# “LuoYu”

## The eavesdropper sneaking in multiple platforms

Leon & Shui

TEAMT5

Persistent Cyber Threat Hunters

# Speakers' Bio

**Shui** is a cyber threat Analyst working for TeamT5. Holding a master's degree from Johns Hopkins SAIS, she has a keen eye for international affairs. She mainly works on Cyber Espionage campaign tracking and involves in the underground market research.

**Leon** is a cyber threat analyst in the Cyber Threat Intelligence team at TeamT5. His major areas of research include APT campaign tracking, malware analysis. He has participated in information security diagnosis services for government and financial institutions and research on vulnerabilities in IoT devices in the past.

# AGENDA

TEAMT5

01 The Luoyu Threat Group Overview

02 Activity Timeline

03 ReverseWindow Analysis

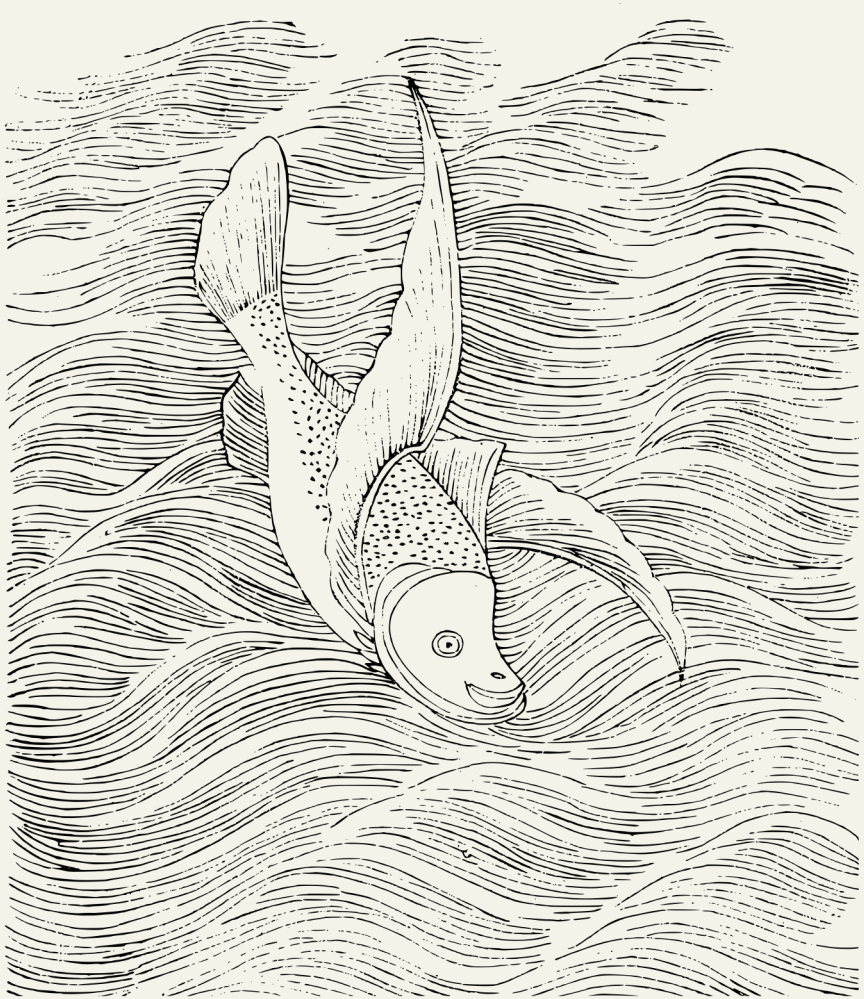
04 Case Study

05 Key Takeaway

# The Luoyu Group Overview

# The name: 鸁魚 (Luoyu)

TEAMT5



- 鸁魚(LuoYu) a Chinese mythological creature
- 鸁魚，魚身而鳥翼，音如鴛鴦，見則其邑大水。
- Translation: Fish with a pair of wings; When it appears, floods always follow.


Profile

## Origin

China

## Malware

ReverseWindow WinDealer SpyDealer

## Target Industry

Technology Media Education

## Target Areas

China Hong Kong Japan Korea Taiwan

TEAMT5

# Goal

TEAMT5


Attack

Message Apps


Collecting information from dissidents?

