Distribution of Kimsuky Group's xRAT (Quasar RAT) Confirmed

By ATCP

Published: 2022-01-27 · Archived: 2026-04-05 21:38:32 UTC

On January 26th, 2022, the ASEC analysis team has discovered that the Kimsuky group was using the xRAT (Quasar RAT-based open-source RAT) malware.

- xRAT Github Address: https://github.com/tidusjar/xRAT

According to the logs collected by AhnLab's ASD (AhnLab Smart Defense) infrastructure, the attacker installed a variant of Gold Dragon on the first infected PC on January 24th. The basis for assuming that the obtained file is a variant of Gold Dragon is as follows:

- Injection method is same as the method used by the original Gold Dragon (behavior of process hollowing on iexplore.exe, svchost.exe,etc.)
- Feature of terminating AhnLab product's real-time detection window class (49B46336-BA4D-4905-9824-D282F05F6576)
- Termination of Daum Cleaner (daumcleaner.exe) process

The attacker installed Gold Dragon through the exclusive installer (installer_sk5621.com.co.exe). The installer downloads Gold Dragon compressed in the form of a Gzip file from the attacker's server, decompresses it as "in[random 4 numbers].tmp" in the %temp% path, then executes it via rundll32.exe.

The installed Gold Dragon has 4 export functions.

- Perform
- Process
- Start
- Work

The installer first executes Gold Dragon by giving the “Start” argument. Once the “Start” export function is executed, Gold Dragon copies itself to a certain path and registers the copied DLL to the autorun registry key. The “Perform” export function is given for DLL execution argument.

Figure 1. Path for registry registration and self-copy

It is assumed that the info leaking feature of the variant that was discovered was modularized. The system information acquisition command execution feature that is mainly used by Gold Dragon did not exist in the Gold Dragon variant. This means that additional payloads can be downloaded from the attacker’s server to obtain system information.

- cmd.exe /c ipconfig/all >>”%s” & arp -a >>”%s”
- cmd.exe /c systeminfo >>”%s”
- cmd.exe /c tasklist >>”%s”

The attacker does not obtain information through system processes, but instead additionally installs xRAT (Filename: cp1093.exe) that allows remote control of the system to the infected PC to perform info-stealing features. Once cp1093.exe is executed, it copies a normal powershell process (powershell_ise.exe) to the “C:\ProgramData\”path and executes xRAT via process hollowing technique.

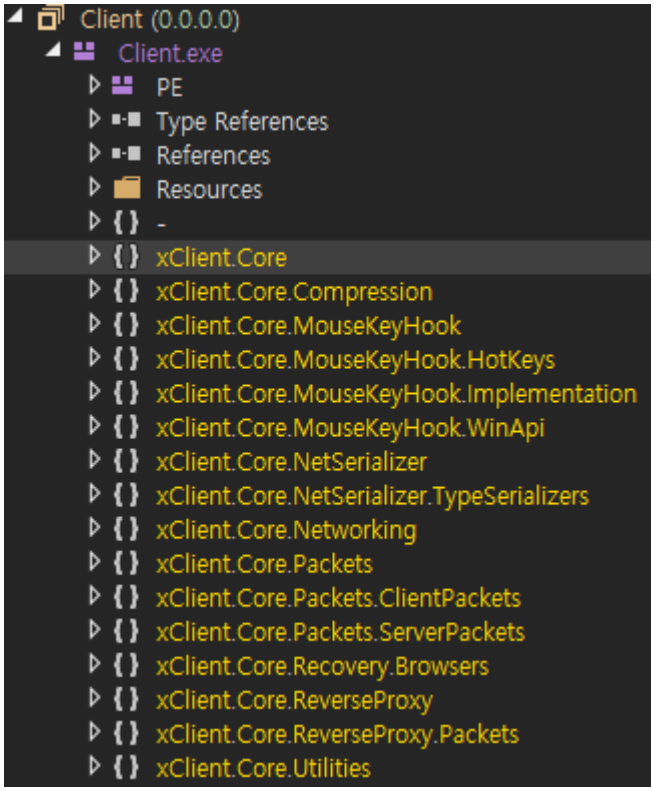

Figure 2. xRAT malware

The attacker was also meticulous enough to also distribute an additional file (UnInstall_kr5829.co.in.exe) along with xRAT to delete the traces of attack existing in the target PC.

```
if ( SHGetSpecialFolderPathW(0, pszPath, 28, 0) )
{
  if ( SHGetSpecialFolderPathW(0, FileName, 28, 0) )
  {
    PathAppendW(FileName, L"Microsoft\\Cmms");
    PathAppendW(FileName, L"pre");
    PathAppendW(FileName, L"unisnt.dat");
    v4 = _wfopen(FileName, L"ab");
    v5 = v4;
    Stream = v4;
    if ( v4 )
    {
      fprintf(v4, "reg deleting...\r\n", v18[0]);
      strcpy(SubKey, "SoftWare\\Microsoft\\Windows\\CurrentVersion\\Run");
      memset(&v31, 0, 214);
      if ( !RegOpenKeyExA(HKEY_CURRENT_USER, SubKey, 0, 0xF003Fu, &phkResult) )
      {
        if ( RegDeleteValueW(phkResult, L"imm32") )
        {
          LastError = GetLastError();
          fprintf(v5, "delete value4 error! (%d)\r\n", LastError);
        }
        else
        {
          fprintf(v5, "delete value 4 ok!\r\n", v18[0]);
        }
        RegCloseKey(phkResult);
      }
      sub_4015E0(v22);
      sub_401BD0();
      v7 = Stream;
      fprintf(Stream, "==========\r\nprocess and file deleting 4 ...\r\n");
      SHGetSpecialFolderPathW(0, pszPath, 28, 0);
      sub_401B70(L"%s\\%s\\%s\\%s", pszPath, L"Microsoft\\Cmms", L"pro", L"imm32.dll");
```

Figure 3. Code related to deletion of traces of infection

AhnLab is constantly monitoring and responding to such APT attacks, and users should refrain from opening attachments from emails from unknown sources and update the security software to the latest version to prevent damage by information leakage.

MD5

070f0390aad17883cc8fad2dc8bc81ba

40b428899db353bb0ea244d95b5b82d9

4ea6cee3ecd9bbd2faf3af73059736df

b841d27fb7fee74142be38cee917eda5

Additional IOCs are available on AhnLab TIP.

URL

http[:]//45[.]77[.]71[.]50[:]8082/

https[:]//sk5621[.]com[.]co/

Additional IOCs are available on AhnLab TIP.

FQDN

kr5829[.]co[.]in

sk5621[.]com[.]co

Additional IOCs are available on AhnLab TIP.
