APT41 新生子群？剖析新生代中國 APT 族群「天吳」針對亞太地區的最新行動

APT41's New Subgroup? Dissecting Chinese APT "Tianwu" Latest Operations in the APAC Region

Silvia Yeh / Leon Chang

TEAMT5
Persistent Cyber Threat Hunters

Speaker

Silvia Yeh

- Threat Intelligence Analyst
- OSINT, APT, InfoOps in APAC
- 2022 Black Hat Asia, 2022 SANS CTI Summit, 2021 CODE BLUE, 2021 HITCON Pacific, etc.

Leon Chang

- Threat Intelligence Researcher
- Reverse engineering, APT campaign tracking in APAC, IoT security
- 2022 Black Hat Asia, 2022 JSAC, 2021 JSAC

Outline

1. Intro: Modular shared tools among Chinese APTs
2. Anatomy of Pangolin8RAT
3. APT Tianwu: Activity Timeline, Target, Attribution
4. Conclusion and outlook

1. Background Information

PlugX, ShadowPad, and modular tools shared among Chinese APTs

PlugX

- First Seen: 2008
- A RAT with modular plugins
- Used by many Chinese APT groups:
  - Amoeba/APT41, APT27, DragonOK, Polaris, menuPass, LuoYu, and more…
- “PlugX” → plugin and malware module features
- Various PlugX variants
  (Some have other communication protocols, including P2P and DNS Tunneling.)

ShadowPad

- First Seen: 2015
- A RAT with modular plugins
- Used by many Chinese APT groups (respectively limited):
  - Amoeba/APT41, Fishmaster, Sanyo,
    LuoYu, Naikon, more…
- Its functions are provided by interchangeable modules
- Protected by layers of encryption and heavy obfuscation
- The modular design resembles PlugX

Related malware families

- PlugX
- ShadowPad
- Pangolin8RAT
- FFRAT
- KeyPlug
- Winnti 2.0
- FunnySwitch
- Natwalk (Sidewalk)
- Crosswalk
- …

Amoeba, Fishmaster, and Tianwu

Tianwu Profile

Origin

Tools

Pangolin8RAT, custom Cobalt Strike Beacon

TTPs

- Phishing, planting backdoor in NAS server
- C2: typosquatting, VPS, possible abuse of Log4J
- Exploit: CVE-2022-24934, possible Chromium exploit
- Possible supply chain attack

Target Region

Target Industry

Gambling, IT, Telecom, Gov, Transport, Dissident, Logistics

2. Anatomy of Pangolin8RAT

Pangolin8RAT’s evolution and its similarities with other malware families

Malware Profile: Pangolin8RAT

Category	Description
Type	Modular backdoor
Naming	The PDB string contains “pangolin” and its RTTI contains “p8rat”
First seen	2019/11
Function	supported 8 communication protocols, including TCP, HTTPS, UDP, DNS, ICMP, HTTPSIPV6, WEB, and SSH
Target industry	Online gaming, gambling, IT, Telecom, Transportation, Gov, Dissident
Linked APT	Tianwu

Naming

The PDB string

- Z:\Disk\pangolin_reload\Release\core\ldr\Mfcldrx64.pdb
- D:\PangolinRev\Release\core\LiteCorex64.pdb
- D:\PangolinRev\Release\core\corex64.pdb

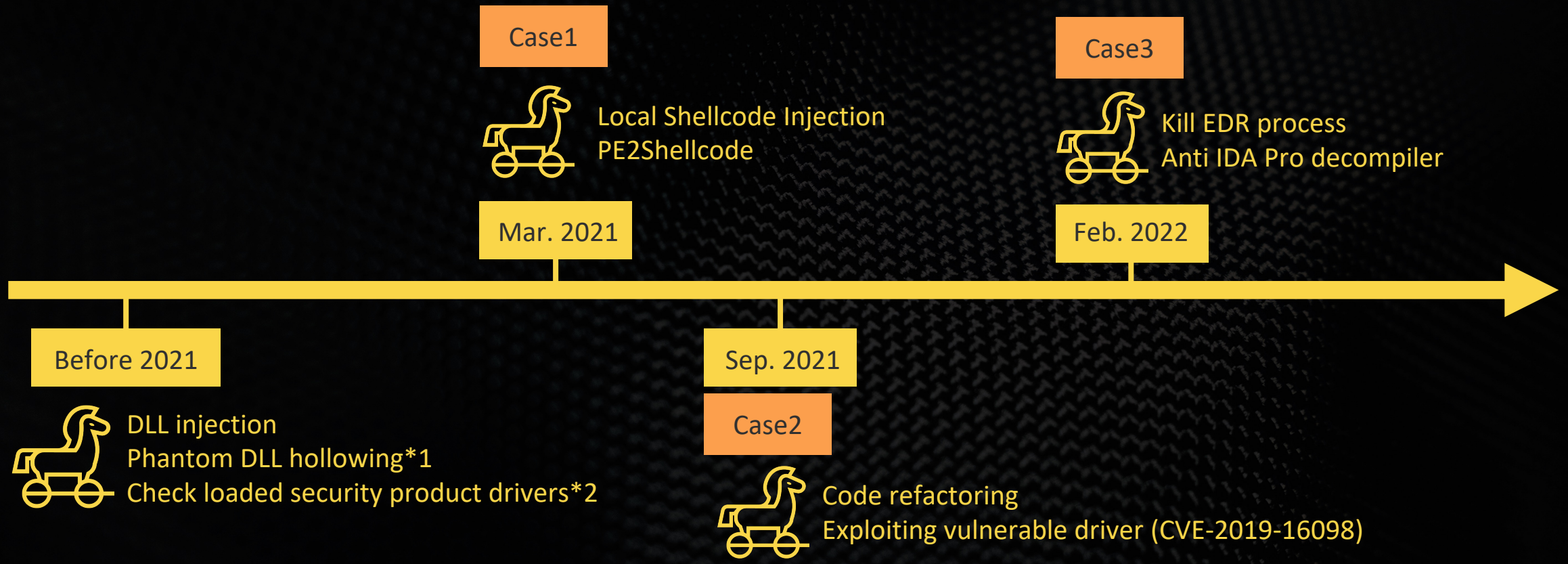
The RTTI

- P8RatCore
- P8CorePluginManager

In-Depth Analysis of Pangolin8RAT

- The evolution of Pangolin8RAT
- The code similarity with FFRAT and Winnti 2.0
- TTPs overlap with Amoeba group malware family