# Activity Timeline

# 2014-2017 China focused

TEAMT5

2014 2015 2016 2017

Spying apps circulating in the wild

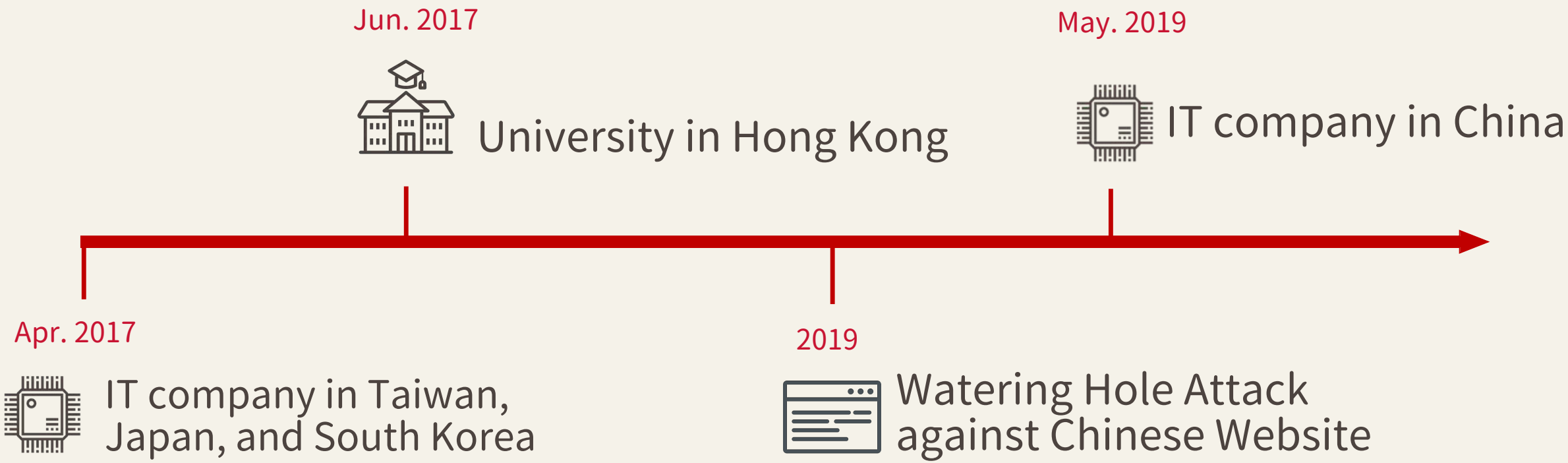
Android malware spying on Apps




And more…

# 2017- now: Expand to East Asia

TEAMT5



# Malware profile: ReverseWindow

# Malware profile: ReverseWindow

TEAMT5

- ReverseWindow(aka sysetmd, OSX.Demsty) is a multi-platform malware, it supports Windows, Linux, Mac, Android.
- Create mutex string prefix “LOOTWODNIW” is the reverse of “WINDOWTOOL”.
- Use DES algorithm for configuration decryption and data encryption.
- Uses TLV(type-length-value) protocol to send and receive data.

# Evolution of ReverseWindow

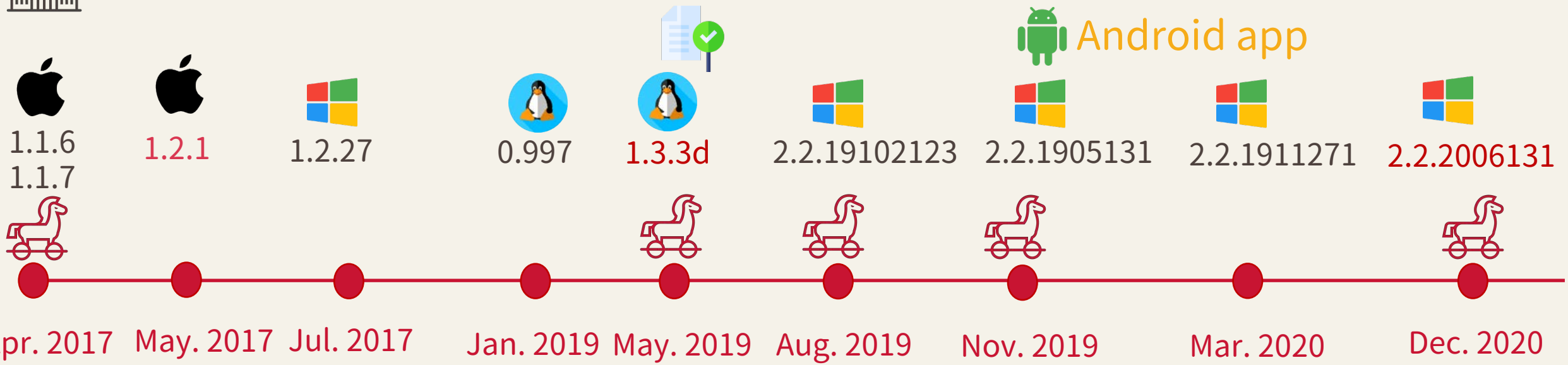
# Evolution of ReverseWindow

TEAMT5

IT company in Taiwan, Japan, and South Korea

IT company in China

University researcher in Hong Kong




Discovery time in the wild(20+ samples)

Icons made by https://www.flaticon.com/authors/freepik
Icons made by https://www.flaticon.com/authors/pixel-perfect

# In-Depth Analysis of ReverseWindow

# Hide the malicious traces

TEAMT5

- At first run, ReverseWindow will make the user think that the file was corrupted.
- Persistence method:
  - Copy self to ” ~/.local/bin/sysetmd”, write .bashrc and create cronjob.

