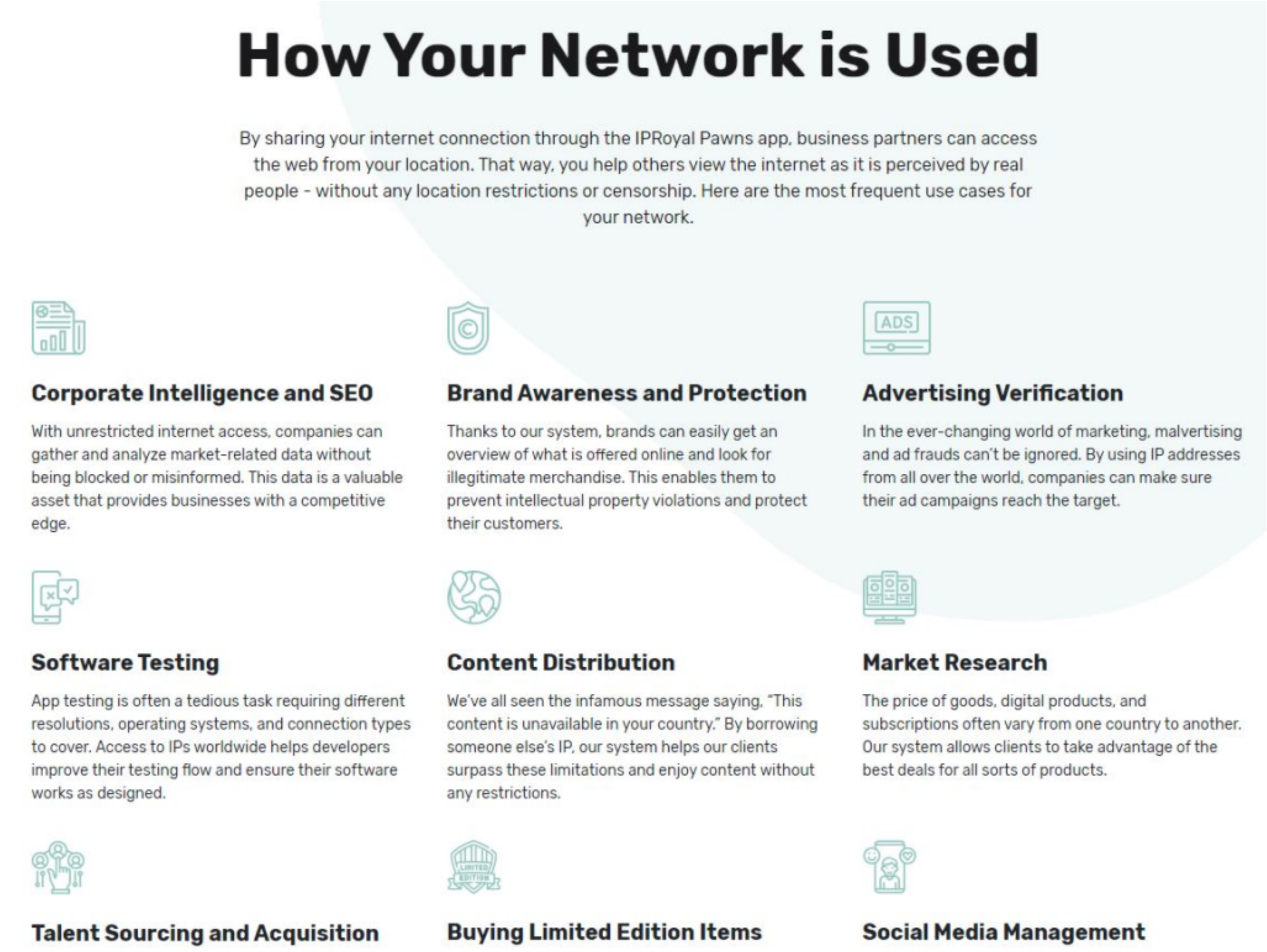
# Attackers Profiting from Proxyware

asec.ahnlab.com/en/37276/

July 28, 2022

Proxyware is a program that shares a part of the Internet bandwidth that is currently available on a system to others. Users who install the program are usually paid with a certain amount of cash in exchange for providing the bandwidth. Companies that provide such a service include **Peer2Profit** and **IPRoyal**. They gain profit by providing the bandwidth to other companies and claim on their webpages that they have various business partners using the service for distributing software, investigating markets, verifying advertisements, testing software, and so on.

