Distribution of NetSupport RAT Malware Disguised as a Pokemon Game

asec.ahnlab.com/en/45312/

By Sanseo January 6, 2023

NetSupport Manager is a remote control tool that can be installed and used by ordinary or corporate users for the purpose of remotely controlling systems. However, it is being abused by many threat actors because it allows external control over specific systems.

Unlike backdoors and RATs (Remote Access Trojans), which are mostly based on command lines, remote control tools (Remote Administration Tools) place emphasis on user-friendliness, so they offer remote desktops, also known as GUI environments. Even though they may not have been developed with malicious intent, if they are installed on infected systems, they can be used for malicious purposes by threat actors, such as for the installation of additional malware or information extortion.

As most remote control tools are used by countless users unlike other backdoors, it is easy for them to be recognized as normal programs. Thus, they have the advantage of allowing attackers to use remote control tools, which are normal programs, to bypass the detection of security software, while simultaneously enabling domination over the infected system in a GUI environment.

The following ASEC blog post covers cases where various remote control tools such as AnyDesk, TeamViewer, Ammyy Admin, and Tmate were used in attacks.

The ASEC analysis team recently found that the NetSupport RAT malware is being distributed from a phishing page disguised as one for a Pokemon card game. Additionally, because it was not distributed in a form used for normal purposes but rather in a form designed for the threat actor to control the infected system, this blog will refer to it as “NetSupport RAT.” NetSupport RAT has been consistently used by threat actors and is still in use even in recent days. It’s distributed via spam emails or phishing pages disguised as those for original programs.

The following is the phishing page disguised as one for a Pokemon card game, and you can see the “Play on PC” button down below. When the user clicks this button to install the game, instead of the Pokemon card game, NetSupport RAT is downloaded.