OSX

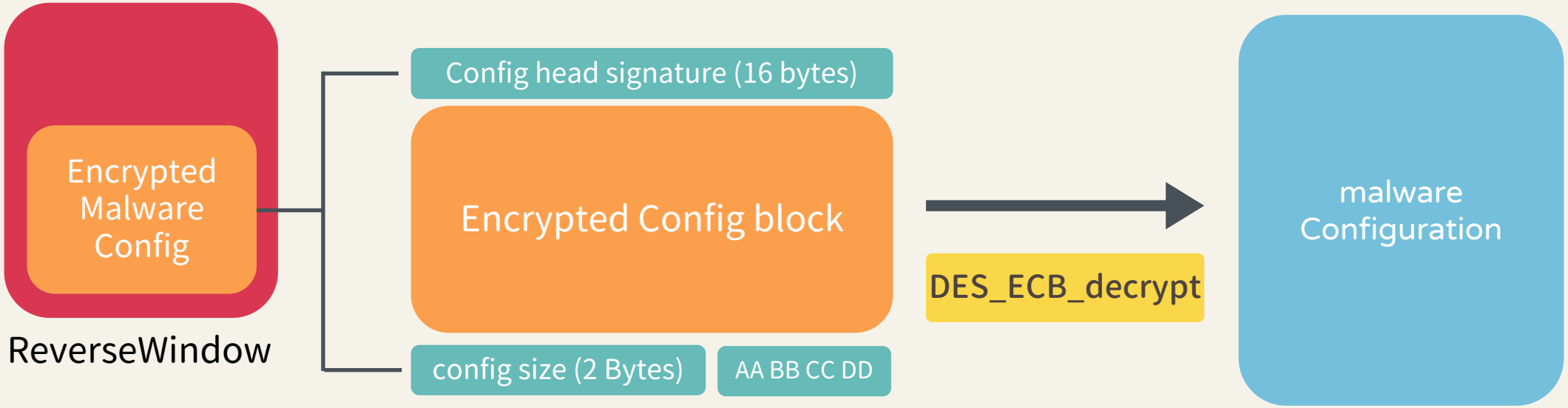
```
fwrite("This file is corrupted and connot be opened\n", 0x2CuLL, 1uLL, __stderrp);
exit_signal();
```

Linux

```
fwrite("Segmentation fault (core dumped)\n", 1uLL, 0x21uLL, stderr);
hookSignal();
umask(0);
```

# Decrypt malware C&C configuration

TEAMT5

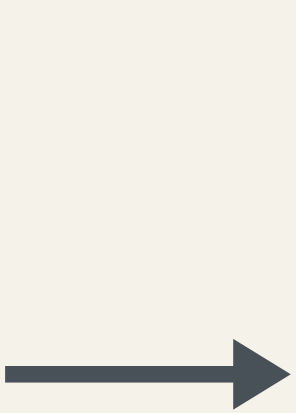


# Decrypt malware C&C configuration

TEAMT5

- Test Sample C2:192.168.8.107:10443

malware Configuration



type length value

```
00000000  01 02 00 00 00 30 31 02 0d 00 00 00 31 39 32 2e  |.....01.....192.|
00000010  31 36 38 2e 38 2e 31 30 37 03 05 00 00 00 31 30  |168.8.107.....10|
00000020  34 34 33 04 02 01 00 00 00 04 da 8c 39 91 bf e4  |443.......9.??|
00000030  1a 29 43 0c 31 4e 60 59 1c 00 bc 52 e4 75 4d a3  |.)C.1N`Y..R?uM?|
00000040  be 67 61 4d 23 31 db 3f a9 62 04 9e ef d4 5f f9  |?gaM#1??b..??_?|
00000050  9f 59 ac d0 a9 ed 5e 7d 9b 08 ee 97 57 1c 57 ba  |.Y??^}..?.W.W?|
00000060  68 1a f7 68 e3 34 14 89 1a d9 f0 29 1a 00 58 31  |h.?h?4...??)..X1|
00000070  4f bd 11 2e 27 49 d8 81 0b ec ca 13 5e 76 42 21  |O?..'I?..??.^vB!|
00000080  47 76 ab 5e cb 8c 2f a0 9d 3f 5e 16 88 9b e7 85  |Gv?^?./?.?^...?.|
00000090  8f 14 e8 5a 0b 9d 9f d9 35 3b 83 78 f4 e1 81 cd  |..?Z...?5;.x??.?|
000000a0  09 60 82 22 5b 47 4a 61 b7 93 00 00 00 00 00 00  |.`."[GJa?.......|
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 00 00 00 00  |................|
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
```

# Collecting host information

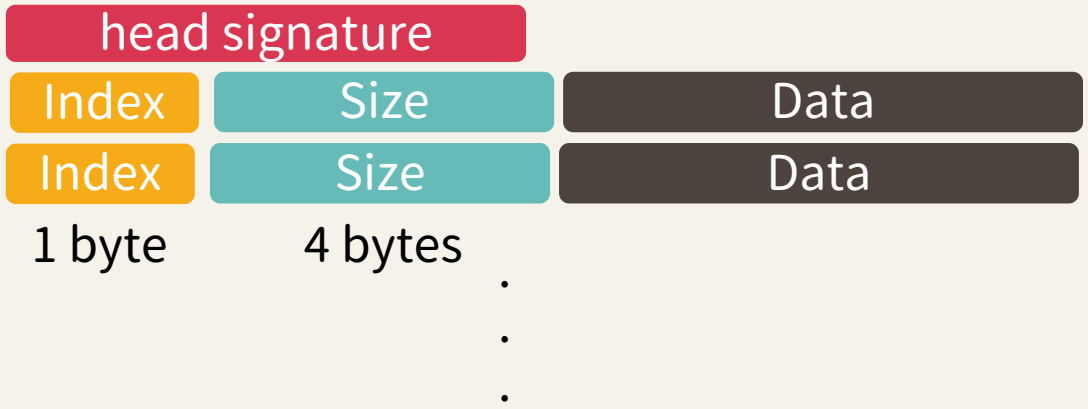
TEAMT5

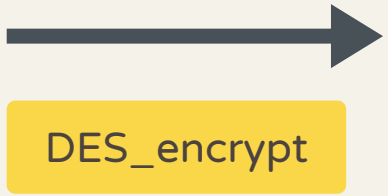
- Hostname
- Operating System Version
- User name
- MAC address and IP address (IPv6,IPv4)
- CPU info
- the amount of physical RAM
- External IP address
- Hard drive volume name (Windows only)
- Removable device file (Windows only)

