“LuoYu”

The eavesdropper sneaking in multiple platforms

Leon & Shui
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

01 The Luoyu Threat Group Overview
02 Activity Timeline
03 ReverseWindow Analysis
04 Case Study
05 Key Takeaway
The Luoyu Group Overview
The name: 嬴魚 (Luoyu)

- 嬴魚(LuoYu) a Chinese mythological creature
- 嬴魚，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.
**Origin**
- China

**Malware**
- ReverseWindow
- WinDealer
- SpyDealer

**Target Industry**
- Technology
- Media
- Education

**Target Areas**
- China
- Hong Kong
- Japan
- Korea
- Taiwan
Goal

Attack

Message Apps

Collecting information from dissidents?

No
Activity Timeline
2014-2017 China focused

- Spying apps circulating in the wild
- Android malware spying on Apps
  - And more…
2017- now: Expand to East Asia

- Apr. 2017: IT company in Taiwan, Japan, and South Korea
- Jun. 2017: University in Hong Kong
- May. 2019: IT company in China
- 2019: Watering Hole Attack against Chinese Website
Malware profile: ReverseWindow
Malware profile: ReverseWindow

- 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

icularly researcher in Hong Kong

IT company in Taiwan, Japan, and South Korea

IT company in China

Discovery time in the wild (20+ samples)

- Apr. 2017: 1.1.6
- May. 2017: 1.2.1
- July. 2017: 1.2.27
- Jan. 2019: 0.997
- May. 2019: 1.3.3d
- Aug. 2019: 2.2.19102123
- Nov. 2019: 2.2.1905131
- Nov. 2019: 2.2.1911271
- Dec. 2020: 2.2.2006131

Android app

IT company in China

IT company in Taiwan, Japan, and South Korea

University researcher in Hong Kong

Discovery time in the wild (20+ samples)
In-Depth Analysis of ReverseWindow
Hide the malicious traces

- 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.

```bash
OSX
fwrite("This file is corrupted and cannot 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

ReverseWindow

Encrypted Malware Config

Config head signature (16 bytes)

Encrypted Config block

config size (2 Bytes)

AA BB CC DD

DES_ECB_decrypt

malware Configuration
Decrypt malware C&C configuration

- Test Sample C2:192.168.8.107:10443
Collecting host information

- 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

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

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

- Send Beacon
- ReverseWindow
- Send victim information
- Send command

Monitor directory

"%temp%\~victim_id\~tmpdata"

Upload any file(*.a) then delete

Windows platform only

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

1. Install Malicious APK
2. Load library ReverseWindow ELF
3. Decrypt config
4. Connect to C2
5. Collect sensitive data
6. Custom spying library

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

- 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
  - Stack string & GetProcessAddress to get WinAPI
- Windows 2.2.1905131: ReverseWindow interest in two popular messaging app and three popular browsers in China (360SE, 360chrome, SougouExplorer)
- Windows 2.2.2006131: Support networking status
<table>
<thead>
<tr>
<th>Command code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0200</td>
<td>File Operations</td>
</tr>
<tr>
<td>0x0300</td>
<td>Shell Command</td>
</tr>
<tr>
<td>0x0400</td>
<td>update RAT</td>
</tr>
<tr>
<td>0x0500</td>
<td>Uninstall RAT</td>
</tr>
<tr>
<td>0x0800</td>
<td>Update malware Config</td>
</tr>
</tbody>
</table>
# Command Details

<table>
<thead>
<tr>
<th>Command code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0900</td>
<td>(Linux) install plug-in</td>
</tr>
<tr>
<td>0x0A00</td>
<td>(Windows only) Screenshot</td>
</tr>
<tr>
<td>0x0B00</td>
<td>Proxy</td>
</tr>
<tr>
<td>0x1200</td>
<td>(Windows only) Enumerate process, Netstat</td>
</tr>
</tbody>
</table>
## Command Details

<table>
<thead>
<tr>
<th>Command code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0900</td>
<td>(Windows) execute a file</td>
</tr>
<tr>
<td>0x0A00</td>
<td>Screenshot</td>
</tr>
</tbody>
</table>

Monitor certain VPN tools Profiles

expatriate
dissident
## Command Details

<table>
<thead>
<tr>
<th>Command code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0700</td>
<td>setTransType</td>
</tr>
<tr>
<td>0x0A00</td>
<td>setCaptureScreen</td>
</tr>
<tr>
<td>0x0F00</td>
<td>setRecordConfig</td>
</tr>
<tr>
<td>0x1000</td>
<td>setSMSConfig</td>
</tr>
<tr>
<td>0x1100</td>
<td>setCallLogConfig</td>
</tr>
</tbody>
</table>
Targeted attack

1. Three popular browsers in China
2. Two messaging apps
3. Proxy Setting
Targeted attack

ReverseWindow → implant → Victim host

Victim host → Collect VPN profiles

VPN tools → connect → Enterprise Firewall

 VPN

C2 Server

Control

Intranet Server

lateral movement
Case Study
Compromised a Chinese news site based in the US
Watering hole attack

- Malicious Files disguised as legitimate programs

qq.exe

youku.exe

WinDealer
More APKs found

C2 Server
IT company in East Asia

2017

ReverseWindow (MacOS ver.)

2019

ReverseWindow
Messaging Apps Focused

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

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

To collect protesters' information?
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

Personal Mobile

Installation

ReverseWindow apk & SpyDealer
Collect personal messages

PCs in companies

Installation

ReverseWindow (MacOS, Windows, Linux)
Collect user information
Key Takeaway
Key Takeaway

- 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!