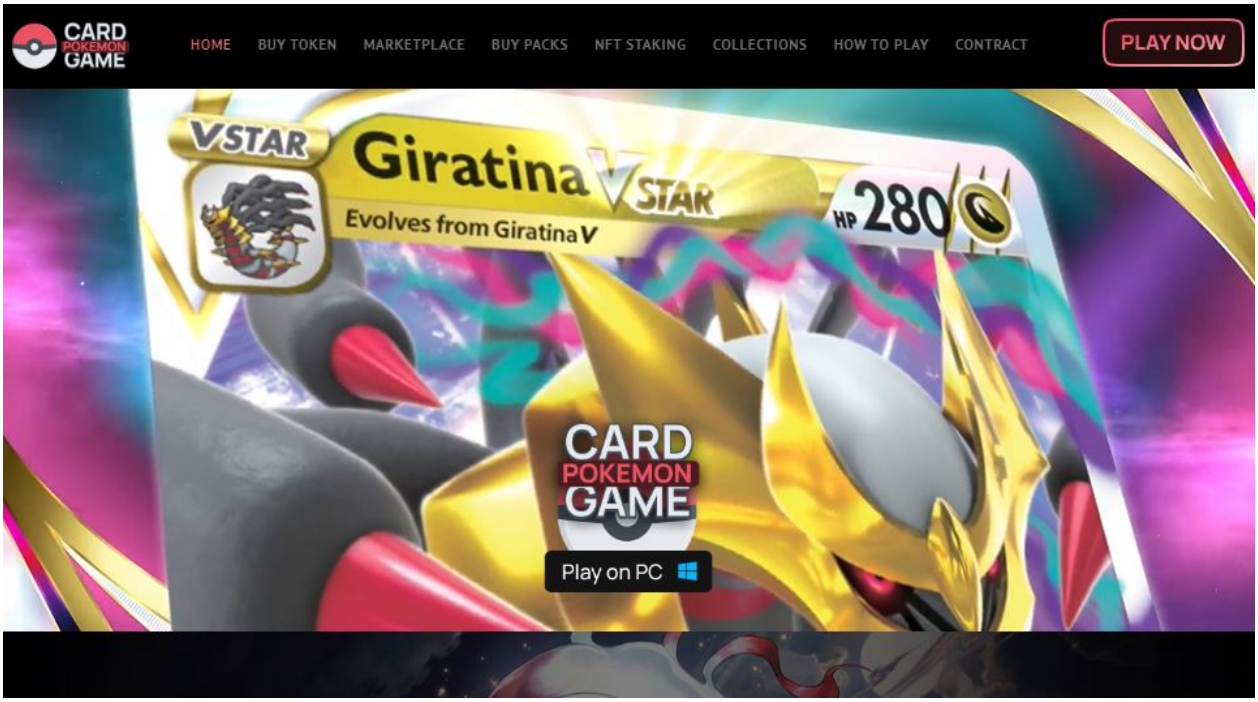

Figure 1. Forged Pokemon card game page

The downloaded file has both a disguised icon and version information, so users are prone to mistaking this for a game program and running it.

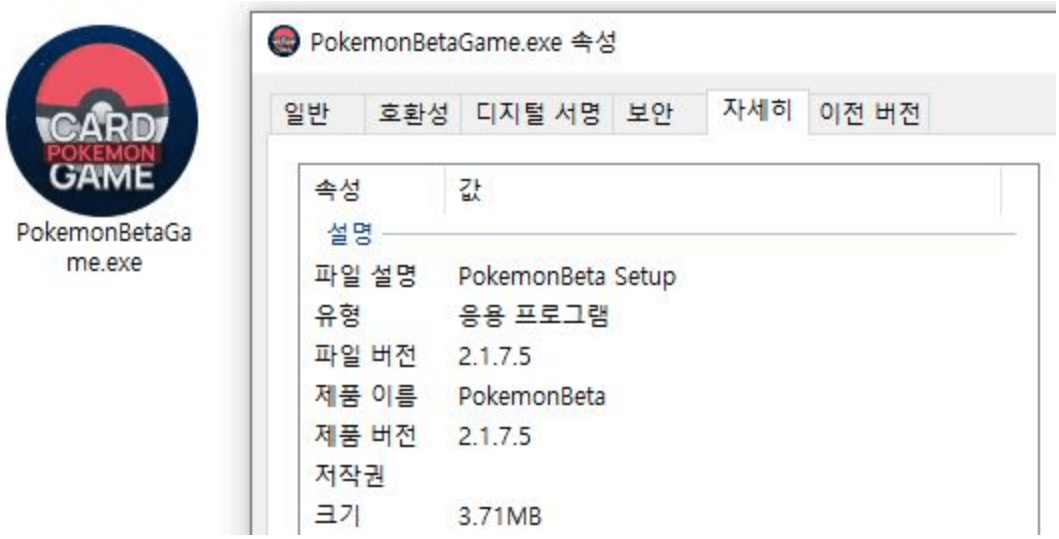

Figure 2. Malware disguised as a Pokemon card game

The malware is an installer malware developed with InnoSetup. When executed, it creates a folder in the %APPDATA% path and creates hidden NetSupport RAT-related files before executing them. It also creates a shortcut in the Startup folder, allowing the malware to be run even after a reboot. client32.exe, the ultimately executed file in the process tree below, is the NetSupport Manager client.

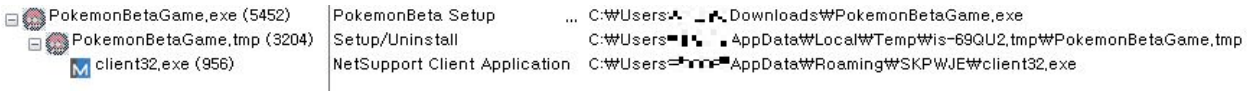

Figure 3. Process tree of NetSupport RAT

While it could be said that the installed NetSupport-related programs themselves are normal programs, we can see that the threat actor's C&C server address is included in the "client32.ini" configuration file, as shown below. When NetSupport is executed, it reads this configuration file, access and establishes a connection to the threat actor's NetSupport server, and then allows the operator to control the infected system.