The evolution of Pangolin8RAT – Timeline



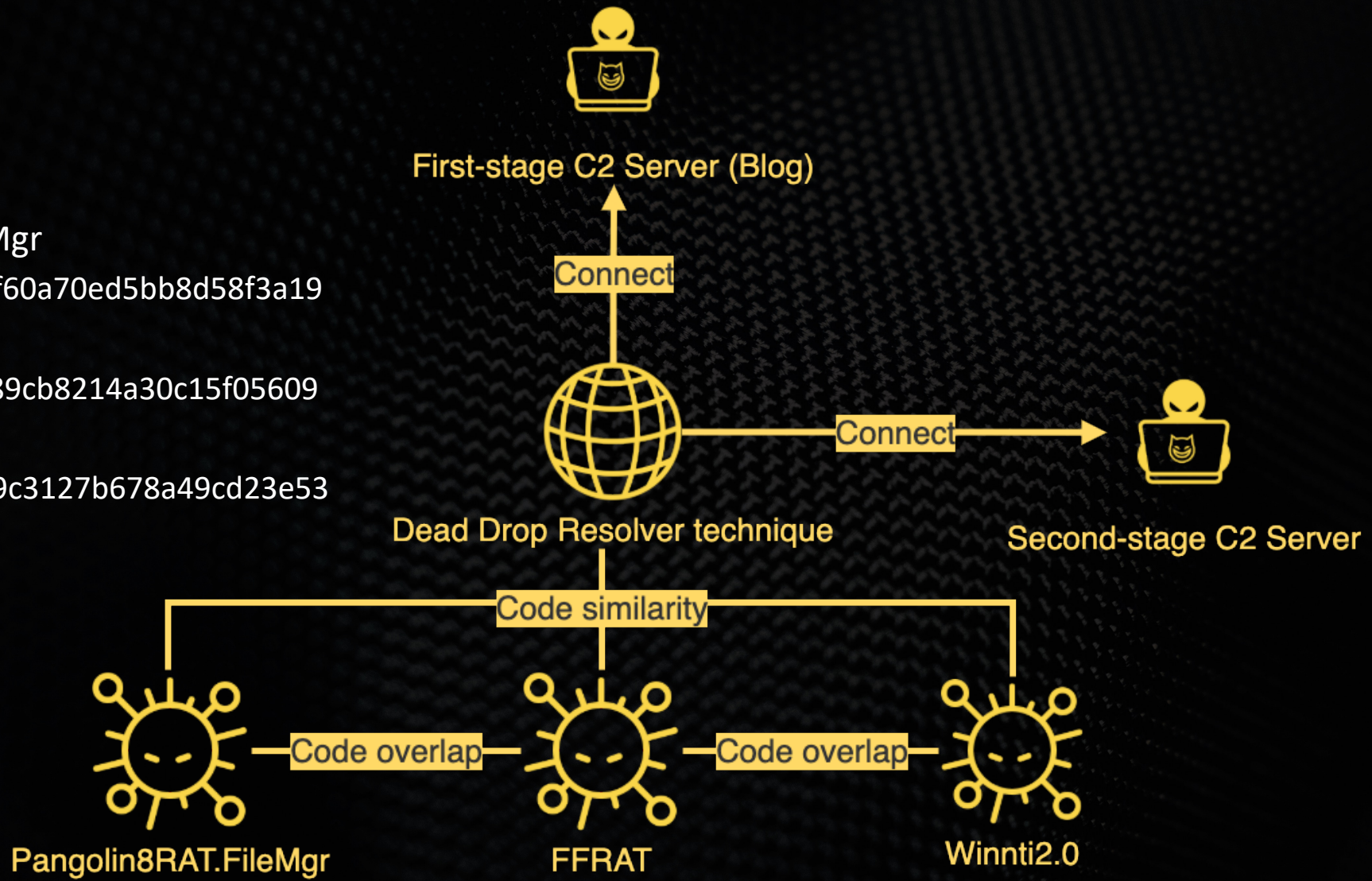
The timeline of TTPs used by Pangolin8RAT

*1: https://github.com/forrest-orr/phantom-dll-hollower-poc
*2: https://gist.github.com/jthuraisamy/4c4c751df09f83d3620013f5d370d3b9

Code similarity with FFRAT and Winnti 2.0

Sample MD5 hash

- Pangolin8RAT.FileMgr
  - 0879125ed34df60a70ed5bb8d58f3a19
- FFRAT
  - 1962a69c204289cb8214a30c15f05609
- Winnti 2.0
  - 5778178a1b259c3127b678a49cd23e53



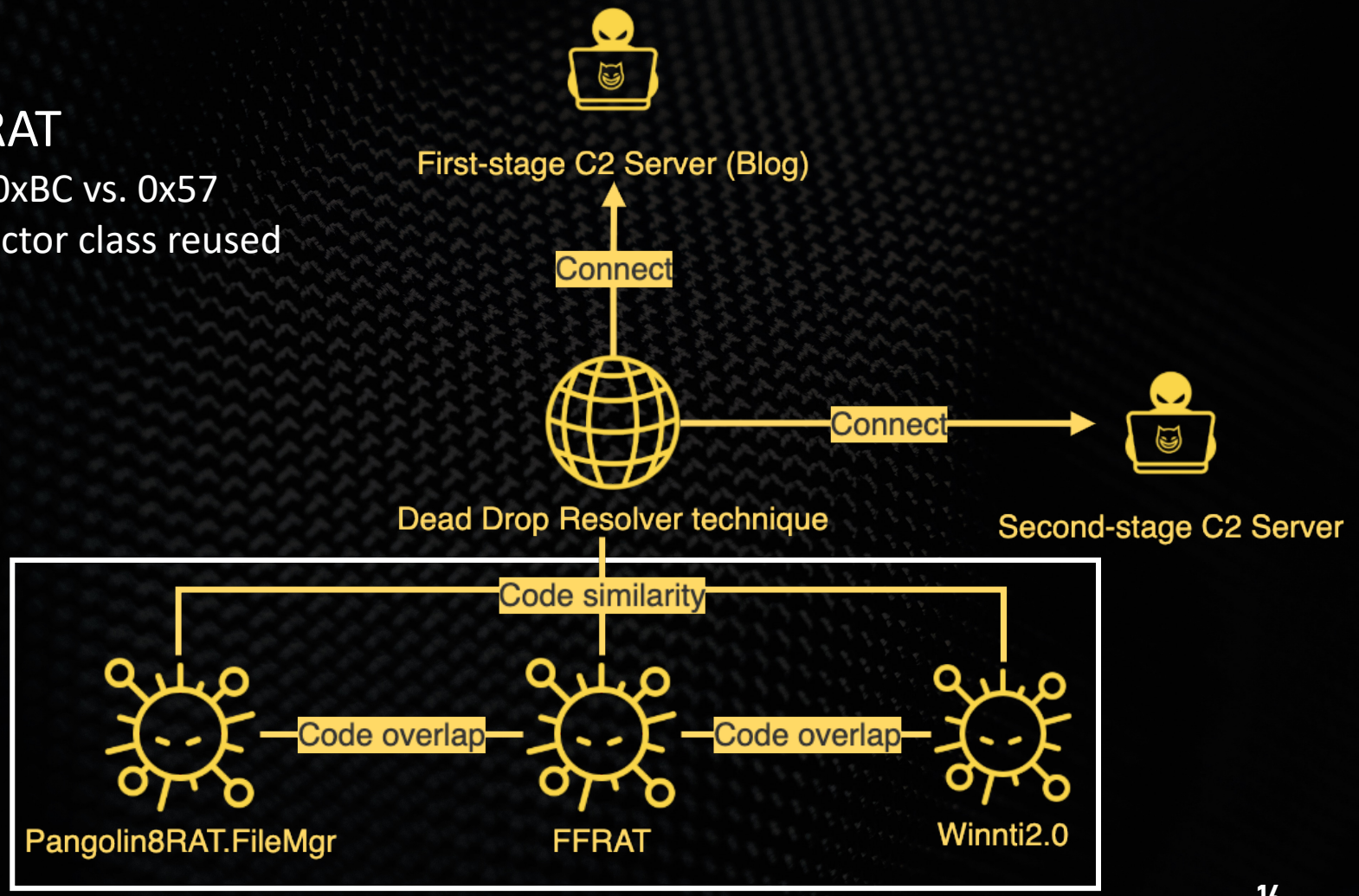
Code similarity with FFRAT and Winnti 2.0

