Threat Thursday: ZingoStealer – The Cost of “Free”

blogs.blackberry.com/en/2022/05/threat-thursday-zingostealer

The BlackBerry Research & Intelligence Team

Summary

Everyone likes a great deal, and the closer something gets to free, the more universal its appeal. In the case of ZingoStealer, the lure of “free” seems to be successfully attracting both predators and prey. Even those who make their living as a cybercriminal might still try to keep their costs in check as they look to wreak havoc, but sometimes there are costs to malware operators for “free” software that aren’t necessarily paid by the victim.

The ZingoStealer information stealer, also known as Ginzo, is malware targeting Windows® systems that was first discovered in March 2022 being distributed by a Russian group called the “Haskers Gang.” On March 4, they uploaded a video to YouTube showcasing the infostealer, announcing that the malware is available for free to its members, distributed via the Ginzo Telegram channel. An additional variant is available for US$3, which contains a crypter malware called “ExoCrypt” that encrypts the threat to help the attacker evade antivirus detection.

The “free” offer seems to be fueling a spike of adoption for the malware. The malware’s victims, primarily home users, are lured in by the appeal of getting something for nothing – in their case, it’s the promise of free access to “cracked” versions of popular video games and software.

ZingoStealer instead steals sensitive user data such as login credentials and cryptocurrencies. Stolen information is returned to the command-and-control (C2) server and used for financial gain by the attacker. The malware also packs an additional punch, delivering malicious payloads to the target machines. For example, in the binary analyzed in this report, an XMRig cryptocurrency miner was dropped to the machine post-execution.

As it turns out, home users trying to score a free download are not the only ones who might be getter somewhat more – or less – than they bargained for. Attackers making use of the free malware could also be getting shortchanged on the “free” offer: As our analysis reveals, the malware authors maintain access to all data stolen by their clients, and they could well be profiting from it in addition to, or even in advance of, their clientele. Not so “free,” after all.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	High
Risk	Medium

Technical Analysis

ZingoStealer is delivered as a highly obfuscated .NET executable. The initial file is obfuscated using ConfuserEx, an open-source protector tool for .NET files. The file is decrypted on the fly using the type initializer ".cctor," which causes error messages when attempting to use automatic deobfuscation tools. This makes readable code more difficult to obtain, providing the attacker with a means of impeding analysis.

