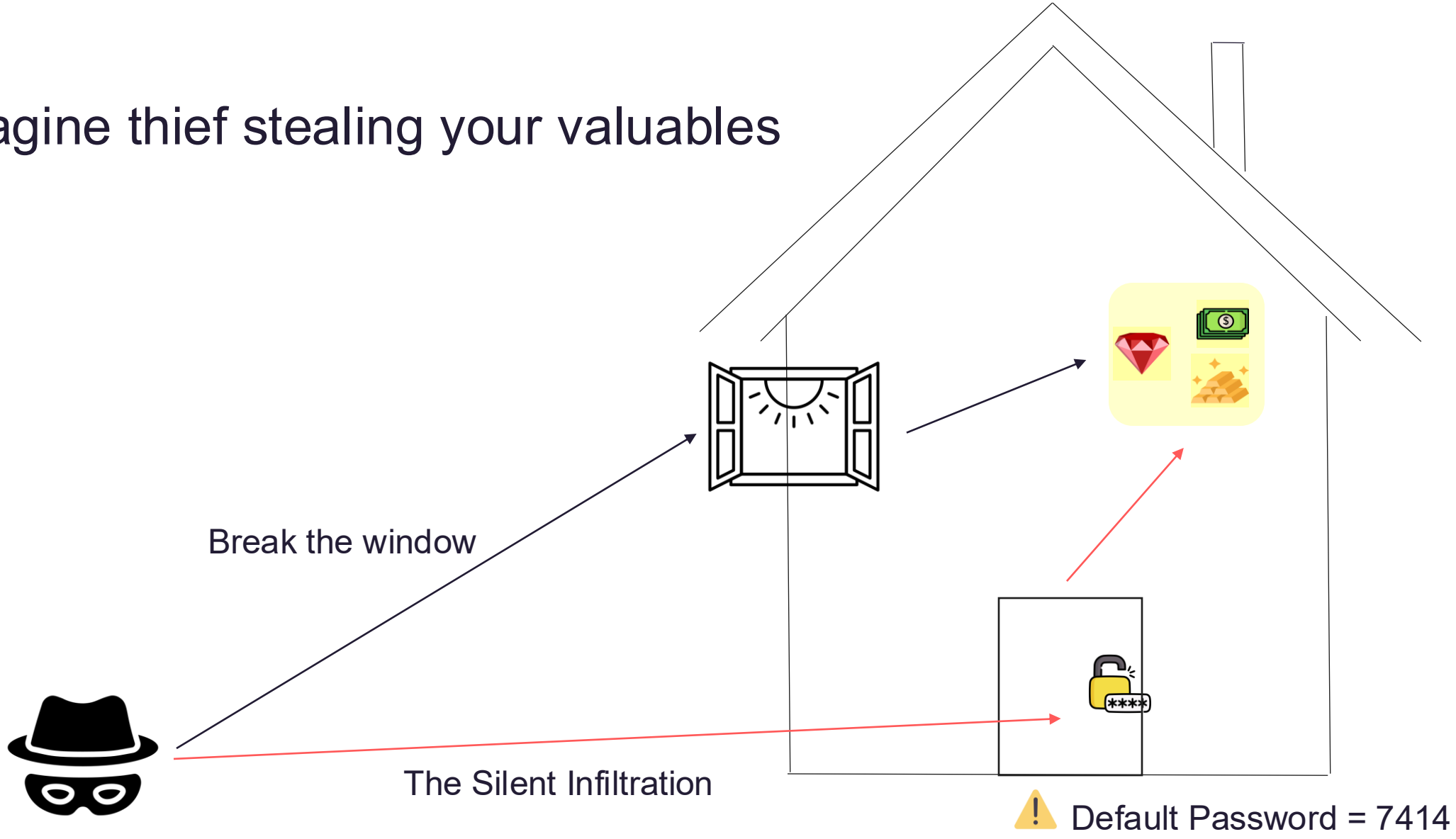
CYCRAFT

The Silent Infiltration: Darknet analysis of corporate data exposures in East Asia

25 09, 2025

Imagine thief stealing your valuables



Yuki Hung (@yukilolz7714)

- Security Researcher @ CYCRAFT
- Focus on Dark Web, CTI, Deep Learning
- Published
  - SINCON 2025
  - Hack.lu 2024
  - HITCON 2023 and 2024

Boik

- Security Research Manager
- Focus on Web and Cloud Security, and CTI
- Published
  - FIRSTCTI24
  - HITB
  - Global AppSec Dublin

Eric Hsieh (@doraeric)

- Cyber Security Researcher
- Focus on CTI, Network security
- Published
  - COSCUP 2025, 2024
  - NCA 2024
  - EuroP4 2022
- HITCON Volunteer

Agenda

- The Silent Infiltration Introduction
  - Key Findings
- Two Fronts of a Cyber War
  - The Silent Infiltration
  - The Noisy Offensive
- Case Study 1: The Silent Infiltration
- Case Study 2: The Noisy Offensive
- Situation in Europe
- Conclusion

Credential Leaks in East Asia

3

Months

5

Regions

849

Domains

67%

Domains with credential leaks

How Credential Leaks Happen

- Infostealers: A recently thriving malware
- They steals sensitive information, including:
  - Keyboard events
  - Screenshots
  - Credential from browsers
- The stolen data is often sold on the dark web

Enterprise Intruders:
They don’t Hack In — they Log In

Scope of Investigation

- Geographic Scope: 5 regions in East Asia
  - Taiwan, Japan, South Korea, Singapore, and Hong Kong
- Target Organizations: A total of 849 domains
  - Major government websites
  - Top companies by market capitalization within each location (script)
- Time Frame
  - 7,000+ leaked data packages (IAB logs) from the last three months

Initial Access Broker (IAB) Logs

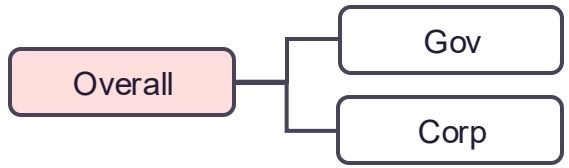
```
# Corporate Access Log - Batch #742
# Source: Redline Stealer Infection Campaign (US-FIN)
# Date: 2025-09-15
# Notes: Credentials extracted from browser password managers and user input.
# Format: URL | Account | Password
# ------------------------------------------------------------------------

# [High Value Target - VPN Access]
https://vpn.megacorp-financial.com/login | a.johnson@external.com | berlin#2025!

# [High Value Target - RDP Gateway]
https://remote.megacorp-financial.com/RDWeb/webclient/ | s.williams@external.com | P@ssw0rd12345

# [Webmail - Outlook Web Access]
https://mail.megacorp-financial.com/owa/auth.owa | alicia.johnson@megacorp-financial.com | VB2025
```