Code overlap/reuse

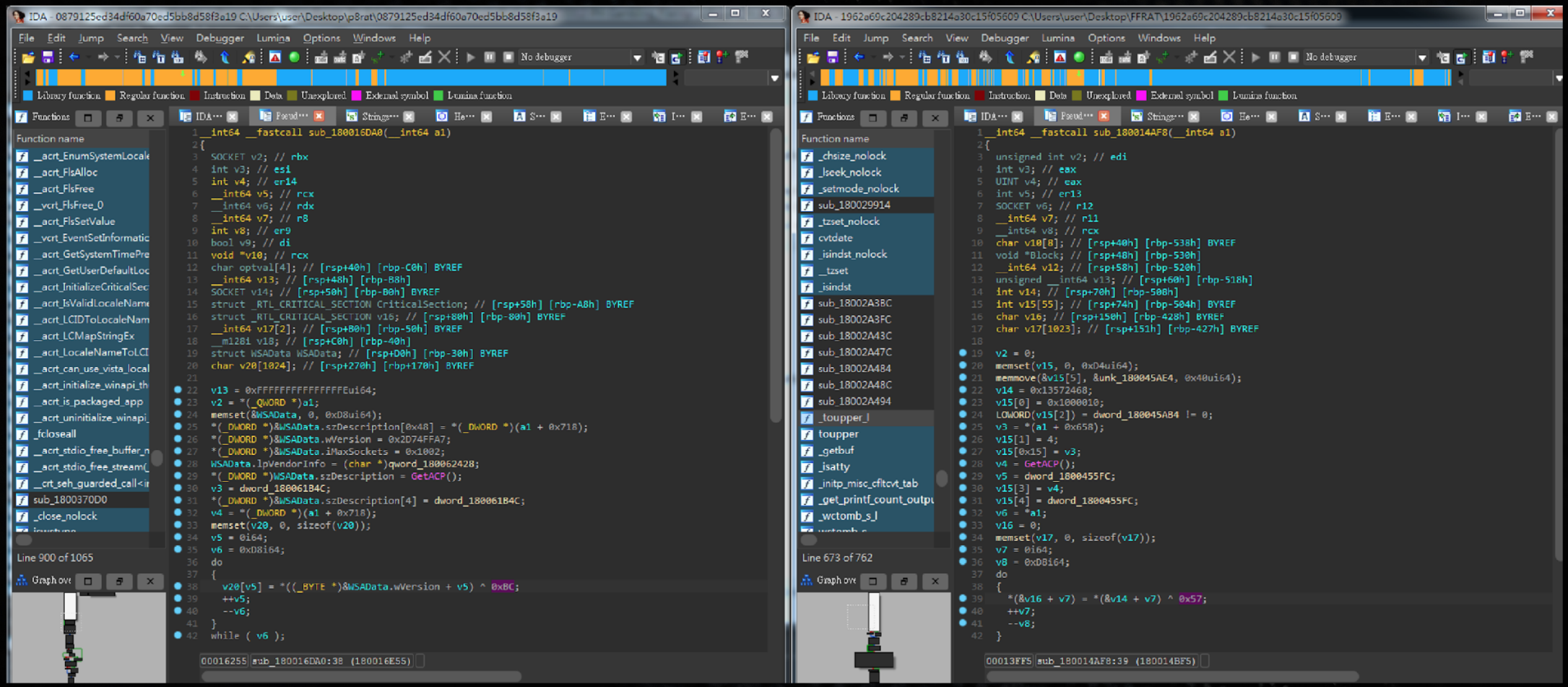
1. Pangolin8RAT.FileMgr vs. FFRAT
   - Code overlap just change XOR key: 0xBC vs. 0x57
   - Same debug string and proxy connector class reused

```
.?AVsocks4a_connector@@
.?AVconnector@@
.?AVsocks4_connector@@
.?AVhttp_tunnel_ntlm@@
.?AVhttp_connect_ntlm@@
.?AVhttp_proxy_connector@@
.?AVsocks5_connector@@
```