# Collecting host information

TEAMT5

- The victim information is arranged by TLV(**type-length-value**) format.
- ReverseWindow encrypts victim data using DES algorithm with hard-coded key table.



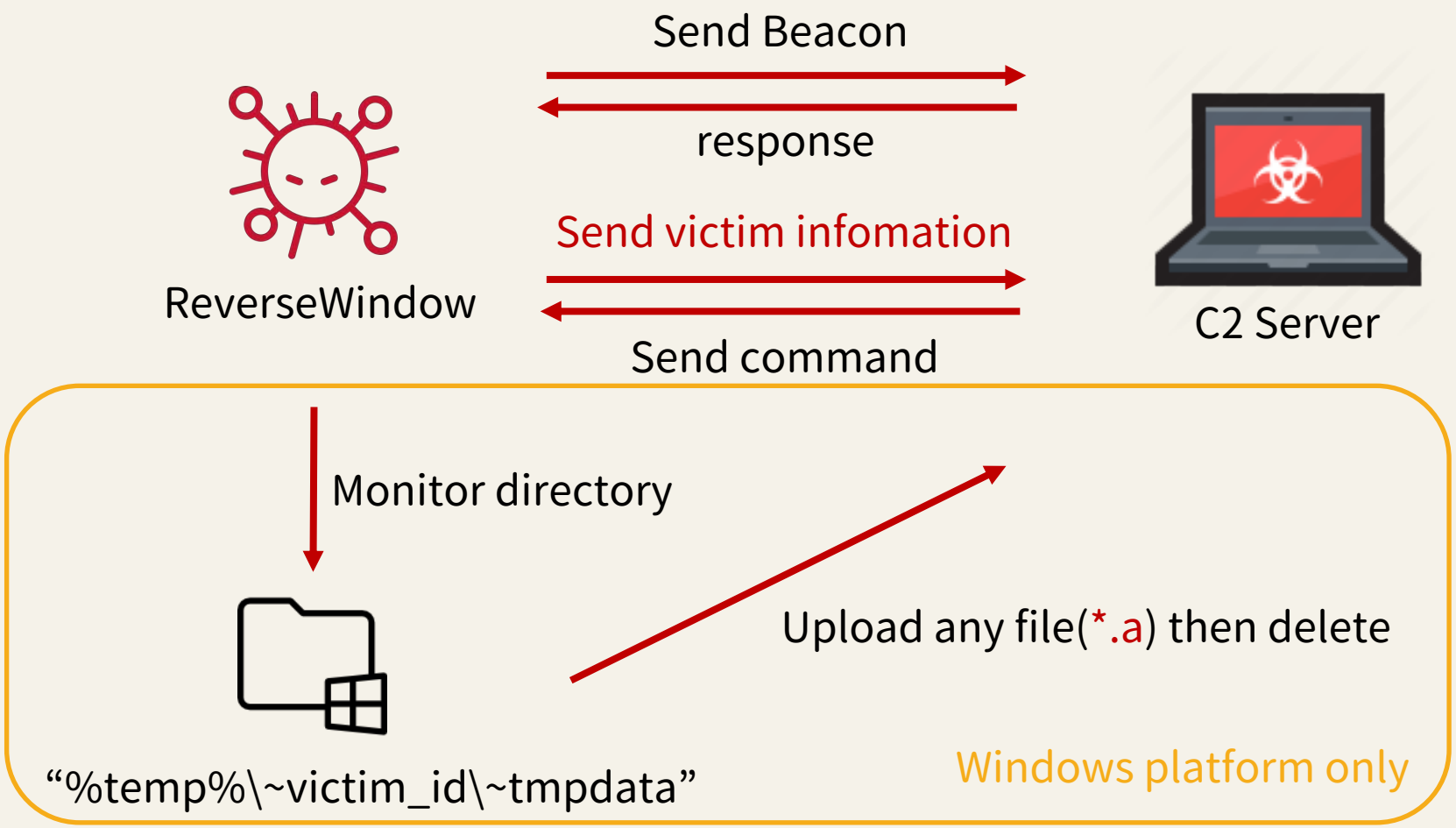




Encrypted victim data

Icons made by https://www.flaticon.com/authors/freepik

# Collecting host information

TEAMT5



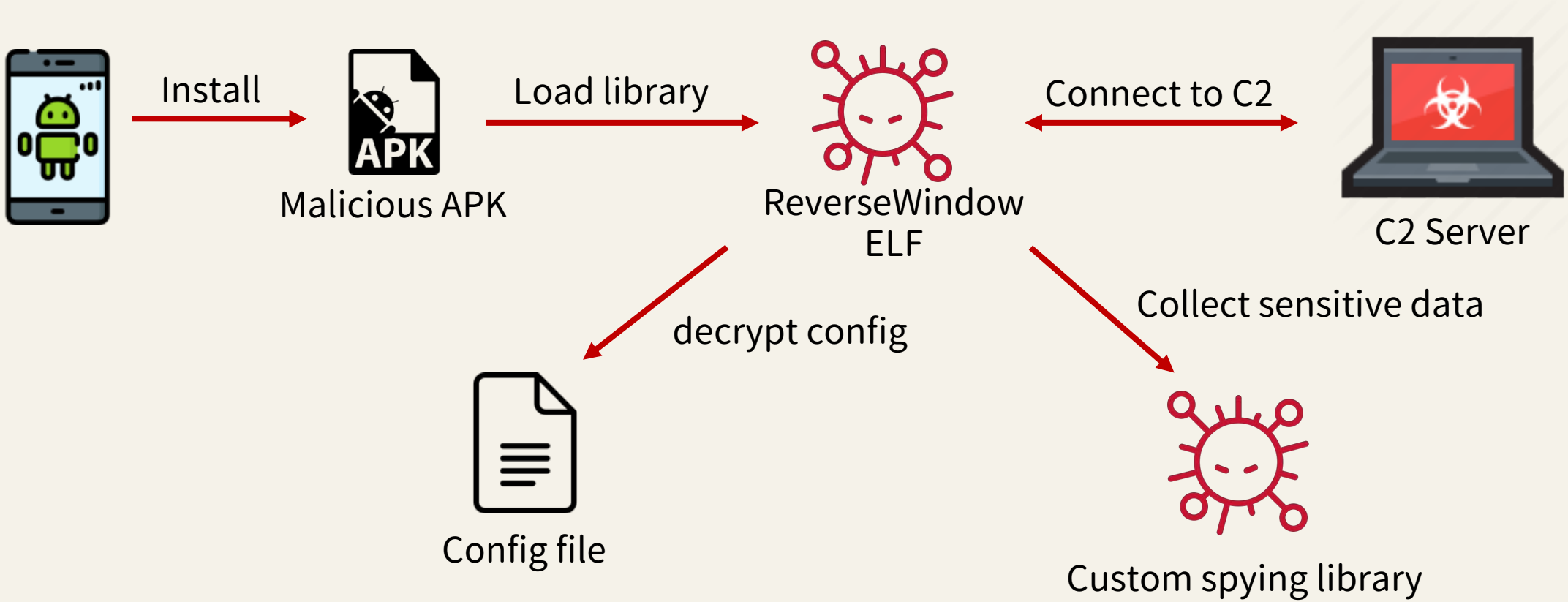

Icons made by https://www.flaticon.com/authors/those-icons

# Custom ReverseWindow Android APK


- In 2019, LuoYu actor developed an Android variant of ReverseWindow.
- We found that the attacker disguised the apk as a popular messaging app.
- The actor also added another custom-developed spying library to the apk.
- Unfortunately, currently, we are unsure how the actor spread the malware.

# Custom ReverseWindow Android APK

TEAMT5




Icons made by https://www.flaticon.com/authors/freepik

# Version changes

TEAMT5

| | |
|---|---|
| Windows 1.2.27 | The command Protocol 0x0100(install Persistence) was only supported in Windows(1.2.27) |
| OSX 1.2.1 | Support proxy setting |
| Windows 2.2.* | String obfuscation<br>Stack string & GetProcessAddress to get WinAPI |
| Windows 2.2.1905131 | ReverseWindow interest in two popular messaging app<br>and three popular browsers in China (360SE, 360chrome, SougouExplorer) |
| Windows 2.2.2006131 | Support networking status |

# Command Details

TEAMT5

Common

| Command code | Description |
| --- | --- |
| 0x0200 | File Operations |
| 0x0300 | Shell Command |
| 0x0400 | update RAT |
| 0x0500 | Uninstall RAT |
| 0x0800 | Update malware Config |

# Command Details

TEAMT5

Common

| Command code | Description |
| --- | --- |
| 0x0900 | (Linux)install plug-in \| (Windows)execute a file |
| 0x0A00 | (Windows only) Screenshot |
| 0x0B00 | Proxy |
| 0x1200 | (Windows only) Enumerate process, Netstat |

# Command Details

TEAMT5

| Command code | Description |
| --- | --- |
| 0x0900 | (Windows) execute a file |
| 0x0A00 | Screenshot |