While users can earn some money from installing proxyware on their systems, they should know they are taking risks by allowing external users to perform certain behaviors by using their networks. For instance, users cannot know in detail the companies that the proxyware platforms claim to use their services. Even if they can verify their customers on their own, it is impossible to check if your bandwidth will be maliciously exploited in the future or not.



**How Your Network is Used**

By sharing your internet connection through the IPRoyal Pawns app, business partners can access the web from your location. That way, you help others view the internet as it is perceived by real people - without any location restrictions or censorship. Here are the most frequent use cases for your network.

**Corporate Intelligence and SEO**

With unrestricted internet access, companies can gather and analyze market-related data without being blocked or misinformed. This data is a valuable asset that provides businesses with a competitive edge.

**Brand Awareness and Protection**

Thanks to our system, brands can easily get an overview of what is offered online and look for illegitimate merchandise. This enables them to prevent intellectual property violations and protect their customers.

**Advertising Verification**

In the ever-changing world of marketing, malvertising and ad frauds can't be ignored. By using IP addresses from all over the world, companies can make sure their ad campaigns reach the target.

**Software Testing**

App testing is often a tedious task requiring different resolutions, operating systems, and connection types to cover. Access to IPs worldwide helps developers improve their testing flow and ensure their software works as designed.

**Content Distribution**

We've all seen the infamous message saying, "This content is unavailable in your country." By borrowing someone else's IP, our system helps our clients surpass these limitations and enjoy content without any restrictions.

**Market Research**

The price of goods, digital products, and subscriptions often vary from one country to another. Our system allows clients to take advantage of the best deals for all sorts of products.

**Talent Sourcing and Acquisition**

**Buying Limited Edition Items**

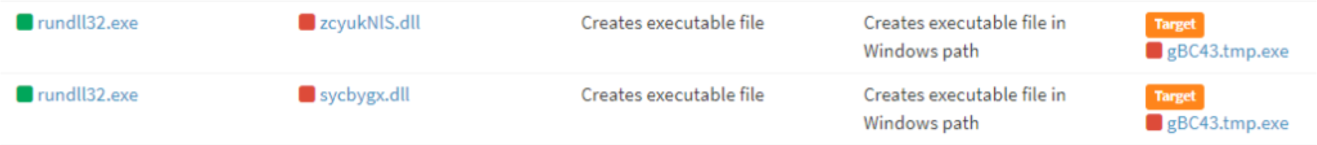
**Social Media Management**

Figure 1. IPROYAL claiming how your network is used

The ASEC analysis team recently discovered malware strains installing proxyware without the user's permission. Users whose systems are infected with the malware have their network bandwidth stolen by attackers to gain profit. The method of earning profit by using the infected system's resources is similar to that of CoinMiner. This type of malware has been continuously around for a while. Cisco Talos once made an analysis on proxyware in 2021.[1]

### 1. Case using Adware

The post will first discuss malware distributed through adware. AhnLab's ASD log shows that the proxyware is installed through adware such as Neoreklami.



