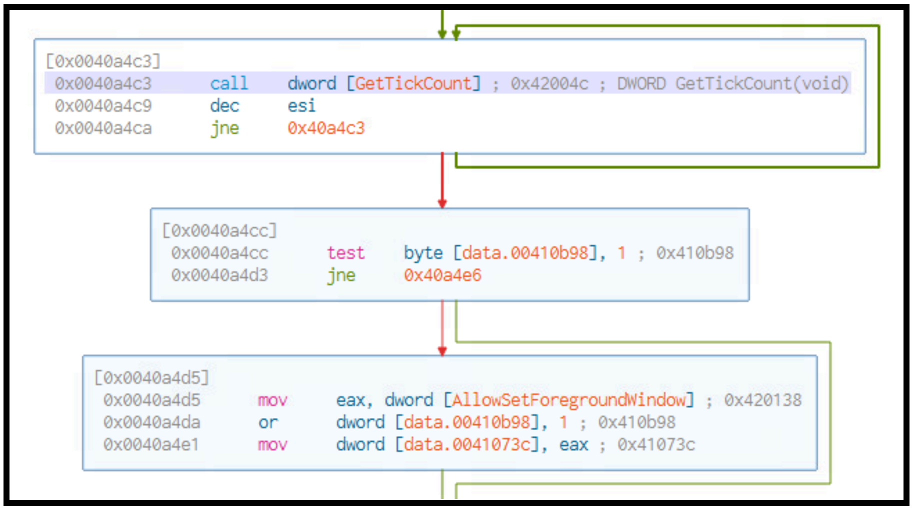
Analysis info

Functions:	64
X-Refs:	2533
Calls:	2406
Strings:	523
Symbols:	77
Imports:	77
Analysis coverage:	44912 bytes
Code size:	150016 bytes
Coverage percent:	29.9381%

Libraries

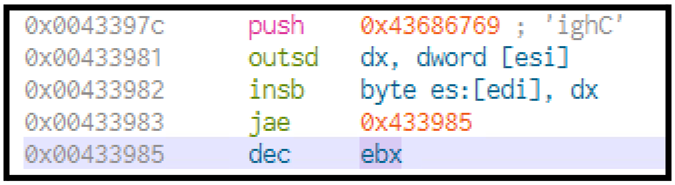
shlwapi.dll
kernel32.dll
user32.dll

By using Cutter, we can see the hashes of the malicious file as well as the libraries it uses and other analysis information.



```
[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
```

The assembly code from the malware entry shows these API calls. The malware calls GetTickCount, which says how long the machine has been powered on for, which enforces the theory that this malware is trying to detect a virtualized environment.



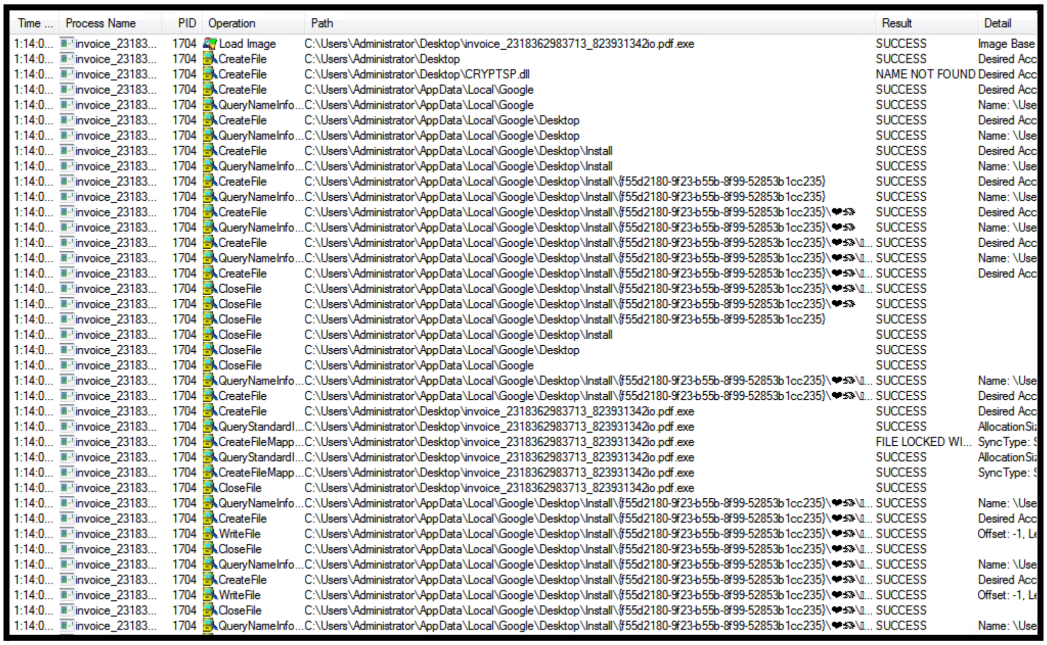
```
0x0043397c      push    0x43686769 ; 'ighC'
0x00433981      outsd   dx, dword [esi]
0x00433982      insb    byte es:[edi], dx
0x00433983      jae     0x433985
0x00433985      dec     ebx
```