Common


Monitor certain VPN tools Profiles

# Command Details

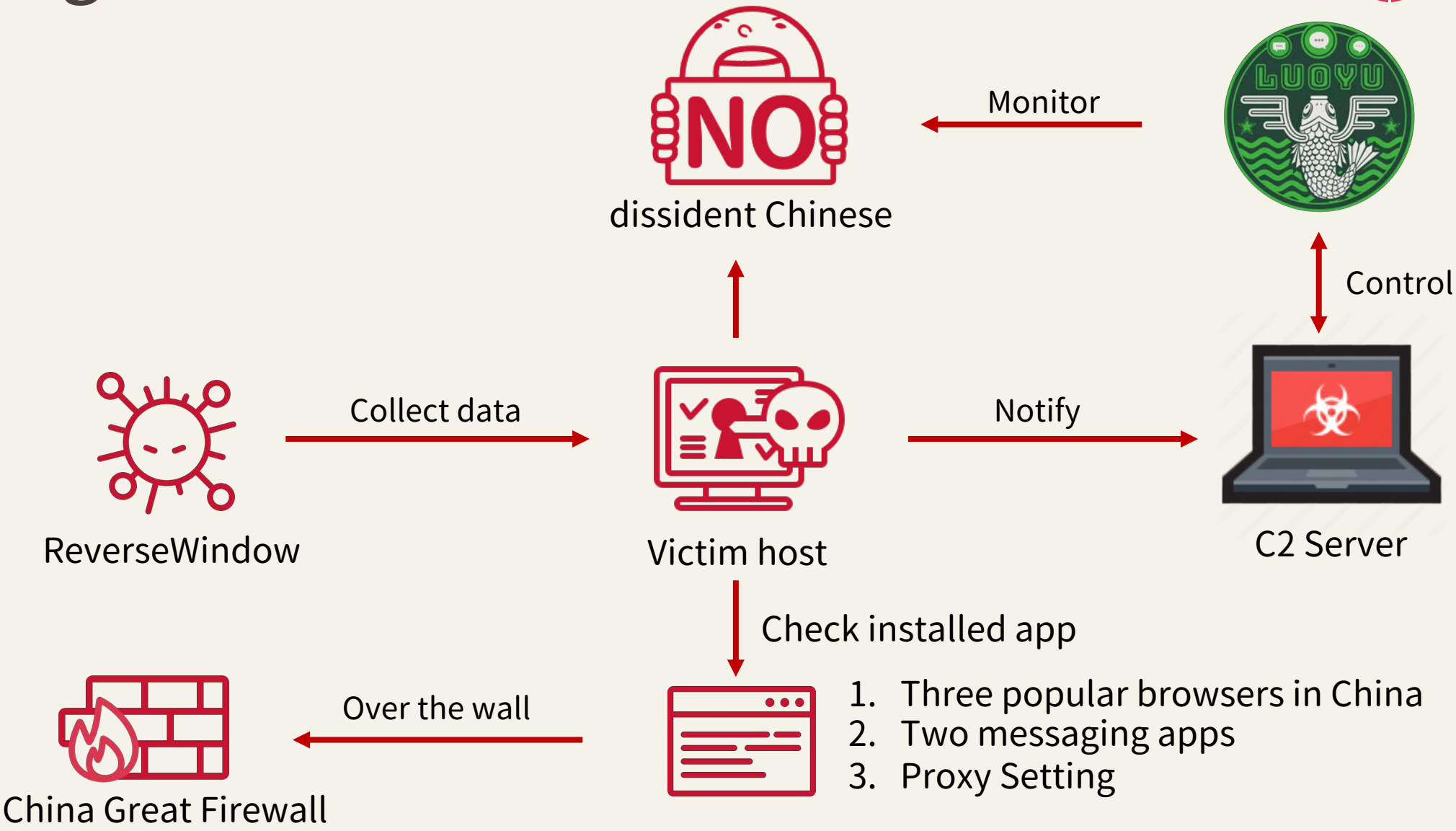
TEAMT5

Android

| Command code | Description |
| --- | --- |
| 0x0700 | setTransType |
| 0x0A00 | setCaptureScreen |
| 0x0F00 | setRecordConfig |
| 0x1000 | setSMSConfig |
| 0x1100 | setCallLogConfig |

