New powerful Prynt Stealer malware sells for just $100 per month

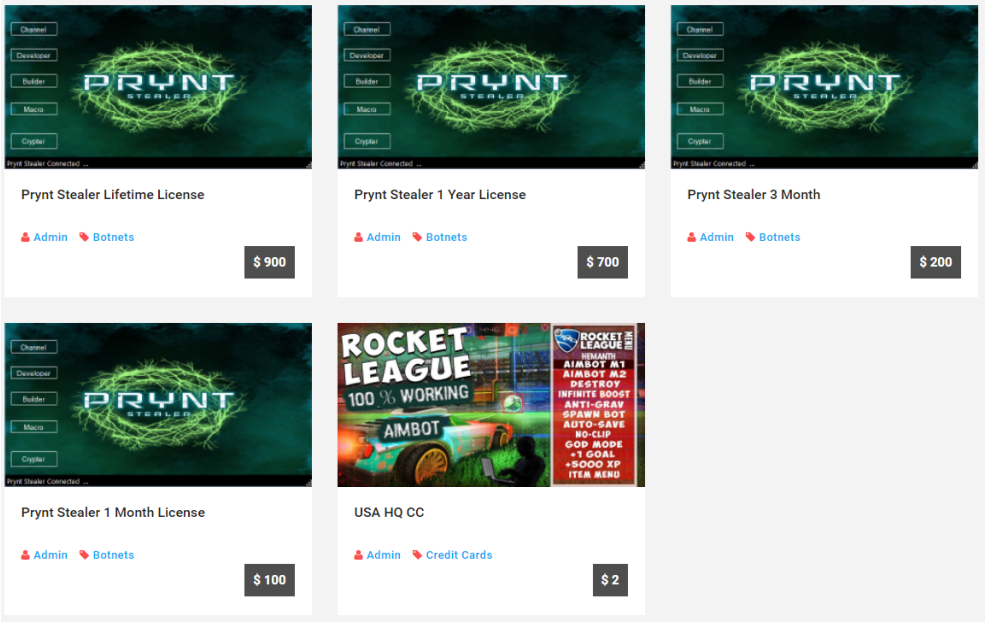
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** April 25, 2022 08:43 AM **0**

Threat analysts have spotted yet another addition to the growing space of info-stealer malware infections, named Prynt Stealer, which offers powerful capabilities and extra keylogger and clipper modules.

Prynt Stealer targets a large selection of web browsers, messaging apps, and gaming apps and can also perform direct financial compromise.

Its authors sell the tool in time-based subscriptions, such as 100$/month, $200/quarter, or $700 for a year, but it is also sold under a lifetime license for $900.

Additionally, buyers may take advantage of the malware's builder to create a specialized, lean, and hard-to-detect spin of Prynt to be deployed in targeted operations.



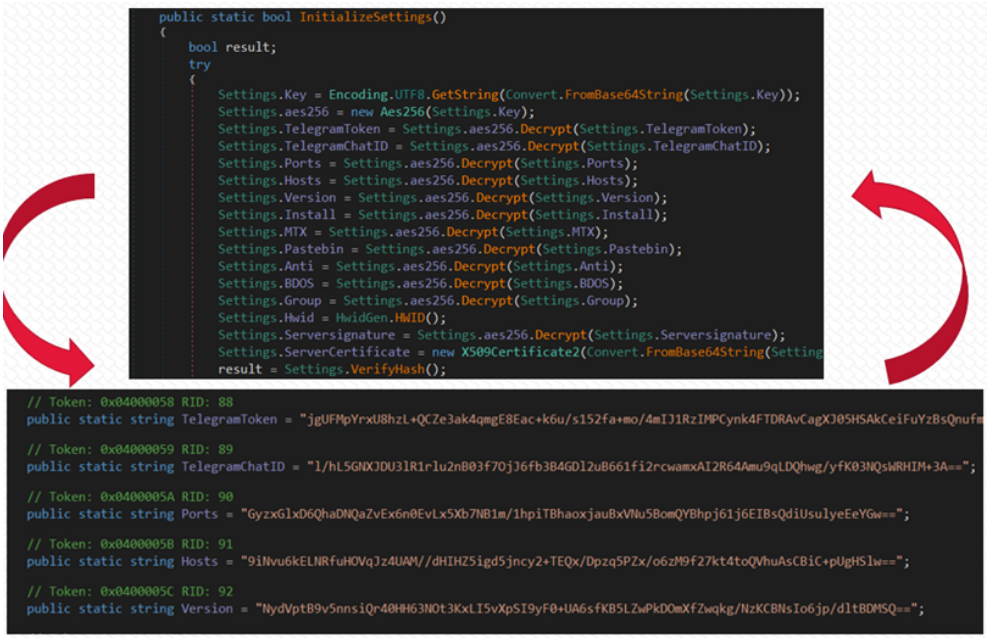
Prynt Stealer's license cost *(Bleeping Computer)*