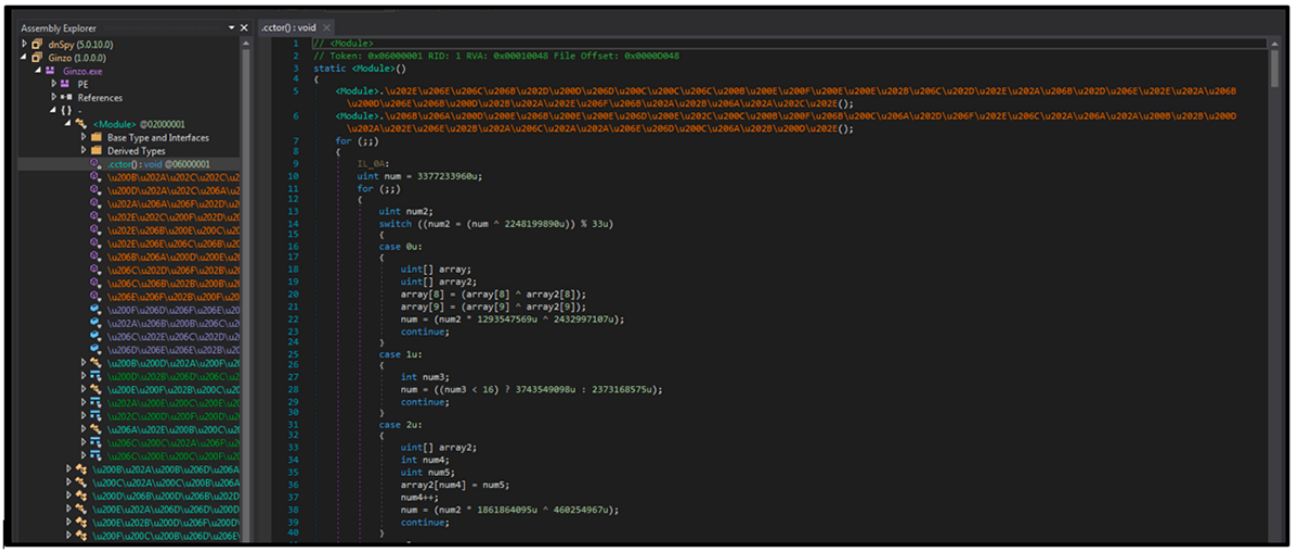

Figure 1 – Obfuscated .NET ZingoStealer executable

When executed, the first thing the malware does is reach out to its C2 server to retrieve a list of dependencies (also shown in Figure 2). These files are dropped into the directory where the malware was initially executed.

- BouncyCastle.Crypto.dll
- DotNetZip.dll
- Newtonsoft.json.dll
- System.Data.SQLite.dll
- SQLite.Interop.dll (x64 and x86)

The files are used by the malware to provide core functionality during the attack.

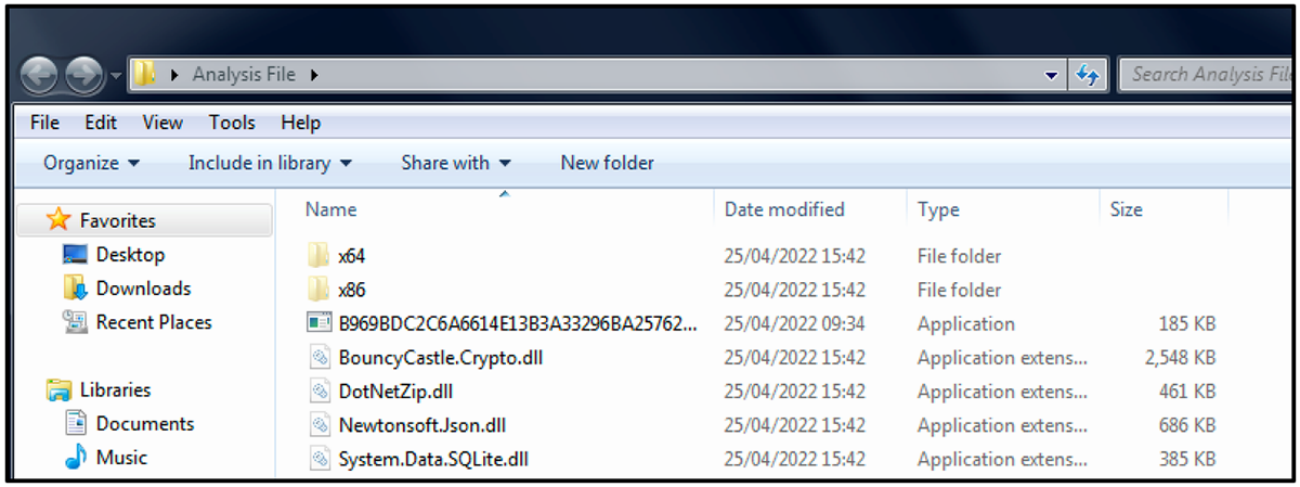

Figure 2 – DLL dependencies dropped into the same folder where the malware was executed

The malware will then create a folder on the target machine in the directory "User\AppData\Local\GinzoFolder." This is where stolen information is stored. As shown in Figure 3 below, three subdirectories are created within this folder using the following

names:

- Browsers
- Wallets
- Desktop Files

Process Name	PID	Operation	Path
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Browsers
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Browsers
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Browsers
B969BDC2C6A...	4284	CloseFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Browsers
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Wallets
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Wallets
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Wallets
B969BDC2C6A...	4284	CloseFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Wallets
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Desktop Files
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Desktop Files
B969BDC2C6A...	4284	CreateFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Desktop Files
B969BDC2C6A...	4284	CloseFile	C:\Users\Analyst\AppData\Local\GinzoFolder\Desktop Files

Figure 3 – Subdirectories are created within the "\GinzoFolder\" directory

Information Stealing

The malware begins its information heist by taking a screenshot of the victim's screen without their knowledge or consent. The screenshot is stored in the ***%AppData%Local%GinzoFolder%*** directory as "Screenshot.Png."