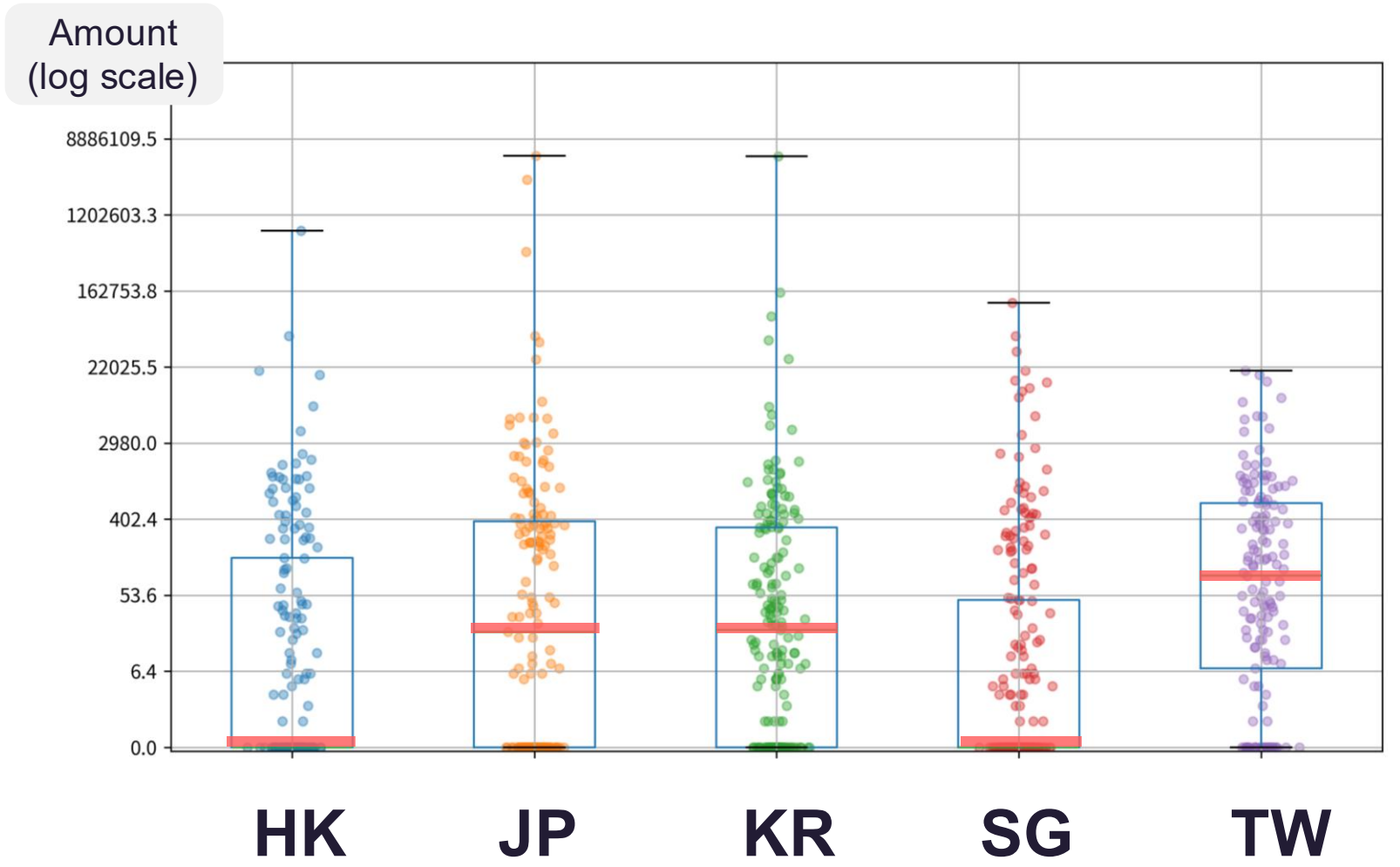
Definitions

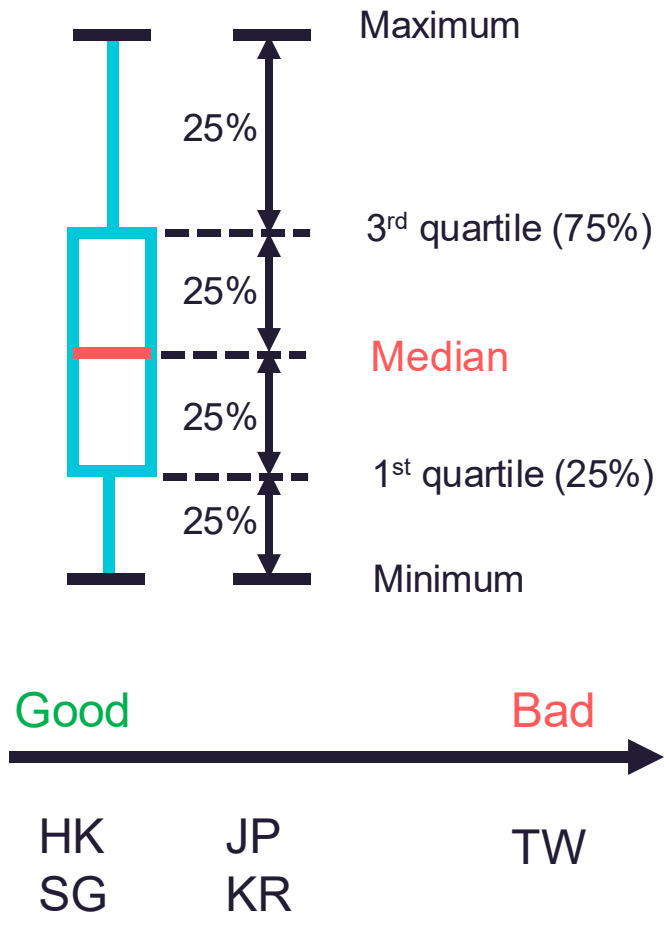
- Client account
  - Leaked email domain **does not match** the website domain
- Employee account
  - Leaked email domain **matches** the website domain
- Third-party service domain
  - An external website where the user email is used for login

```
URL: https://www.company-a.com.tw/career
Username: bob@gmail.com
Password: my_secret_password
Application: Microsoft_[Edge]_Default
===============
URL: https://www.company-a.com.tw/Login
Username: admin@company-a.com
Password: password
Application: Microsoft_[Edge]_Default
===============
URL: https://company-a.sharepoint.com/
Username: alice@company-a.com
Password: pass123123
Application: Microsoft_[Edge]_Default
```

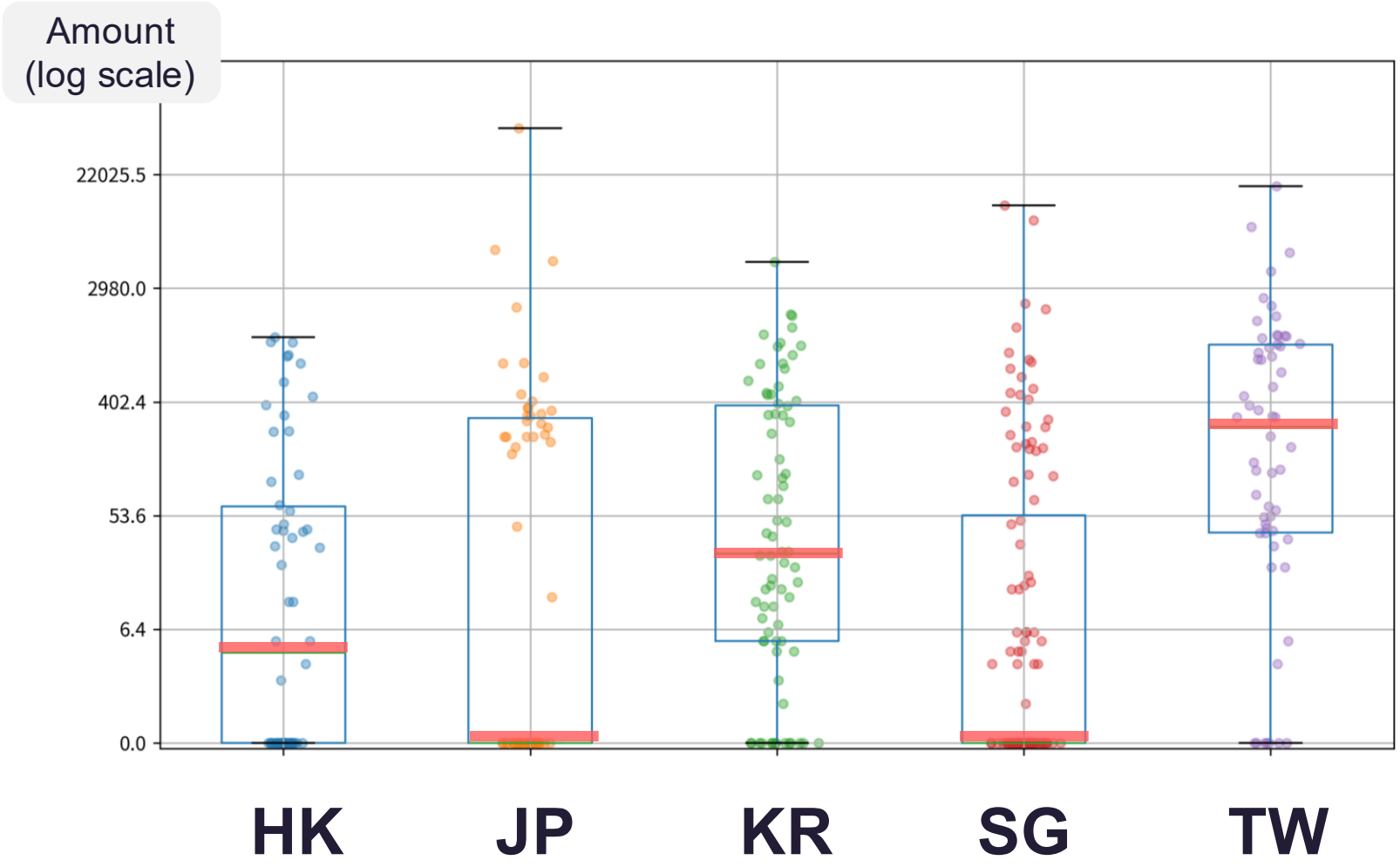
Overall Leaked Accounts







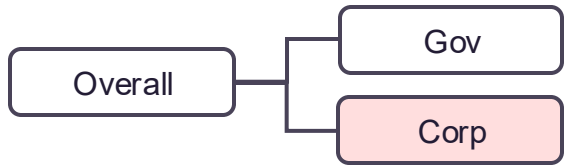
Leaks on Government Domain



- Japan: gov performs great
- Taiwan: nearly 10 times worse than KR

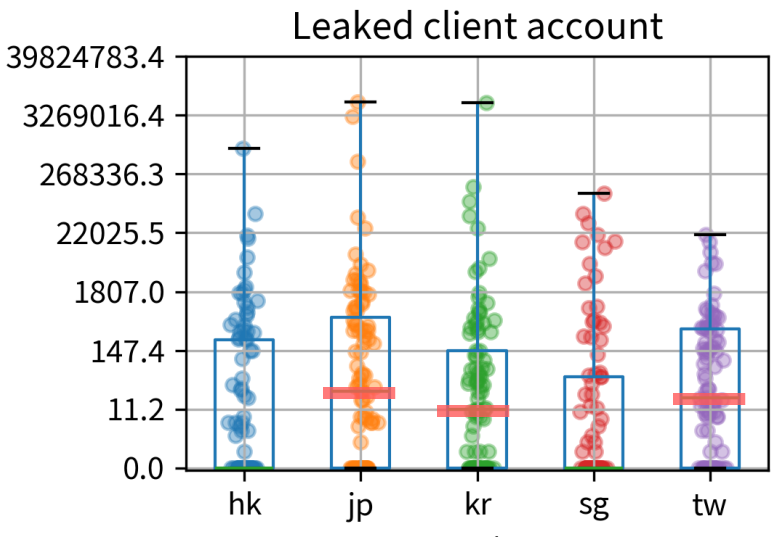
Good → Bad

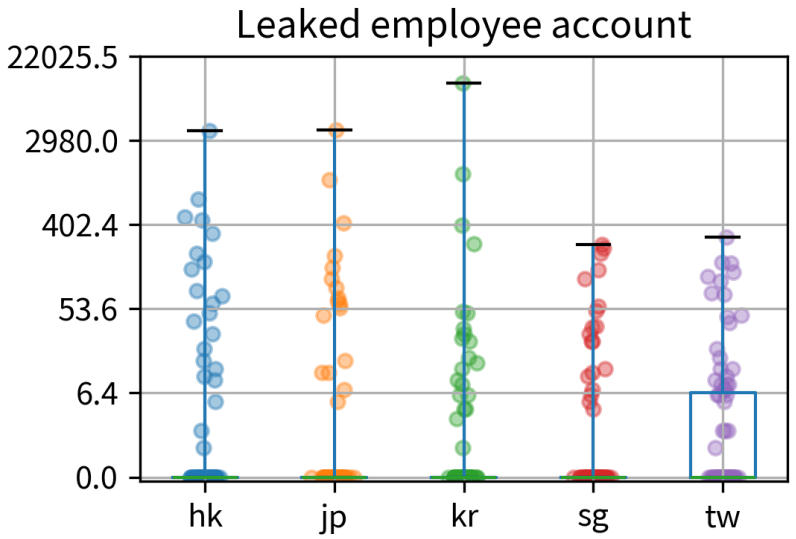
JP SG | HK KR | TW

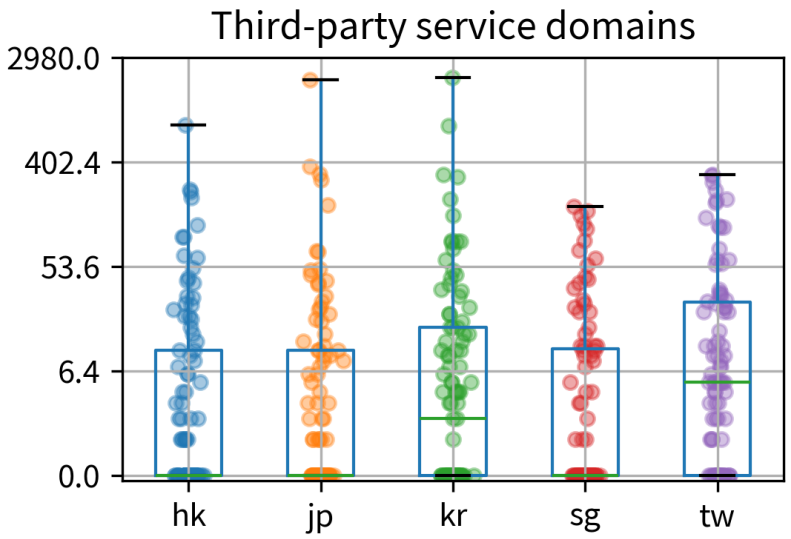


Insights into Corporate Leakage

- Client: Leaks correlate with regional population.
- Employee: Lower leak rate, but still a risk.
- Third-party: Essential platforms like Office, Webex, Zoom, AWS







