Fast, Frank, and Friendly
Financials ISAC Japan

Cyber Threat Landscape

Keisuke Kamata
Managing Director / CTO
Financials ISAC Japan
kamata@f-isac.jp

Introduction: Financials ISAC Japan

Japanese financial industry cybersecurity collaboration organization.
Membership based and 433 members across Japan. Established in 2014.

We recognize cybersecurity as "collaboration" domain not as "competitive" domain.

Industry wide best practice development, cybersecurity exercise, human resource development, information sharing, security conference, workshop etc.

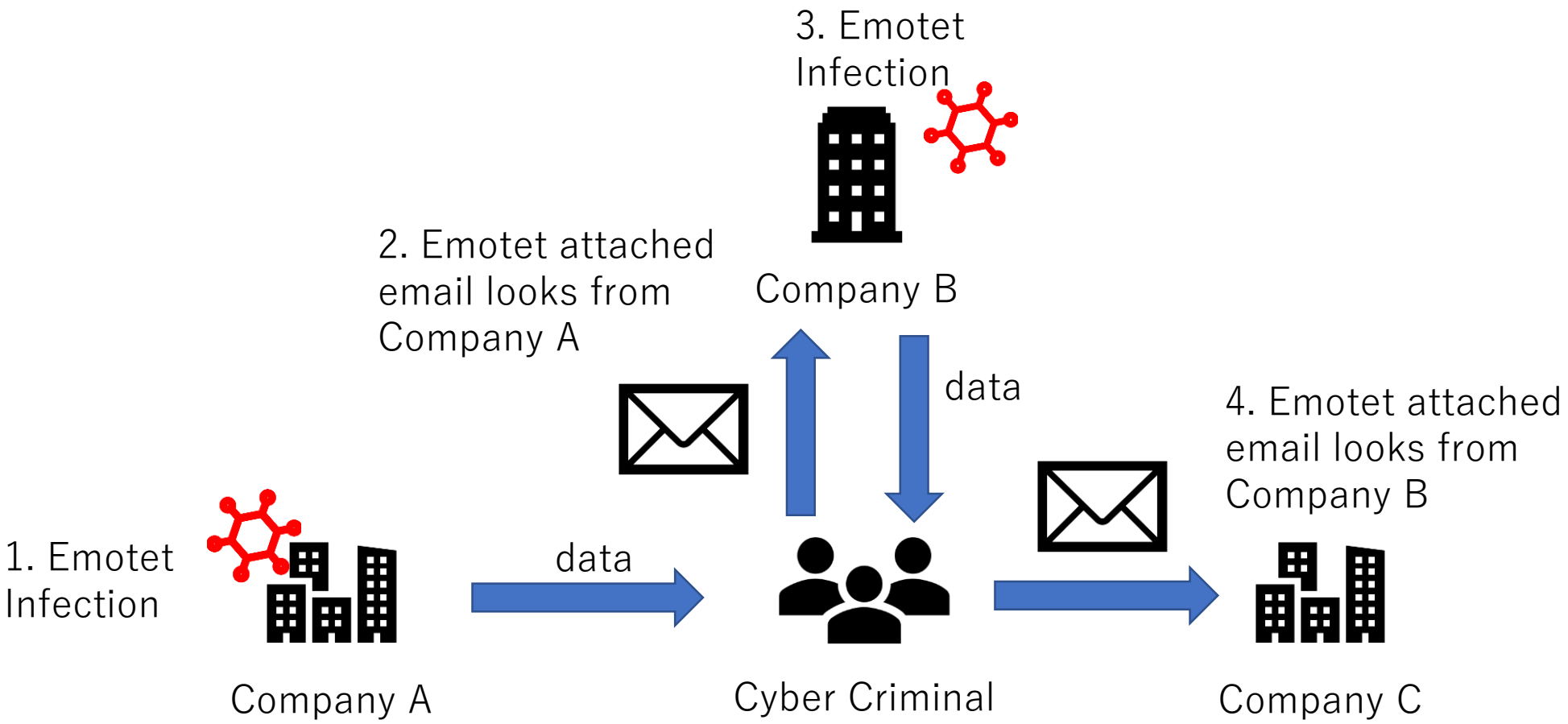
Major threats

- Emotet (malware)
- Ransomware (malware)
- DDoS Attack
- Vulnerability Exploitation Attempt
- Fraud
- Supply Chain risk in each Threat