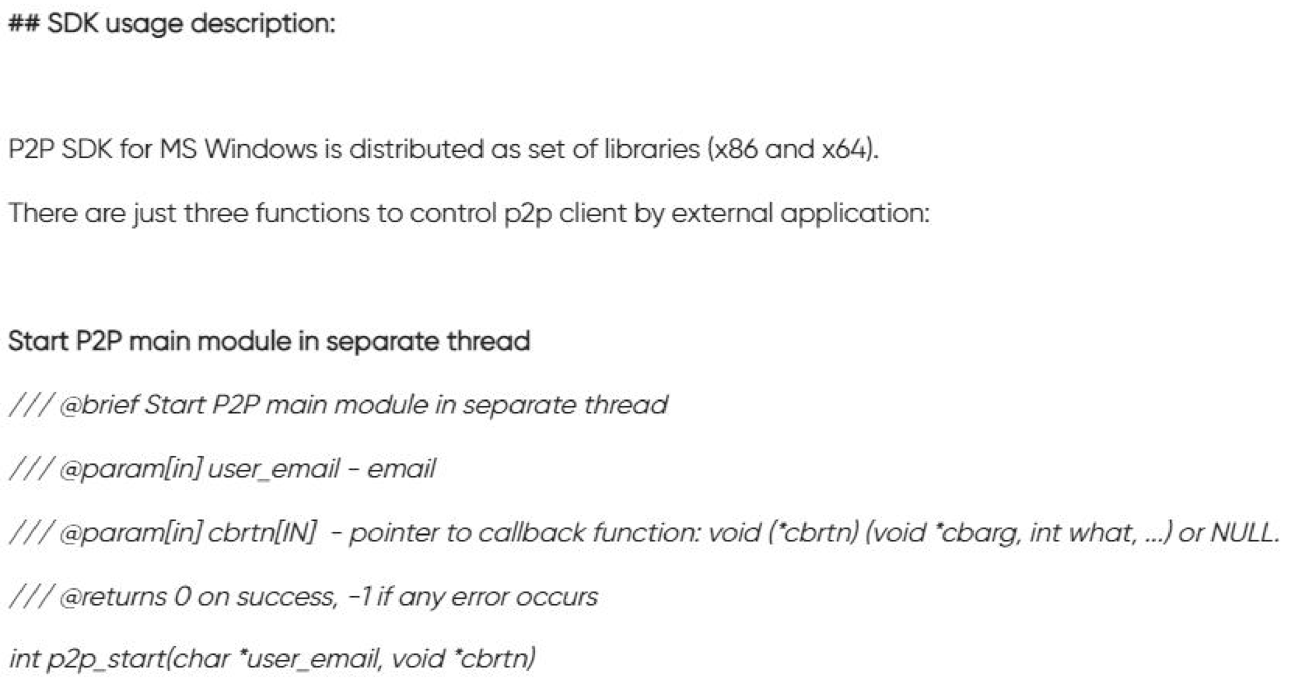
| | | | | |
|---|---|---|---|---|
| 🟩 rundll32.exe | 🟥 zcyukNIS.dll | Creates executable file | Creates executable file in Windows path | Target<br>🟥 gBC43.tmp.exe |
| 🟩 rundll32.exe | 🟥 sycbygx.dll | Creates executable file | Creates executable file in Windows path | Target<br>🟥 gBC43.tmp.exe |

Figure 2. Proxyware installed through Neoreklami

It is a dropper-type malware that installs proxyware of Peer2Profit and IPROYAL on the system as a user account without the user's permission.

…. **1.1. PEER2PROFIT**

As for Peer2Profit, the malware creates Peer2Profit SDK DLL saved in the data section in the same path. According to the manual shown below, Peer2Profit SDK can use the p2p_is_active() function to check if a proxy client is running or not. It can also start a proxy with the p2p_start() function.



## SDK usage description:

P2P SDK for MS Windows is distributed as set of libraries (x86 and x64).

There are just three functions to control p2p client by external application:

Start P2P main module in separate thread

*/// @brief Start P2P main module in separate thread*

*/// @param[in] user_email - email*

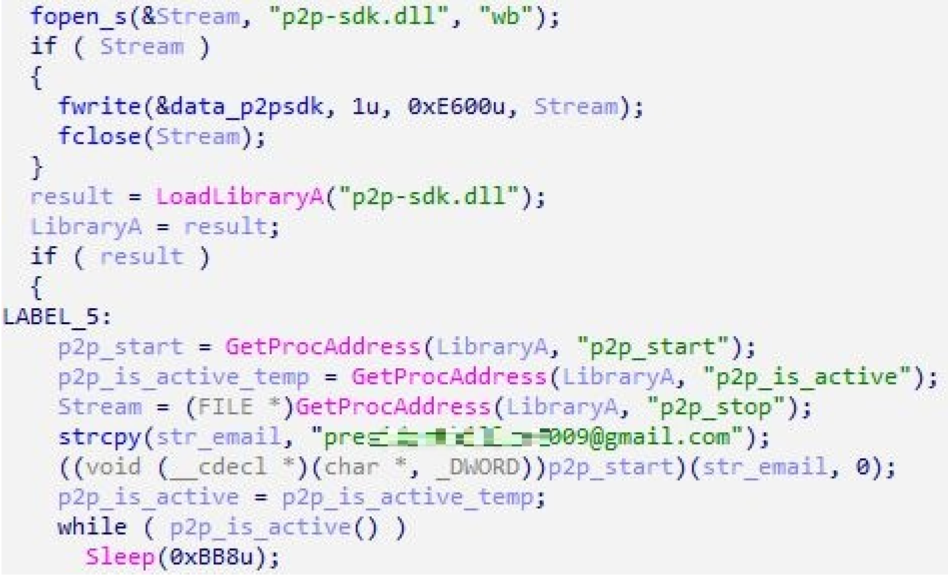
*/// @param[in] cbrtn[IN]  - pointer to callback function: void (*cbrtn) (void *cbarg, int what, ...) or NULL.*