Extensive stealing capabilities

Malware analysts at Cyble (https://blog.cyble.com/2022/04/21/prynt-stealer-a-new-info-stealer-performing-clipper-and-keylogger-activities/) have analyzed Prynt to evaluate the new info-stealer and report that the tool was crafted with stealthiness as a priority, featuring binary obfuscation and Rijndael encrypted strings.

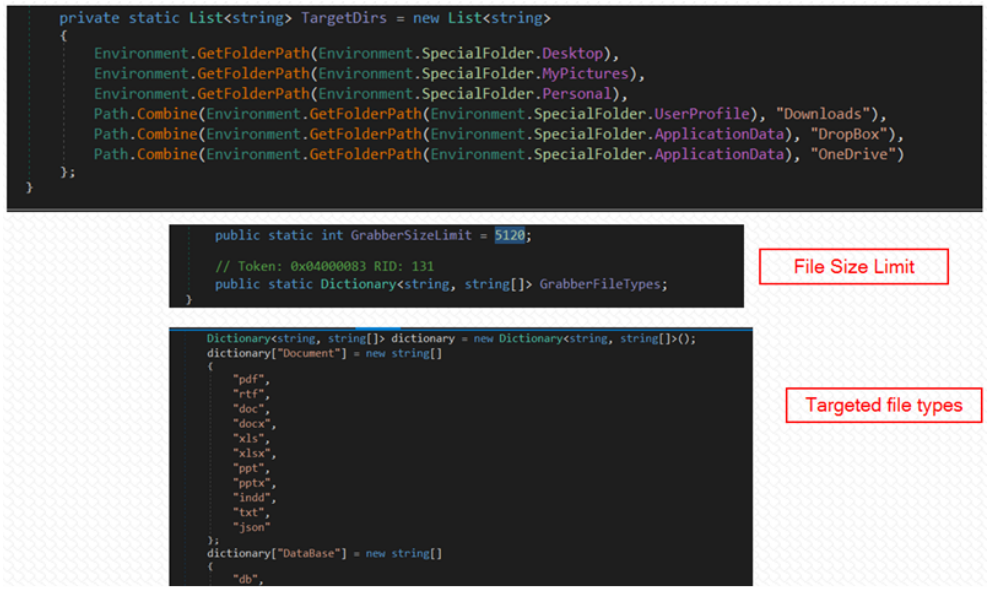
Prynt's obfuscated binary *(Cyble)*

Moreover, all its C2 communications are encrypted with AES256, while the AppData folder (and subfolders) created for temporarily storing the stolen data before exfiltration are hidden.



Hardcoded string decryption *(Cyble)*

At first, Prynt Stealer scans all drives in the host and steals documents, database files, source code files, and image files that have a size below 5,120 bytes (5 KB).



Stealing small files from the host *(Cyble)*

Next, the malware targets autofill data, credentials (account passwords), credit card info, search history, and cookies stored in Chrome-based, MS Edge, and Firefox-based web browsers.

```
foreach (string str in Directory.GetDirectories(path))
{
    string text2 = sSavePath + "\\" + Crypto.BrowserPathToAppName(text);
    Directory.CreateDirectory(text2);
    List<CreditCard> cCC = CreditCards.Get(str + "\\Web Data");
    List<Password> pPasswords = Stealer.Get(str + "\\Login Data");
    List<Cookie> cCookies = Cookies.Get(str + "\\Cookies");
    List<Site> sHistory = History.Get(str + "\\History");
    List<Site> sHistory2 = Downloads.Get(str + "\\History");
    List<AutoFill> aFills = Autofill.Get(str + "\\Web Data");
    List<Bookmark> bBookmarks = Bookmarks.Get(str + "\\Bookmarks");
    cBrowserUtils.WriteCreditCards(cCC, text2 + "\\CreditCards.txt");
    cBrowserUtils.WritePasswords(pPasswords, text2 + "\\Passwords.txt");
    cBrowserUtils.WriteCookies(cCookies, text2 + "\\Cookies.txt");
    cBrowserUtils.WriteHistory(sHistory, text2 + "\\History.txt");
    cBrowserUtils.WriteHistory(sHistory2, text2 + "\\Downloads.txt");
    cBrowserUtils.WriteAutoFill(aFills, text2 + "\\AutoFill.txt");
    cBrowserUtils.WriteBookmarks(bBookmarks, text2 + "\\Bookmarks.txt");
}
```