Emotet (malware)

- Emotet attached email distribution
  - Initially seen in 2014 as banking trojan.
  - Widely seen in Nov/2021, active again in Feb/2022
  - then Mar/2023 again.
- Characteristics
  - Phishing Emails (social engineering)
  - Small file size zip attached, 500MB extracted.
  - MS Excel, Doc, OneNote files
- Impact
  - Probably to steal data/info from infected machine

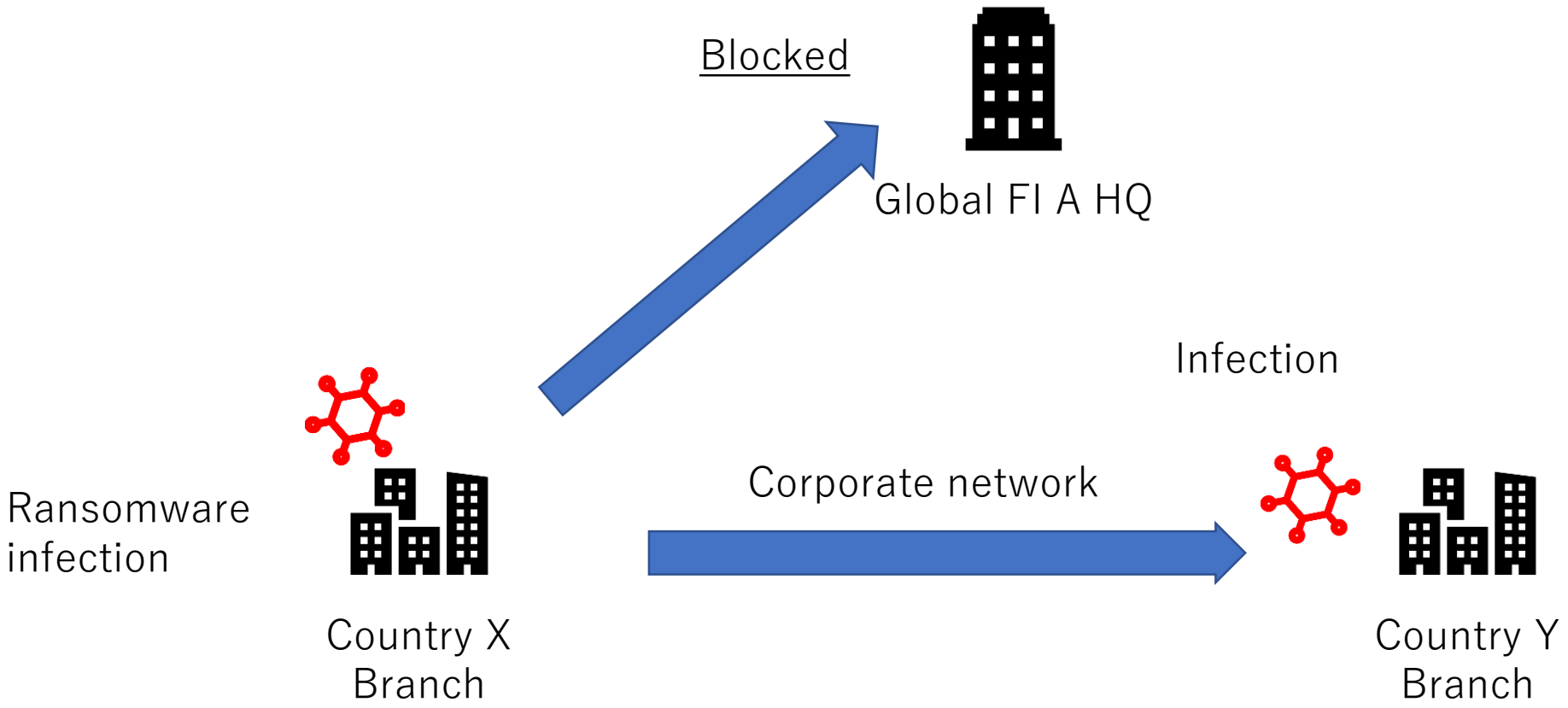
Supply chain case in Emotet



Ransomware

- Global issue
- Not very actively seen in Japanese FIs
- Global FIs' foreign subsidiaries cases
- Network connection between branches matter