2. FFRAT vs. Winnti 2.0
   - Same debug string
     - "m_ServerComplete Continue\n"
     - "SrvCode", "DrvCode"



Code similarity with FFRAT and Winnti 2.0



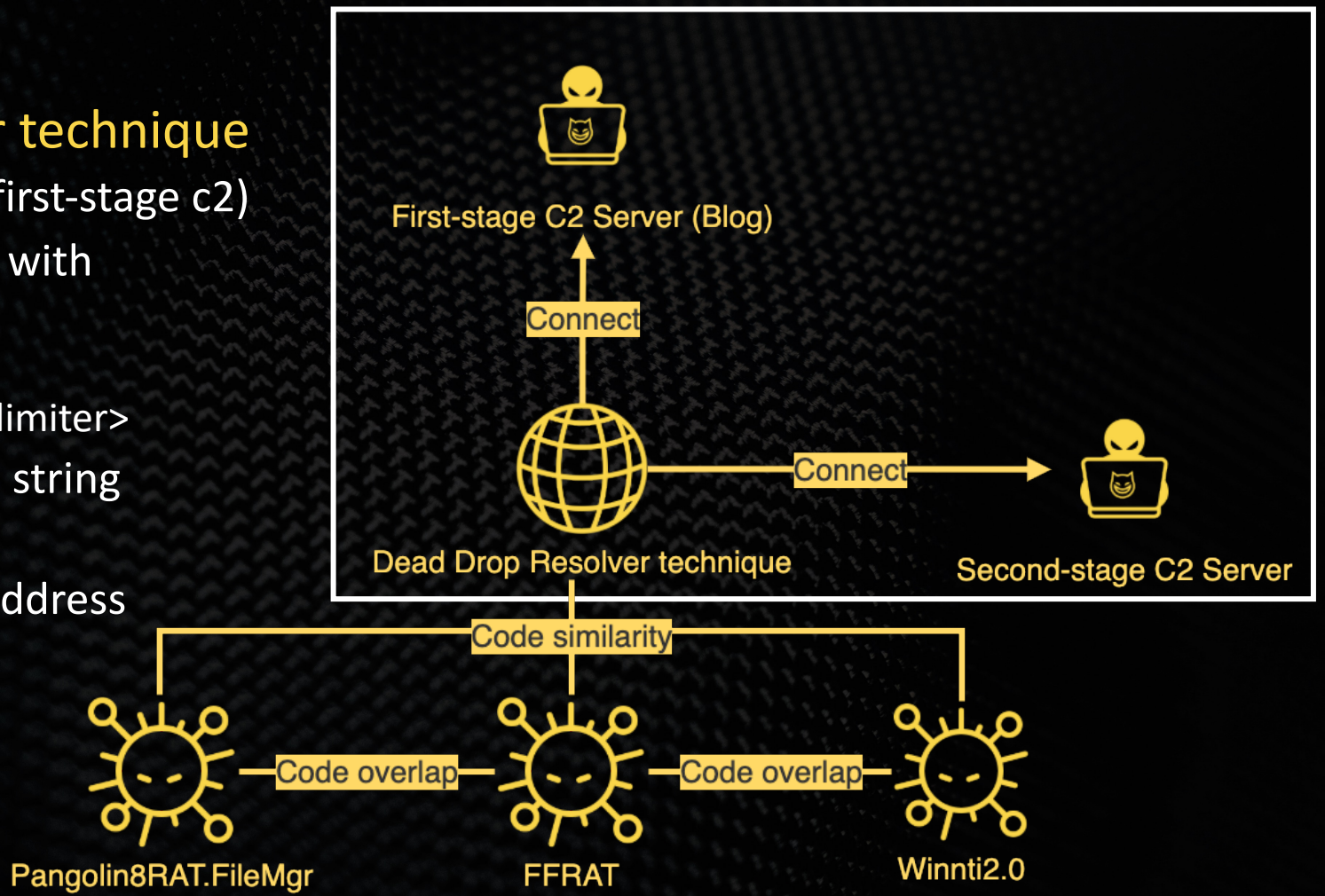
Pangolin8RAT.FileMgr vs. FFRAT

Code overlap just change XOR key: 0xBC vs. 0x57

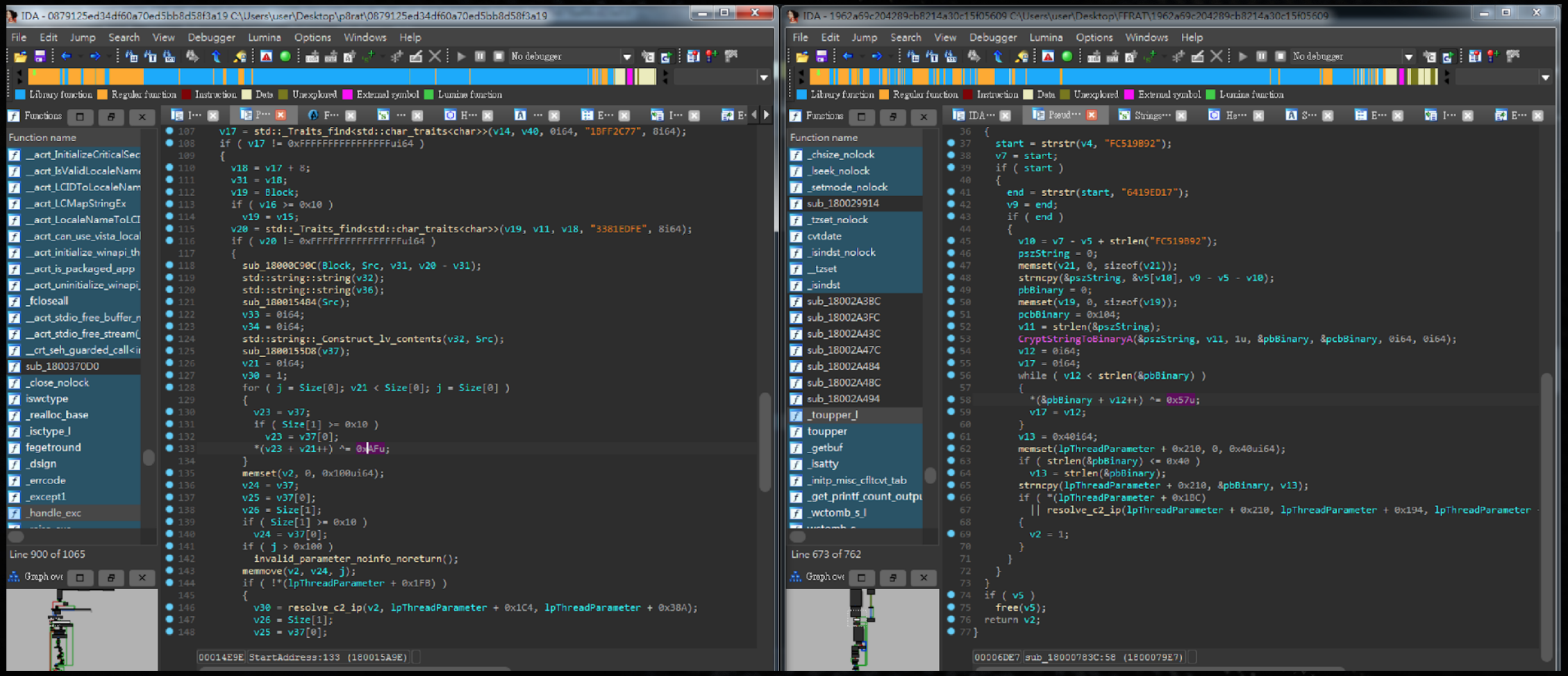
Code similarity with FFRAT and Winnti 2.0

Code similarity - Dead Drop Resolver technique

- Step1: Get response from web server (first-stage c2)
- Step2: Parse encrypted/encoded string with hardcoded delimiters
  - Format: <start_delimiter>binary_data<end_delimiter>
- Step3: covert data to bytes and decode string
  - C2 Format: ”<ipv4 or domain>:<port>”
- Step4: resolve the second-stage C2 ip address



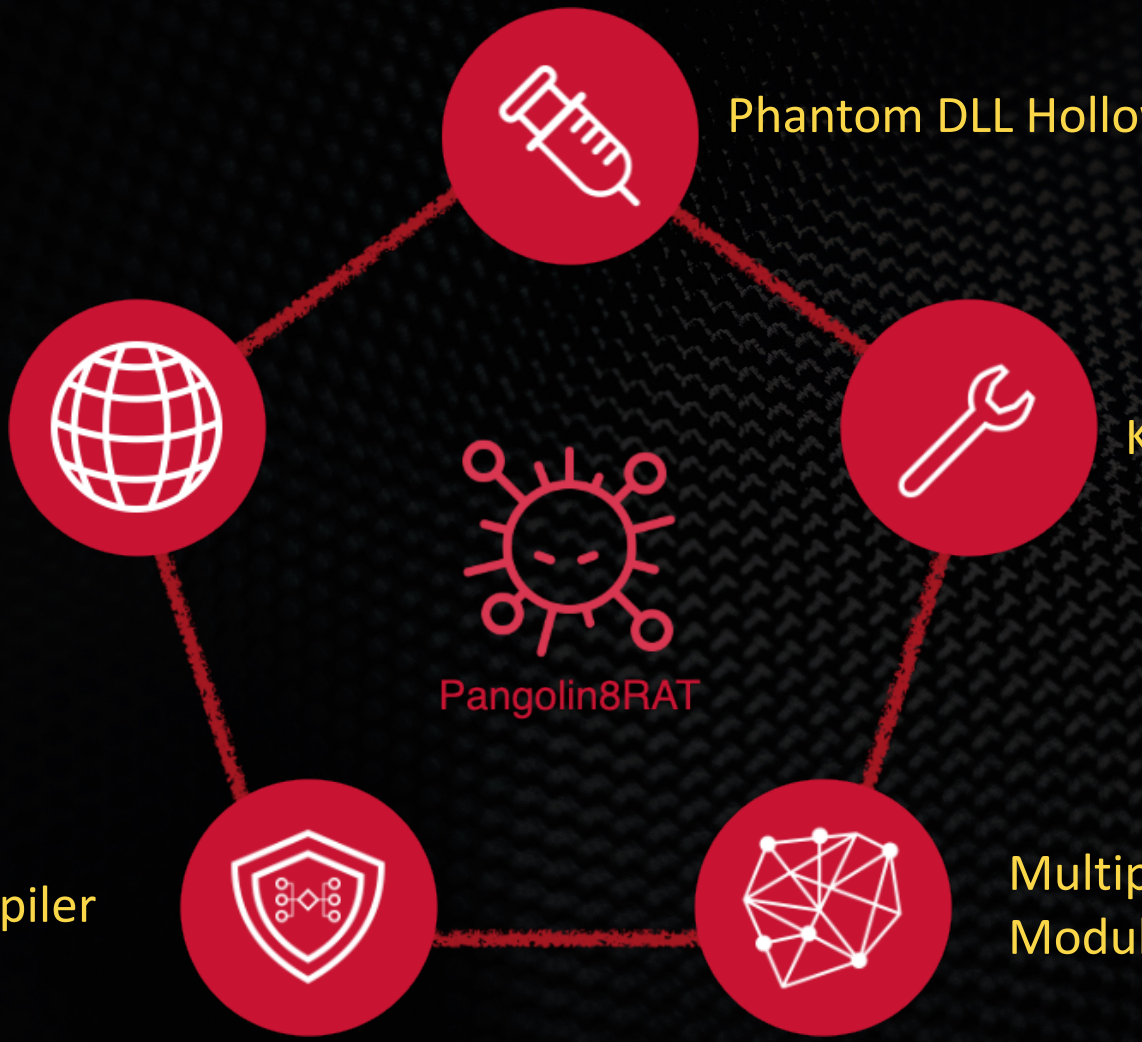
Code similarity with FFRAT and Winnti 2.0