CYCRAFT

Ranking

Rank by amount	Government	Corporate	Overall
🥇	TW	TW, JP	TW
🥈	KR, HK	KR	JP, KR
🥉	JP, SG	SG, HK	HK, SG

🏆

Taiwan is number one

in data leaks…

Findings

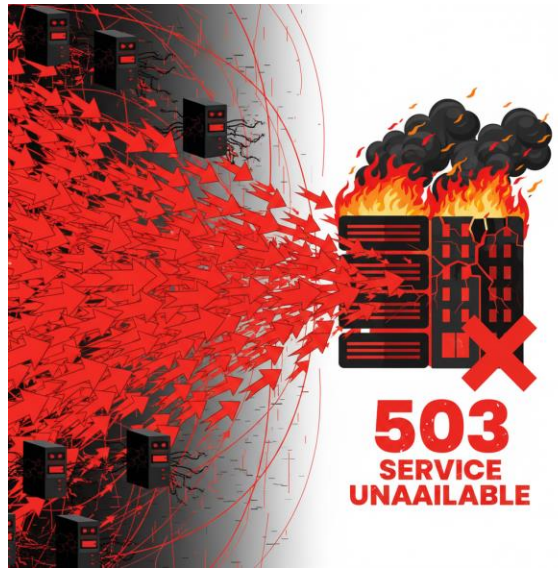
- Taiwan Gov sites: higher leakage observed
  - Being a more frequent target
- Singapore performs the best
- Massive leaks in JP & KR: consumer electronics firms
- Client account compromise is a predictable risk
- Third-party breaches: a severe and frequently underestimated security threat

Two Fronts of a Cyber War

The noisy offensive

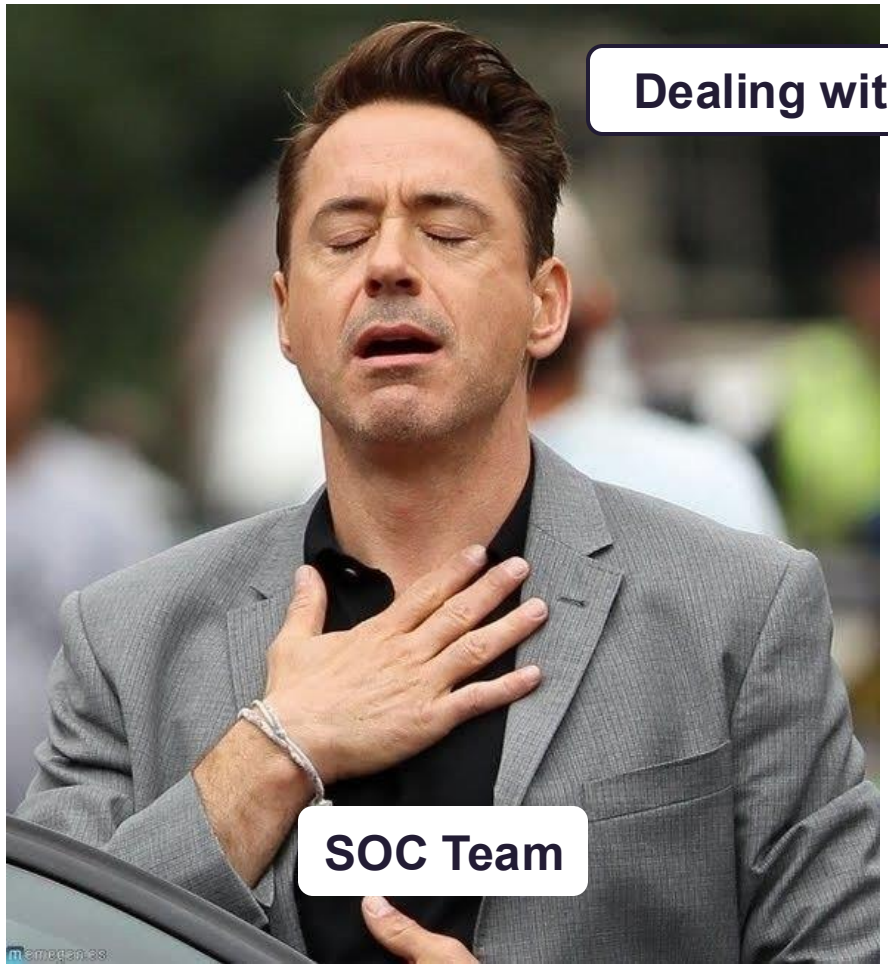
Tactics in Cyber War

Characteristic	Silent Infiltration	Noisy Offensive
Tactic	Steal Data, Gain Control	Disrupt Service
Technique	Credential Stuffing, Phishing	DDoS, Web Defacement
Visibility	**Low** - Stealthy & Persistent	**High** - Immediate & Obvious

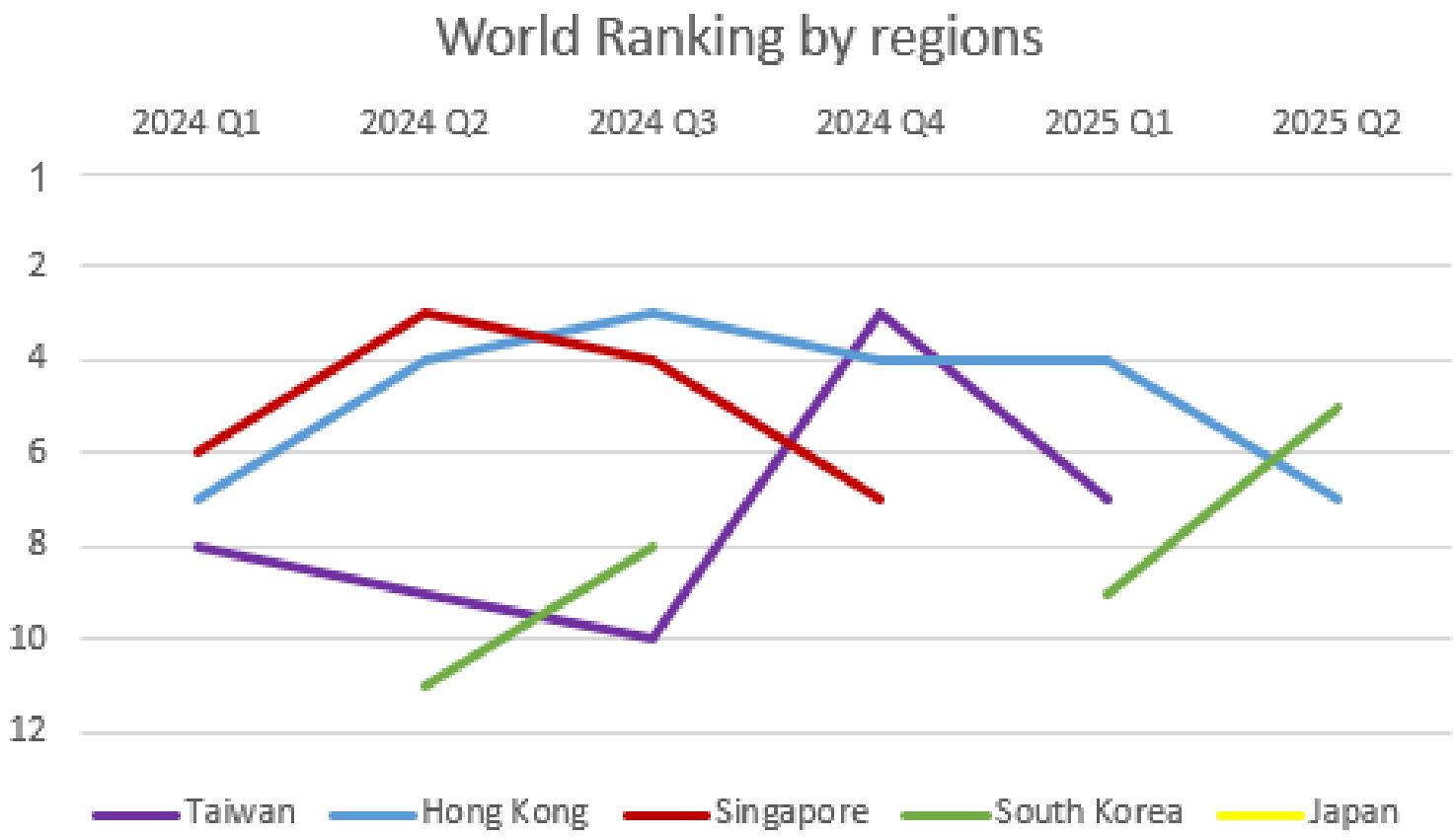


CYCRAFT

Combination Attack (script)



Global DDoS Target Ranking (Cloudflare)