Supply chain case in Ransomware

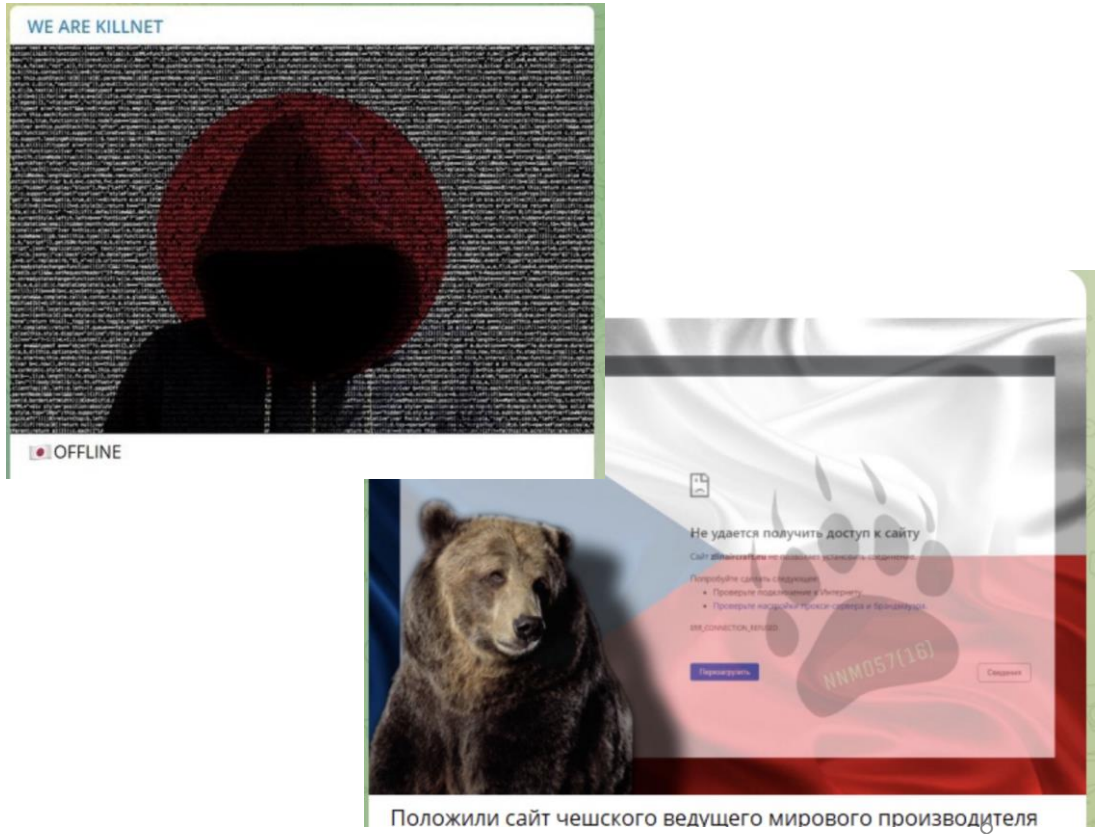


DDoS Attack

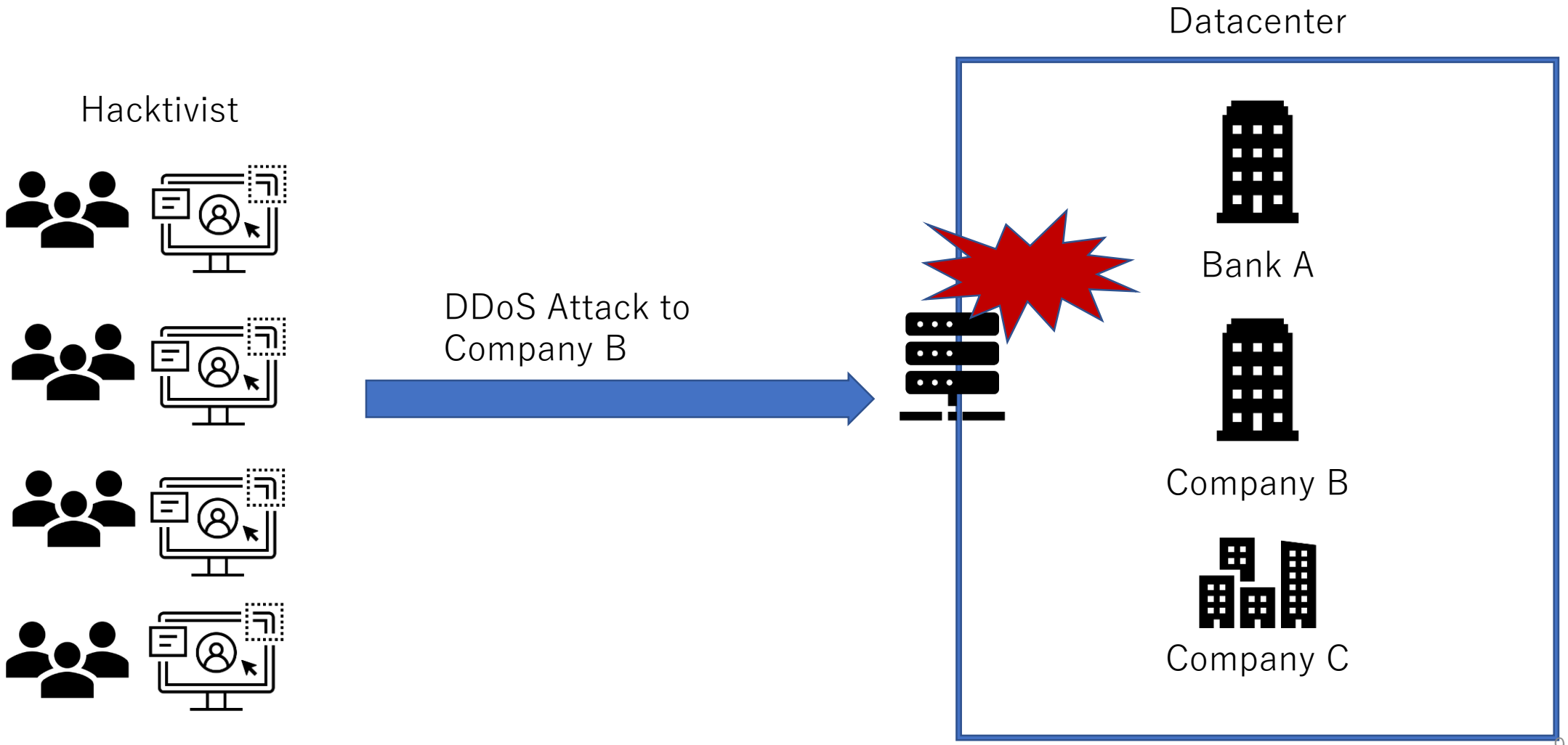
- Russian hacktivist targeted Japanese FIs as a part of their operation.
  - Killnet : Sep/2022
  - NoName057 : Feb/2023