Pangolin8RAT.FileMgr vs. FFRAT

Different hardcoded delimiters and XOR key: 0xAF vs. 0x57

TTPs overlap with Amoeba malware family



TTPs overlap with Amoeba malware family

Phantom DLL hollowing

- ChatLoader[2] (aka. StealthVector)

Dead Drop Resolver

- Natwalk[2] (aka. Sidewalk[5], ScrambleCross[9])
  - Natwalk is one of the backdoors loaded by the ChatLoader
- KeyPlug[4] (tech community forums)
- ShadowPad (MSDN forums, github), PlugX(MSDN forums, pastebin)
- Winnti[13] (MSDN forums), FFRAT
- 9002 RAT

Anti IDA Pro decompiler

- The linux variant of Natwalk
  - Specter botnet[3] is the predecessor of Natwalk.linux

TTPs overlap with Amoeba malware family

KCP Protocol

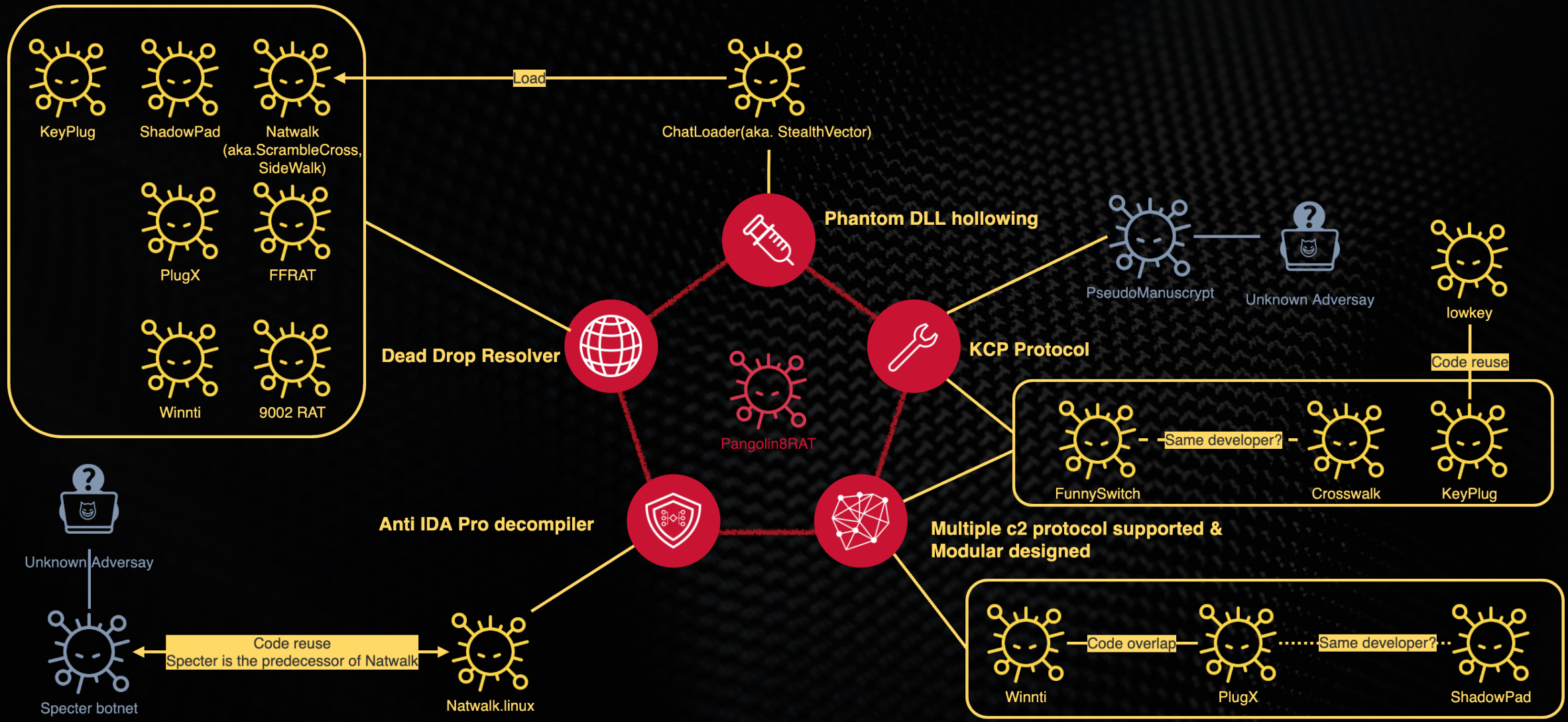
- KeyPlug
- FunnySwitch[6]
- Crosswalk[6] [7]
- PseudoManuscrypt[8](unknown adversary)

Multiple c2 protocol supported & Modular designed

- KeyPlug (HTTP, KCP, TCP, WSS)
- Crosswalk (TCP, HTTP, KCP)
- FunySwitch (RPC, TCP, HTTP)
- Winnti (ICMP, UDP, TCP, Reuse port)
- PlugX[7] (DNS, ICMP, HTTP, TCP, UDP), ShadowPad[7](TCP, UDP, HTTP, DNS)


Liar: 跟APT41有關的後門
實際上與APT41有關的報告

TTPs overlap with Amoeba malware family



TTPs overlap with Amoeba malware family

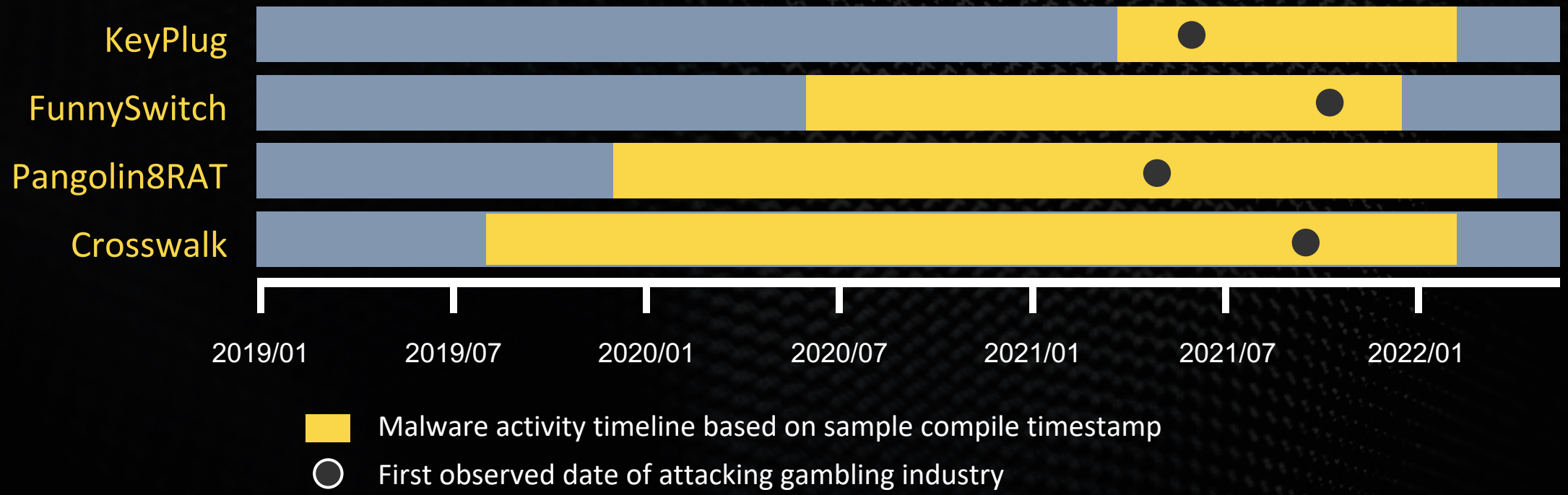
Targets online gaming/gambling industry

- Natwalk, Crosswalk, FunnySwitch, Spyder
- ShadowPad, Winnti, PlugX
- KeyPlug

CobaltStrike technique

- Abusing Cloudflare Workers to hide the real IP address
- Modify XOR-key
- Early bird code injection

The timeline of malware family with KCP Protocol



The New Era of Chinese APT analysis?