ZingoStealer also performs a fingerprint of the victim's system, as seen in Figure 4, gathering information about the target machine and storing it in a text file called "system.txt," in the **%GinzoFolder%** mentioned above. This information includes the following:

- Windows Version
- AV Information
- Username
- CPU Name
- GPU Name
- RAM Amount
- Public and Local IP Address and location
- Screen Resolution

```
private static void StealInfo()
{
    LibraryDownloader.Download();
    GinzoFolderCreator.CreateGinzoDirectories();
    SpyInfo.TakeScreenshot();
    SpyInfo.CheckHasInternet();
    CookieExtractor.StealChromeCookies();
    CookieExtractor.StealFirefoxCookies();
    CookieExtractor.StealOperaCookies();
    CookieExtractor.StealOperaGXCookies();
    Console.WriteLine("All cookies count:" + CookieExtractor.CookieTotalCount().ToString());
    PasswordExtractor.StealChromePasswords();
    PasswordExtractor.StealFirefoxPasswords();
    PasswordExtractor.StealOperaPasswords();
    PasswordExtractor.StealOperaGXPasswords();
    Console.WriteLine("All passwords count:" + PasswordExtractor.TotalStolenPasswords().ToString());
    SpyInfo.BuildSystemTxtFile();
    SpyInfo.StealDiscord();
    GClass5.StealDesktopFiles(GinzoFolderCreator.ginzoFolder);
    GClass6.StealTelegramSessionData();
    Class6.StealCryptoCurrExtensionData();
    Class12.SendStolenData();
    GinzoSteal.DeleteDirectory(GinzoFolderCreator.ginzoFolder, true);
    Class7.smethod_0();
```

Figure 4 – Core infostealing functionality of ZingoStealer

Browsers

ZingoStealer next scans the victim's device in an effort to collect sensitive information related to popular web browsers. The information gathered includes login data, cookies, browser extensions, auto-fill information and any other sensitive data. The malware targets the following browsers:

- Google Chrome
- Firefox
- Opera and Opera GX

Cryptocurrency

One of the main functions of ZingoStealer is its cryptocurrency stealing ability. The malware scours the target machine in search of any data associated with the crypto wallet extensions seen below. A crypto wallet is an application used to both cold-store and retrieve digital cryptocurrency assets.

Binance Wallet	Guarda	EQUAL Wallet	BitApp Wallet	iWallet
Wombat	Brave Wallet	Coinbase Wallet	MathWallet	MetaMask
Nifty Wallet	Tron Link	Bitcoin	Dash	Litecoin

ZingoStealer checks browser extensions for wallet credentials for popular cryptocurrency services, such as Binance and Coinbase.

Additionally, the malware will search the **%AppData%** directory for any wallet data that is related to the following cryptocurrencies:

Coinomi	Ethereum	Atomic	Exodus	Jaxx Liberty
Bytecoin	Guarda	Armory	Electrum	Zcash

Exfiltration

The malware will perform exfiltration of all gathered data from the target machine back to the C2 server. In the case of the binary used in this analysis, it was hosted at 172[.]67[.]129[.]178. All information stored within the directory **%GinzoFolder%** is compressed into "ginzoarchive.zip" as seen in Figure 5 and is sent back to the C2 server via a POST request.

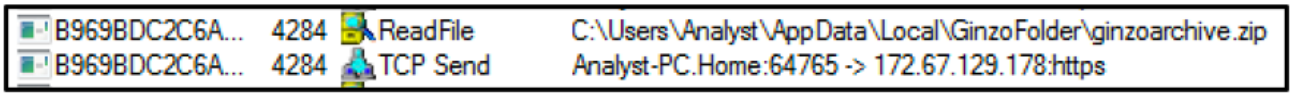

Figure 5 – Data is read from the Ginzo archive file and sent to the C2 server

The malware also stores a datetime value in a file called "ChromeUploadTime.txt" within the **%AppData%Local%** directory. This value is used to ensure that the harvested data is not being sent too frequently to the server. This helps the malware to stay under the radar and evade detection.