*/// @returns 0 on success, -1 if any error occurs*

*int p2p_start(char *user_email, void *cbrtn)*

Figure 3. Peer2Profit SDK manual

The malware follows the instruction shown in the manual: it loads the created SDK DLL and gives the attacker’s email address as an argument to execute the p2p_start() function. The malware can operate in the infected system without the user realizing it to steal the Internet bandwidth as a result. The attacker can gain profit through the designated email address (the attacker’s account).

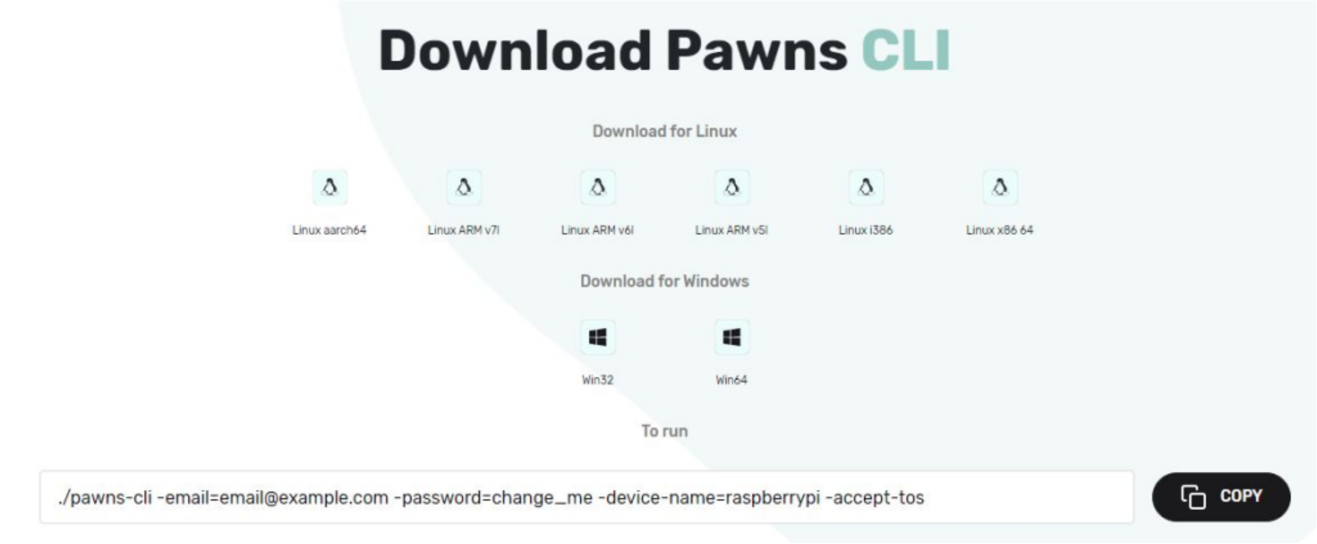


```
  fopen_s(&Stream, "p2p-sdk.dll", "wb");
  if ( Stream )
  {
    fwrite(&data_p2psdk, 1u, 0xE600u, Stream);
    fclose(Stream);
  }
  result = LoadLibraryA("p2p-sdk.dll");
  LibraryA = result;
  if ( result )
  {
LABEL_5:
    p2p_start = GetProcAddress(LibraryA, "p2p_start");
    p2p_is_active_temp = GetProcAddress(LibraryA, "p2p_is_active");
    Stream = (FILE *)GetProcAddress(LibraryA, "p2p_stop");
    strcpy(str_email, "pre[redacted]009@gmail.com");
    ((void (__cdecl *)(char *, _DWORD))p2p_start)(str_email, 0);
    p2p_is_active = p2p_is_active_temp;
    while ( p2p_is_active() )
      Sleep(0xBB8u);
```