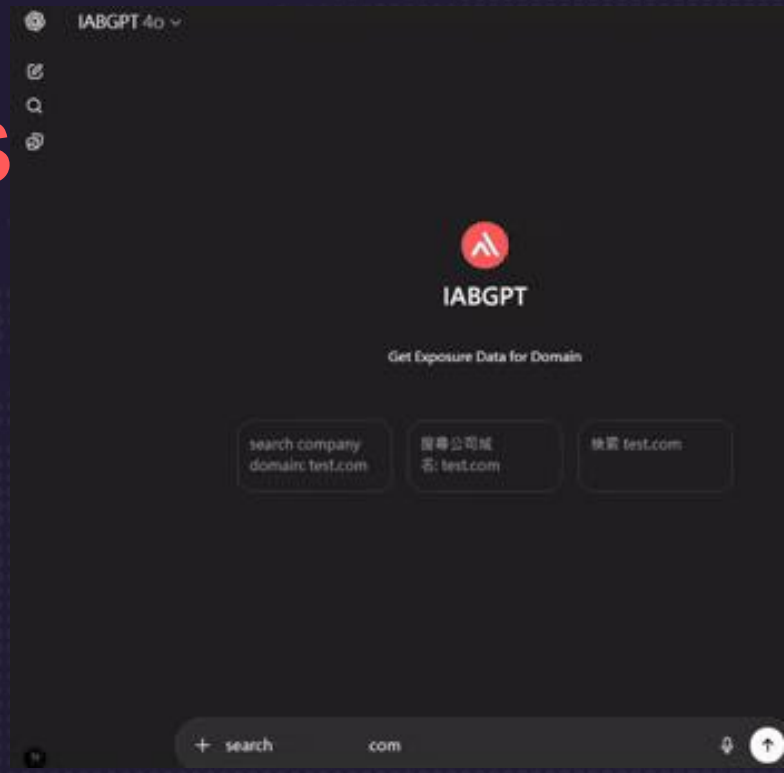
Mitigation

- **The Silent Infiltration**
  - **Primary Goal:** Assume Breach & Hunt for Threats
  - Multi-Factor Authentication (MFA)
  - Regularly change password
  - Trace the source of data breach
- **The Noisy Offensive**
  - **Primary Goal:** Ensure Availability & Resilience
  - Firewall / WAF
  - DDoS Mitigation service
  - Rate Limiting & Geo-Blocking

Case Study 1
The Silent Infiltration

How to obtain valid credentials

- Approaches
  - Deploying infostealer
  - Paying employees at targeted organizations
  - Purchasing credential from forums
  - Searching public code repositories
- We use ChatGPT plugin to demonstrate a leak example in Taiwan



Analysis of "[redacted].tw"

The domain [redacted]tw belongs to [redacted] which operates the [redacted] The website serves as a customer interface for ticket booking, member services, corporate partnerships, and vendor access.

This report analyzes the exposure of credentials and URLs related to [redacted] for the period between **June 13, 2025, and September 11, 2025**, highlighting potential security risks and offering mitigation recommendations.

Compromised Credentials

There is **no evidence of compromised employee credentials**, but **4,427 client accounts** associated with the domain have appeared in leaked datasets.

Observations

Examples of exposed client emails include:

- ****yu@mail2000.com.tw ↗ (22 times)
- ****ox721@gmail.com ↗ (19 times)

The wide range of domains and repeated occurrences suggest these are likely members or users of [redacted] customer portal, possibly affected through password reuse or malware.

Password Strength Analysis

Employee Passwords

No employee password data is available for the review period.

User Passwords

Password strength for client credentials is as follows:

- **Medium**: 2,323 (52.5%)
- **Weak**: 1,937 (43.8%)
- **Strong**: 167 (3.8%)

Observations

More than **43% of passwords are weak**, and less than 4% are considered strong. These weak credentials pose a high risk for account takeover attacks, especially if reused across services or accessed from compromised devices.

Potentially Exposed URLs

Employee URLs

No internal employee portals were exposed.

User URLs

The [redacted] member platform and login endpoints are heavily referenced in leaked data, including:

- (Member Page) [redacted] — 1,080 times
- (Member Login Page) [redacted] — 165 times
- (Main Member Portal) [redacted] — 699 times
- (Corporate Supplier Login) [redacted] — 40 times

This likely reflects credential harvesting or repeated login attempts from exposed endpoints.

Third-Party Domains Referenced

Third-party URLs found in the data include:

- (Microsoft Login Page) [redacted]
- (Microsoft v2 OAuth) [redacted]
- (Microsoft Live Login) [redacted]

Security Concerns

- **Large-scale user credential exposure** with over 4,400 affected clients
- **Extremely poor password hygiene** among users, with nearly 44% weak passwords
- **Public exposure of login URLs**, which may facilitate brute-force and phishing attacks
- **Third-party references**, such as Microsoft and shopping portals, hinting at potential cross-service credential misuse

---

Recommended Actions

- **Force Password Reset** for all users whose credentials were identified in breach corpora
- **Implement Account Lockout Policies** and rate-limiting for login pages
- **Deploy MFA** (Multi-Factor Authentication) for all user and supplier accounts
- **Educate Customers** via website banners or email campaigns on the importance of using strong, unique passwords
- **Conduct Regular Audits** on URL exposure and third-party script dependencies

---

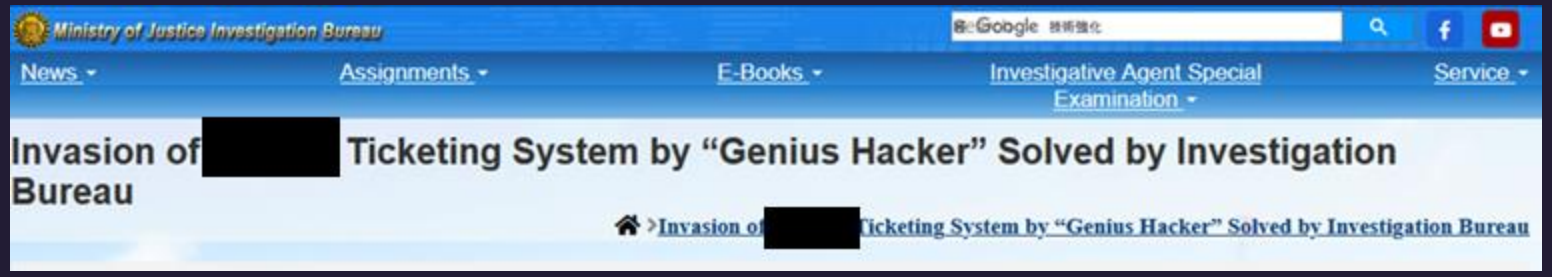
Further Investigation

For deeper analysis of compromised users and credentials, please contact CyCraft at (here)[https://www.cycraft.com/en/contact-us ↗].

CYCRAFT

Leak Impact

- Attacker logs in with internal account
- Obtain partner company coupons and resell for profit
  - Potential supply chain attack
- Access user activity info
  - Use for advanced phishing or customized fraud attack



Key points

- Public-facing services are the top source of leaks
- Third-party logins also carry a high risk of credential exposure
- Most users do not use strong passwords
- Need regular password changes with MFA

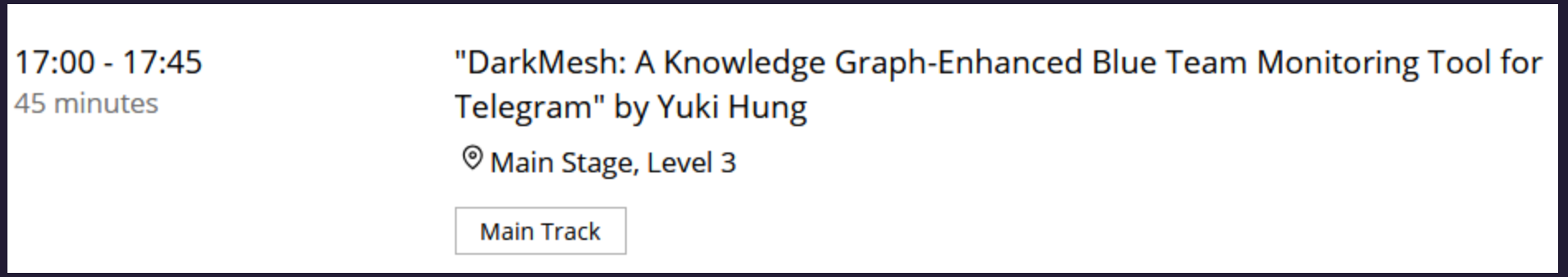
Case Study 2
The Noisy Offensive

The Noisy Offensive

- In this case, we analyze three telegram groups “RipperSec”, “NoName057” and “4exploitation”
- These are all pro-Russian hacker groups
- Claimed DDoS and Website Defacement on telegram group
- They have many attack targets all over the world, including Europe and East Asia

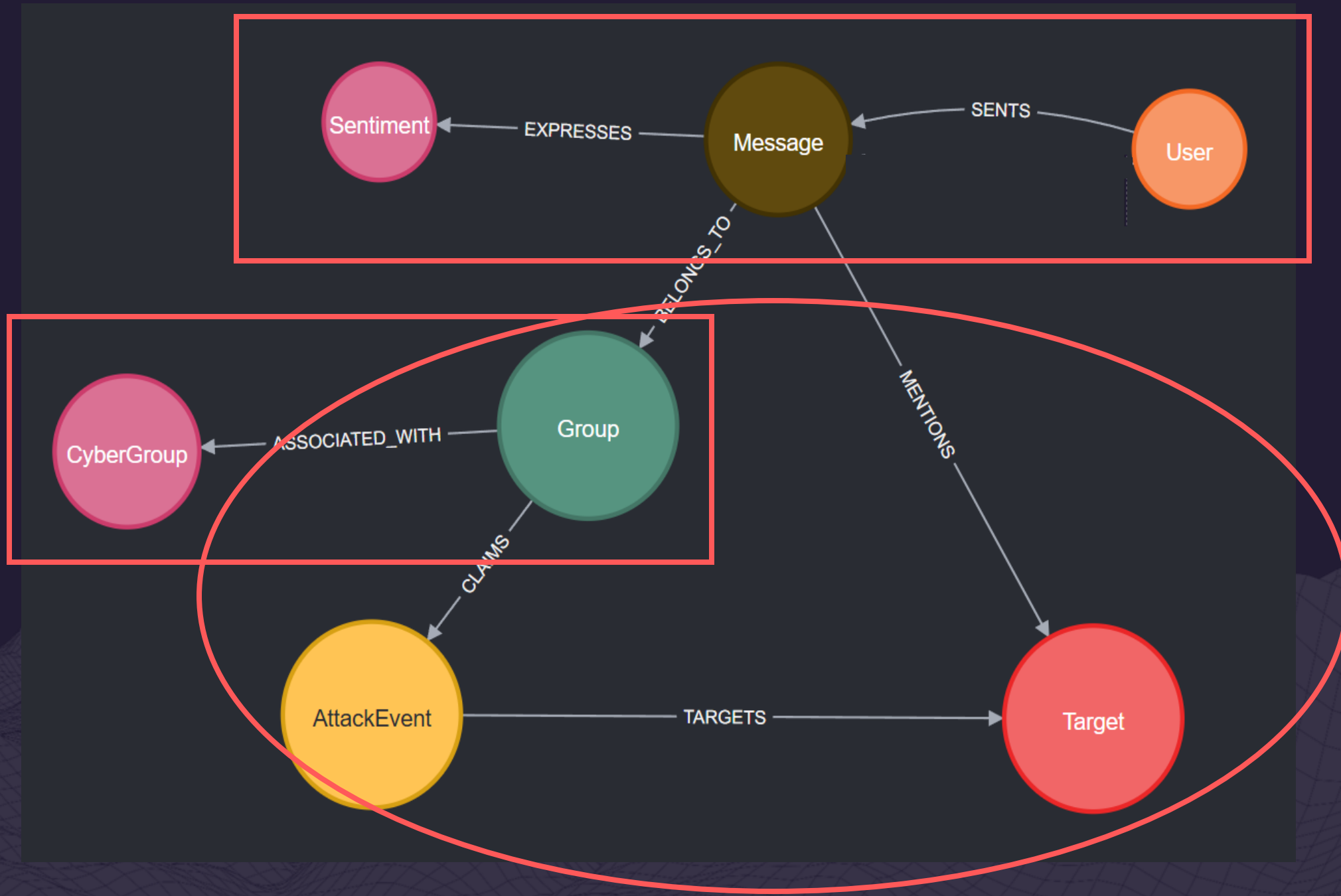
DarkMesh

- Use DarkMesh system we proposed at SINCON 2025
  - **Automated analysis of Telegram conversations, generating reports based on conversation topics and presenting knowledge graphs.**

