2024.01.25

Unveiling TeleBoyi: Chinese APT Group Targeting Critical Infrastructure Worldwide

Yi-Chin Chuang, Yu-Tung Chang

TEAMT5

Persistent Cyber Threat Hunters

$whoami

Yi-Chin Chuang

- Threat Intelligence Researcher @ TeamT5
- Focus on APAC APT

Yu-Tung Chang

- Threat Intelligence Researcher @ TeamT5
- Focus on APAC APT
- Speaker of Conferences: Code Blue

Agenda

01 Introduction

02 Dive into TeleBoyi

03 Relation with other APT groups

04 Conclusion

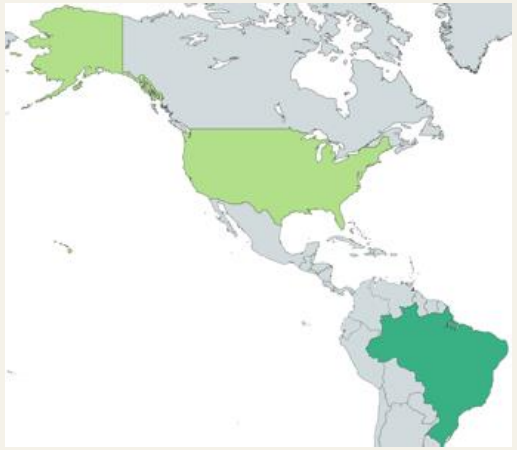
Introduction

TeleBoyi Profile

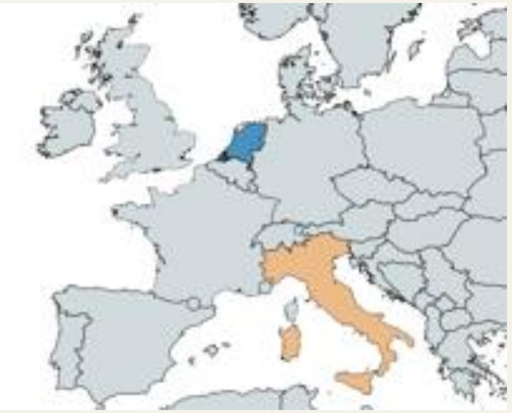
TEAMT5

- 猼訑(Boyi)
- China-nexus APT group
  - Since 2014
- Targeted Country:
  - Worldwide, especially APAC region
- Targeted Industry:
  - Critical Infrastructure, mainly Telecom
- Malware:
  - PlugX, LibreCoin, DoubleShell, TripleZero, …

Target Scope



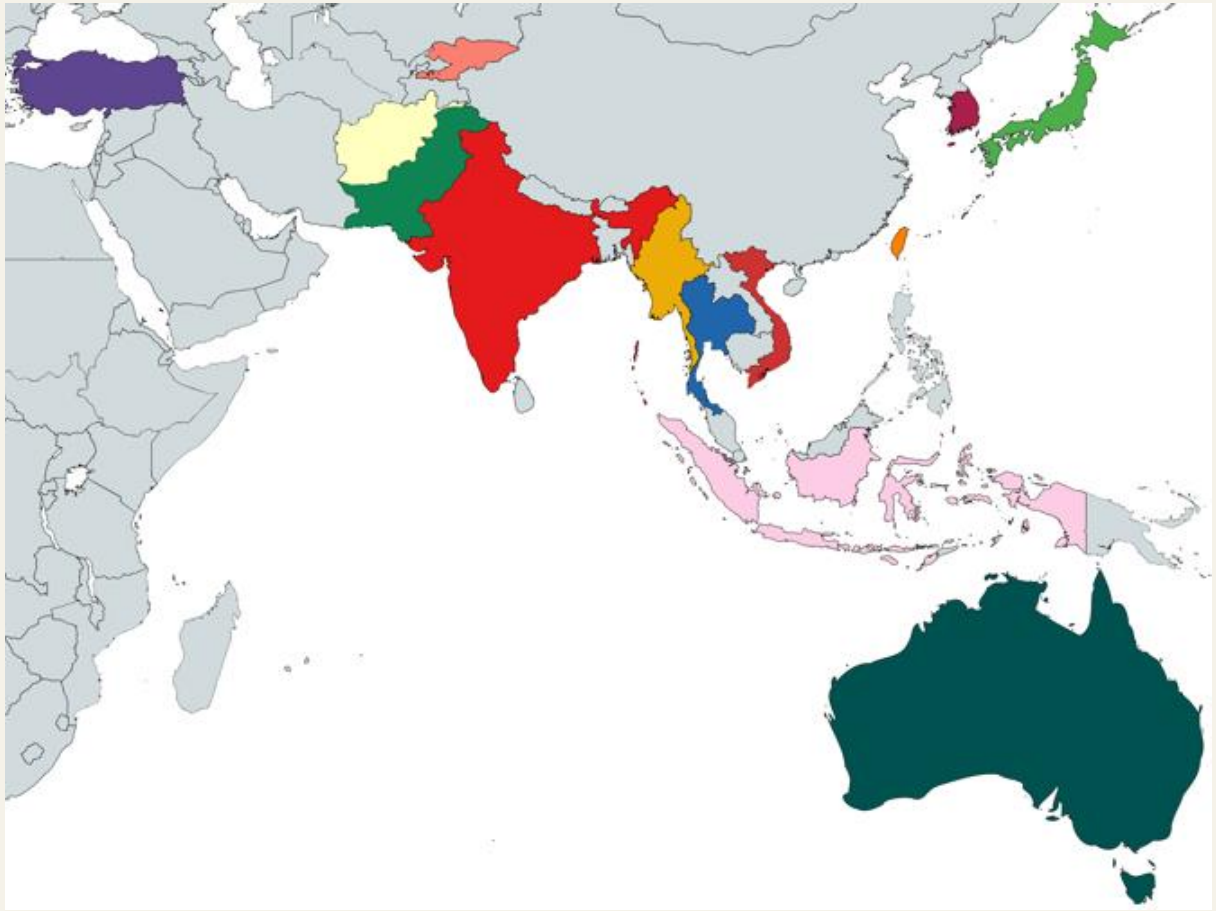
Americas



Europe

TeleBoyi

APAC Region

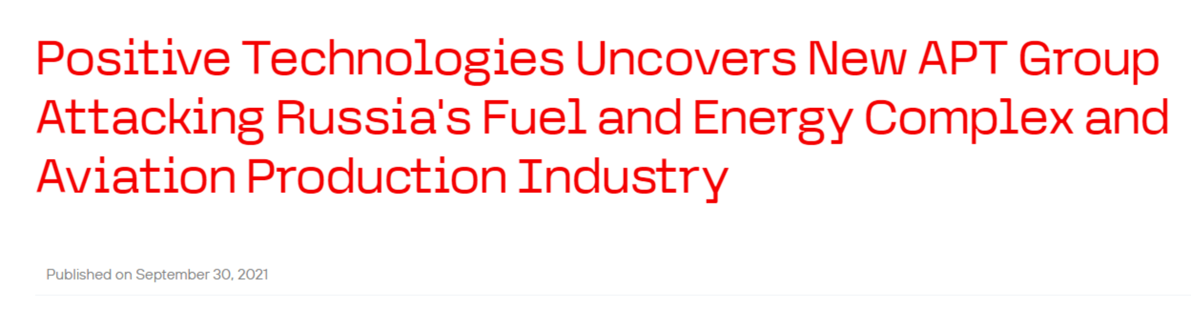


Target Industry

- Telecommunications
- Information Technology
- Critical Manufacturing
- Financial Services
- Government Facilities
- Healthcare
- Energy
- Nuclear

Chinese APT Targeting CI

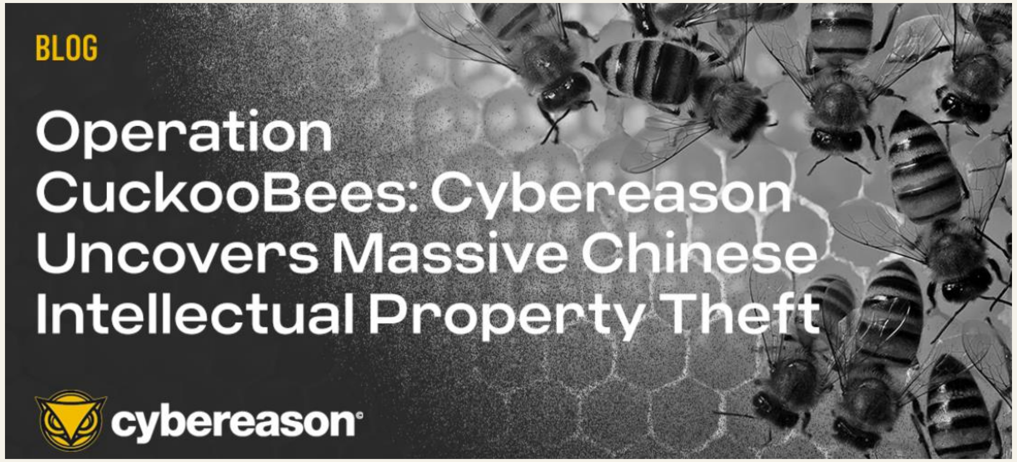
- ChamelGang (CamoFei)
  - Target : Energy and Aviation in Russia
  - other victims : 🇺🇸 🇳🇵 🇹🇼 🇯🇵 …



Positive Technologies Uncovers New APT Group Attacking Russia's Fuel and Energy Complex and Aviation Production Industry

Published on September 30, 2021

- APT41 (Amoeba)
  - Target Industry :
  - Target Scope : North America, Europe, Asia



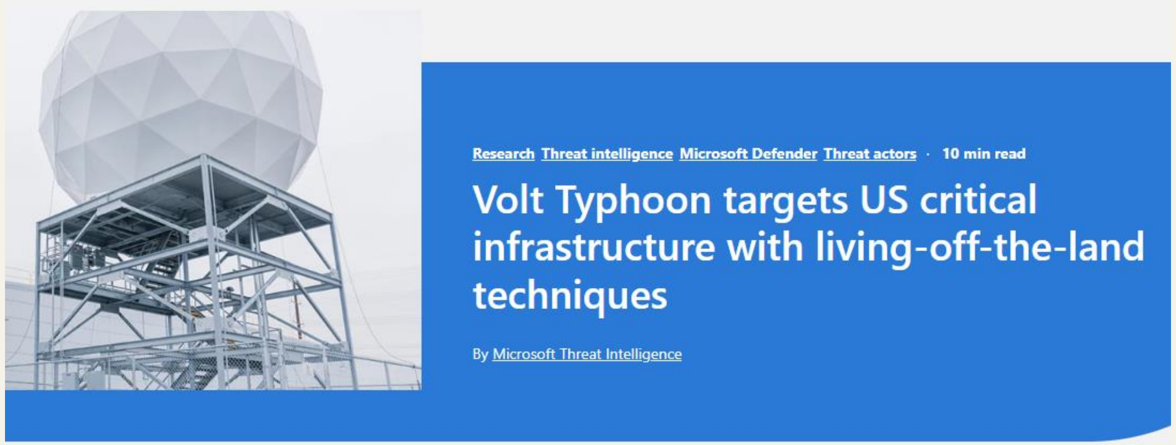
BLOG

Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft

cybereason

Chinese APT Targeting CI (Cont.)