- Also saw cases that bypass ddos protection

- DNS random subdomain ddos



Supply chain case in DDoS



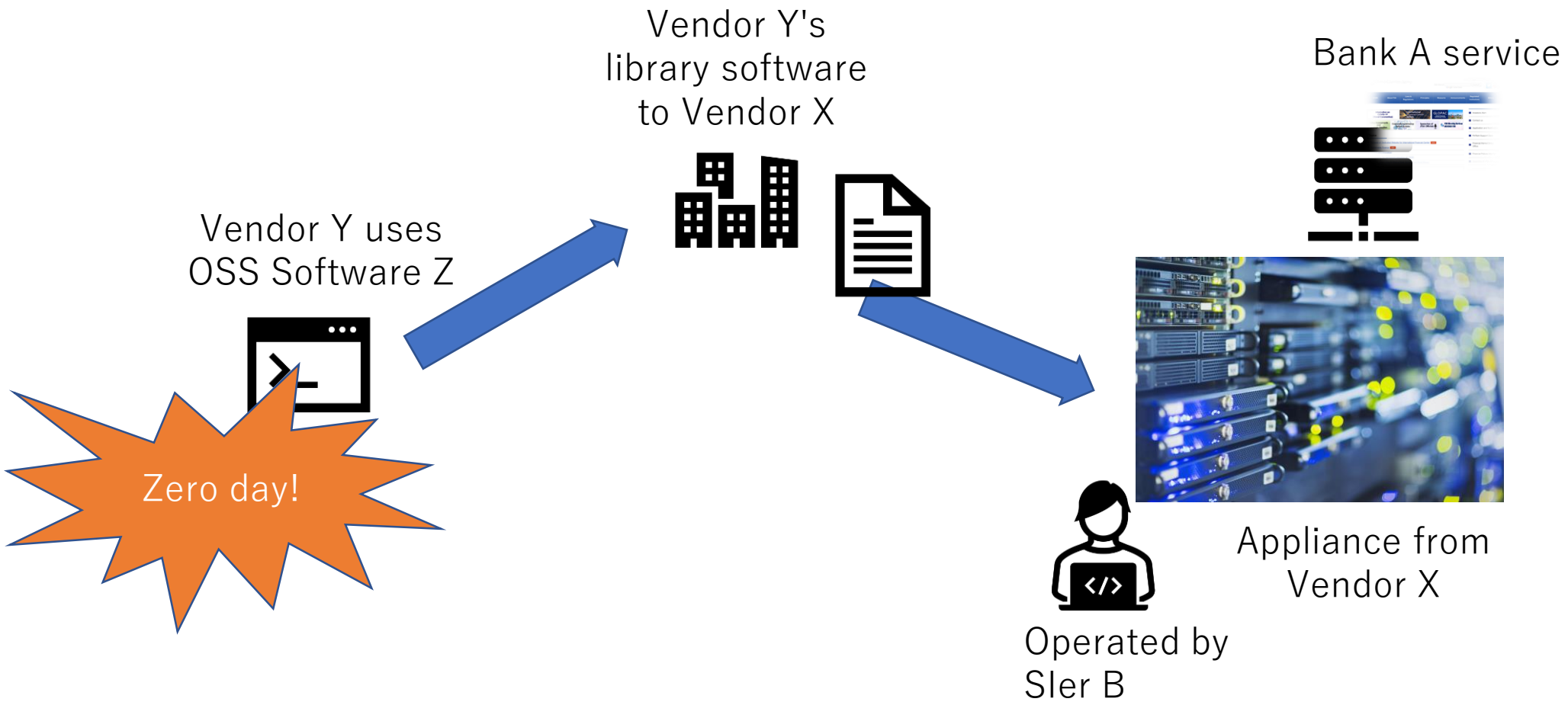
Vulnerability Exploitation Attempt

- Various vulnerability exploitation attempt has seen
  - Open source Vulnerability assessment tool
  - Newly published vulnerability PoC attempt
  - Zero-day

- Difficulty of vulnerability management
  - Vulnerability risk evaluation and apply patch

- Difficulty of Asset management
  - Where are the vulnerable IT assets?