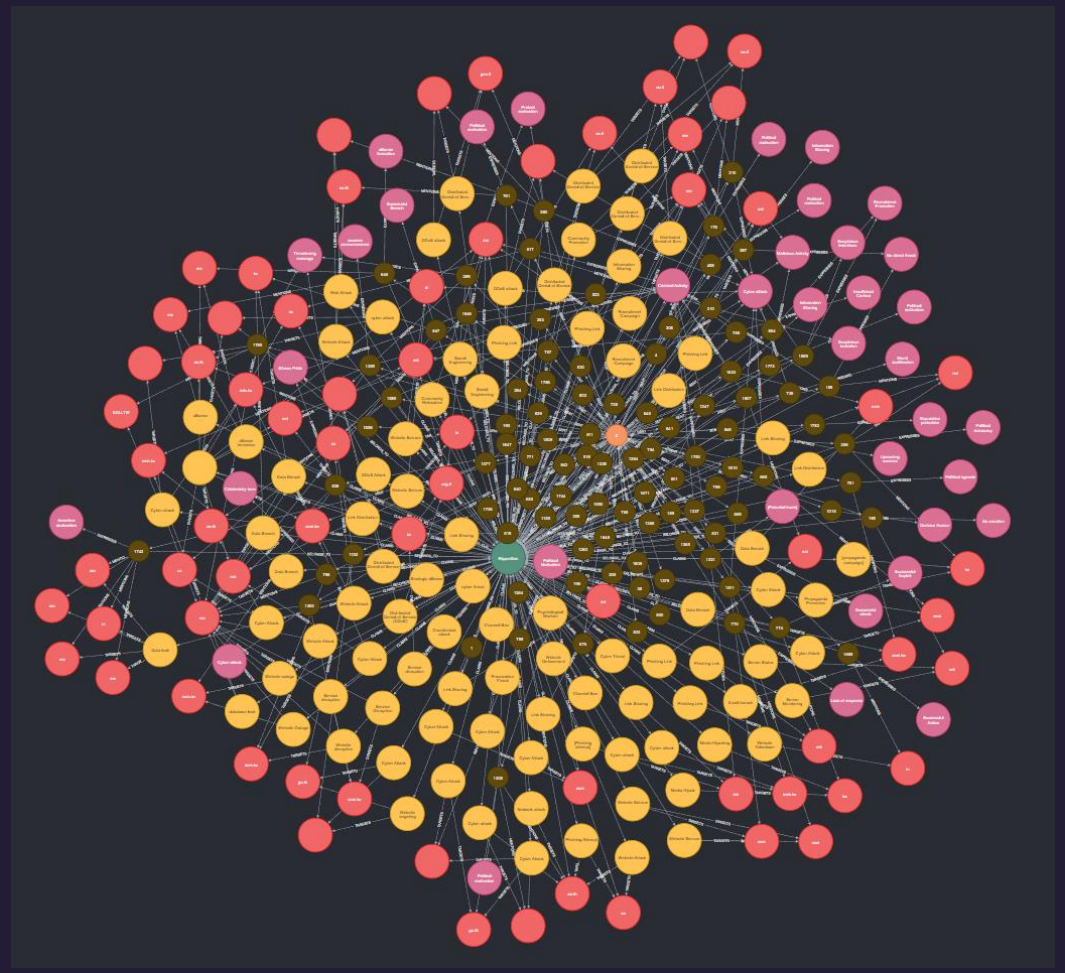


https://www.infosec-city.com/schedule/sin25-con

Schema

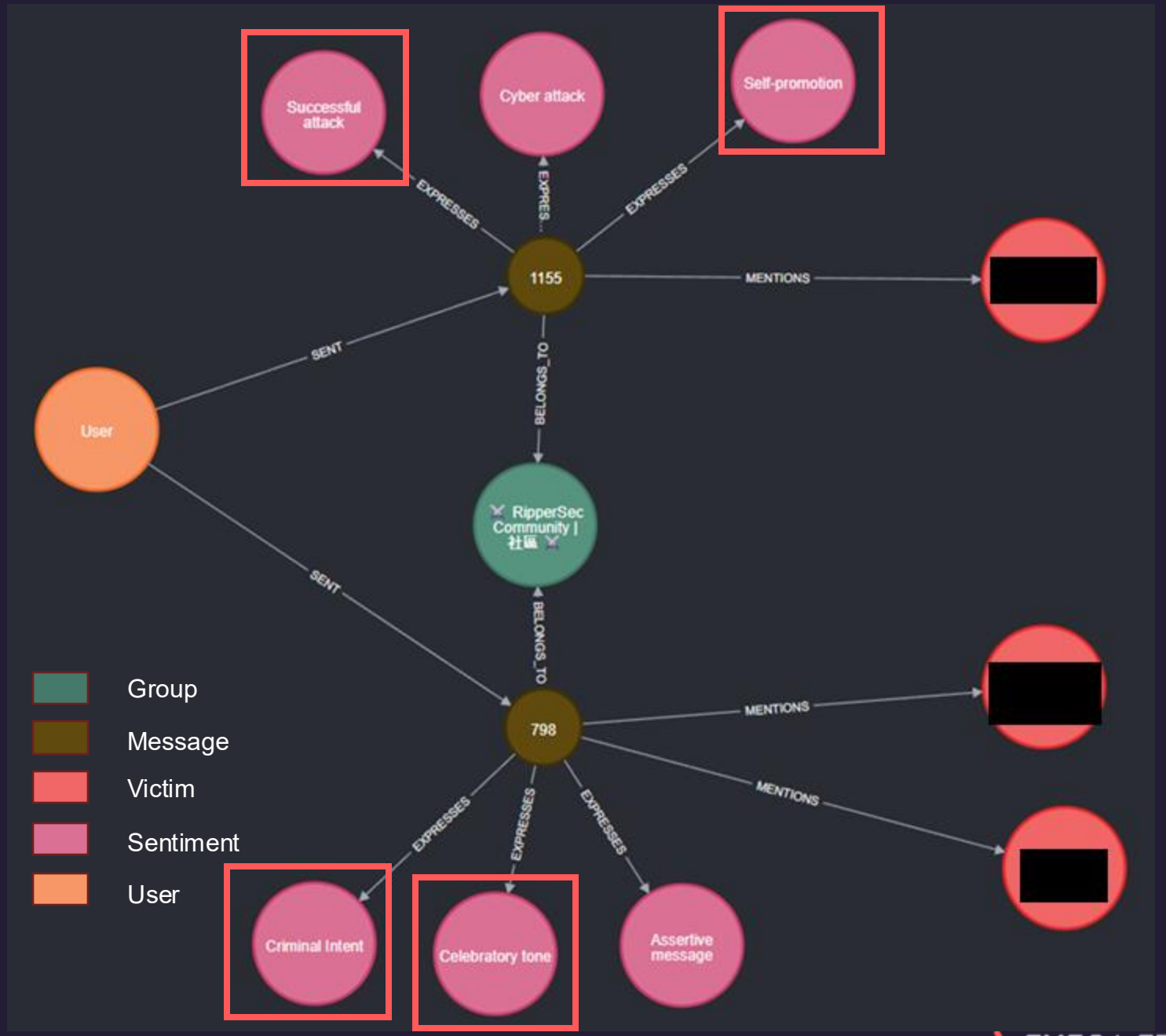

Sentiment
EXPRESSES
Message
SENTS
User
BELONGS_TO
CyberGroup
ASSOCIATED_WITH
Group
MENTIONS
CLAIMS
AttackEvent
TARGETS
Target