- Volt Typhoon
  - Target Industry : 📡 🦾 🚆 …
  - Target Country : 🇺🇸 🇬🇺



Research Threat intelligence Microsoft Defender Threat actors · 10 min read

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

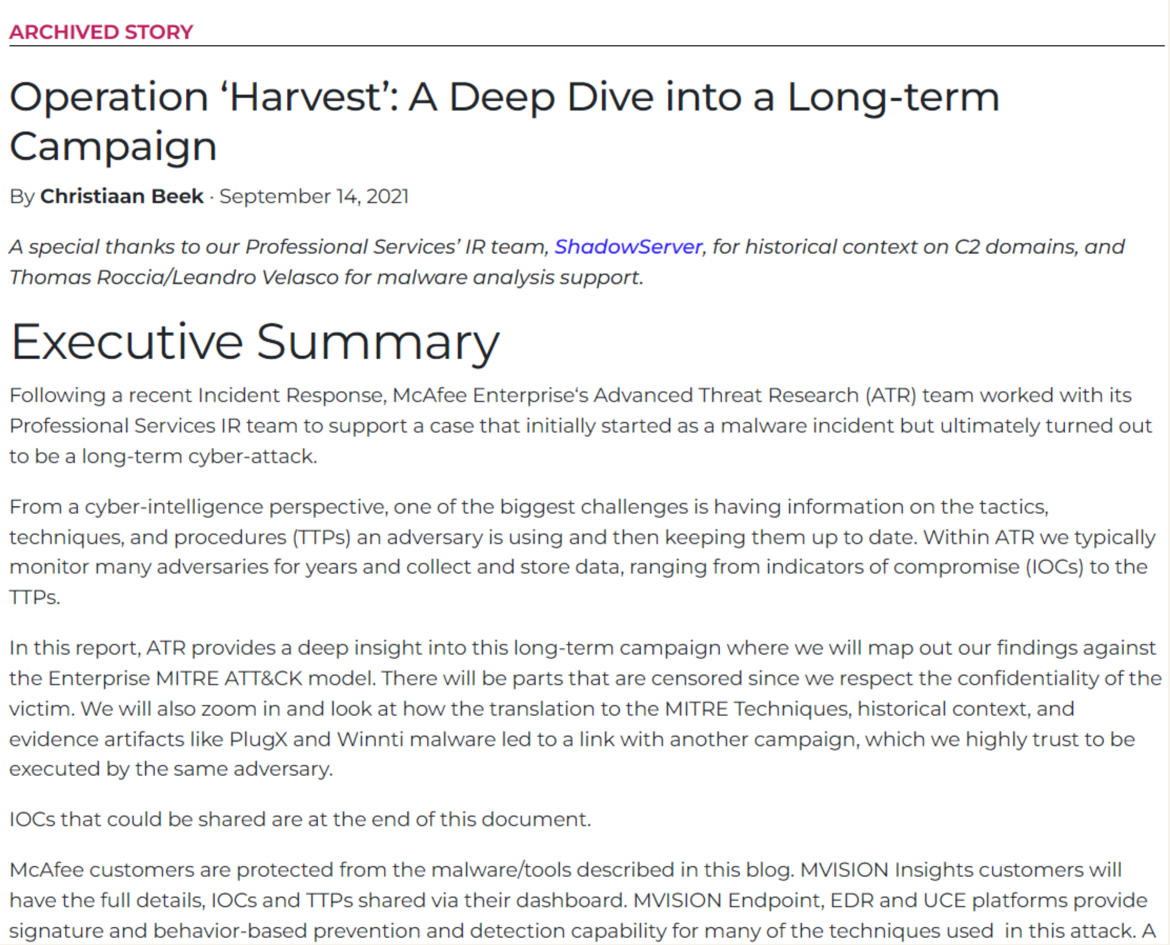
By Microsoft Threat Intelligence

Reason for Chinese APT targeting CI

- Espionage and Information Gathering
  - ChamelGang
- Technology Theft
  - APT41
- Preparation for Future Operations
  - Volt Typhoon

Operation ‘Harvest’

- Reported by McAfee
  - Cyber espionage
  - Observed in 2019/2020
- Backdoor
  - PlugX, Winnti
- C2
  - sery.brushupdata.com
  - center.asmlbigip.com
  - sec.asmlbigip.com



ARCHIVED STORY

Operation ‘Harvest’: A Deep Dive into a Long-term Campaign

By **Christiaan Beek** · September 14, 2021

A special thanks to our Professional Services’ IR team, ShadowServer, for historical context on C2 domains, and Thomas Roccia/Leandro Velasco for malware analysis support.

Executive Summary

Following a recent Incident Response, McAfee Enterprise‘s Advanced Threat Research (ATR) team worked with its Professional Services IR team to support a case that initially started as a malware incident but ultimately turned out to be a long-term cyber-attack.

From a cyber-intelligence perspective, one of the biggest challenges is having information on the tactics, techniques, and procedures (TTPs) an adversary is using and then keeping them up to date. Within ATR we typically monitor many adversaries for years and collect and store data, ranging from indicators of compromise (IOCs) to the TTPs.

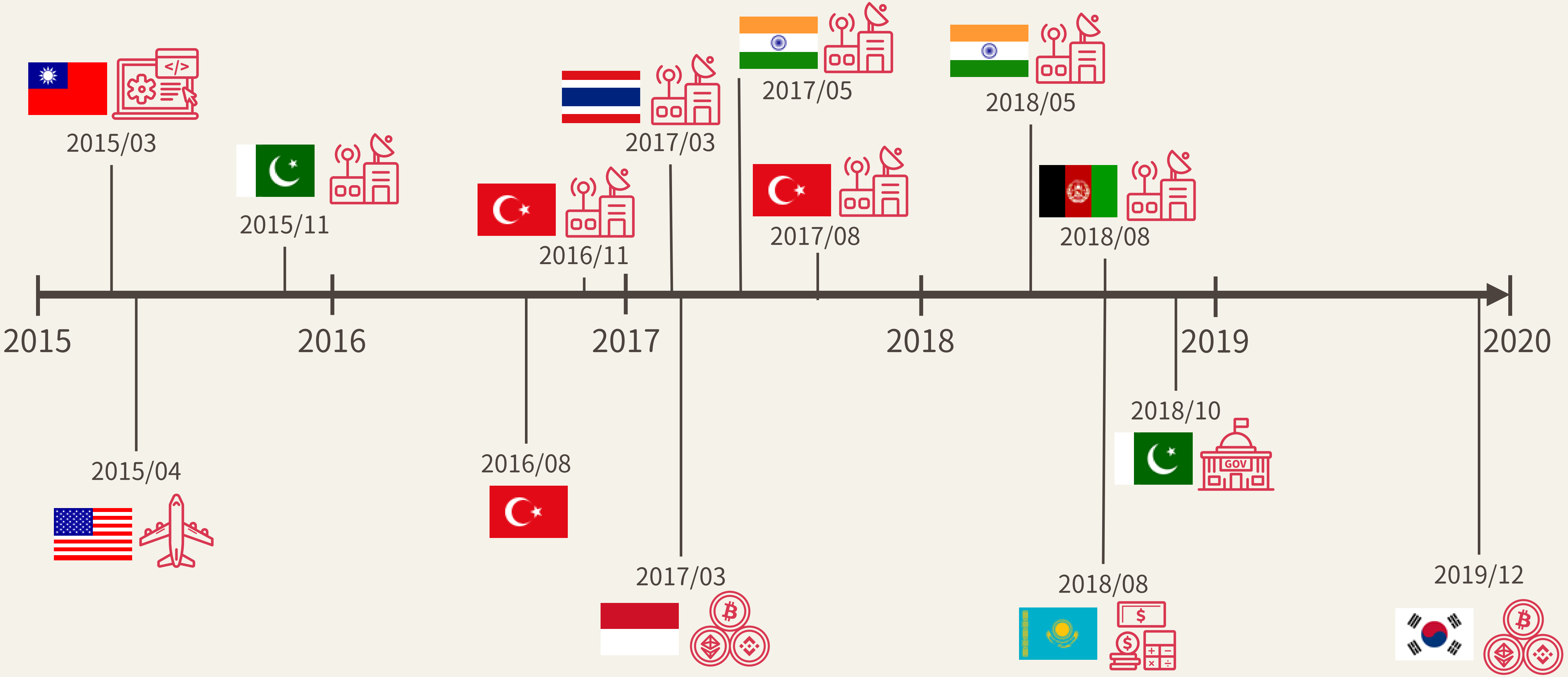
In this report, ATR provides a deep insight into this long-term campaign where we will map out our findings against the Enterprise MITRE ATT&CK model. There will be parts that are censored since we respect the confidentiality of the victim. We will also zoom in and look at how the translation to the MITRE Techniques, historical context, and evidence artifacts like PlugX and Winnti malware led to a link with another campaign, which we highly trust to be executed by the same adversary.

IOCs that could be shared are at the end of this document.

McAfee customers are protected from the malware/tools described in this blog. MVISION Insights customers will have the full details, IOCs and TTPs shared via their dashboard. MVISION Endpoint, EDR and UCE platforms provide signature and behavior-based prevention and detection capability for many of the techniques used in this attack. A