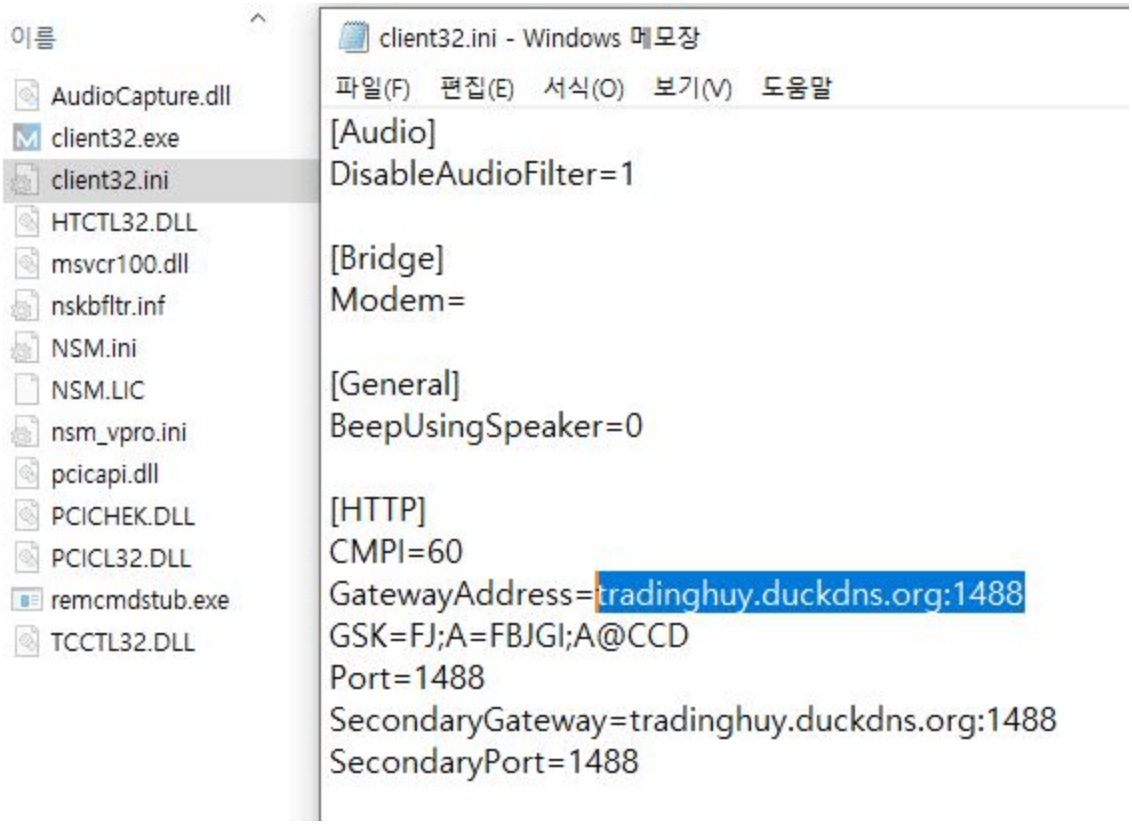

Figure 4. Installed NetSupport files and the configuration file

```
POST http://65.108.67.37/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:    22
Host: 65.108.67.37
Connection: Keep-Alive

CMD=POLL
INFO=1
ACK=1
HTTP/1.1 200 OK
Server: NetSupport Gateway/1.7 (Windows NT)
Content-Type: application/x-www-form-urlencoded
Content-Length:    61
Connection: Keep-Alive

CMD=ENCD
ES=1
DATA=.g+$.[redacted]
POST http://65.108.67.37/fakeurl.htm HTTP/1.1
User-Agent: NetSupport Manager/1.3
Content-Type: application/x-www-form-urlencoded
Content-Length:   258
Host: 65.108.67.37
Connection: Keep-Alive
```

Figure 5. Packet data of NetSupport RAT

While relevant files were being examined with our ASD (AhnLab Smart Defense) infrastructure and VirusTotal, we identified a different phishing page with the same format as a fake Pokemon card game page. Each phishing page has been distributing multiple NetSupport RAT Dropper malware since around December 2022. Moreover, while the files themselves are all different, they all include the same C&C server address in the “client32.ini” configuration file.

Among the ones uploaded to VirusTotal, there were malware samples with icons disguised as Visual Studio, and just like the original program, NetSupport RAT is installed in the path %APPDATA%\Developer\. From this, we can infer that the threat actor is using normal programs other than the Pokemon game to distribute malware.