Q1: What did they say to Taiwan & Singapore

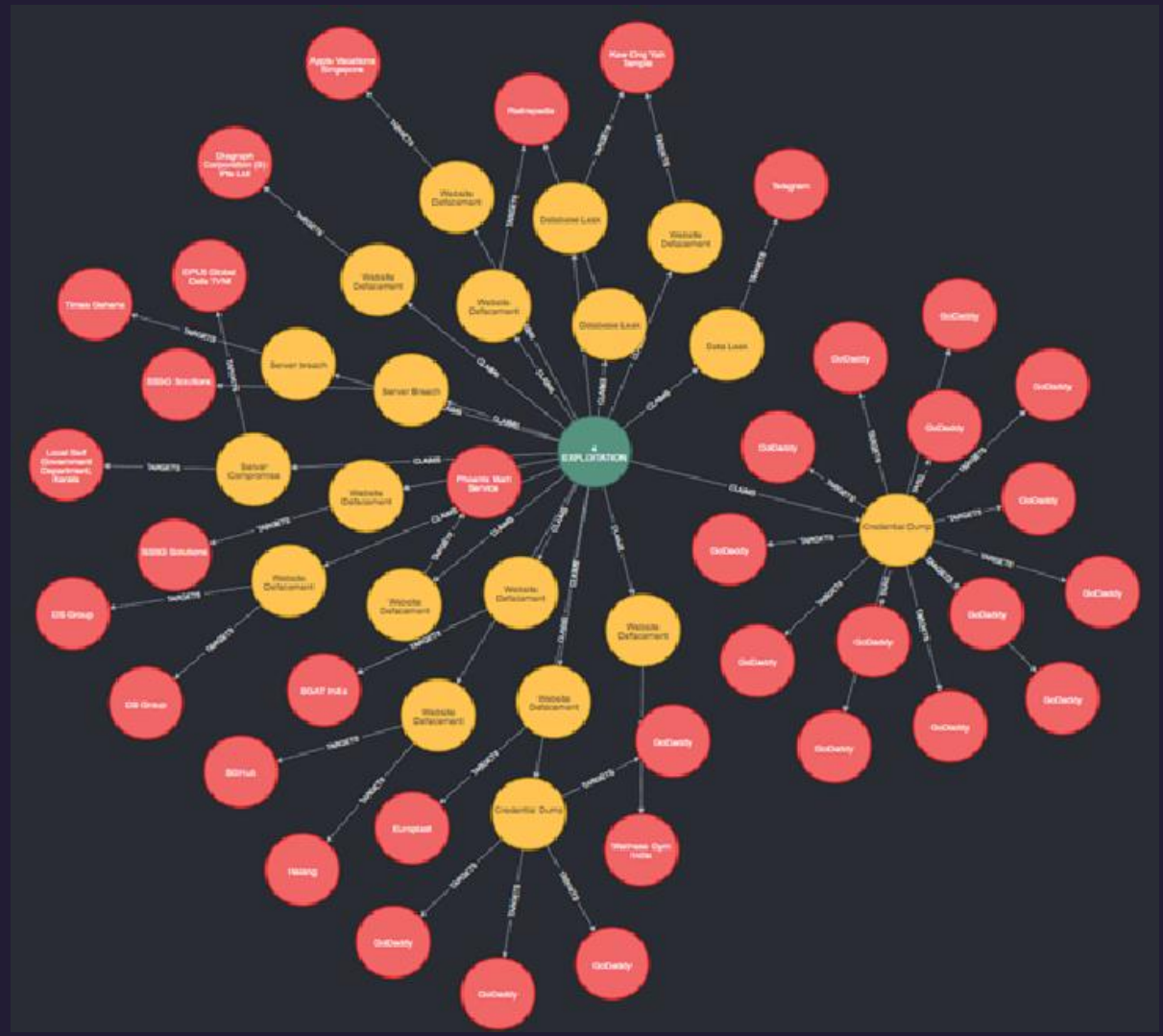


Threatening
by RipperSec

- Sentiment
  - Sucessful attack
  - Self-promotion
  - Criminal Intent
  - Celebratory tone
  - ...



Q2: Who’re the victims

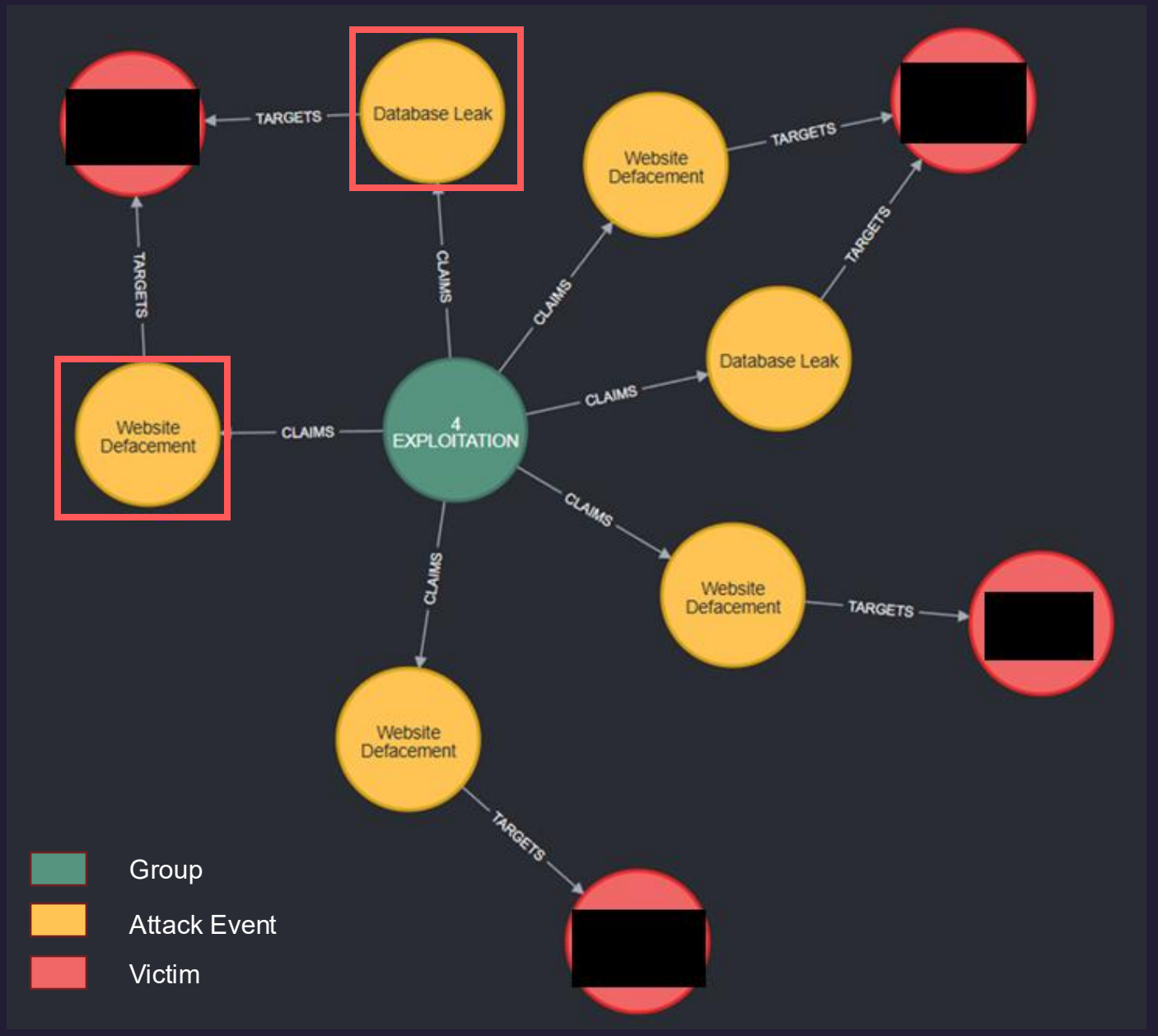


4 Exploitation

Node properties

Target

<elementId>	4:19b0789a-0ffc-4da6-a4f7-4c0812eeb082:8279
<id>	8279
domain	[redacted]
industry	Personal Finance / Retirement Planning
label	Target
name	[redacted]
node_key	Target_https://[redacted]sg/
tld	sg
url	https://[redacted]sg/