Timeline

TEAMT5



2015/03

2015/04

2015/11

2016/08

2016/11

2017/03

2017/03

2017/05

2017/08

2018/05

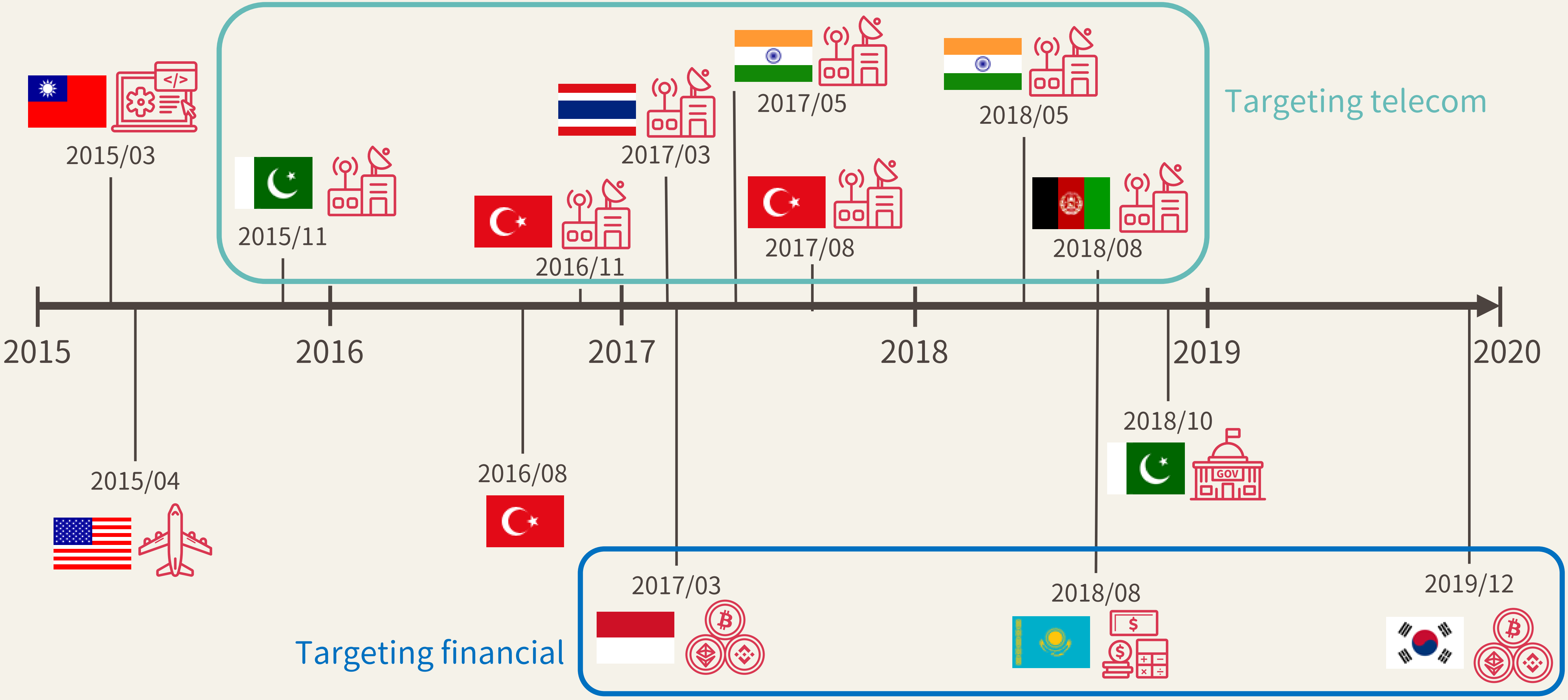
2018/08

2018/08

2018/10

2019/12

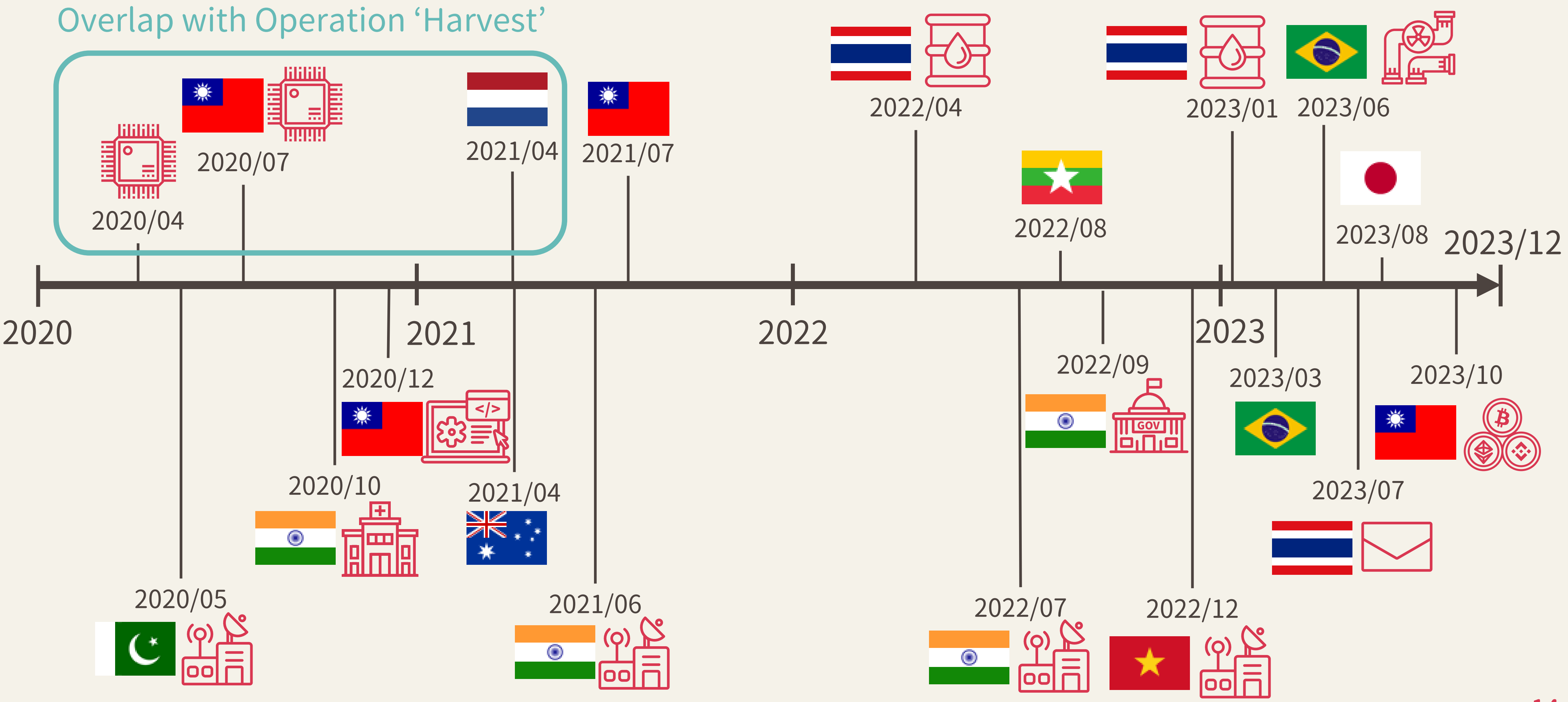
Timeline



2015/03
2015/11
2016/11
2017/03
2017/05
2018/05
2017/08
2018/08
Targeting telecom
2015
2016
2017
2018
2019
2020
2015/04
2016/08
2018/10
GOV
2017/03
2018/08
2019/12
Targeting financial

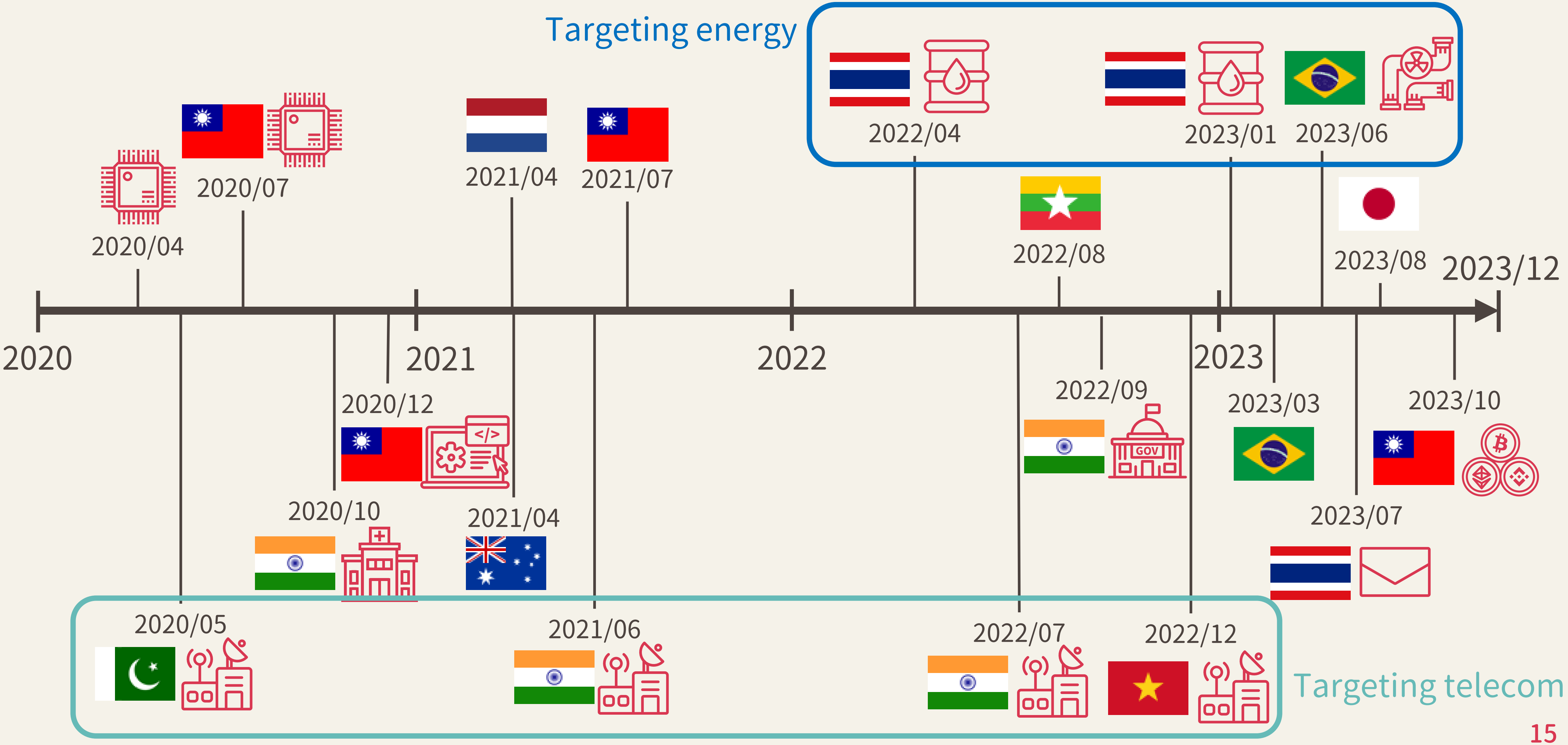
Timeline (Cont.)

TEAMT5



Timeline (Cont.)

TEAMT5



Targeting energy

2020/04

2020/07

2021/04

2021/07

2022/04

2022/08

2023/01

2023/06

2023/08

2023/12

2020

2021

2022

2023

2020/12

2020/10

2021/04

2022/09

2023/03

2023/10

2023/07

2020/05

2021/06

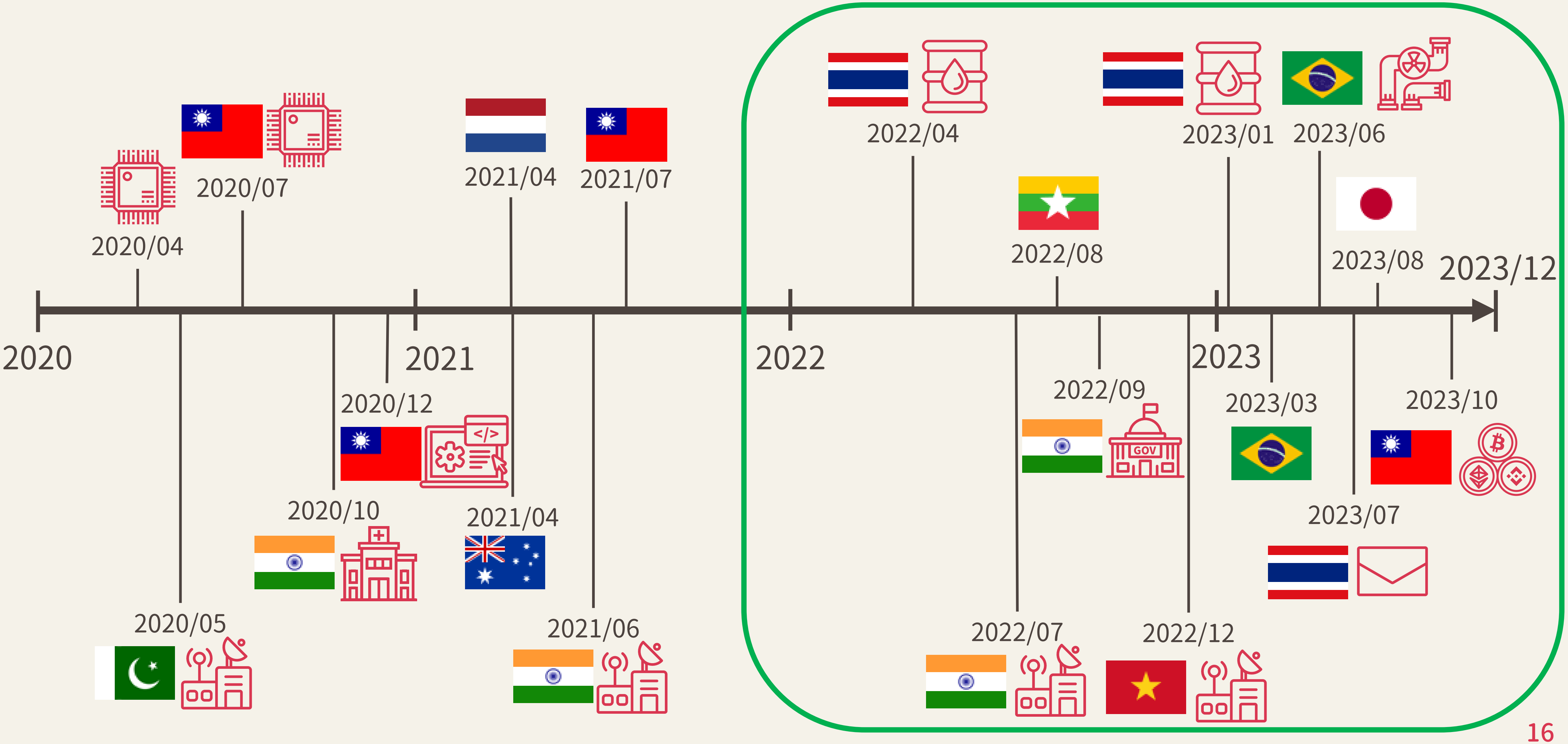
2022/07

2022/12

Targeting telecom

Timeline (Cont.)

TEAMT5



TeleBoyi’s interest in the CI

- Telecommunication
  - Cooperating to develop 5G networks in Turkey.
  - China’s telecom products have been banned in India and Vietnam.
- Semiconductor
  - The semiconductor tech blockade.
- Energy
  - Investment in the energy sector in both Thailand and Brazil.

Dive into TeleBoyi

Malware Delivery

- Fake Applications/Documents
  - Disguise malware as fake application or documents
- Malicious document files
  - Document with macro, HTA
- Exploit Public-Facing Application

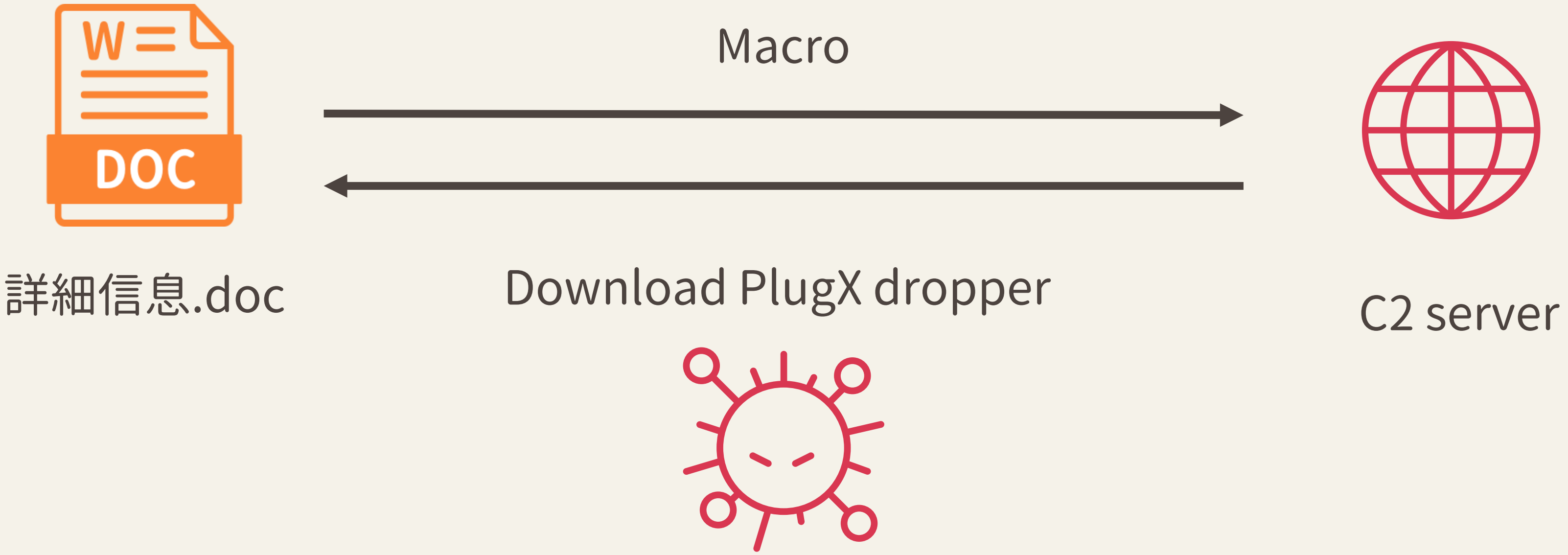
Fake Applications/Documents

- Ofis_personeli_yolsuzluk_raporu.exe
  - Turkish, translate: Office staff corruption report