- Increasing intricacy of malware families
- Increasing tendency of malware sharing

Malware-as-a-Service among APT groups?

3. Tianwu

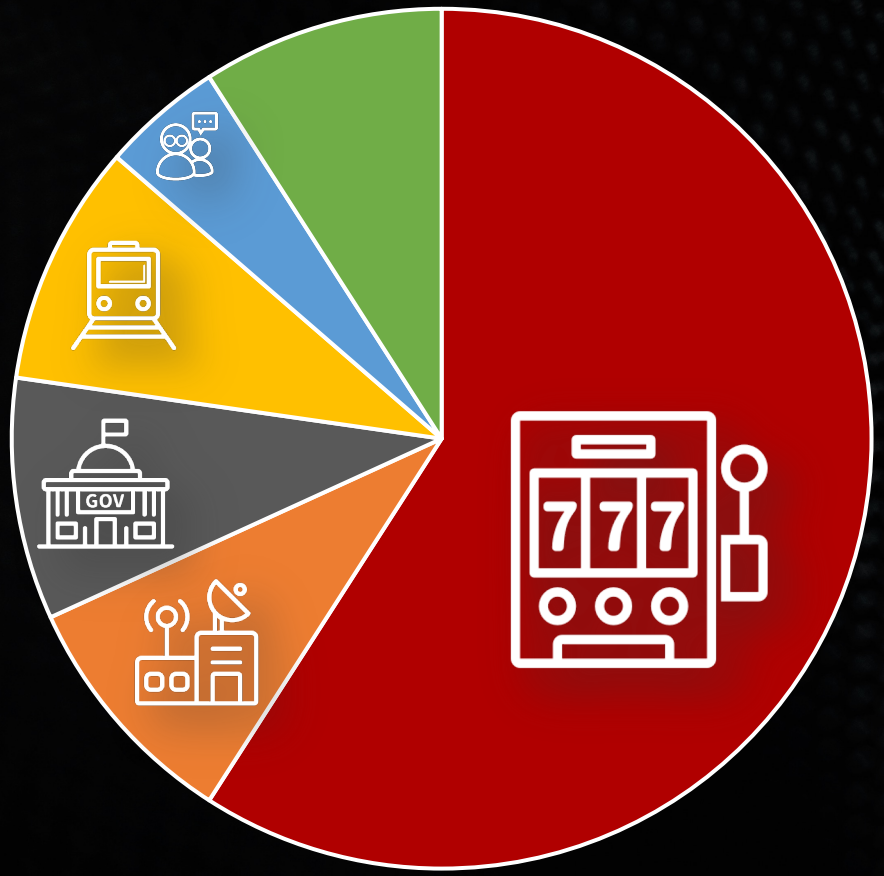
TTPs, Activity Timeline, Target, Attribution

Tianwu (天吳)

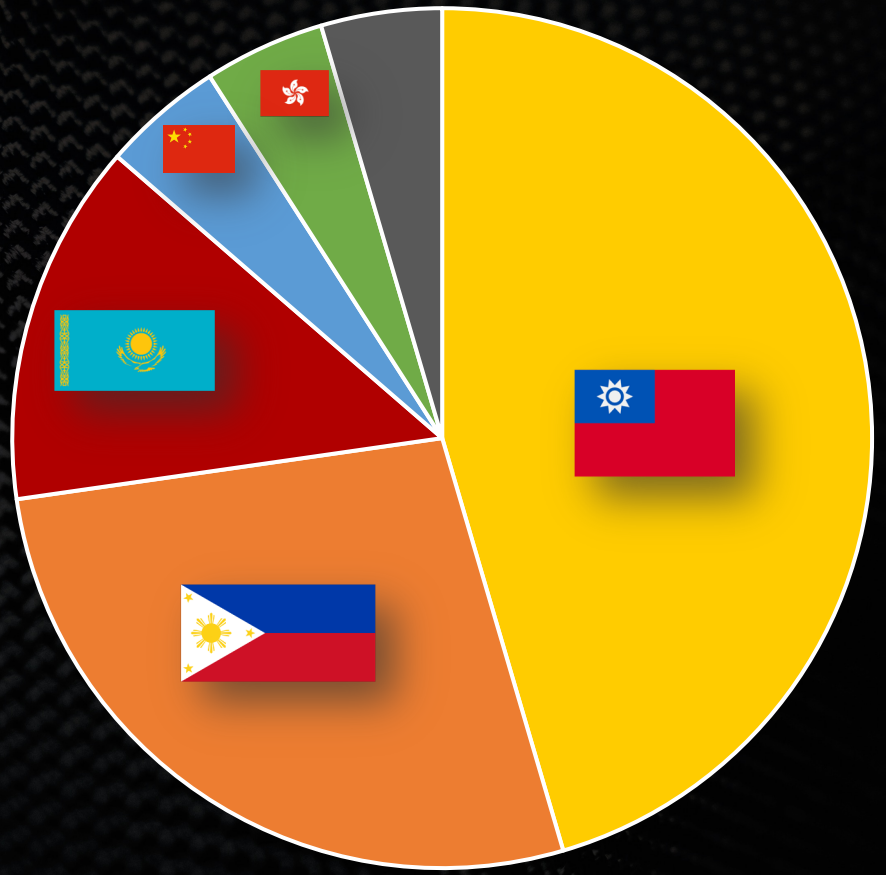
- A beast with 8 human heads, 8 feet and 8 tails
  - Modular features of Pangolin8RAT
  - Amalgamation of different groups of actors
- The Classic of Mountains and Seas (山海經)