Stealing data from Chromium browsers *(Cyble)*

At this stage, the malware uses ScanData () to check if any keywords relevant to banking, cryptocurrency, or porn sites are present in the browser data and steals them if they are.

```
public static void ScanData(string value)
{
    Banking.DetectBankingServices(value);
    Banking.DetectCryptocurrencyServices(value);
    Banking.DetectPornServices(value);
}
```

Scanning for specific services *(Cyble)*

Next, Prynt targets messaging apps like Discord, Pidgin, and Telegram and also snatches Discord tokens if present on the system.

Gaming app authorization files, save game files, and other valuable data from Ubisoft Uplay, Steam, and Minecraft are also stolen.

```
public static void SaveAll(string sSavePath)
{
    if (!Directory.Exists(Minecraft.MinecraftPath))
    {
        return;
    }
    try
    {
        Directory.CreateDirectory(sSavePath);
        Minecraft.SaveProfiles(sSavePath);
        Minecraft.SaveServers(sSavePath);
        Minecraft.SaveScreenshots(sSavePath);
        Minecraft.SaveMods(sSavePath);
        Minecraft.SaveVersions(sSavePath);
    }
    catch
    {
    }
}
```

Stealing Minecraft data *(Cyble)*

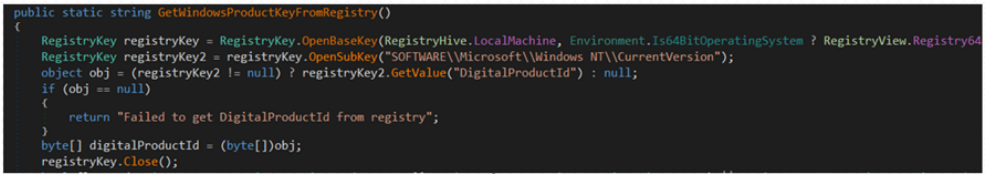
Then, the malware queries the registry to locate the data directories for cryptocurrency wallets, such as Zcash, Armory, Bytecoin, Jaxx, Ethereum, AtomicWallet, Guarda, and the Coinomi cryptocurrency wallets.

As these data directories contain the actual wallet configuration files and databases, the threat actors collect them to steal the cryptocurrency stored within them.

Scanning the registry for wallets *(Cyble)*

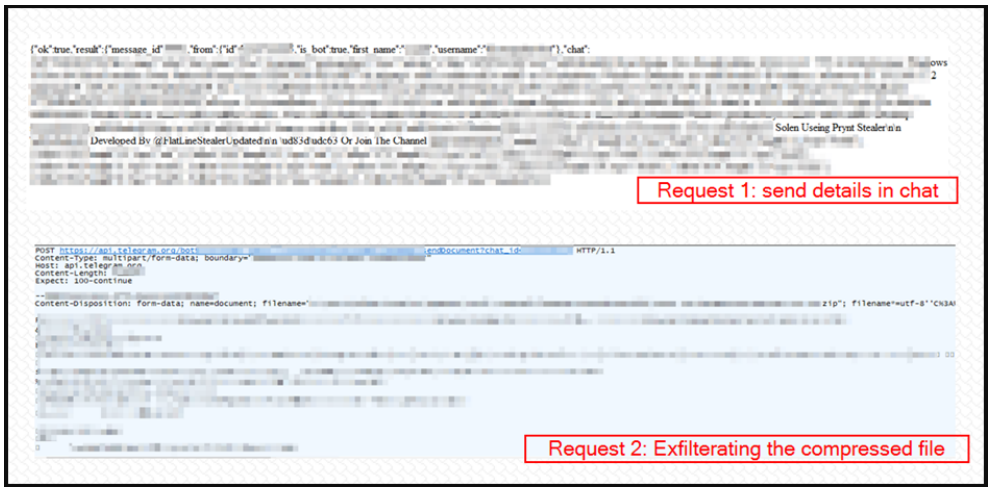
Finally, Prynt steals data from FileZilla, OpenVPN, NordVPN, and ProtonVPN, copying the associated account credentials on the corresponding subfolder in AppData.