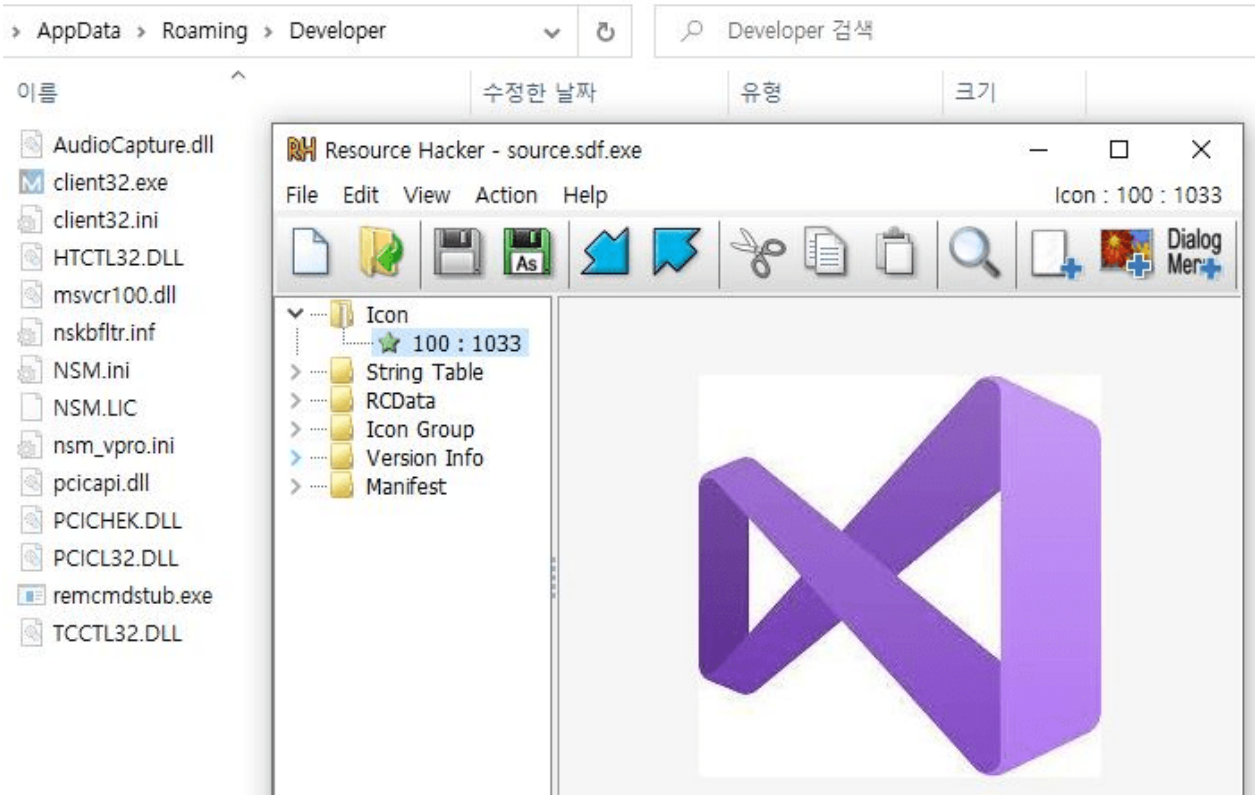

Figure 6. NetSupport RAT dropper disguised as Visual Studio

There was also a type that creates the file “csvs.exe” disguised as a normal Windows program, svchost.exe, instead of installing the NetSupport client, “client32.exe” in the installation directory. While the icon and file size are different, the internal routine or PDB information shows that this is a “client32.exe” file modified by the threat actor to bypass detection.