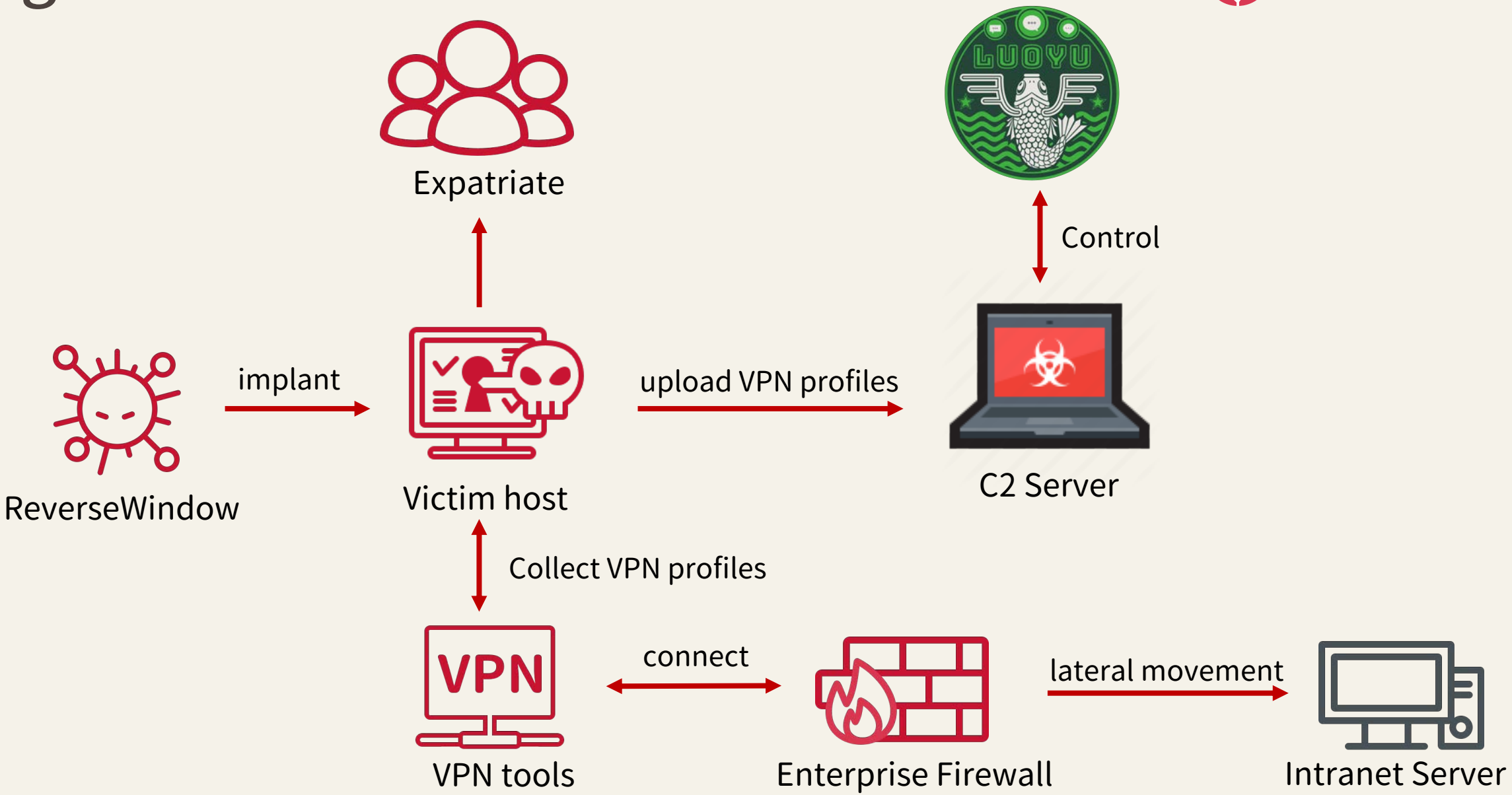
# Targeted attack

TEAMT5



# Targeted attack

TEAMT5



# Case Study

# Watering hole attack

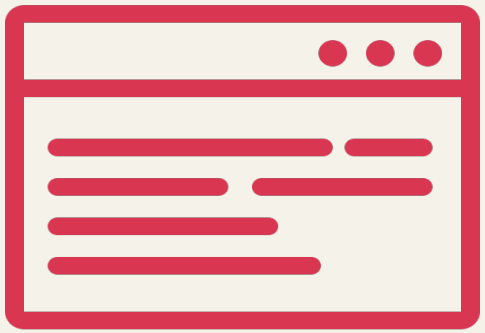
TEAMT5

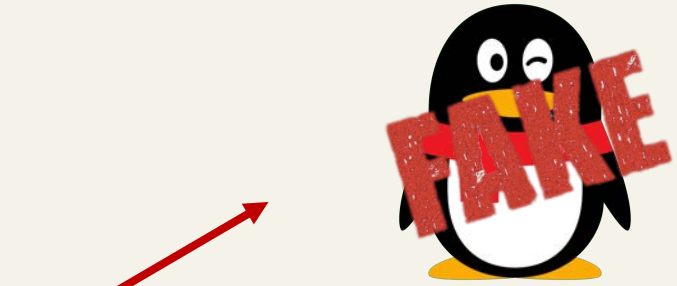
- Compromised a Chinese news site based in the US