Figure 4. Creating and running Peer2Profit SDK

…. **1.2. IPROYAL PAWNS**

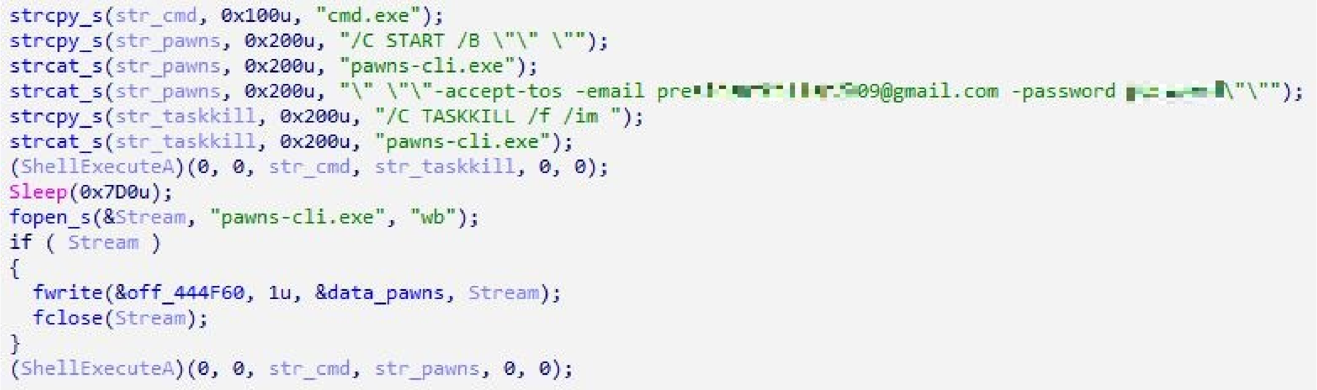
The dropper malware also installs IPRoyal’s Pawns as well. The dropper initially used the CLI exe form of Pawns. IPRoyal programs are usually in GUI forms. Yet as it supports the CLI form as well, it can be executed with command lines and installed without users recognizing the process.



```
./pawns-cli -email=email@example.com -password=change_me -device-name=raspberrypi -accept-tos
```