- 無法注冊網頁出現亂碼.exe
  - Translate: Unable to register, the webpage is garbled

- News about National *** *** University.exe

Malicious Document Files



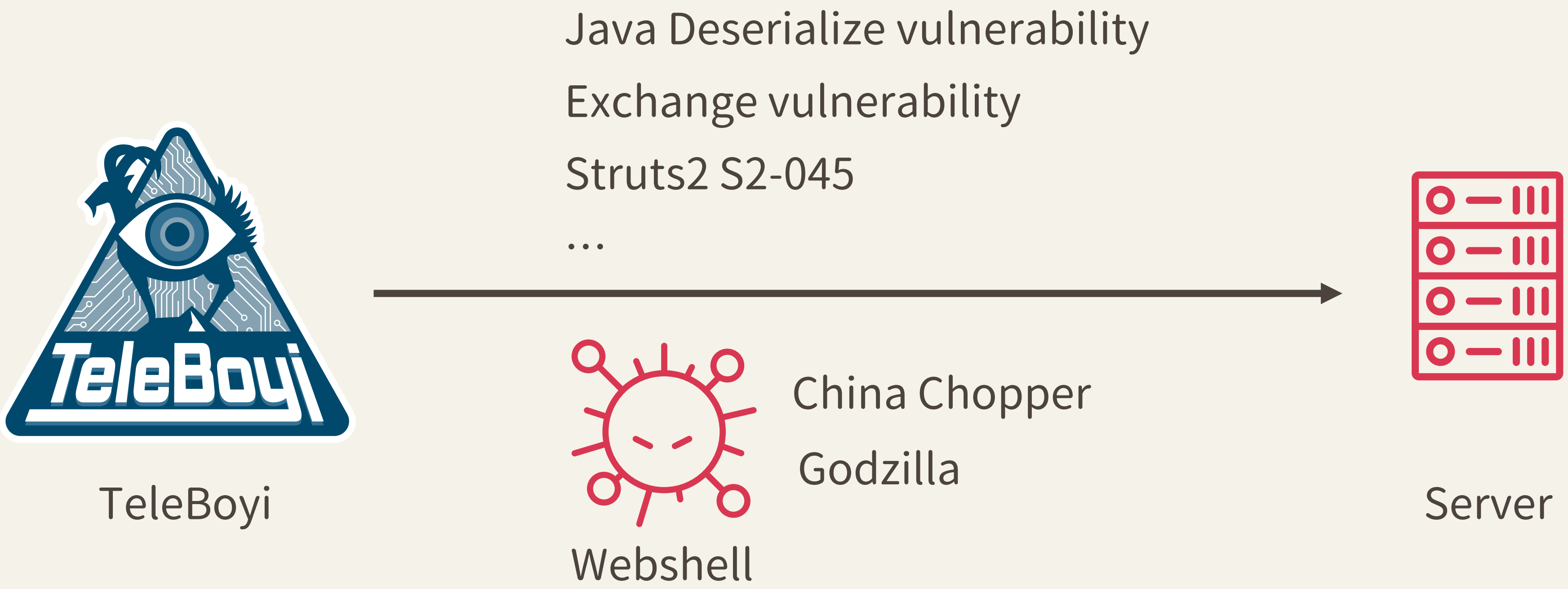
詳細信息.doc

Macro

Download PlugX dropper

C2 server

Exploit Public-Facing Application



Java Deserialize vulnerability

Exchange vulnerability

Struts2 S2-045

…

China Chopper

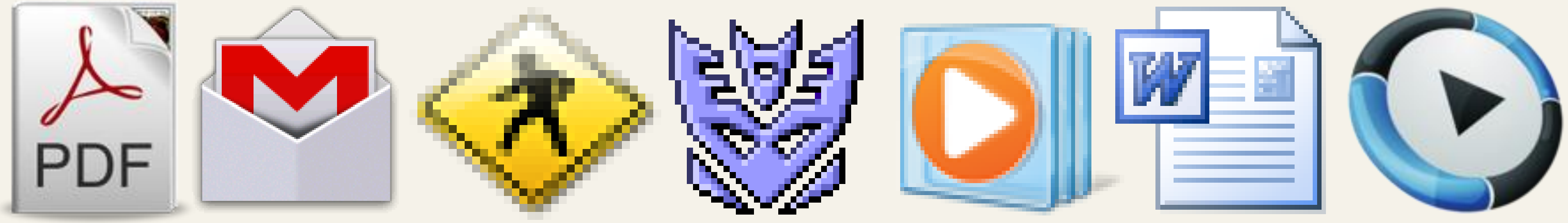
Godzilla

Webshell

Malware Packing

TEAMT5

- Self-Extracting Archive (SFX)
- Flexible deployment
  - Disguise malware as fake application or document
  - Easier installation by macro/HTA
  - Easier installation through webshell
- Icons



TeleBoyi’s Arsenal

TeleBoyi’s Arsenal

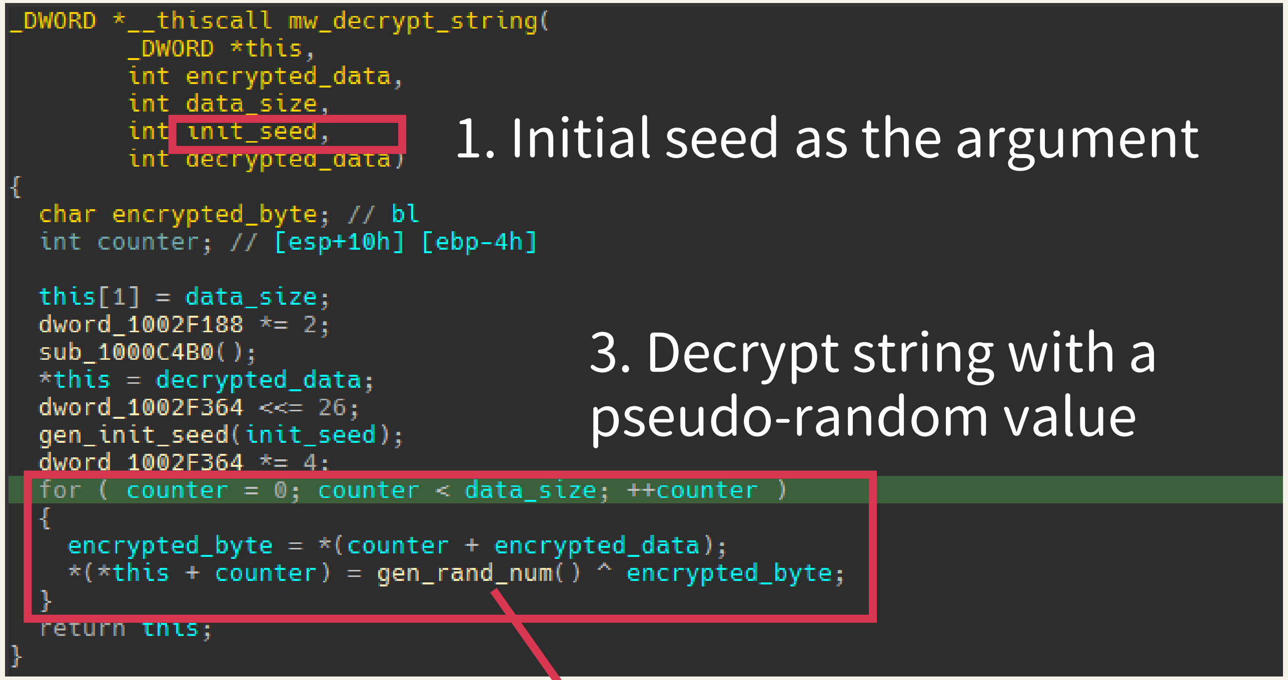
- Malware
  - PlugX
  - Winnti
  - ShadowPad
  - DeedRAT
  - TripleZero (Mélofée)
  - LibreCoin (RatelS)
  - DoubleShell
  - FakeWorker
  - CobaltStrike
  - Sliver
  - AsyncRAT
- Hacking tool
  - Web shell
  - Credential dumping tool
  - Others

PlugX

- First seen: 2008
- A modular malware with multiple capabilities
- Used by several Chinese APT groups
    - TeleBoyi, APT41, Mustang Panda, APT27, menuPass, and more

TeleBoyi’s Custom Loader

- Payload
  - PlugX
  - CobaltStrike
- Packer
  - Themida
  - VMProtect
- Payload decryption
  - XOR
- String decryption
  - Pseudo random generation (PRNG)

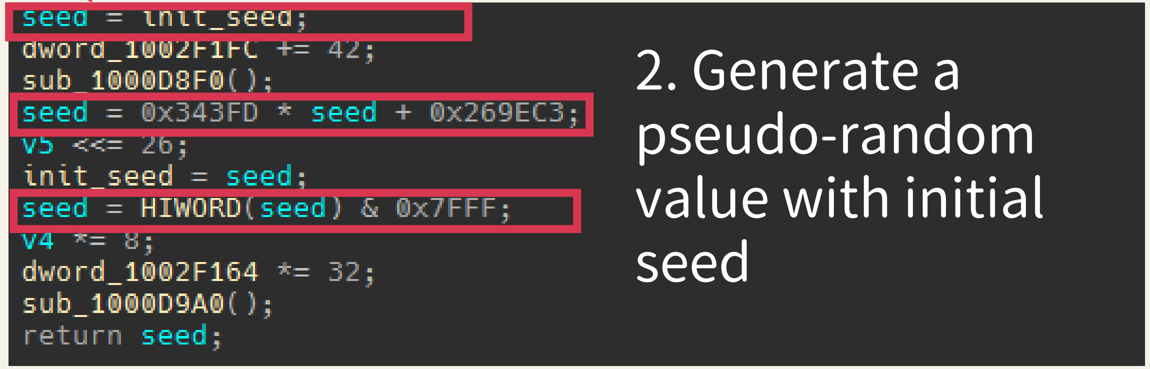


```
_DWORD *__thiscall mw_decrypt_string(
        _DWORD *this,
        int encrypted_data,
        int data_size,
        int init_seed,
        int decrypted_data)
{
  char encrypted_byte; // bl
  int counter; // [esp+10h] [ebp-4h]

  this[1] = data_size;
  dword_1002F188 *= 2;
  sub_1000C4B0();
  *this = decrypted_data;
  dword_1002F364 <<= 26;
  gen_init_seed(init_seed);
  dword_1002F364 *= 4;
  for ( counter = 0; counter < data_size; ++counter )
  {
    encrypted_byte = *(counter + encrypted_data);
    *(*this + counter) = gen_rand_num() ^ encrypted_byte;
  }
  return this;
}
```