Additional Payloads – XMRig Miner

Another functionality of ZingoStealer, which makes it more dangerous than your average infostealer, is that it drops additional payloads to the victim's machine. The payload dropped by the malware varies depending on how it was set up by the malware operator. For example, samples have been observed dropping copies of RedLine infostealer (previously analyzed by the BlackBerry Research & Intelligence Team) onto the target machine. Such payloads provide additional monetization methods for the ZingoStealer authors and users.

In the instance of the sample analyzed in this report, an injector for the XMRig cryptocurrency miner was dropped to the system. Cryptocurrency miners are used in attacks to steal computing power to mine for coins; this process is also known as cryptojacking.

The file for XMRig was dropped into the %**AppData\%Local%** directory, as shown in Figure 6. Its filename is generated using a random 6-digit hex number, in this case it was "346590.exe."

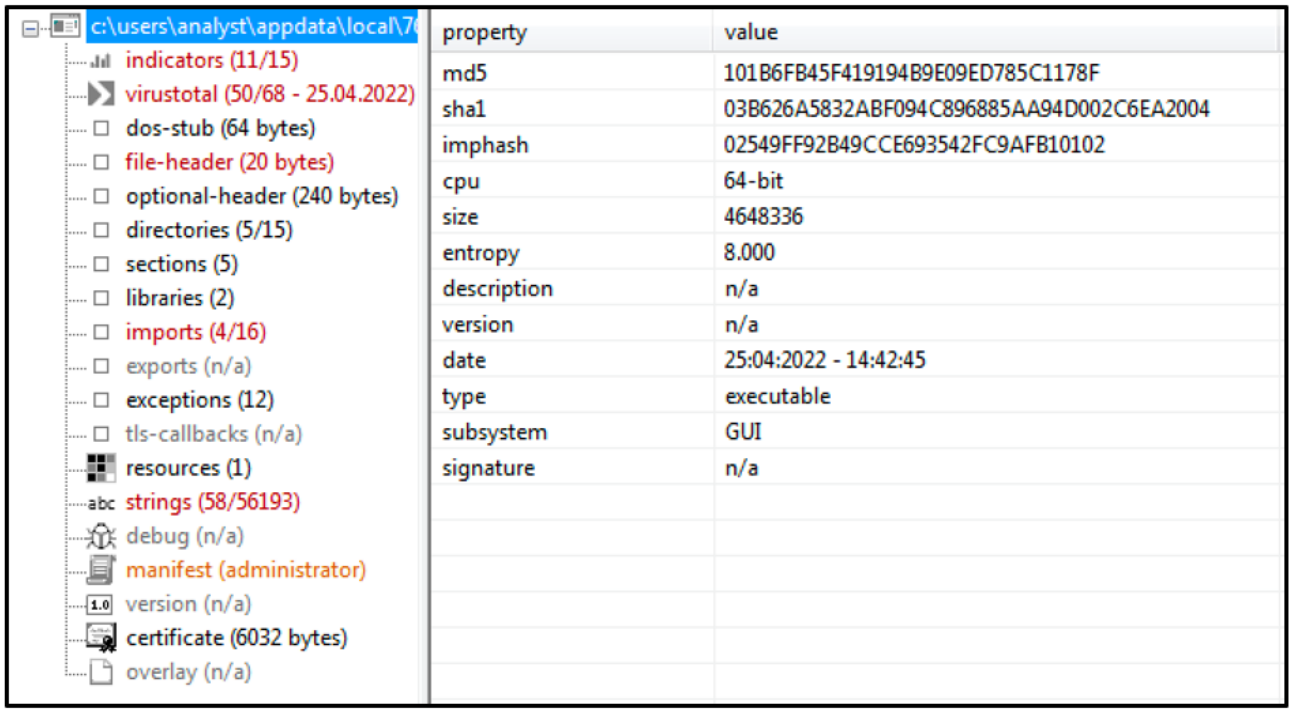

Figure 6 – Additional payload XMRig dropped to the AppData\Local directory

The file for XMRig is dropped and executed when the initial ZingoStealer file is launched. ZingoStealer does this by utilizing its file "conhost.exe" to issue the command ***"C:\Windows\System32\conhost.exe" "C:\Users\<USERNAME>\AppData\Local\346590.exe."***

Once executed, the malware launches PowerShell to issue the base64-encoded command seen in Figure 7 below.