Figure 5. IPRoyal Pawns CLI programs

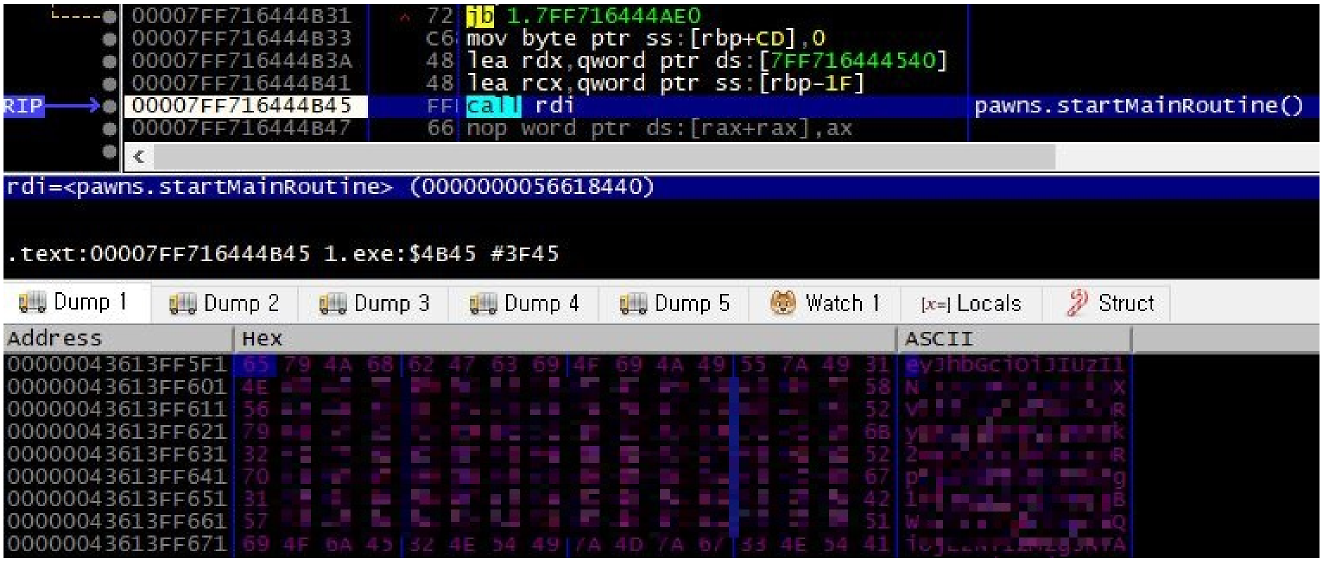
The file forcibly terminates Pawns in CLI form if it is currently running. It then creates Pawns in the same path, similar to Peer2Profit SDK. It gives the attacker’s email address and password as arguments to run Pawns, gaining profit from the infected system.



```
strcpy_s(str_cmd, 0x100u, "cmd.exe");
strcpy_s(str_pawns, 0x200u, "/C START /B \"\" \"");
strcat_s(str_pawns, 0x200u, "pawns-cli.exe");
strcat_s(str_pawns, 0x200u, "\" \"\"-accept-tos -email pre[redacted]09@gmail.com -password [redacted]\"\"");
strcpy_s(str_taskkill, 0x200u, "/C TASKKILL /f /im ");
strcat_s(str_taskkill, 0x200u, "pawns-cli.exe");
(ShellExecuteA)(0, 0, str_cmd, str_taskkill, 0, 0);
Sleep(0x7D0u);
fopen_s(&Stream, "pawns-cli.exe", "wb");
if ( Stream )
{
  fwrite(&off_444F60, 1u, &data_pawns, Stream);
  fclose(Stream);
}
(ShellExecuteA)(0, 0, str_cmd, str_pawns, 0, 0);
```

Figure 6. Installation routine for IPRoyal Pawns

Recent cases use Pawns in DLL form instead. The dropper creates pawns.dll in the same path and loads it. It then calls two functions Initialize() and startMainRoutine().

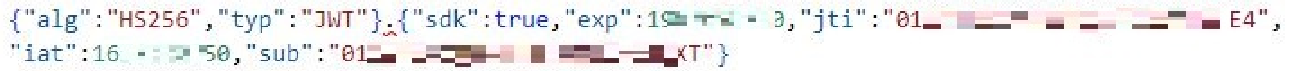


```
      00007FF716444B31    72 jb 1.7FF716444AE0
      00007FF716444B33    C6 mov byte ptr ss:[rbp+CD],0
      00007FF716444B3A    48 lea rdx,qword ptr ds:[7FF716444540]
      00007FF716444B41    48 lea rcx,qword ptr ss:[rbp-1F]
RIP → 00007FF716444B45    FF call rdi                              pawns.startMainRoutine()
      00007FF716444B47    66 nop word ptr ds:[rax+rax],ax

rdi=<pawns.startMainRoutine> (0000000056618440)

.text:00007FF716444B45 1.exe:$4B45 #3F45
```

```
Address          Hex                                               ASCII
00000043613FF5F1 65 79 4A 68 62 47 63 69 4F 69 4A 49 55 7A 49 31  eyJhbGciOiJIUzI1
00000043613FF601 4E [redacted]                                 58  N[redacted]X
00000043613FF611 56 [redacted]                                 52  V[redacted]R
00000043613FF621 79 [redacted]                                 6B  y[redacted]k
00000043613FF631 32 [redacted]                                 52  2[redacted]R
00000043613FF641 70 [redacted]                                 67  p[redacted]g
00000043613FF651 31 [redacted]                                 42  1[redacted]B
00000043613FF661 57 [redacted]                                 51  W[redacted]Q
00000043613FF671 69 [redacted]
```