1. Initial seed as the argument

3. Decrypt string with a pseudo-random value



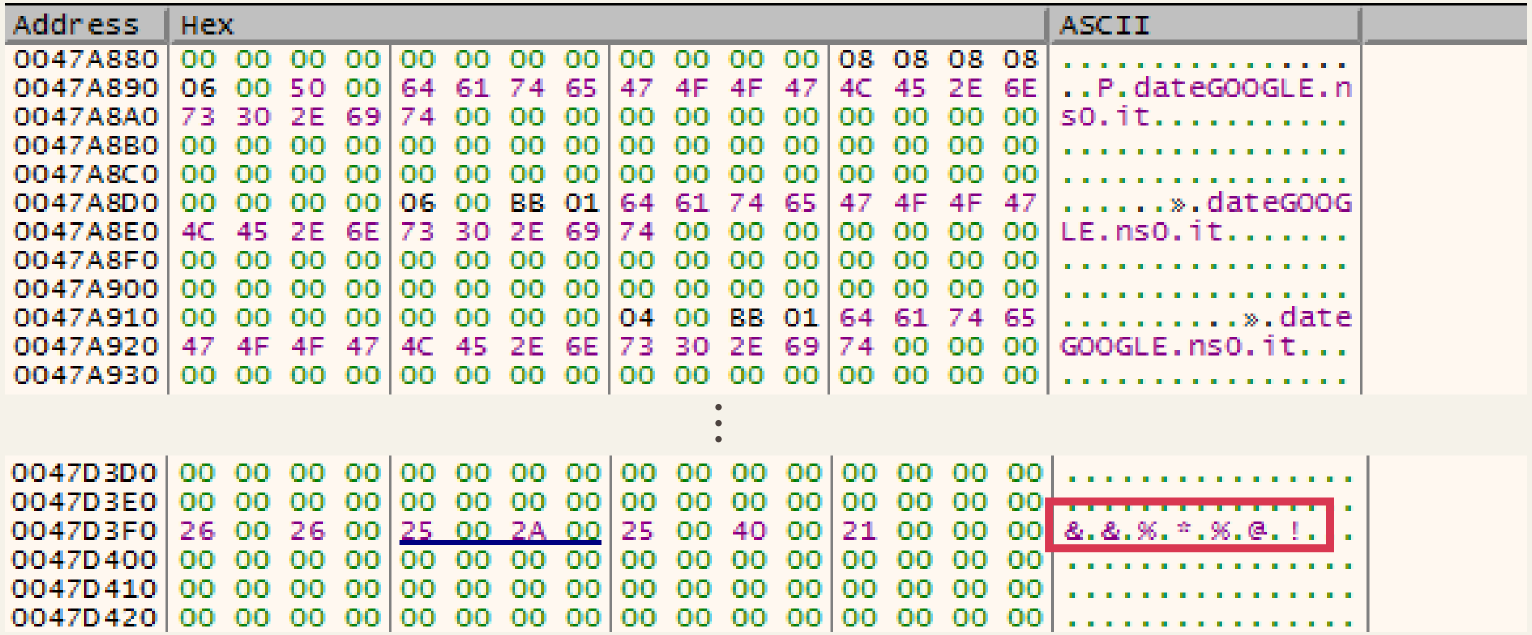
```
seed = init_seed;
dword_1002F1FC += 42;
sub_1000D8F0();
seed = 0x343FD * seed + 0x269EC3;
v5 <<= 26;
init_seed = seed;
seed = HIWORD(seed) & 0x7FFF;
v4 *= 8;
dword_1002F164 *= 32;
sub_1000D9A0();
return seed;
```

2. Generate a pseudo-random value with initial seed

TeleBoyi’s PlugX vs. Other Threat Actors’ PlugX?

TeleBoyi’s PlugX

- Special configuration password
  - &&%*%@! (shift + 7758521)
- 7758521
  - 亲亲我吧我爱你, which means “Kiss me I love you”



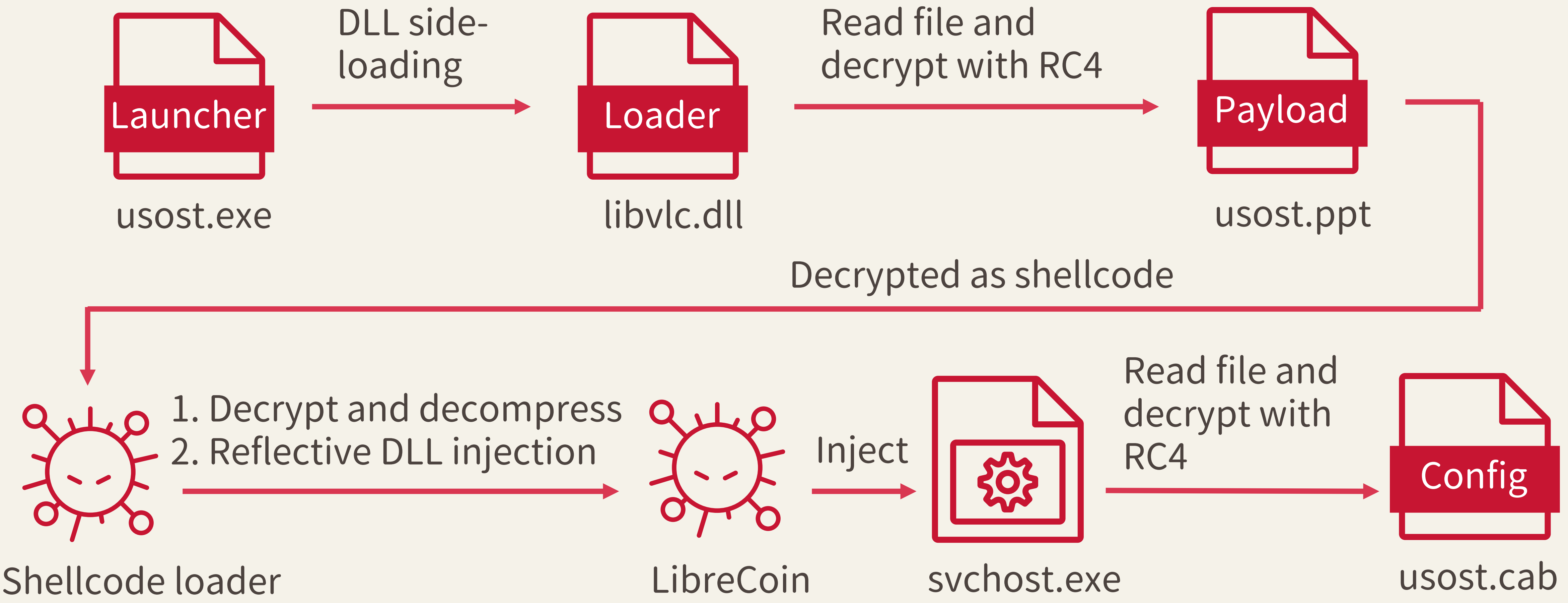
```
Address   Hex                                              ASCII
0047A880  00 00 00 00 00 00 00 00 00 00 00 00 08 08 08 08  ................
0047A890  06 00 50 00 64 61 74 65 47 4F 4F 47 4C 45 2E 6E  ..P.dateGOOGLE.n
0047A8A0  73 30 2E 69 74 00 00 00 00 00 00 00 00 00 00 00  s0.it...........
0047A8B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047A8C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047A8D0  00 00 00 00 06 00 BB 01 64 61 74 65 47 4F 4F 47  ......».dateGOOG
0047A8E0  4C 45 2E 6E 73 30 2E 69 74 00 00 00 00 00 00 00  LE.ns0.it.......
0047A8F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047A900  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047A910  00 00 00 00 00 00 00 00 04 00 BB 01 64 61 74 65  ..........».date
0047A920  47 4F 4F 47 4C 45 2E 6E 73 30 2E 69 74 00 00 00  GOOGLE.ns0.it...
0047A930  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
                                 ⋮
0047D3D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D3E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D3F0  26 00 26 00 25 00 2A 00 25 00 40 00 21 00 00 00  &.&.%.*.%.@.!...
0047D400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D410  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0047D420  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

LibreCoin

- Alias
  - RatelS
- First seen
  - 2022/03
- Connection
  - Reverse mode
  - Listen mode
- Protocol
  - TCP
  - HTTP/HTTPS
  - TLS

- Capability
  - Command shell
  - File operations
  - Proxy
  - Screenshot
  - Keylogger
  - And more...

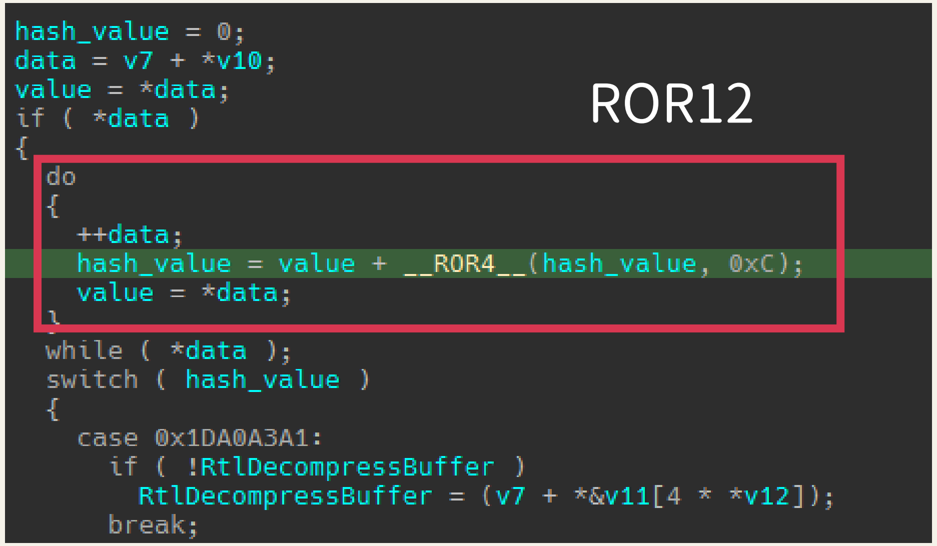
LibreCoin – Execution Flow



Something Interesting About This Shellcode Loader...

Shellcode Loader

- Special API hashing
  - ROR12
- Payload decryption
  - XOR + LZNT1
- Reflective DLL injection
- Shared among certain Chinese APT groups
  - LibreCoin
  - Earth Berberoka’s CoinLess (the variant of CLAMBLING)
  - FamousSparrow’s CobaltStrike
  - GroundPeony’s micDown



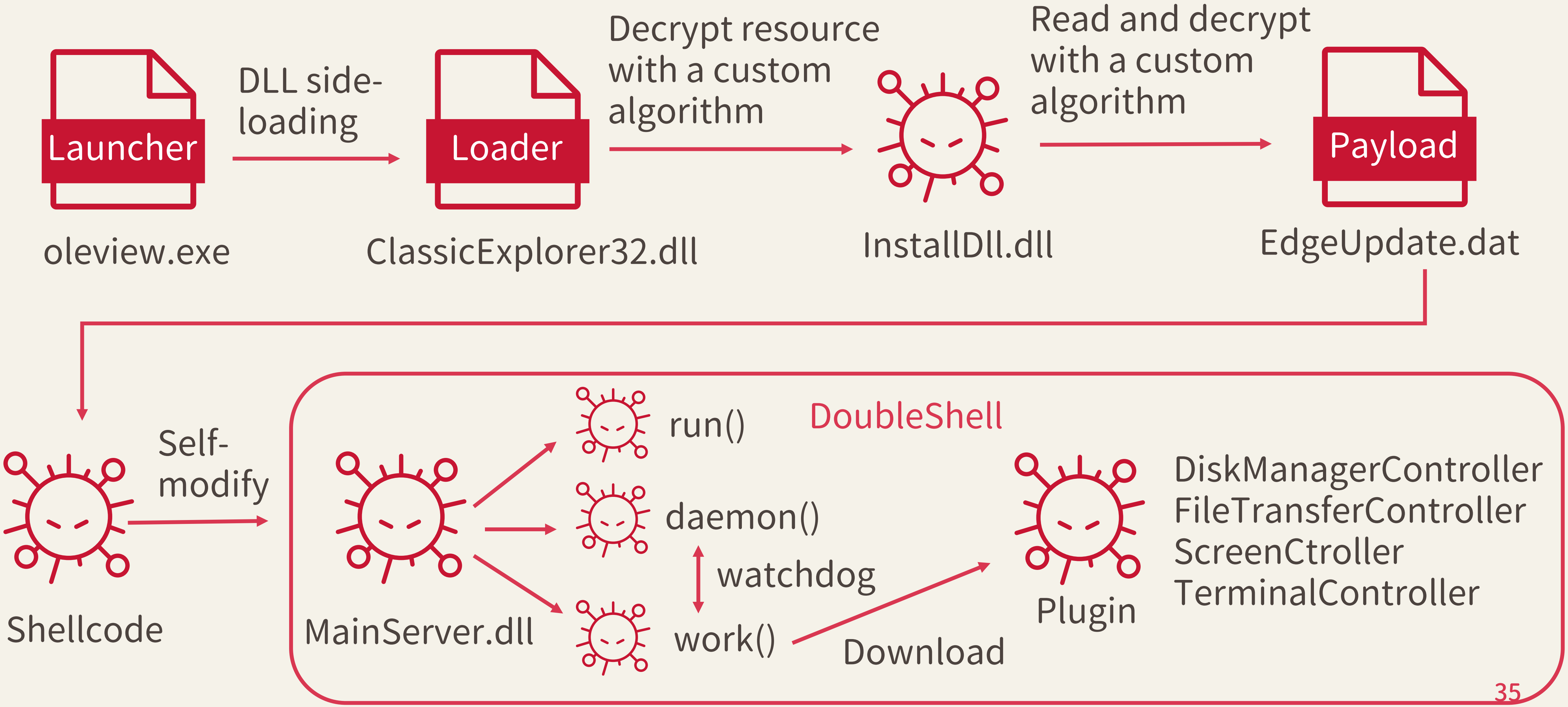
ROR12