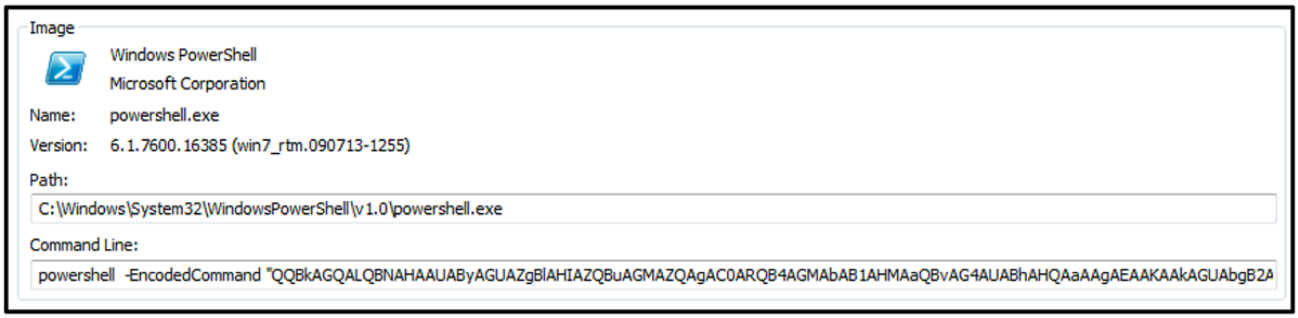

Figure 7 – PowerShell launched and base64-encoded command executed utilizing the "-EncodeCommand" option

Decoding this command reveals its functionality: It is used to create two exclusions in Windows Defender to avoid being detected.

- Add-MpPreference -ExclusionPath @($env:UserProfile,$env:SystemDrive) -Force

- Add-MpPreference -ExclusionExtension @('exe','dll') -Force

The XMRig malware attempts to achieve persistence by creating a copy of itself in the **%AppData%Roaming%Chrome%** directory under the filename “updater.exe,” as shown in Figure 8. In addition to this, it creates a scheduled task to ensure that this executable runs at system startup.

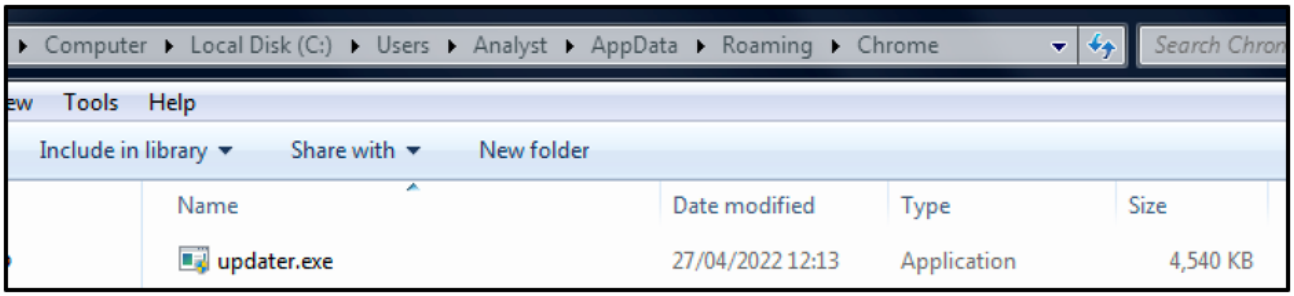

Figure 8 – Miner creates a copy of itself in the \Roaming\Chrome directory under the name "updater.exe"

The newly created executable also drops a binary into the **%Roaming%Windows%Telemetry%** directory called “sihost64.exe.” The XMRig miner is then injected into the “explorer.exe” process where cryptocurrency mining operations begin. The miner will periodically send beacon updates back to the C2 server, as seen in Figure 9.