Figure 7. Execution routine for DLL form of Pawns

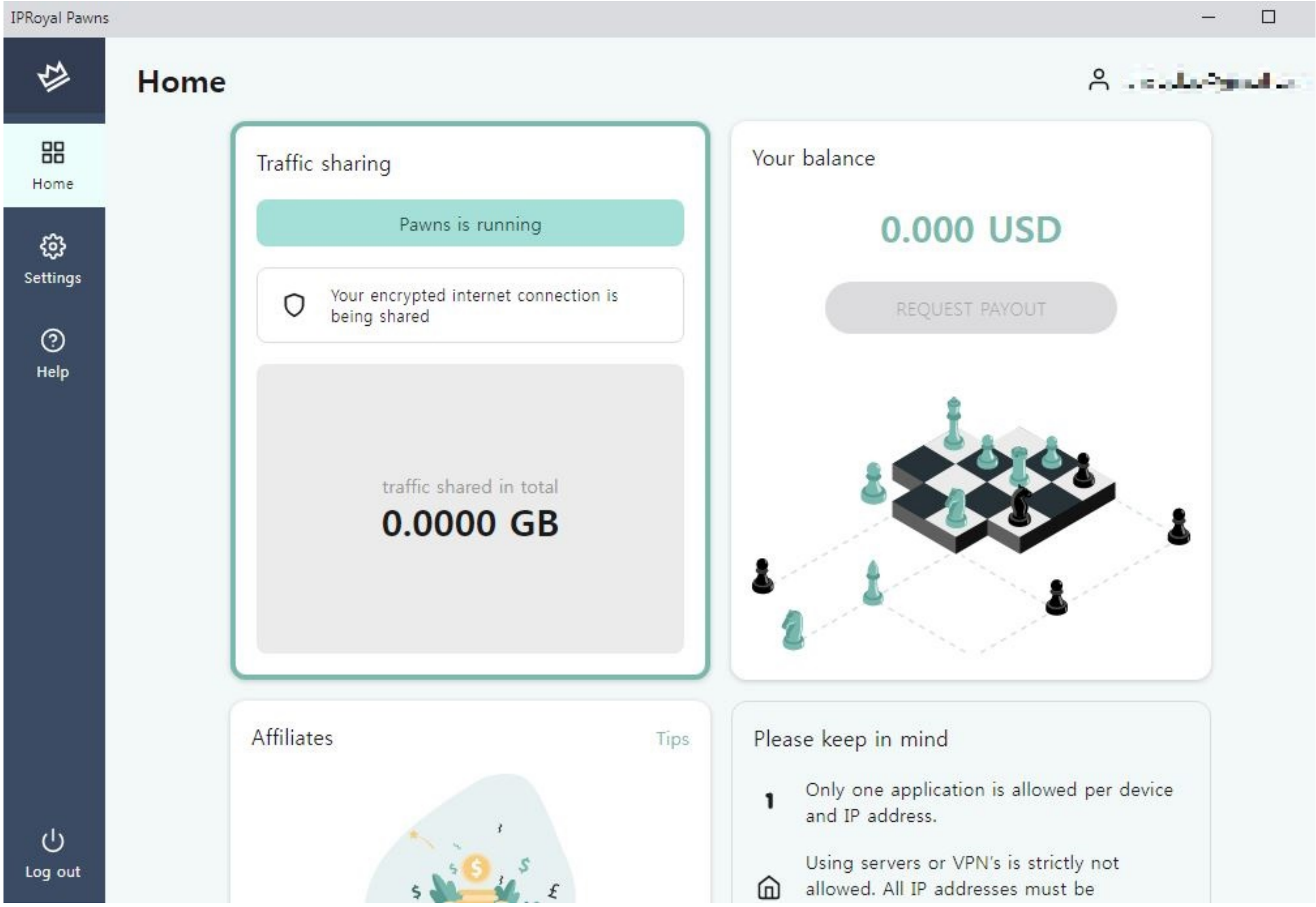
Unlike Pawns in CLI form that received the attacker's email address and password directly through command line arguments, Pawns in DLL form receives encoded data as an argument. The string is Base64-encoded. Decoding it will show the following json settings data.