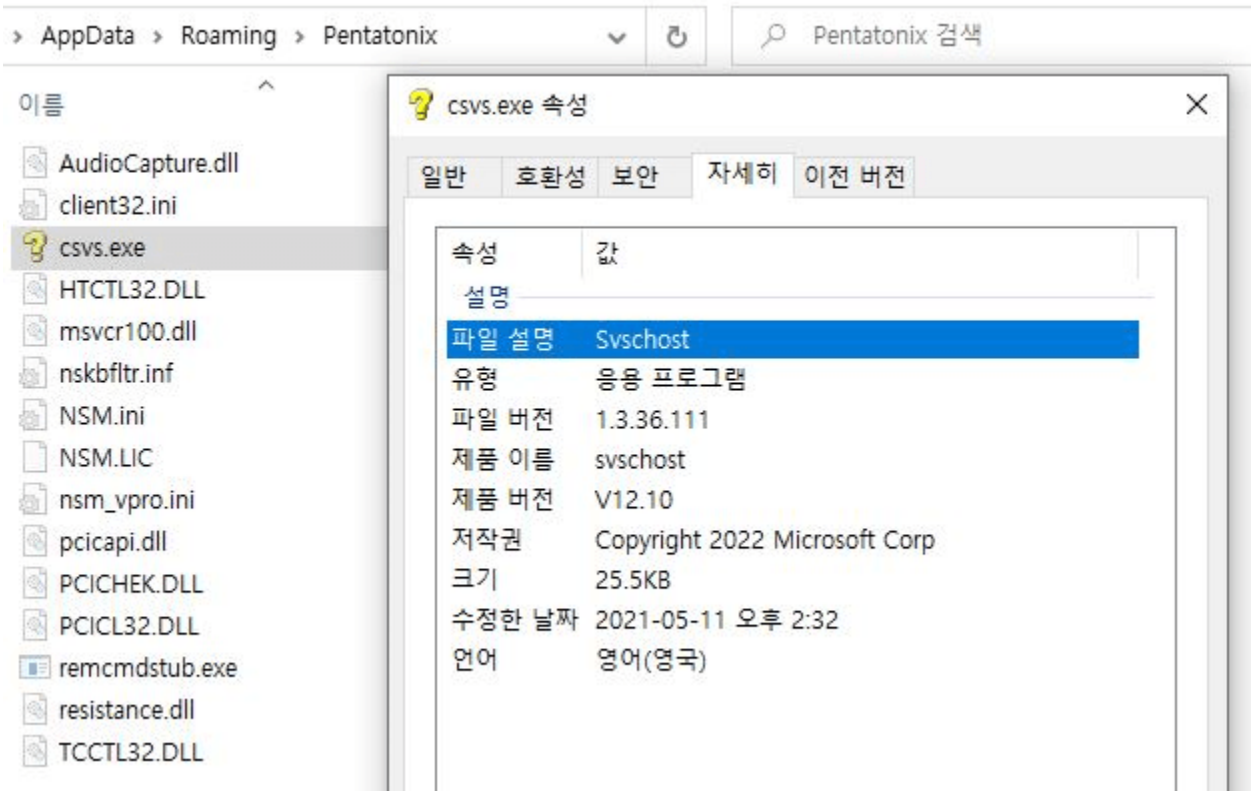

Figure 7. client32.exe seen to have been modified by the threat actor

NetSupport RAT is being used by various threat actors. Major cases show that they are recently being distributed through spam emails disguised as those for invoices, shipment documents, and purchase orders.**[1]** Additionally, in the second half of the year, there was a case where users were led to install the malware themselves from a phishing page disguised as an update page for a software called SocGholish.**[2]**

When NetSupport RAT is installed, the threat actor can gain control over the infected system. Features supported by NetSupport by default include not only remote screen control but also system control features such as screen capture, clipboard sharing, collecting web history information, file management, and command execution. This means that the threat actor can perform various malicious behaviors such as extorting user credentials and installing additional malware.