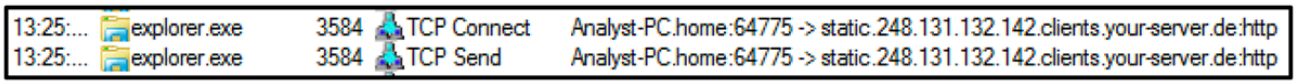

Figure 9 – Miner injected into the "explorer.exe" process sends beacon updates to the C2 server

Control Panel

The ZingoStealer malware provides a C2 Control panel for its users (the malware operators) to login and access all harvested data. The panel is hosted at the address “network[.]nominally[.]ru/admin/login.php.”

It is important to remember that all harvested data is being funneled to the threat actors’ servers. This means that they can also access any stolen data, and it would come as no surprise if they were using data harvested by those malware operators for their own monetary gain. After all, the malware is being offered for free!

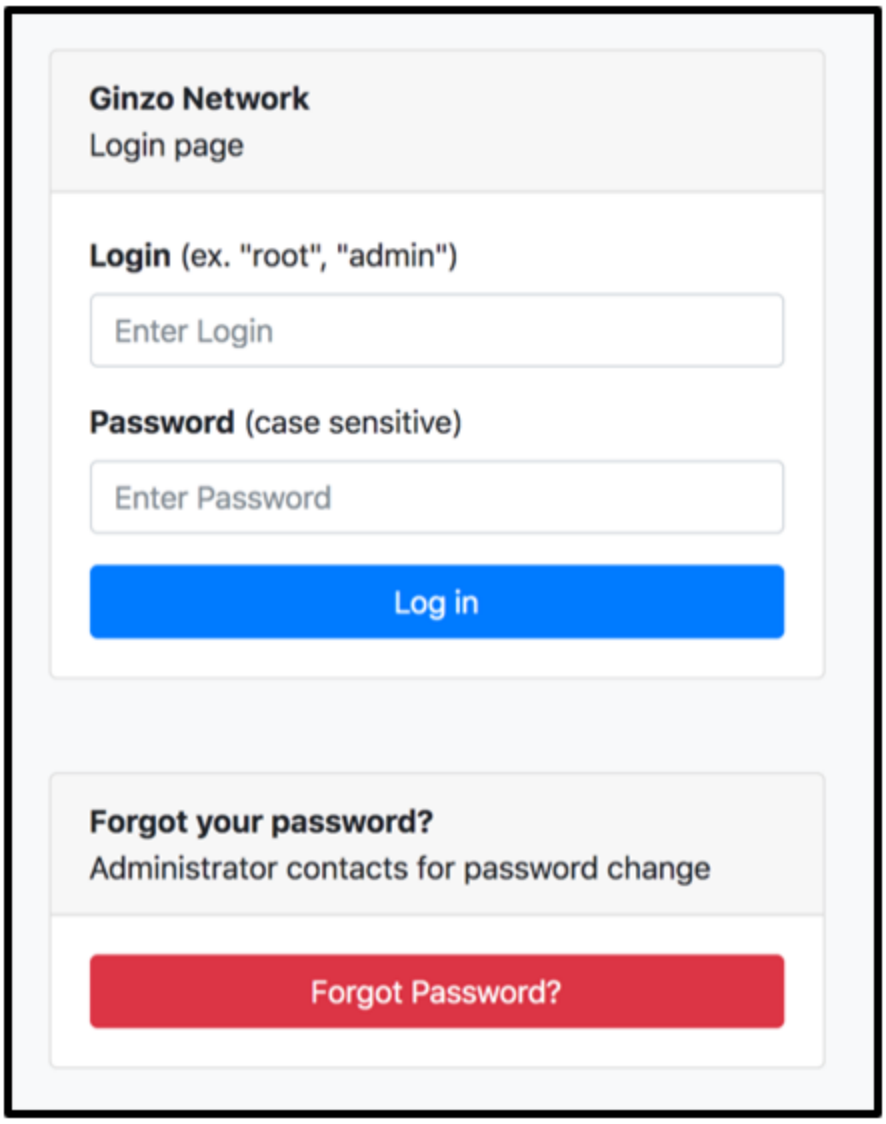

Figure 10 – ZingoStealer control panel which can be used to access harvested data

Conclusion

ZingoStealer contains all the functionality expected from a typical infostealer. What sets it apart from its peers within the malware landscape is its ability to deliver additional, and potentially more dangerous, payloads. At present, the malware has been observed delivering XMRig and RedLine. However, since the malware is available for free and offered as a Malware-as-a-Service (MaaS), it would come as no surprise to see these additional payloads continue to vary in coming months.