{"alg":"HS256","typ":"JWT"}.{"sdk":true,"exp":1[redacted]0,"jti":"01[redacted]E4",
"iat":16[redacted]50,"sub":"01[redacted]XT"}

Figure 8. Base64-decoded argument data

The data is presumably used for verification. In fact, the GUI form IPRoyal uses a similar method. When logging in to IPRoyal, the GUI client loads libpawns.dll file (libpawns32.dll in the x86 environment) located in %PROGRAMFILES%\IPRoyal Pawns\resources\packages\main\resources\libpawns inside the installation path and gives the settings data encoded in the same method as an argument to call the startMainRoutine() function.



Your encrypted internet connection is being shared

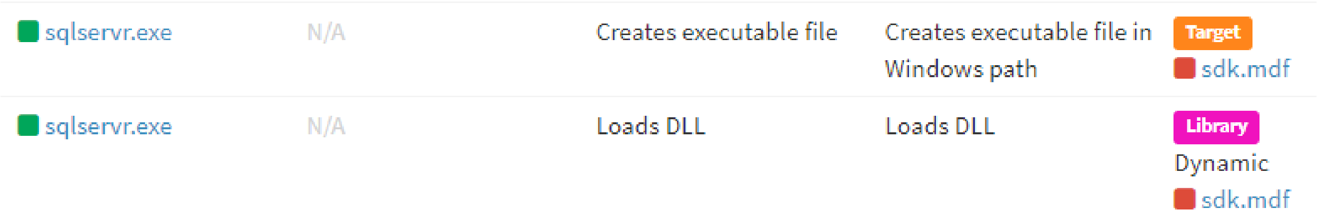
1 Only one application is allowed per device and IP address.

Using servers or VPN's is strictly not allowed. All IP addresses must be

Figure 9. GUI form of IPRoyal client

### 2. Cases of attacks targeting vulnerable MS-SQL servers

Peer2Profit is used by other attackers as well. The Figure 10 shows a log of Peer2Profit SDK being installed on a vulnerable MS-SQL server. The system also has infection logs of various malware strains distributed through the dictionary attack such as CoinMiner and backdoor. It is likely that the malware installing proxyware was distributed through the dictionary attack as the system had vulnerable account credentials.



| | | | | |
|---|---|---|---|---|
| 🟩 sqlservr.exe | N/A | Creates executable file | Creates executable file in Windows path | Target<br>🟥 sdk.mdf |
| 🟩 sqlservr.exe | N/A | Loads DLL | Loads DLL | Library<br>Dynamic<br>🟥 sdk.mdf |

Figure 10. Peer2Profit SDK installed through a vulnerable MS-SQL process

The “sdk.mdf” file is packed with UPX. It has been installed on multiple vulnerable MS-SQL servers starting from early June in 2022. Due to the nature of Peer2Profit, the file is a DLL and sends the attacker’s email address as an argument for the export function: the file alone cannot reveal additional information such as the attacker’s email address.

The proxyware dropper malware that is recently being discovered is similar to CoinMiner in that it gains profit by exploiting the infected system's resources. The malware strains are distributed through adware or installed on vulnerable MS-SQL servers. Users should refrain from installing programs from unknown sources. If their systems are installed with database servers, they should manage access control policies and account credentials settings appropriately. Also, V3 should be updated to the latest version so that malware infection can be prevented.

**[File Detection]**
– Dropper/Win.Proxyware.C5173477 (2022.07.18.03)
– Dropper/Win.Proxyware.C5173478 (2022.07.18.02)
– Dropper/Win.Proxyware.C5210584 (2022.07.18.02)
– Unwanted/Win.Peer2Profit.R505332 (2022.07.18.02)
– Unwanted/Win.Pawns.C5211846 (2022.07.21.01)
– Unwanted/Win.Pawns.C5211847 (2022.07.21.01)

**[IOC]**
**MD5**
**Dropper**
– 05ed95d997662ee0ba15f76949955bf0
– dd709b8529802d6489311a27372044aa
– 29cbc8a8cdb0e24f3561fac8ac0c0174

**Peer2Profit SDK**
– b1781c2670a2e0a35a10fb312586beec
– e34d9ec5d43501dc77ee93a4b464d51b

**IPRoyal Pawns**
– 7f8c85351394fd8221fc84d65b0d8c3e
– 3e4bb392494551a89e090fbe1237f057

**Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.**

Categories:Malware Information

Tagged as:Adware, IPRoyal, Peer2Profit, proxy, Proxyware