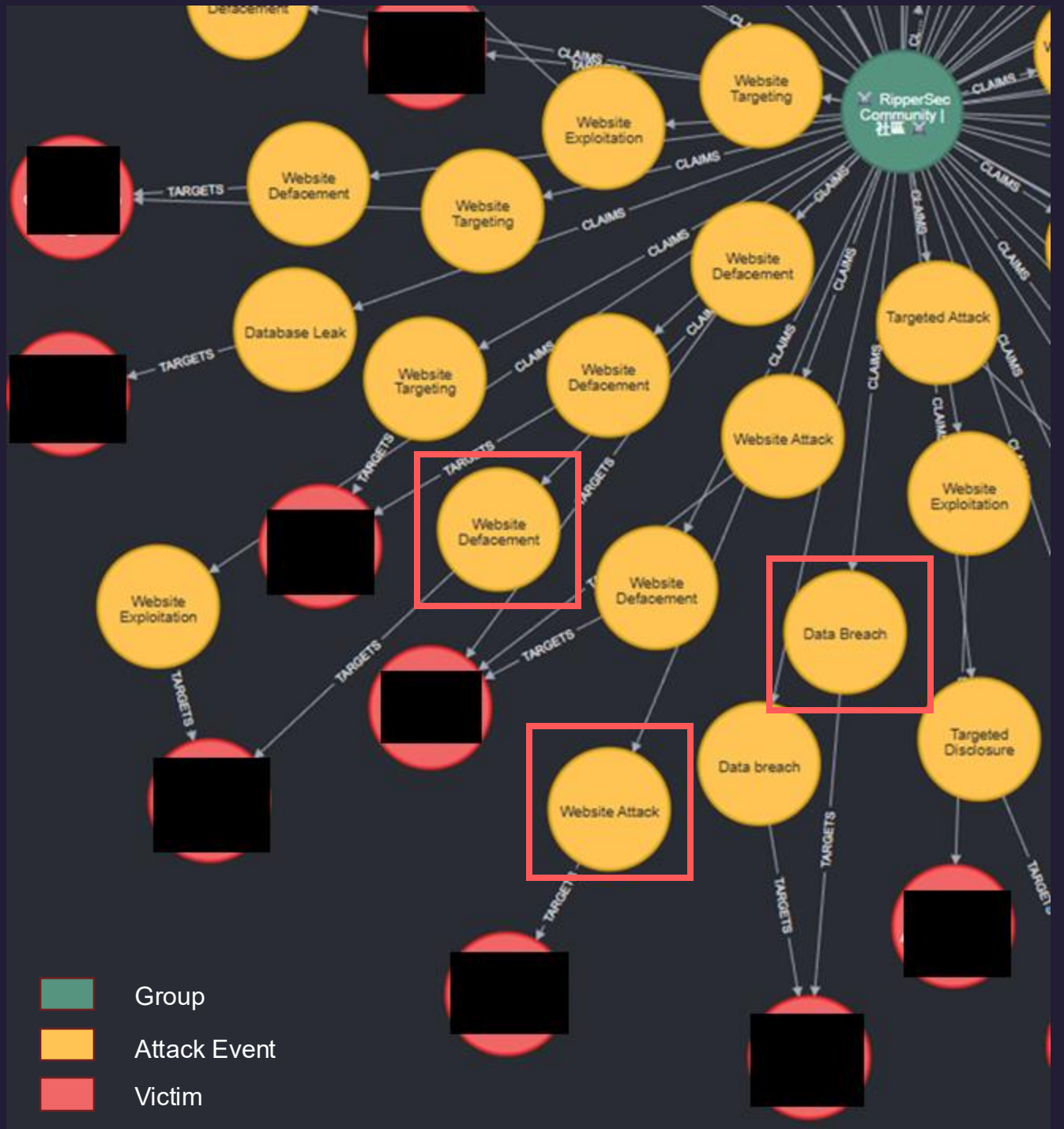


- Victims of Singapore
  - Retirement
  - Tourism
  - Temple

CYCRAFT

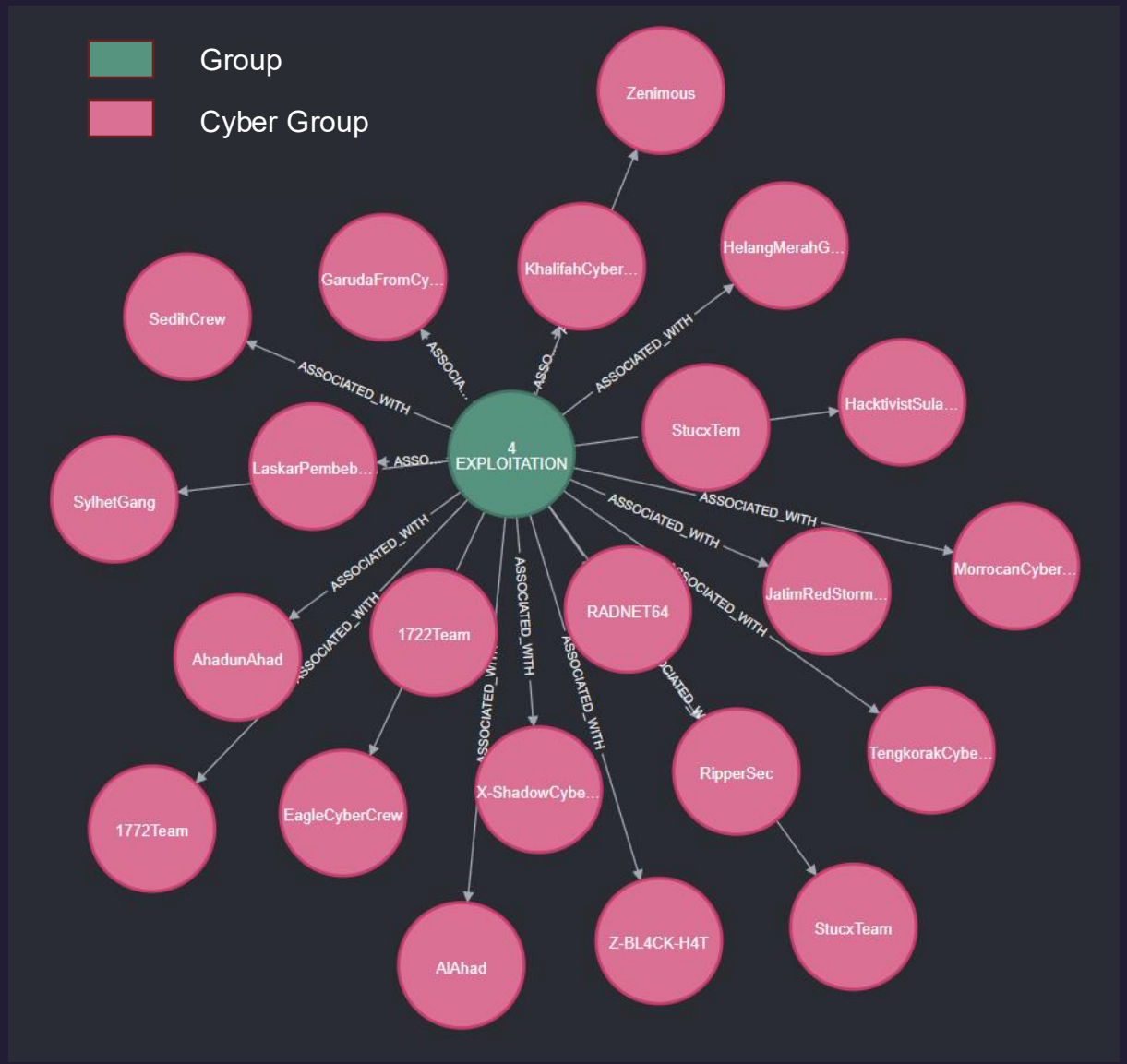
RipperSec

- Victims of Taiwan
  - Education
  - Finance
  - Government
  - ...



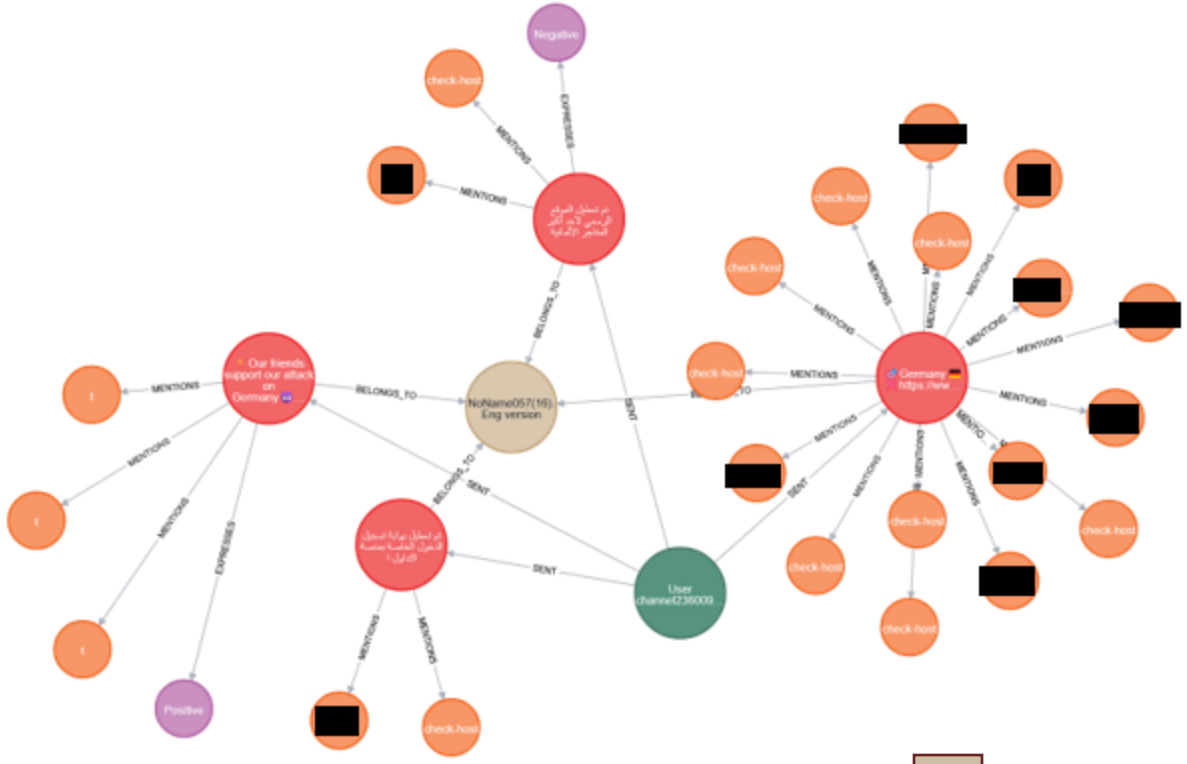
Q3: Who are they associated with

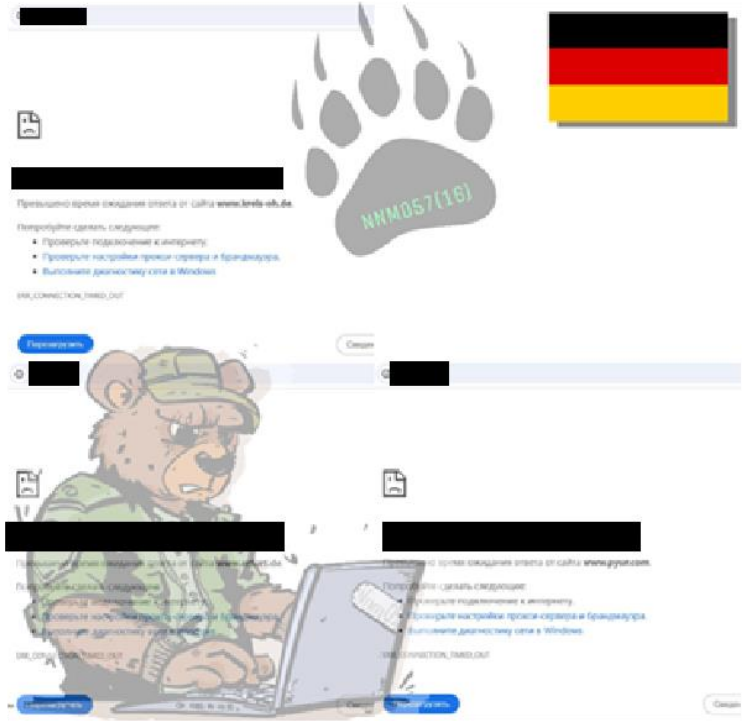
- Pro-Russian groups
  - Noname057
  - RipperSec
  - 4 Exploitation
  - EagleCyberCrew
  - Stucx Team



Does Europe face the same problems as Asia?

European victims (By NoName057)