ZingoStealer has experienced a rapid increase in popularity, considering it was first discovered in March. At the time of writing this, a retrohunt was carried out on VirusTotal using the YARA rule attached to this report. The results returned 950+ positive hits for different binaries of the malware. As this threat's popularity continues to rise, it will be interesting to see how the malware operator's choice of additional malicious payloads bundled with the malware evolves.

As the malware seems to be primarily targeting home users, and is being spread by masquerading as a “cracked” version of popular video games and software, people must be extra vigilant when visiting websites to download new software. It’s important to only download from trusted links provided by legitimate vendors, rather than third-party or “pirate” websites. Also, for those who store cryptocurrencies on their devices, ensure you have sufficient security measures in place around accessing and storing this information.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule ZingoStealer {
   meta:
      description = "Detects ZingoStealer Infostealer"
      author = "BlackBerry Threat Research Team"
      date = "2022-04-22"
      license = "This Yara rule is provided under the Apache License 2.0 (https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as you use it under this license and ensure originator credit in any derivative to The BlackBerry Research & Intelligence Team"

   strings:
      $s1 = "Ginzo.pdb"
      $s2 = "Ginzo.exe"
      $s3 = "Org.BouncyCastle.Crypto"
      $s4 = "DotNetZip"
      $s5 = ".cctor"
      $s6 = "Newtonsoft.Json.Linq"
      $s7 = "System.Data.SQLite"

   condition:
   (
   //PE File
   uint16(0) == 0x5a4d and

   //Imphash
   pe.imphash() == "f34d5f2d4577ed6d9ceec516c1f5a744" and

   //All Strings
   all of ($s*) )
}
```

Indicators of Compromise (IoCs)

Hashes
b969bdc2c6a6614e13b3a33296ba25762b9f6935f7cb0674e5f84c96c9640e71
- Zingo .NET
ee1524e4980cac431ae0f92888ee0cc8a1fa9e7981df0be6abd7efa98adf9a45
– Miner
1b3d0f2b2a65b7791e277851802a57536928fbc2f34d1eea747bb59467608d60
– sihost64.exe

Files
Jvm.exe

IP Address
172[.]67[.]129[.]178

Download URLs
hxxps://nominally[.]ru/cis.txt
hxxps://nominally[.]ru/ginzolist.txt
hxxps://nominally[.]ru/library/System.Data.SQLite.dll
hxxps://nominally[.]ru/library/Newtonsoft.Json.dll
hxxps://nominally[.]ru/library/BouncyCastle.Crypto.dll
hxxps://nominally[.]ru/library/x86/SQLite.Interop.dll
hxxps://nominally[.]ru/library/x64/SQLite.Interop.dll
hxxps://nominally[.]ru/library/antiwm.exe
hxxps://nominally[.]ru/library/generation.exe

C2 Panels
network[.]nominally[.]ru/admin/login.php - ZingoStealer
control[.]nominally[.]ru/login.php – XMRig Cryptominer

Folders
%LOCALAPPDATA%\ChromeUploadTime.txt
%LOCALAPPDATA%\GinzoFolder
%LOCALAPPDATA%\GinzoFolder\Wallets
%LOCALAPPDATA%\GinzoFolder\Browsers
%LOCALAPPDATA%\GinzoFolder\DesktopFiles
%LOCALAPPDATA%\GinzoFolder\ ginzoarchive.zip
%LOCALAPPDATA%\GinzoFolder\Screenshot.png
%LOCALAPPDATA%\GinzoFolder\system.txt

References

https://blog.talosintelligence.com/2022/04/haskers-gang-zingostealer.html

https://blogs.blackberry.com/en/2021/07/threat-thursday-redline-infostealer

https://www.youtube.com/watch?v=3Myj1yT6-ro – Haskers Gang announcement video

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back