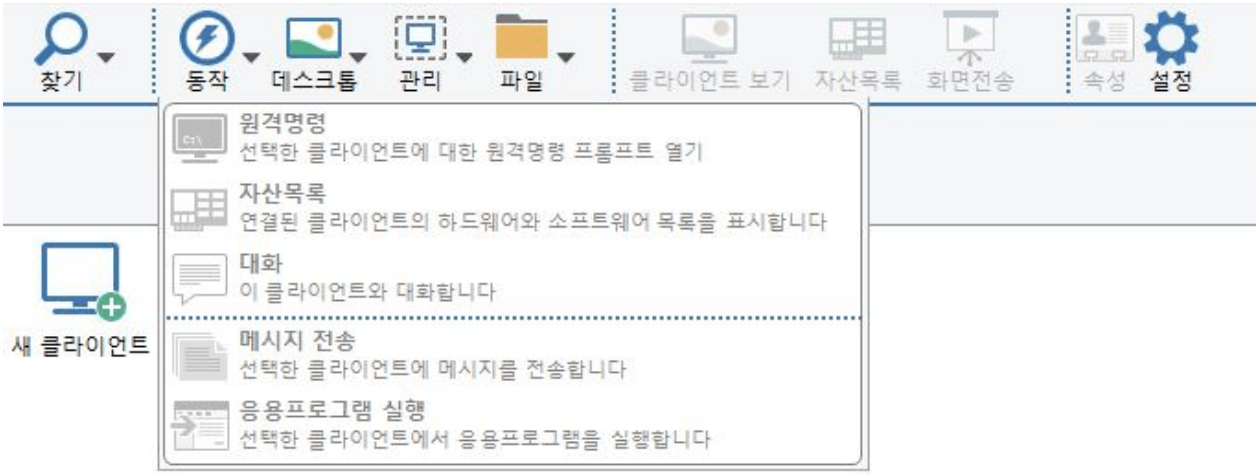

Figure 8. Features supported by NetSupport

Recently, threat actors have been abusing remote control tools used by various users such as NetSupport in their attacks. When infected with such remote control malware, the system is overtaken by the threat actor and becomes subject to damages such as information extortion and additional malware installation.

When installing externally sourced software, users are advised to purchase or download them from their official websites and refrain from opening attachments in suspicious emails. Users should also apply the latest patch to programs such as their OS and internet browsers and update V3 to the latest version to prevent malware infection in advance.

File Detection
– Dropper/Win.NetSupport.C5345365 (2022.12.30.01)
– Malware/Win.Generic.C5339867 (2022.12.23.03)
– Malware/Win.Generic.C5335414 (2022.12.17.01)
– Malware/Win.Generic.C5333592 (2022.12.15.01)
– Malware/Win.Malware-gen.C5331507 (2022.12.13.02)
– Trojan/Win.NetSupport.C5345361 (2022.12.30.01)
– Backdoor/Text.NetSupport (2022.12.30.02)

IOC
MD5
– 097051905db43d636c3f71f3b2037e02 : NetSupport RAT dropper (PokemonBetaGame.exe)
– 1dc87bfb3613d605c9914d11a67e2c94 : NetSupport RAT dropper disguised as a Pokemon card game
– 5e6b966167c7fd13433929e774f038ee : NetSupport RAT dropper disguised as a Pokemon card game
– a9dba73b0cf1c26008fc9203684c6c22 : NetSupport RAT dropper disguised as a Pokemon card game
– adbe1069f82a076c48f79386812c1409 : NetSupport RAT dropper disguised as a Pokemon

card game
– fcdc884dd581701367b284ad302efe4d : NetSupport RAT dropper disguised as a Pokemon card game
– ed68e69534ebdf6c8aa1398da032c147 : NetSupport RAT dropper disguised as Visual Studio (source.sdf)
– e7792e09b0283b87b9de37b3420f69d5 : NetSupport RAT dropper disguised as a Pokemon card game (creates csvs.exe)
– 7ca97fe166c4d8a23d7d9505d9fcc1c0 : Patched client32.exe (csvs.exe)
– 59048c3248025a7d4c7c643d9cf317a5 : NetSupport configuration file (client32.ini)
– f26b26f6d29a4e584bd85f216b8254b9 : NetSupport configuration file (client32.ini)

C&C
– tradinghuy.duckdns[.]org:1488

Phishing Page
– hxxps://pokemon-go[.]io/
– hxxps://beta-pokemoncards[.]io/

Download
– hxxps://pokemon-go[.]io/PokemonBetaGame.exe
– hxxps://beta-pokemoncards[.]io/PokemonCardGame.exe
– hxxps://beta-pokemoncards[.]io/PokemonBetaCard.exe
– hxxps://beta-pokemoncards[.]io/PokenoGameCard.exe

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

Categories:Malware Information

Tagged as:Game,NetSupport,Pokemon,rat