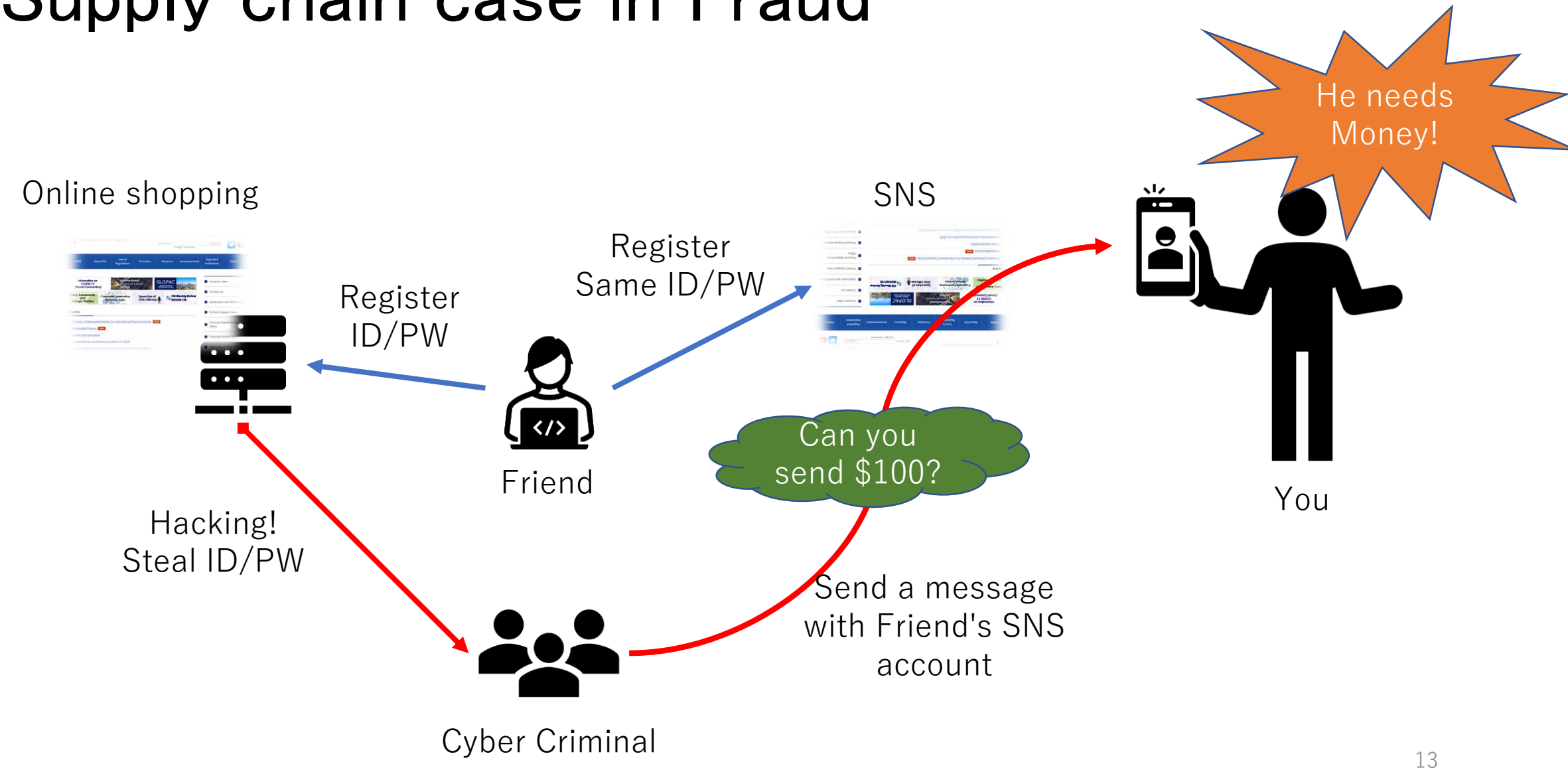
Supply chain case in VEA



Fraud

- Cyber criminals(?) are stealing various information
  - Personal information
  - Bank account info
  - Credit card numbers
  - Online credentials
  - etc
- Criminals can correlate individual person PII
  - And selling
- Phishing, Social Engineering, Malware, etc
  - email/sms/site/SNS

Supply chain case in Fraud



Conclusion

- Supply chain risk is everywhere in every threats.
- Difficult to catch up the latest threat landscape
- Collaboration among financial industry is a key
- Flexibility and agility required
- Availability vs Security

Fast, Frank and Friendly