# Watering hole attack

TEAMT5

- Malicious Files disguised as legitimate programs





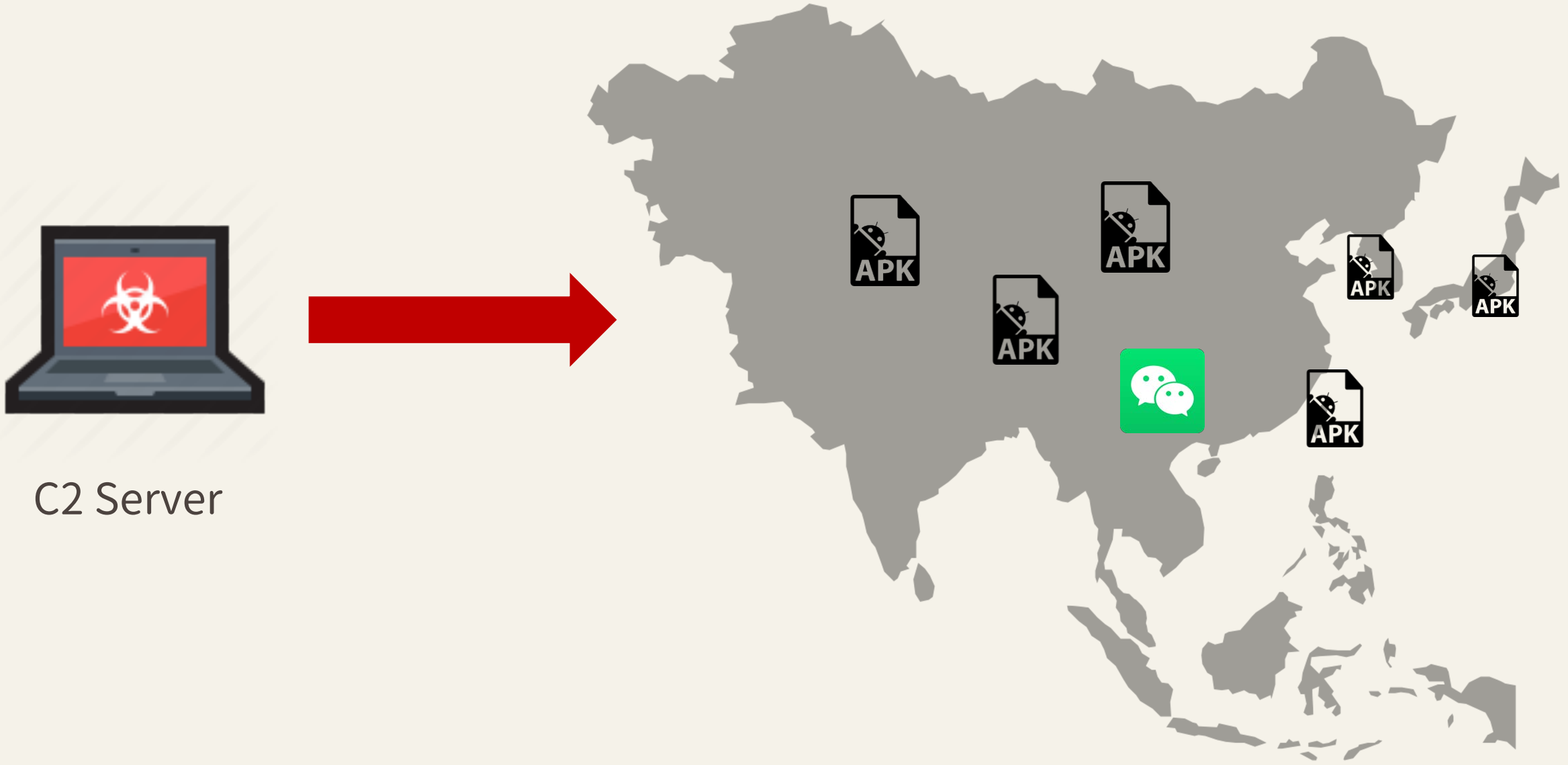

qq.exe


youku.exe

WinDealer

# More APKs found

TEAMT5

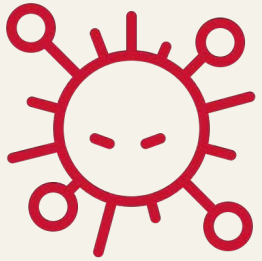



C2 Server

# IT company in East Asia

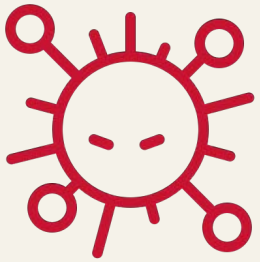
TEAMT5

2017



ReverseWindow
(MacOS ver.)

2019



ReverseWindow

# Messaging Apps Focused

TEAMT5

2015-2017

Android malware spying on Apps



2018

APK disguised as Wechat

2017&2019

Attack IT companies in East Asia

# Collecting information from messaging apps

TEAMT5

- The 2019 attack overlapped with Hong Kong anti-extradition bill protest

To collect protesters' information?

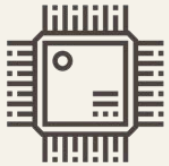
TEAMT5

## Before 2017

- Monitoring messaging apps of individual users


## After 2017

- Monitoring messaging apps of individual users
- Attack the IT company which develops apps for direct user information?



# Threat for both users and company

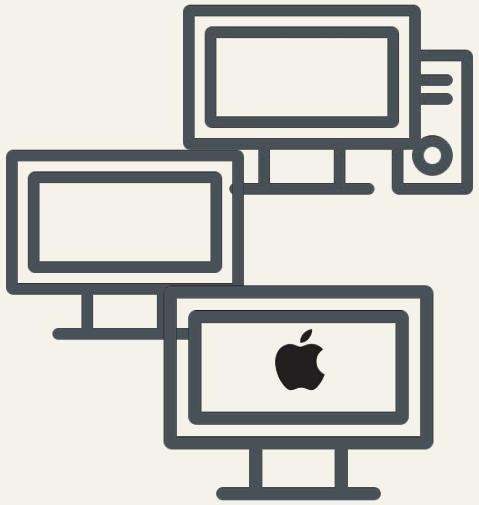
TEAMT5

Personal Mobile

Installed


ReverseWindow apk
&
SpyDealer

Collect personal messages

PCs in companies

Installed

ReverseWindow
(MacOS, Windows, Linux)

Collect user information

# Key Takeaway

# Key Takeaway

TEAMT5

- Luoyu is a well-developed Chinese APT.
- Its cyber attacks have started since 2014
  - Keep developing malware crossing multi-platform
  - Monitoring **expatriate** and **dissident**
- It has expanded its target scope.
  - China’s neighbor countries
  - Against **IT companies**

# THANK YOU!