The string CellrotoCrudUntohighCols comes right before a function call, KERNEL32.CreateFileA. This assembly code shows a section of the string being pushed (‘ighC’). The function call comes very close after, in the highlighted line.

Dynamic Analysis

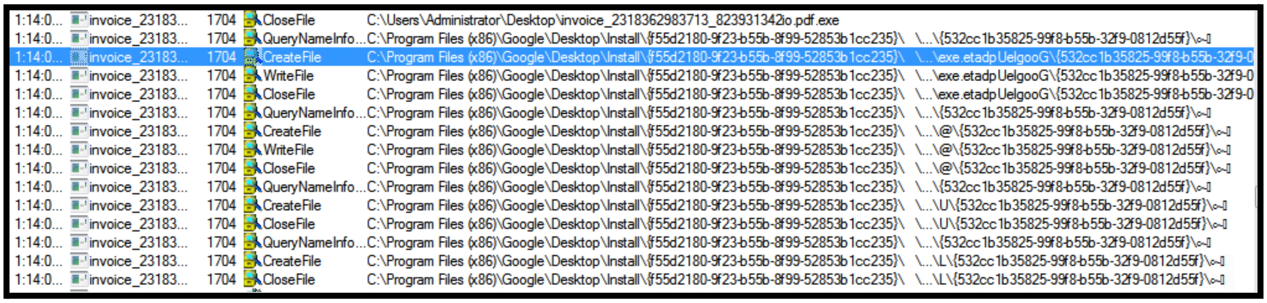
Initial observation: The file deletes itself once executed, likely after establishing persistence.

Process Monitor (Procmon)



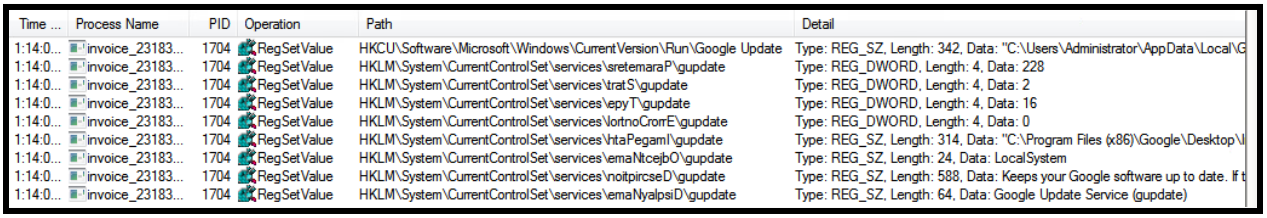
Time ...	Process Name	PID	Operation	Path	Result	Detail
1:14:0...	invoice_23183...	1704	Load Image	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	Image Base
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\Desktop	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\Desktop\CRYPTSP.dll	NAME NOT FOUND	Desired Acc
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍	SUCCESS	
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}	SUCCESS	
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install	SUCCESS	
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop	SUCCESS	
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google	SUCCESS	
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	QueryStandardI...	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	AllocationSi
1:14:0...	invoice_23183...	1704	CreateFileMapp...	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	FILE LOCKED WI...	SyncType: S
1:14:0...	invoice_23183...	1704	QueryStandardI...	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	AllocationSi
1:14:0...	invoice_23183...	1704	CreateFileMapp...	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	SyncType: S
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe	SUCCESS	
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	WriteFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Offset: -1, Le
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Name: \Use
1:14:0...	invoice_23183...	1704	CreateFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Desired Acc
1:14:0...	invoice_23183...	1704	WriteFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Offset: -1, Le
1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Users\Administrator\AppData\Local\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\❤⅍\I...	SUCCESS	Name: \Use