```
hash_value = 0;
data = v7 + *v10;
value = *data;
if ( *data )
{
  do
  {
    ++data;
    hash_value = value + __ROR4__(hash_value, 0xC);
    value = *data;
  }
  while ( *data );
  switch ( hash_value )
  {
    case 0x1DA0A3A1:
      if ( !RtlDecompressBuffer )
        RtlDecompressBuffer = (v7 + *&v11[4 * *v12]);
      break;
```

DoubleShell

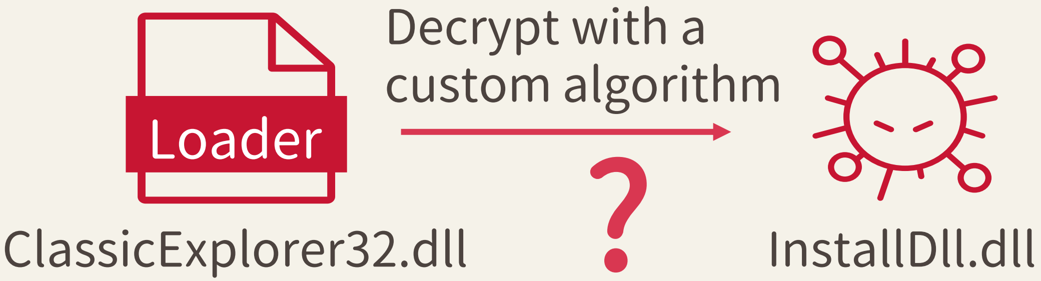
- First seen
  - 2020
- Multi-staged
- Capability
  - Disk management
  - File management
  - Screenshot
  - Command shell

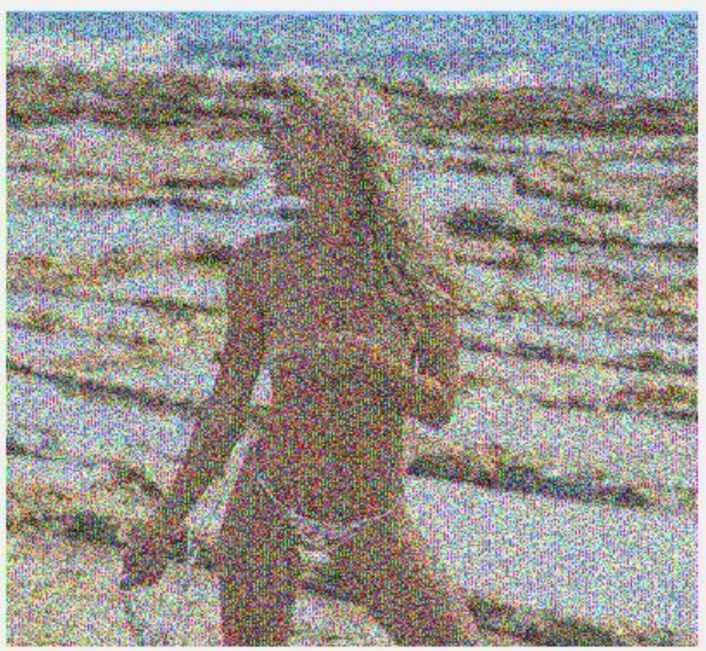
DoubleShell – Execution Flow



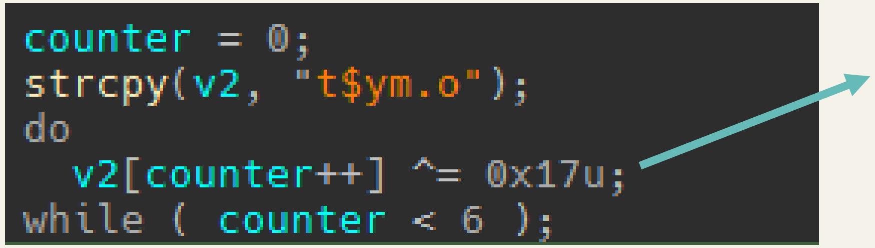
DoubleShell – Custom Algorithm

- Load resource
- Extract binary blob from even-numbered offsets of resource





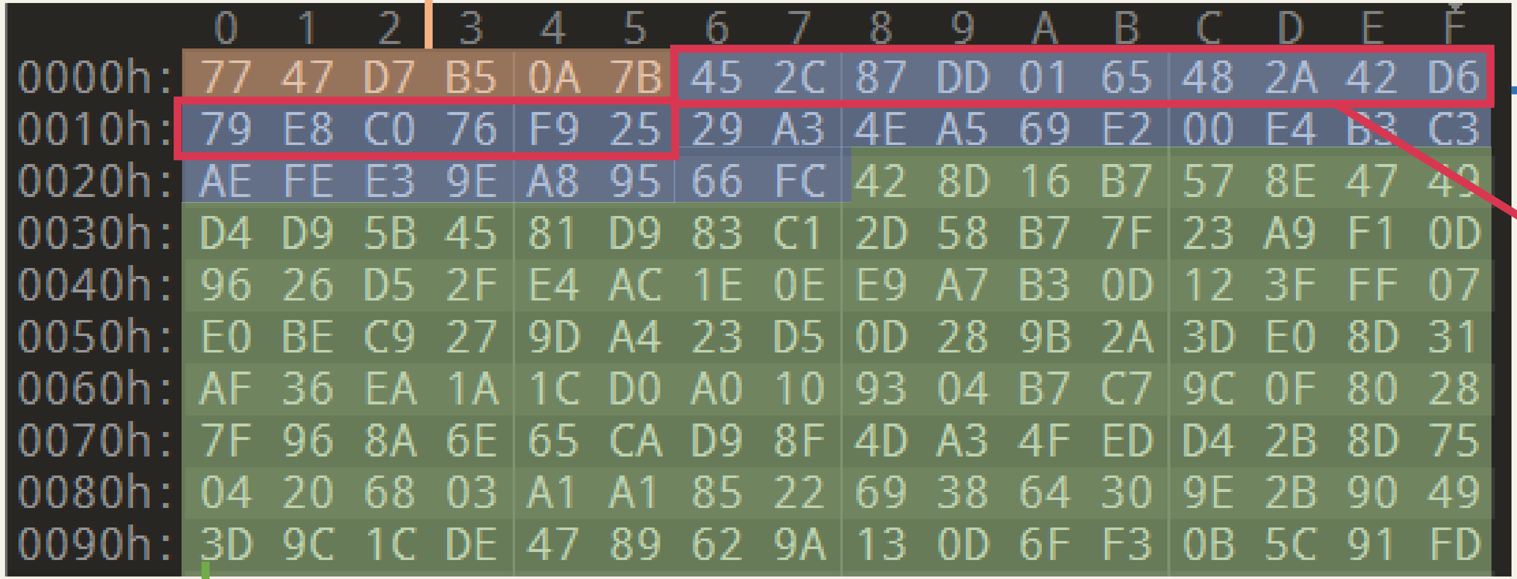
DoubleShell – Custom Algorithm



```
counter = 0;
strcpy(v2, "t$ym.o");
do
  v2[counter++] ^= 0x17u;
while ( counter < 6 );
```

1. XOR decrypt a string as “c3nz9x”

2. Try all the permutation of string “c3nz9x” as RC4 key to decrypt it; if the result matches the key, the result will be a 2nd RC4 key



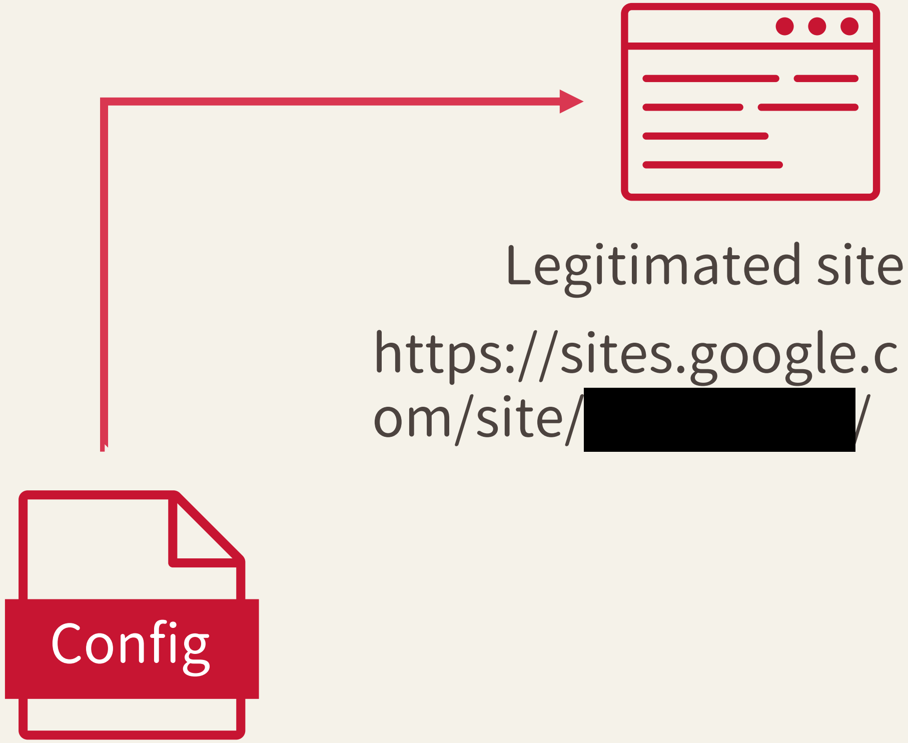
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000h: 77 47 D7 B5 0A 7B 45 2C 87 DD 01 65 48 2A 42 D6
0010h: 79 E8 C0 76 F9 25 29 A3 4E A5 69 E2 00 E4 B3 C3
0020h: AE FE E3 9E A8 95 66 FC 42 8D 16 B7 57 8E 47 49
0030h: D4 D9 5B 45 81 D9 83 C1 2D 58 B7 7F 23 A9 F1 0D
0040h: 96 26 D5 2F E4 AC 1E 0E E9 A7 B3 0D 12 3F FF 07
0050h: E0 BE C9 27 9D A4 23 D5 0D 28 9B 2A 3D E0 8D 31
0060h: AF 36 EA 1A 1C D0 A0 10 93 04 B7 C7 9C 0F 80 28
0070h: 7F 96 8A 6E 65 CA D9 8F 4D A3 4F ED D4 2B 8D 75
0080h: 04 20 68 03 A1 A1 85 22 69 38 64 30 9E 2B 90 49
0090h: 3D 9C 1C DE 47 89 62 9A 13 0D 6F F3 0B 5C 91 FD
```

3. Decrypt it using the 2nd RC4 key

4. The first 16-byte will be 3rd RC4 key

5. Decrypt it with 3rd RC4 key as next-stage loader (e.g., InstallDll.dll)

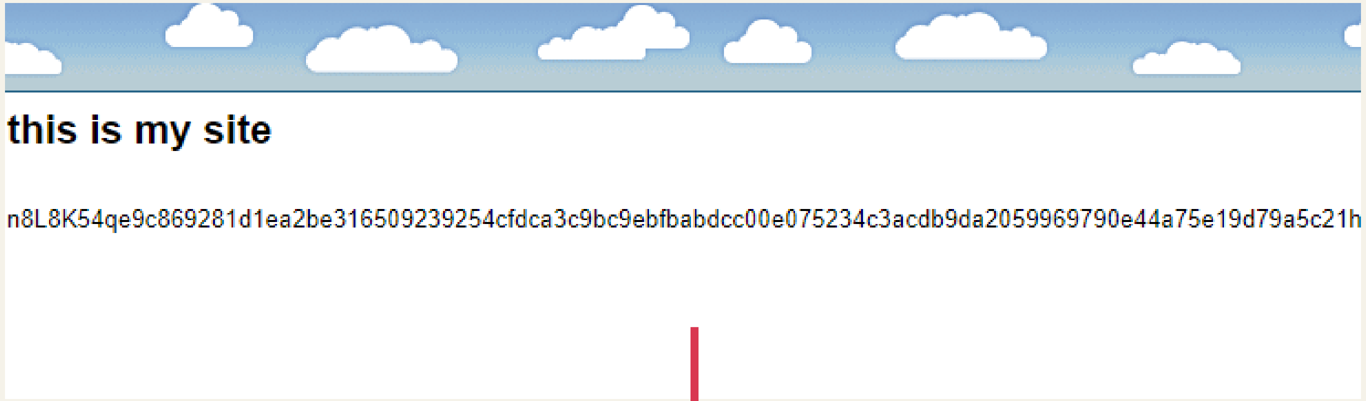
DoubleShell – Dead Drop Resolver



Legitimated site

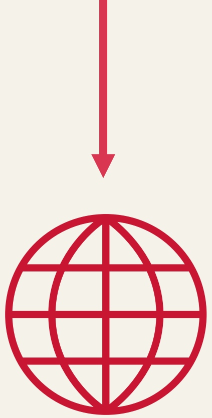
https://sites.google.com/site/[redacted]/