Target Industry and Region

Target Industry

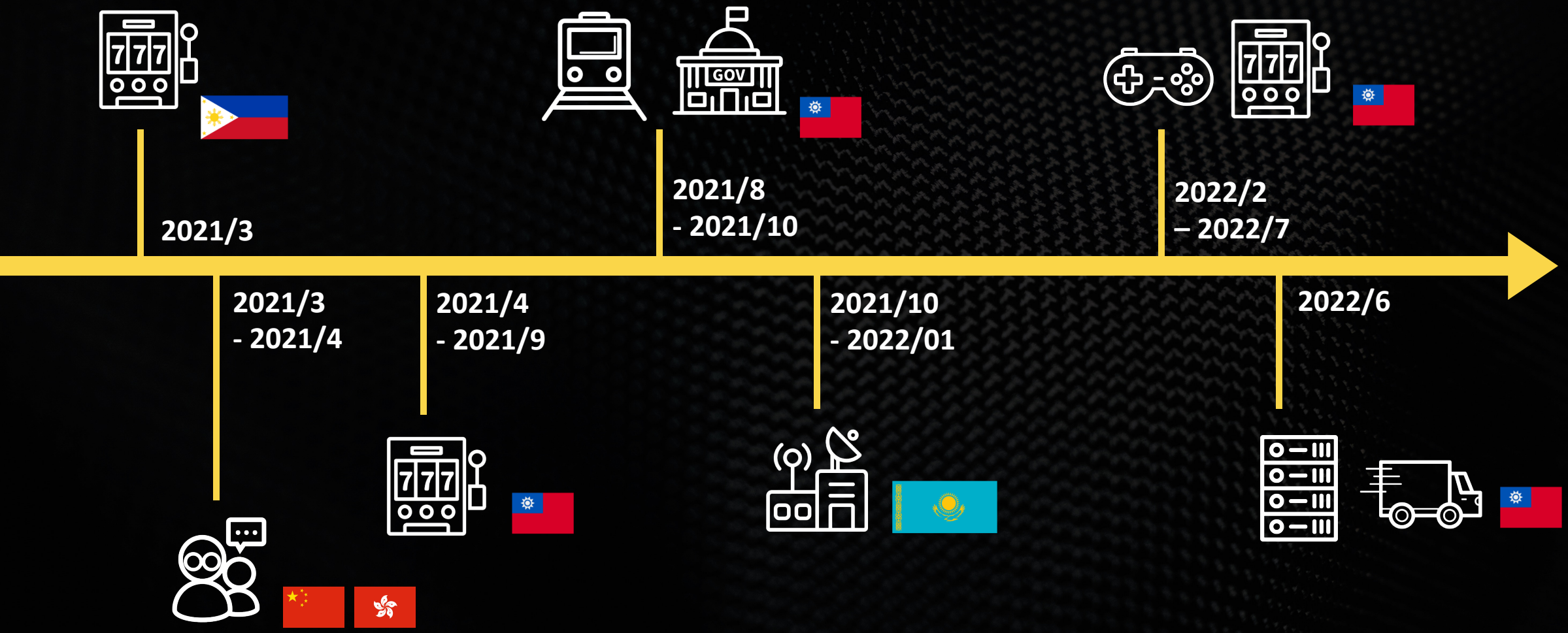


Target Region



Gambling Telecom Government Transport Dissident Other Taiwan The Philippines Kazahstan China Hong Kong Other

Activity Timeline



Case Study:
Months-long campaign against KZ Telecom

Victim

- Kazakhstan telecom

First attack spotted in 2021/10,
latest attack spotted in 2022/01

Tools

- Pangolin8RAT
- CobaltStrike Beacon with specific watermark

C2

- C2 domain disguised as the victim's domain
- VPS provided by Leaseweb

Case Study:
Campaign against TW gambling/gaming firms

Victim

- Taiwanese gambling/gaming firms

First attack spotted in 2021/04,
latest attack spotted in 2022/07

Tools

- Pangolin8RAT
- Cobalt Strike Beacon with specific watermark
- Hacking tool
  - Attempts to collect info of victims' browser and messaging software

Case Study: Campaign against TW gambling/gaming firms (cont.)

Victim

- Taiwanese gambling/gaming firms

First attack spotted in 2021/04, latest attack spotted in 2022/07

Possible Supply Chain Attack

- Attacks against software and services used in online gambling/gaming services

Case Study:
Attack against TW transport industry

Victim

- Taiwanese public transport-related firm

Time: 2021/08

Tools

- Pangolin8RAT
- 8 C2 configs were populated in the RAT

C2

- Disguised as the enterprise management software used by the victim
- C2 infra also used in attack against PH gambling firms

Case Study:
Campaign against Chinese-speaking dissident

Victim

- Chinese-speaking dissident

Time: 2021/03-2021/04

Delivery

- Phishing via Forum
- Disguised as TW IT Company

"How to put ads on abuoluowang.com"

Case Study: Campaign against Chinese-speaking dissident (cont.)

Exploit

- Possible Chromium exploit targeting Chromium-based browser users
  - eg: QQ browser

Tools

- Malicious WeChat CRX (Chrome extension)
  - Pangolin8RAT
  - CobaltStrike

Tianwu and Amoeba overlaps

- Delivery Method
  - Forum phishing, planting backdoor in NAS devices
- Malware feature
  - KCP protocol
  - Utilization of multiple C2 protocols
  - Phantom DLL hollowing
- C2
  - Abusing Cloudflare Workers to hide the real IP address
- Target Scope
  - Interests in online gaming/gambling industry

Attribution: Another Amoeba?

Possible scenarios:

Amalgamation of civilian hackers

- Operation mode like Chengdu404
- Operate bid projects of the national/public security agencies
- Motive: espionage, domestic surveillance

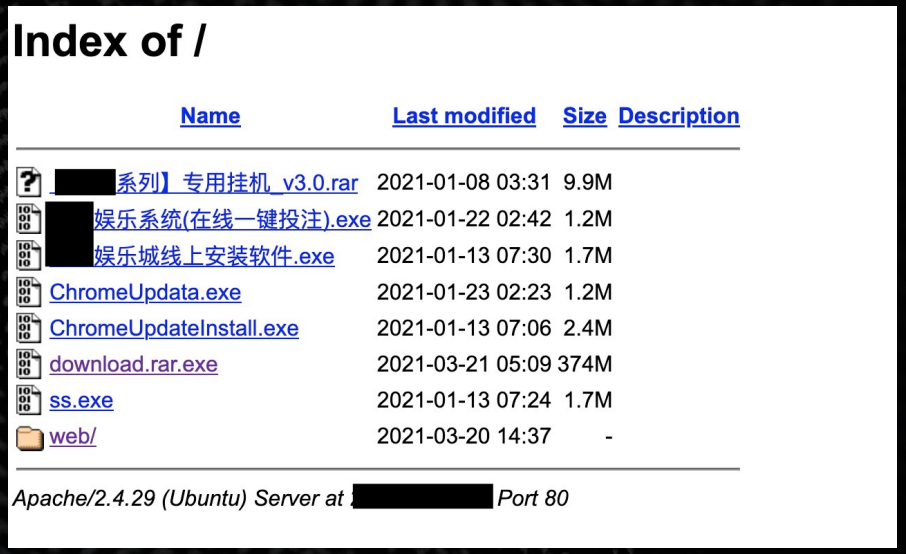
Subgroup of Amoeba

- No shared infra and tools detected so far

Open Directory

Information collected

- Staffs and operators’ personal info
- Credentials
- Software source code
- Business info



Threat Landscape: New APT Operation Mode

Difficulty of pinning down actors' motive
- Target scope spans different industry
- Espionage operations outsourced by MSS/MPS?