Before exfiltration, Prynt Stealer performs a general system profiling action involving the enumeration of running processes, taking a screenshot of the summary, and bundling it with the network credentials and the Windows product key used in the host machine.



Windows key stolen too *(Cyble)*

The eventual theft of the compressed data is done via a Telegram bot that employs a secure encrypted network connection to pass everything to the remote server.



The Telegram data exfiltration step *(Cyble)*

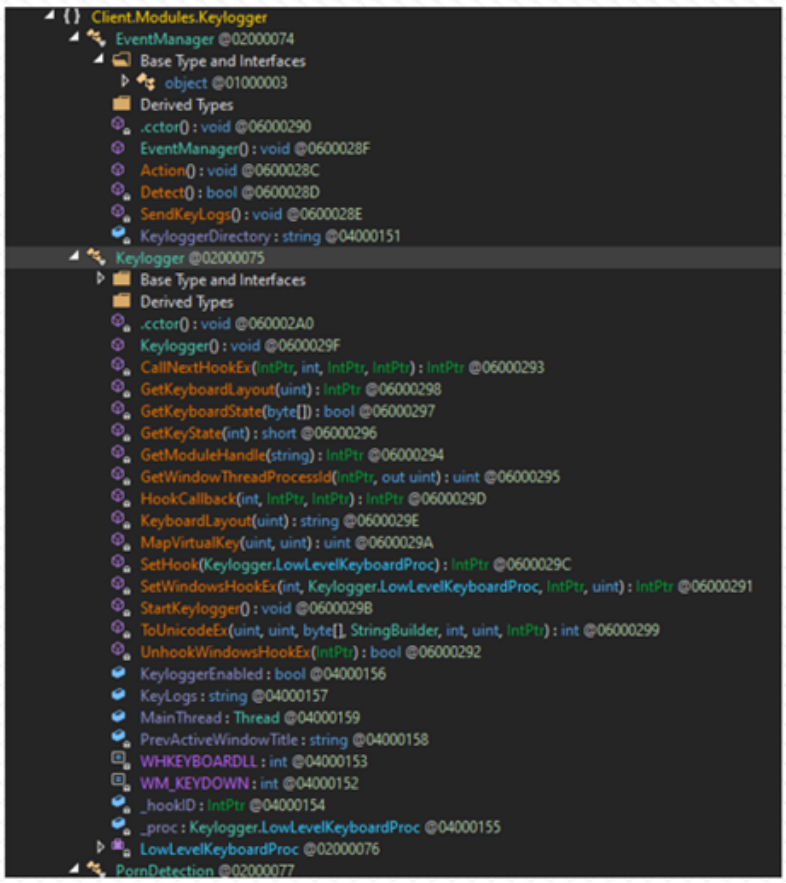
Clipper and keylogger

Apart from the above features, which are in line with what most info-stealers are capable of nowadays, Prynt also comes with a clipper and a keylogger.

A clipper is a tool that monitors copied data on the compromised machine's clipboard to identify cryptocurrency wallet addresses and replace them on-the-fly with one under the threat actor's control.

Whenever the victim attempts to pay with cryptocurrency to a specific address, the malware covertly switches the recipient's address, and the payment is diverted to the hackers.

The keylogger is another additional module that enables remote malware operators to perform bulk information stealing by recording all key presses.



Prynt's keylogger module *(Cyble)*

Prynt is another addition to a plethora of available info-stealing malware tools that cybercriminals can choose from, many of which recently appeared in the wild.

While its keylogger, clipper, and extensive stealing capabilities combined with a stealthy operation make it a good candidate for broad deployment, its relatively high cost (compared to other recently emerged malware) and doubtful server infrastructure reliability might put a brake on its rise.

Still, Prynt is a dangerous malware that can steal sensitive user information and lead to significant financial damages, account compromise, and data breach.