DoubleShell's config



this is my site

```
n8L8K54qe9c869281d1ea2be316509239254cfdca3c9bc9ebfbabdcc00e075234c3acdb9da2059969790e44a75e19d79a5c21h
```



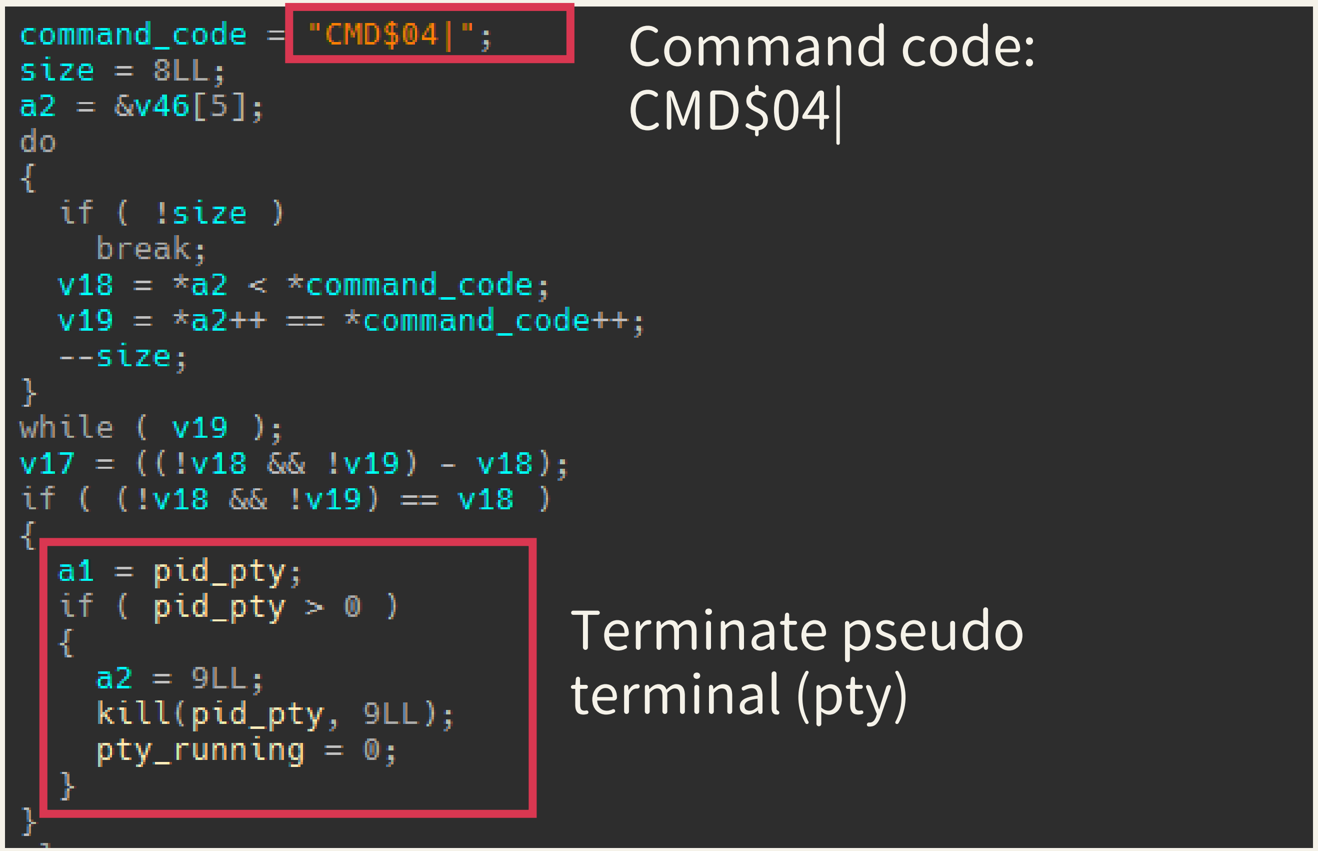
185.236.78.3

New C2 server

TEAMT5

FakeWorker

- First seen
  - 2022/04
- Target
  - Linux
- Capability
  - Upload file
  - Download file
  - Pseudo terminal (pty)
- Command code
  - CMD$0X| (X:1~7)



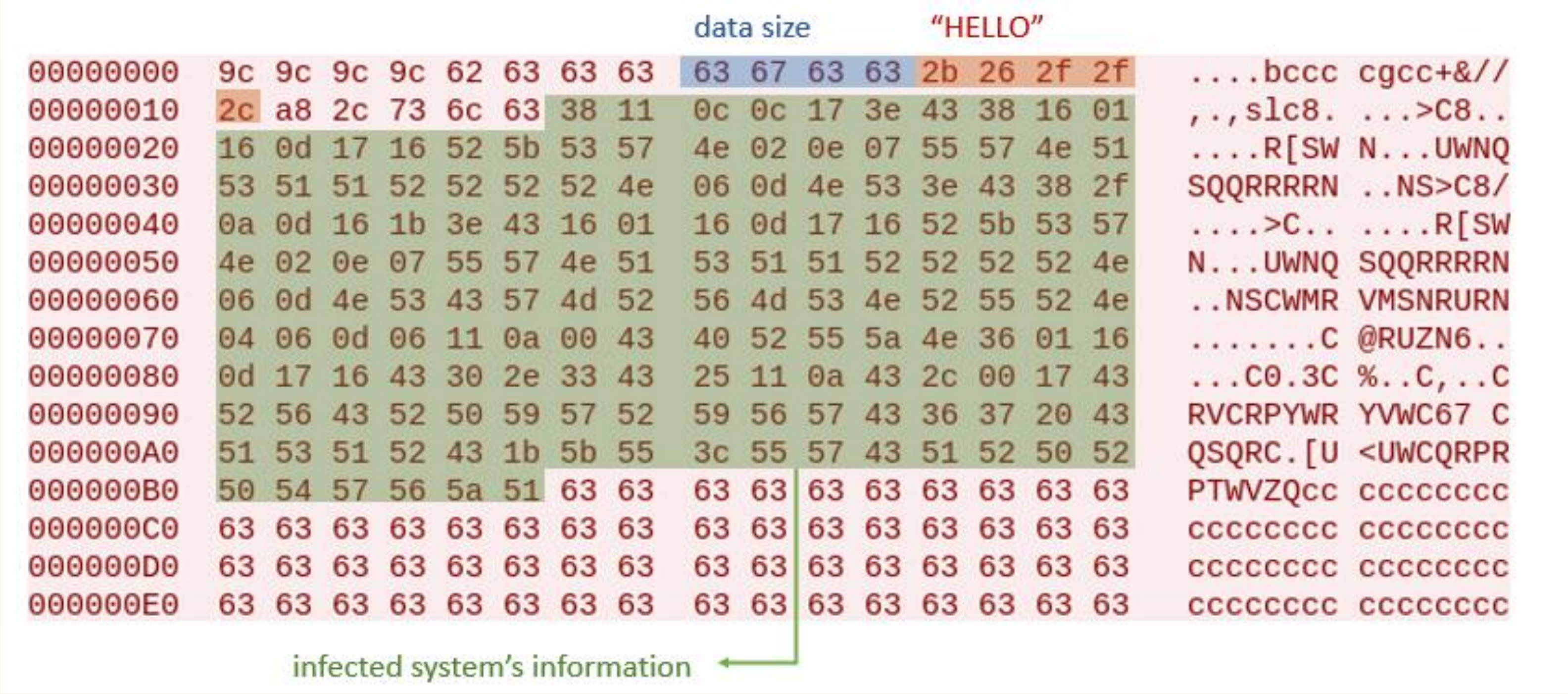
```
command_code = "CMD$04|";
size = 8LL;
a2 = &v46[5];
do
{
  if ( !size )
    break;
  v18 = *a2 < *command_code;
  v19 = *a2++ == *command_code++;
  --size;
}
while ( v19 );
v17 = ((!v18 && !v19) - v18);
if ( (!v18 && !v19) == v18 )
{
  a1 = pid_pty;
  if ( pid_pty > 0 )
  {
    a2 = 9LL;
    kill(pid_pty, 9LL);
    pty_running = 0;
  }
}
```

Command code:
CMD$04|

Terminate pseudo terminal (pty)

FakeWorker

- Protocol
  - KCP
- C2 communication
  - XOR encryption
  - XOR key: 99 (0x63)

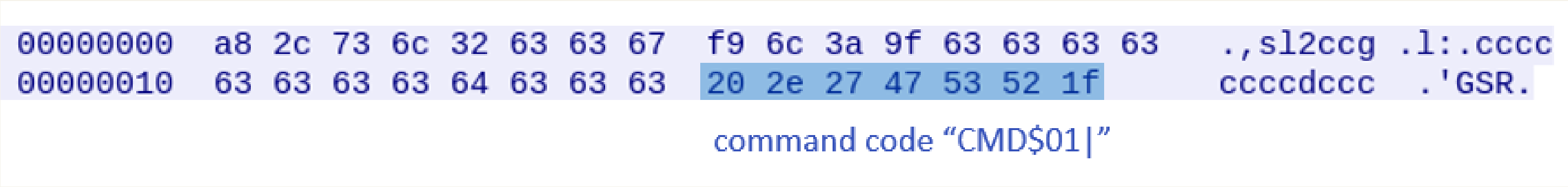


data size

"HELLO"

```
00000000  9c 9c 9c 9c 62 63 63 63  63 67 63 63 2b 26 2f 2f  ....bccc cgcc+&//
00000010  2c a8 2c 73 6c 63 38 11  0c 0c 17 3e 43 38 16 01  ,.,slc8. ...>C8..
00000020  16 0d 17 16 52 5b 53 57  4e 02 0e 07 55 57 4e 51  ....R[SW N...UWNQ
00000030  53 51 51 52 52 52 52 4e  06 0d 4e 53 3e 43 38 2f  SQQRRRRN ..NS>C8/
00000040  0a 0d 16 1b 3e 43 16 01  16 0d 17 16 52 5b 53 57  ....>C.. ....R[SW
00000050  4e 02 0e 07 55 57 4e 51  53 51 51 52 52 52 52 4e  N...UWNQ SQQRRRRN
00000060  06 0d 4e 53 43 57 4d 52  56 4d 53 4e 52 55 52 4e  ..NSCWMR VMSNRURN
00000070  04 06 0d 06 11 0a 00 43  40 52 55 5a 4e 36 01 16  .......C @RUZN6..
00000080  0d 17 16 43 30 2e 33 43  25 11 0a 43 2c 00 17 43  ...C0.3C %..C,..C
00000090  52 56 43 52 50 59 57 52  59 56 57 43 36 37 20 43  RVCRPYWR YVWC67 C
000000A0  51 53 51 52 43 1b 5b 55  3c 55 57 43 51 52 50 52  QSQRC.[U <UWCQRPR
000000B0  50 54 57 56 5a 51 63 63  63 63 63 63 63 63 63 63  PTWVZQcc cccccccc
000000C0  63 63 63 63 63 63 63 63  63 63 63 63 63 63 63 63  cccccccc cccccccc
000000D0  63 63 63 63 63 63 63 63  63 63 63 63 63 63 63 63  cccccccc cccccccc
000000E0  63 63 63 63 63 63 63 63  63 63 63 63 63 63 63 63  cccccccc cccccccc
```

infected system's information



```
00000000  a8 2c 73 6c 32 63 63 67  f9 6c 3a 9f 63 63 63 63  .,sl2ccg .l:.cccc
00000010  63 63 63 63 64 63 63 63  20 2e 27 47 53 52 1f     ccccdccc  .'GSR.
```

command code "CMD$01|"

C&C Infrastructure

C&C Infrastructure

- Consists of
  - VPS server
  - Compromised website
- Domains containing companies related to the target

Targeted Sector	C&C Domain	Legitimate Company
Semiconductor	asmlupdata.com, center.asmlbigip.com, sec.asmlbigip.com	ASML
Telecommunication	idupea.controlliamo.com	Idea Cellular
Aerospace	fanuc.gre6gbuf4f.com	FANUC
Cryptocurrency	erc.acefinance.asia, www.acefinance.asia, acefinance.asia	ACE Exchange