Chinese authorities' crackdown on online gaming/gambling industry
- Abundant money and data (personal info and cash flow)
- Data collection for authorities' crackdown campaign

Civilian hacker/front company aiming for personal gain
- Participation in cybercrime
- Software source code for sale in underground market

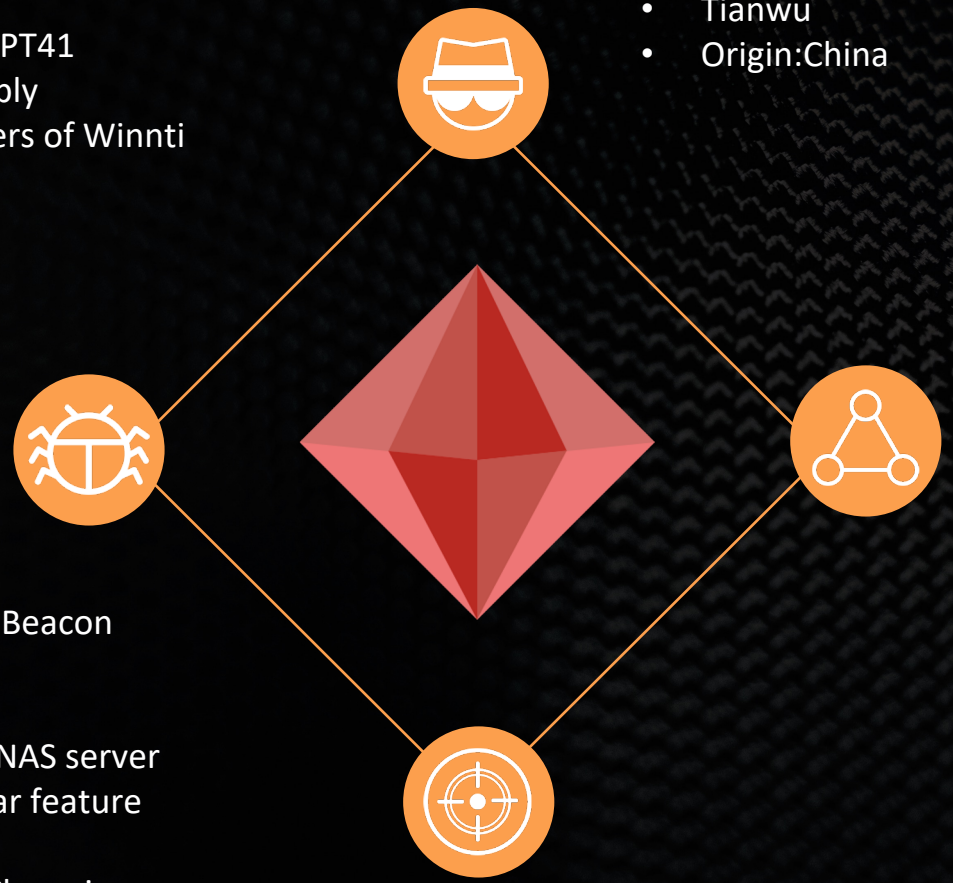
Tianwu's Operations in Diamond Model

Technical Axis

- Tools and TTPs resemble APT41
- Proprietary malware possibly developed by the developers of Winnti and FFRAT

Adversary

- Tianwu
- Origin:China



Social-Political Axis

- China's crackdown on its domestic gaming industry
  - Data collection of service providers
- China's crackdown on Macau gambling industry forced gambler move online
  - Data collection of gamblers and cash flow

Capability

Tools:
- Pangolin8RAT
- Custom Cobalt Strike Beacon

TTPs:
- Social Engineering
- Planting backdoor in NAS server
- Malware with modular feature and KCP protocol
- Exploit: WPS Office, Chromium

Infrastructure

- C2 disguised as legitimate websites
- C2 hosted on VPS
- Abused Cloudflare Workers to hide the real IP address
- Recent C2 activity indicated possible abuse of Log4j

Victim

- Geography: Taiwan, the Philippines, Kazakhstan, Hong Kong, China
- Industry: Gambling, gaming, IT, telecom, gov, transport, dissident

4. Conclusion

Outlook and suggestions

Conclusion and Outlook

Pangolin8RAT could be the next gen PlugX/ShadowPad

- Modular-featured RATs become more popular
- Highly possible to be shared or even sold among Chinese threat groups
- Both espionage and financially driven operations

Conclusion and Outlook

New mode of APT operations

- Trends of malware sharing
- Malware with similar structure and techniques
- Malware-as-a-Service among APT groups

Tianwu might operate as:
a collaborator of APT41, a subgroup of APT41, or
a digital quartermaster of Chinese APTs

Countermeasures

Defend your organization with all-level Intelligence

- Tactical
  - Feed CTI vendor’s IoCs to cybersecurity infra
- Operational
  - Patch servers in timely manner
  - Beware of new social engineering tactics
  - Apply in-memory detection
- Strategic
  - New operation mode of Chinese APTs makes attribution/group tracking more difficult
  - China’s policies/crackdown heavily affects cyberspace in APAC region

IoC

Pangolin8RAT

- 0f44724d498f77a59bc542be7d17dc89
- 47b3627c3900e29bdef6d36cfdf61bbf
- ea76ad28a3916f52a748a4f475700987
- cfae9252291fdf63f0c3d485a162a444
- bfa657d3eca9df2b122d0908ac23c1ed
- 4fb9b38e9c4b3c98b6f13c153bbe6f6a
- bf421d42174edb2f31007cbede9cf5b9
- 8b6a63e522fd6b3f23f476a101720bf9
- ea2e29b351d4e07460e5955b8e1b4d5d
- 641d23463a53bcb29673d179379e1a8f
- 81d9be954a09774887eb75b5a23db9b4
- 9c4df895509a8906a09be0b19bf5c05a

CobaltStrike

- 3e08c0e69fc1bbd36b2bb09086fd30ad
- c4e31051dc80d87927d15d0fbed704d0
- 544a7746c8769866574452082055175O

IoC

- www.tiger266[.]com
- help.tiger266[.]com
- new.mkdjgame[.]com
- help.mkdjgame[.]com
- www.ffyl-bet[.]com
- help.ffyl-bet[.]com
- zk.full-subscription[.]com
- cs.full-subscription[.]com
- yd.full-subscription[.]com
- www.animal777[.]com
- time.daytimegamers[.]com
- themerecord[.]com
- static.daytodayup[.]com
- mirrors.centos.8788912[.]com
- stat.8788912[.]com
- login.good-enough-8fe4[.]com
- cdn2.twmicrosoft[.]com
- cdn.1685810[.]com
- static.1685810[.]com
- cachedownload.goldenrose88[.]com
- backup.microsupdate[.]com
- api.gpk-demo[.]com
- static.gpk-demo[.]com
- api.geming8888[.]com
- 23.106.122[.]171
- 23.106.123[.]134
- 23.106.124[.]156
- 23.106.125[.]132
- 45.153.242[.]41
- 74.119.193[.]139

Reference

1. Operation Dragon Castling: APT group targeting betting companies, March 22, 2022 https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies/
2. Evolution after prosecution: Psychedelic APT41, November 27, 2021 https://vblocalhost.com/uploads/2021/09/VB2021-12.pdf
3. Ghost in action: the Specter botnet, September 25, 2020 https://blog.netlab.360.com/ghost-in-action-the-specter-botnet/
4. Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments, March 08, 2022 https://www.mandiant.com/resources/apt41-us-state-governments
5. The SideWalk may be as dangerous as the CROSSWALK, August 24, 2021 https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/
6. Higaisa or Winnti? APT41 backdoors, old and new, January 14, 2021 https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/
7. SHADOWPAD: A MASTERPIECE OF PRIVATELY SOLD MALWARE IN CHINESE ESPIONAG, August, 2021 https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

Reference

8. PseudoManuscrypt: a mass-scale spyware attack campaign, December 16, 2021 https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/
9. Earth Baku Returns, August 24, 2021 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns
10. Delving Deep: An Analysis of Earth Lusca's Operations , January 17, 2022 https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf
11. This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits, March 25, 2020 https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
12. LOWKEY: Hunting for the Missing Volume Serial ID, October 15, 2019 https://www.mandiant.com/resources/lowkey-hunting-missing-volume-serial-id
13. "Winnti" More than just a game, April 11, 2013 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf

Thank you!

TEAMT5
杜浦數位安全

為您量身訂製　專屬勒索防護

立即前往 主題攤位 L04 量身

品牌專頁
QR Code