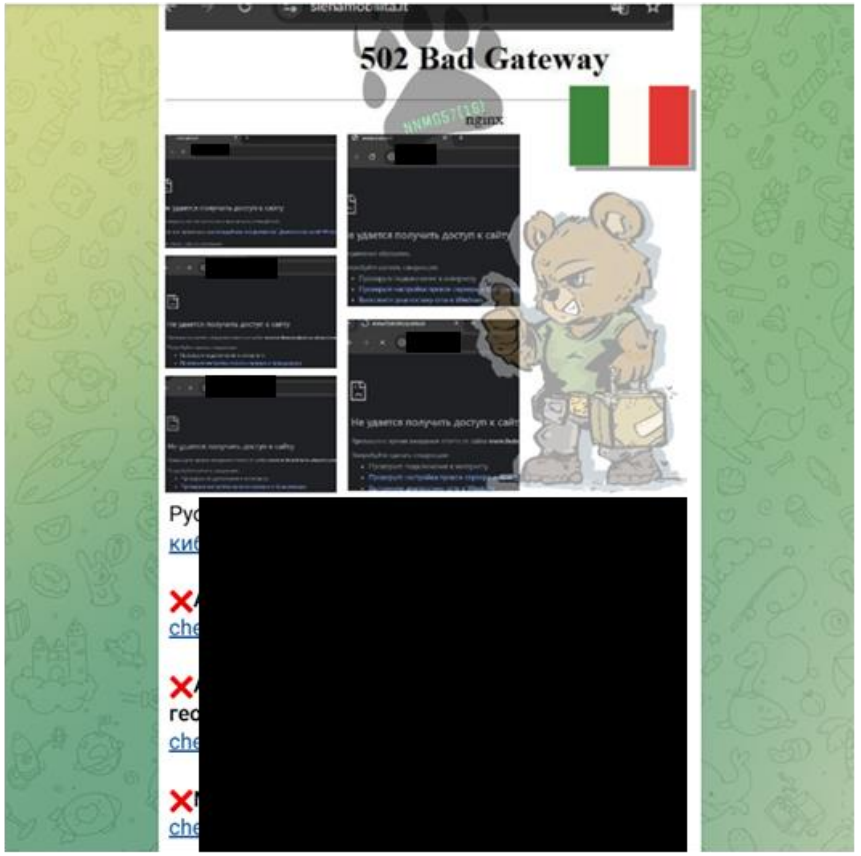
- Germany

Group
Message
Victim
Sentiment
User

CYCRAFT

European victims

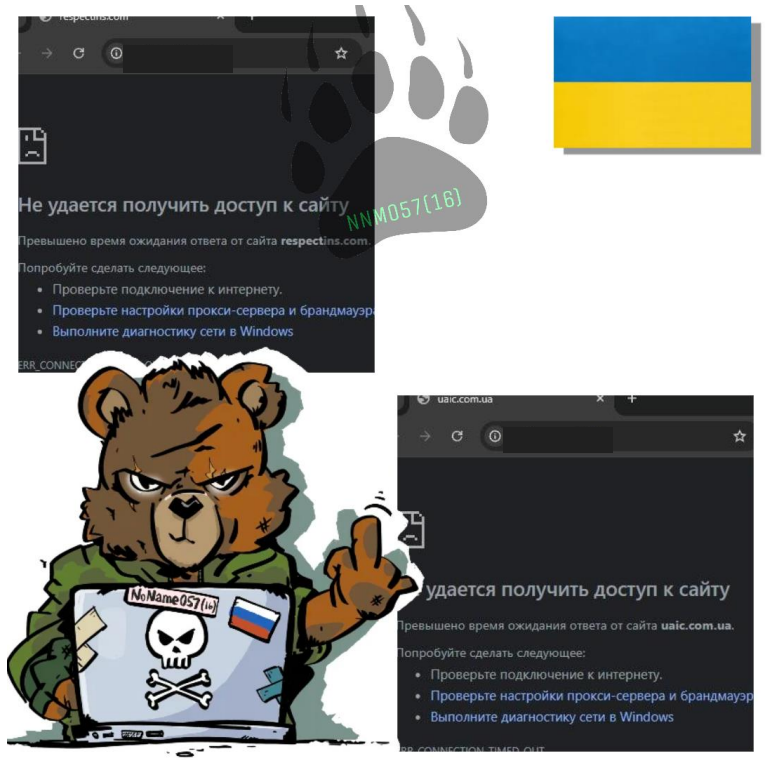
- Group
- Message
- Victim
- User

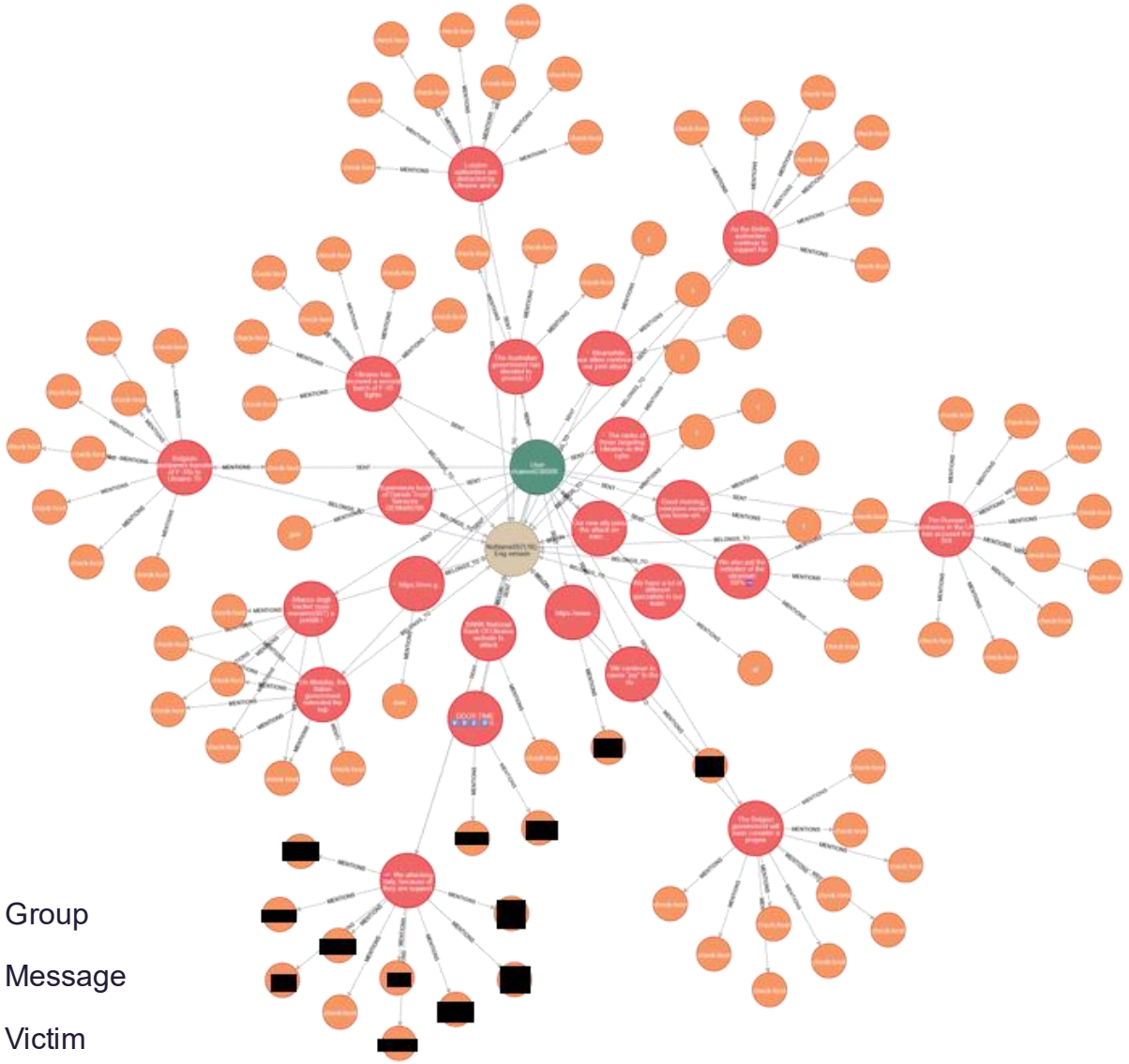


> Italy

Ukrainian victims

- Major victim of NoName057

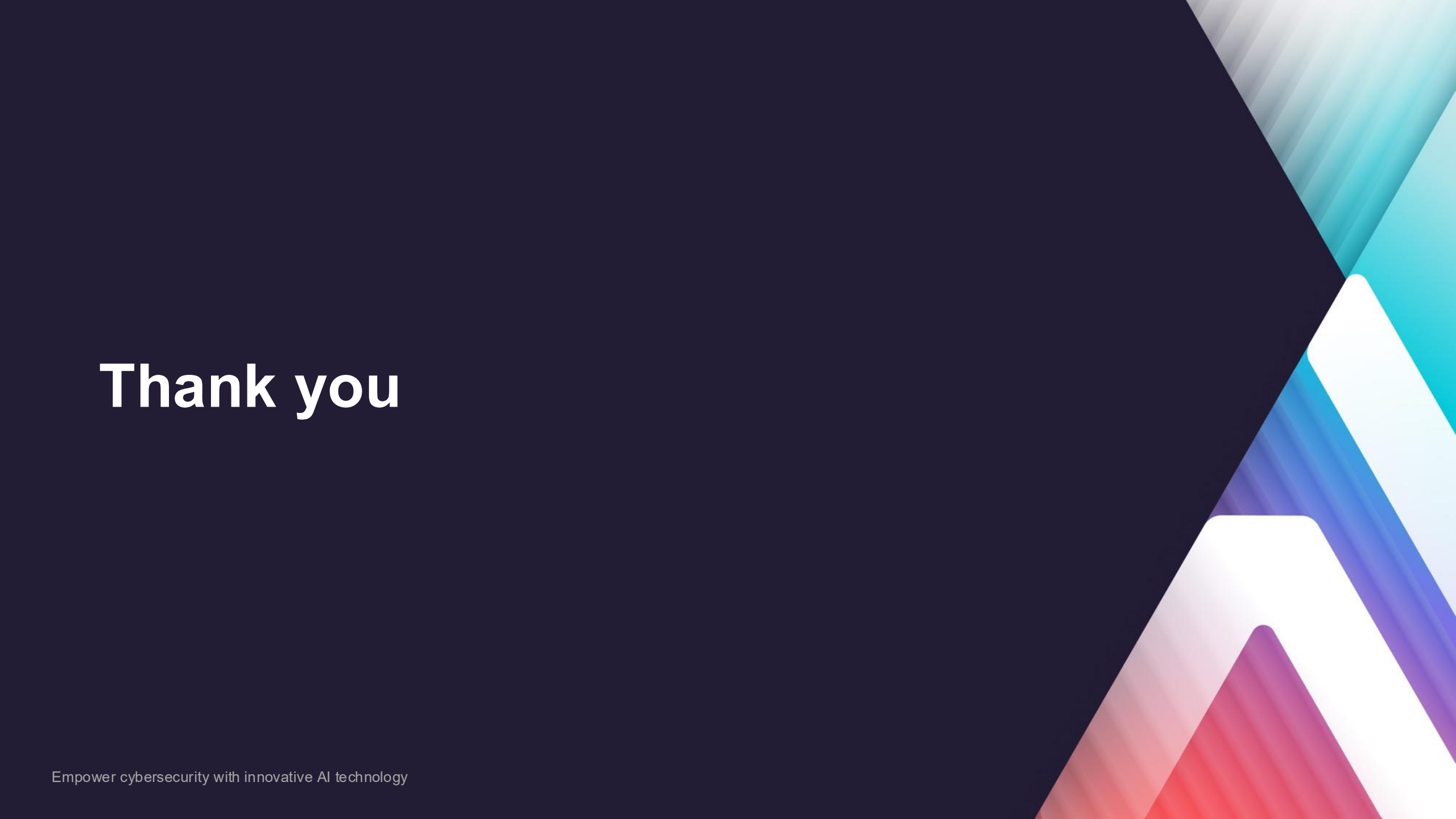




Conclusion

- Public-facing services are the top source of leaks
- Leaks via third-party platforms are often overlooked
- Taiwan ranks #1 in number of leaks across East Asia
  - Government agencies leaked 10× more than South Korea (ranked #2)
- DDoS attacks and dark web leaks are global threats
- They don’t Hack In — they Log In

Thank you



Empower cybersecurity with innovative AI technology

Q&A