This data from Procmon shows all the operations that the malicious file performed. It also created randomly named files in the C:\Users\...\Google\Desktop\Install directory.



1:14:0...	invoice_23183...	1704	CloseFile	C:\Users\Administrator\Desktop\invoice_2318362983713_823931342io.pdf.exe
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CreateFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\exe.etadpUelgooG\{532cc1b35825-99f8-b55b-32f9-0
1:14:0...	invoice_23183...	1704	WriteFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\exe.etadpUelgooG\{532cc1b35825-99f8-b55b-32f9-0
1:14:0...	invoice_23183...	1704	CloseFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\exe.etadpUelgooG\{532cc1b35825-99f8-b55b-32f9-0
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CreateFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\@\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	WriteFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\@\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CloseFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\@\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CreateFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\U\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CloseFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\U\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	QueryNameInfo...	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CreateFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\L\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷
1:14:0...	invoice_23183...	1704	CloseFile	C:\Program Files (x86)\Google\Desktop\Install\{f55d2180-9f23-b55b-8f99-52853b1cc235}\ \...\L\{532cc1b35825-99f8-b55b-32f9-0812d55f}\⊸⌷

More files are being created in the C:\Program Files (x86)\...\Desktop\Install directory, specifically a file called exe.etadpUelgooG, which is the reverse of GoogleUpdate.exe. This is likely the malware's attempt to obfuscate the file from security software.



Time ...	Process Name	PID	Operation	Path	Detail
1:14:0...	invoice_23183...	1704	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Google Update	Type: REG_SZ, Length: 342, Data: "C:\Users\Administrator\AppData\Local\G
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\sretemaraP\gupdate	Type: REG_DWORD, Length: 4, Data: 228
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\tratS\gupdate	Type: REG_DWORD, Length: 4, Data: 2
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\epyT\gupdate	Type: REG_DWORD, Length: 4, Data: 16
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\lortnoCrorrE\gupdate	Type: REG_DWORD, Length: 4, Data: 0
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\htaPegamI\gupdate	Type: REG_SZ, Length: 314, Data: "C:\Program Files (x86)\Google\Desktop\I
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\emaNtcejbO\gupdate	Type: REG_SZ, Length: 24, Data: LocalSystem
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\noitpircseD\gupdate	Type: REG_SZ, Length: 588, Data: Keeps your Google software up to date. If t
1:14:0...	invoice_23183...	1704	RegSetValue	HKLM\System\CurrentControlSet\services\emaNyalpsiD\gupdate	Type: REG_SZ, Length: 64, Data: Google Update Service (gupdate)

In this screenshot, there are more reversed file/folder names that the malware is setting as values in the registry. In the first row, the value in Google Update is being set by one of the files it created in the filesystem. It is possible that the malware establishes persistence in the registry through Google Update.

Conclusion

In the static analysis of the malicious sample, we found the entire list of strings used in the sample, which contains API calls, URLs, and gibberish that are suspected to be obfuscated function names, given its close proximity to legit function calls. One of the capabilities of the sample is the detection of a sandboxed environment. This is likely so it can avoid being analyzed. By using Cutter, you can see the assembly code of the malware, showing what functions were called and when. GetTickCount was used by the malware to see how long the machine has been powered on for, likely to see if it is being run in a virtualized environment. In the dynamic analysis, Process Monitor was used to see what operations were being performed by the malicious program. Files of random names were created in the filesystem and the Google Update registry value was set to one of the malicious files it created. This was likely the mechanism for establishing persistence.

Source

▶ Analyzing the Zeus Banking Trojan - Malware Analysis Project 101