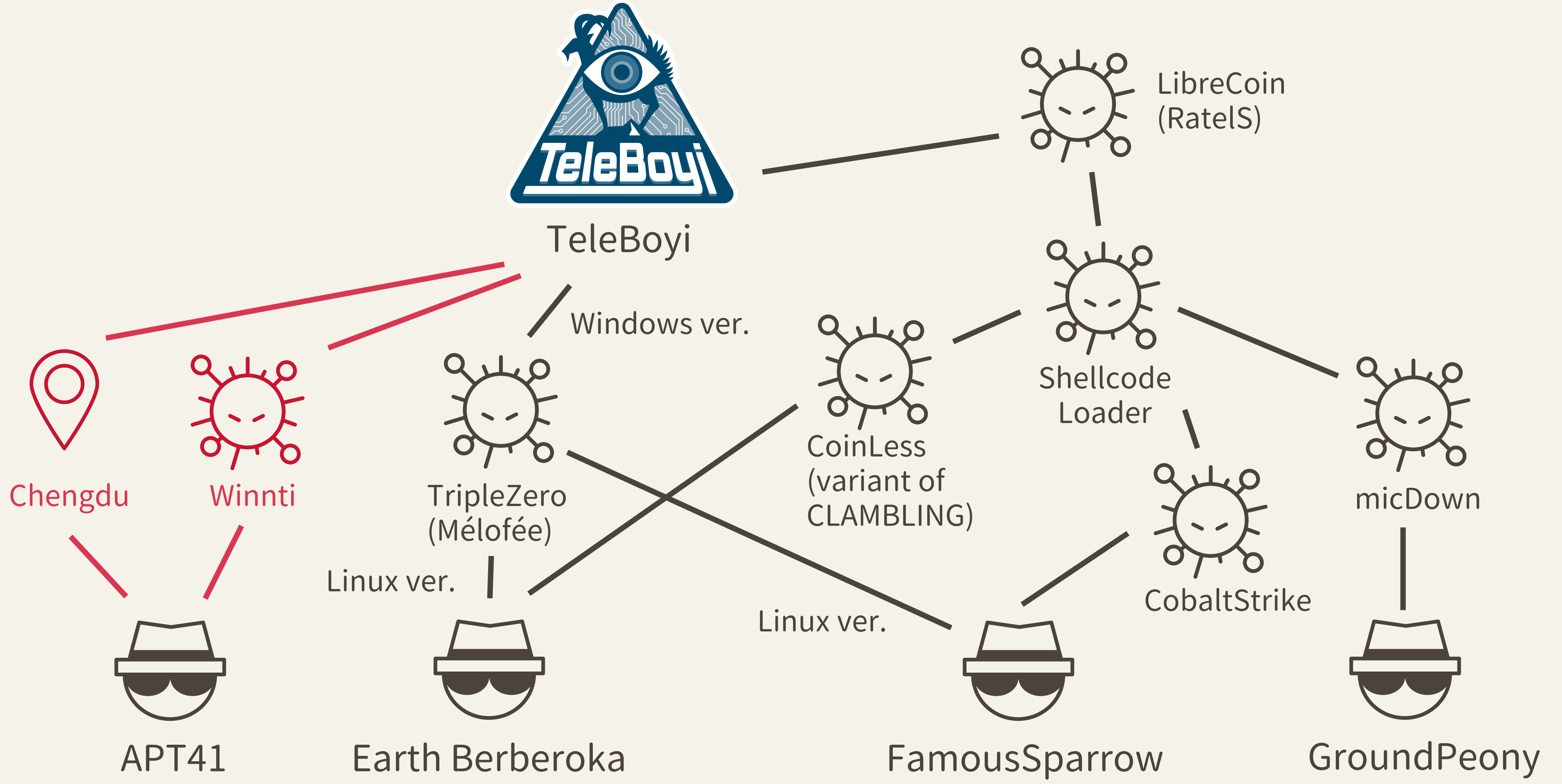
C&C Infrastructure

- Domains containing famous companies

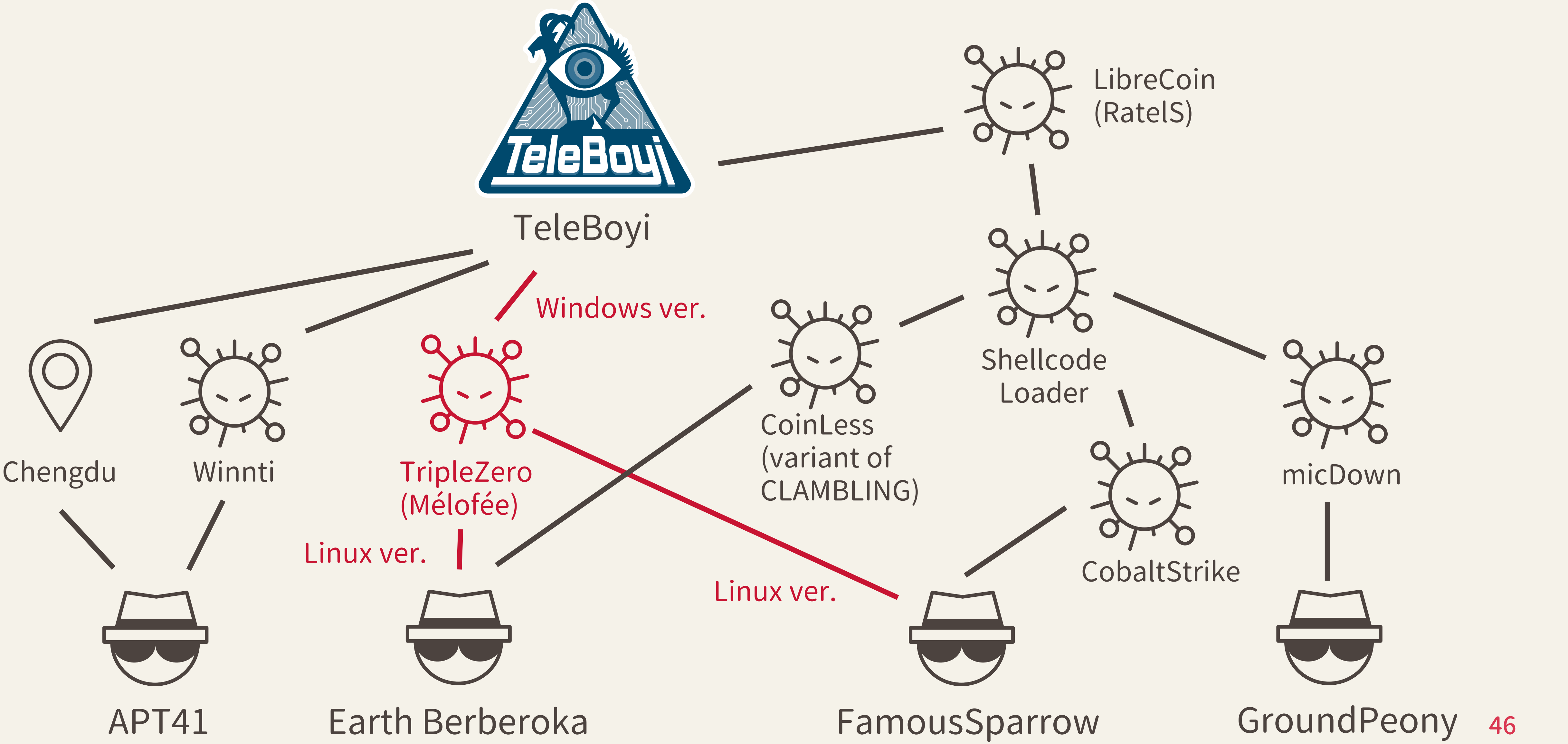
Legitimate Company	C&C Domain
Microsoft	microsoftupdatebaks.ns0.it, newupdatemicrosoft.homepc.it, microsoftstate.homepc.it, sery.mirsoftcheckie.com
Google	dategoogle.ns0.it, googlegmail.ns0.it
LINE	cdn.statics12.line-mychat.com, cdn.static10.line-mychat.com
PChome	pc.pchomecache.com, cdn.pchomecache.com

Relation with other APT groups

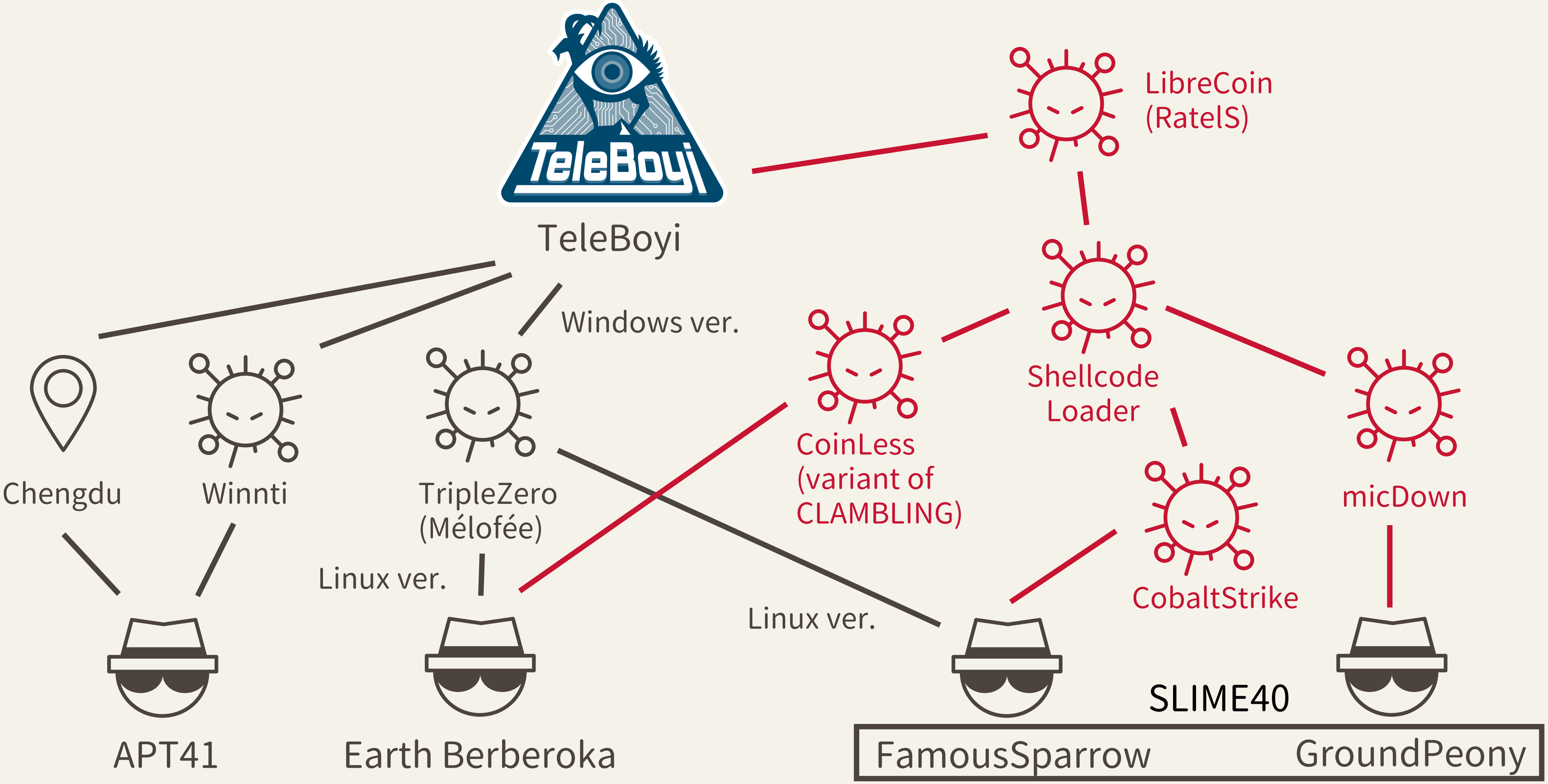
Relation with other APT groups



Relation with other APT groups



Relation with other APT groups



Relation with other APT groups

- Potential collaboration between TeleBoyi and other APT groups, including APT41, Earth Berberoka, SLIME40
- Malware supply chain among these groups due to malware sharing

Conclusion

Key Takeways

- TeleBoyi is a Chinese APT group that targets critical infrastructure worldwide
- TeleBoyi leverages three different ways to gain initial access, including fake applications, malicious documents, exploit public-facing application
- TeleBoyi relies on shared tools heavily; we also found two malware named DoubleShell and FakeWorker that have not been disclosed before
- TeleBoyi has a close connection with APT41, Earth Berberoka, and SLIME40
- Chinese APT groups tend to use shared tools in their attacks nowadays

THANK YOU!

Yi-Chin Chuang
rax@teamt5.org

Yu-Tung Chang
tako@teamt5.org

TEAMT5

Persistent Cyber Threat Hunters