Insights on Cyber Security Trends for SMEs

中小企網絡保安趨勢的見解分享

Yu On NG
Manager, Cyber Security
HKPC
7/28/2021

HKCERT services

01 Security Alert Monitoring and Early Warning

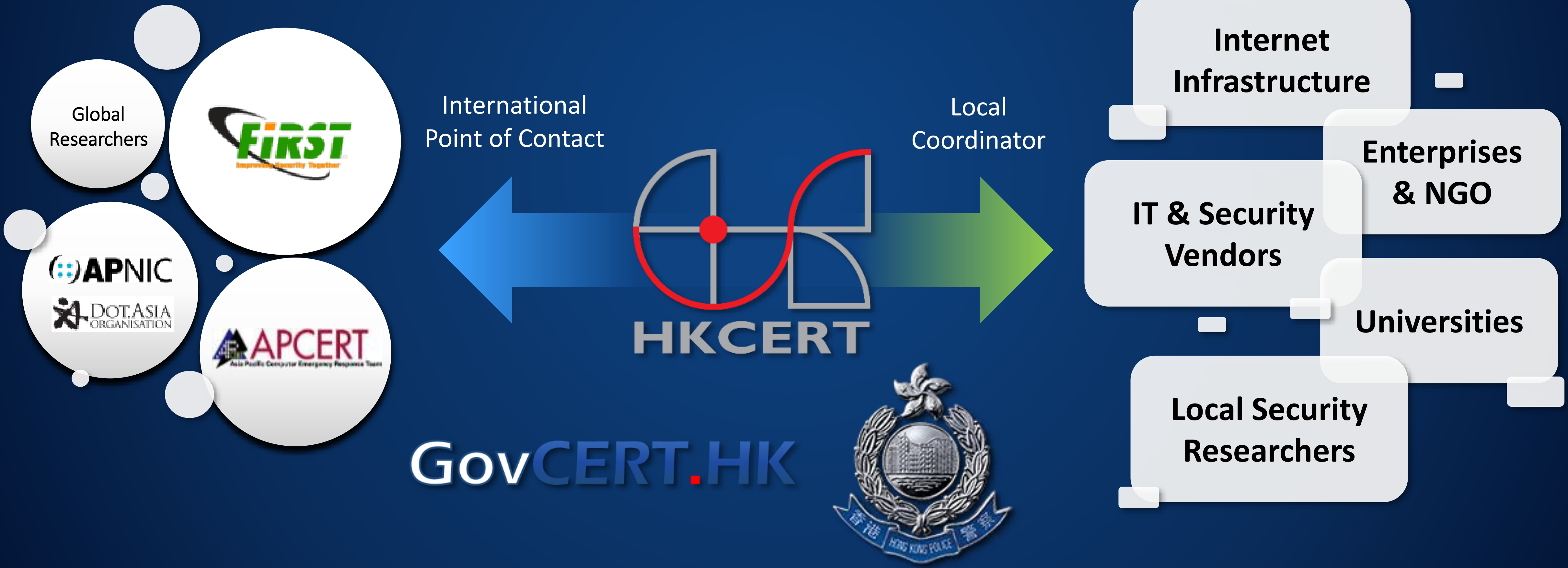
02 Report and Response

03 Publication of Security Guidelines and Informatior

04 Promotion of Information Security Awareness

HKCERT acts as

point of contact for cross-border cyber security incidents for Hong Kong



Global Researchers

International Point of Contact

Local Coordinator

Internet Infrastructure

Enterprises & NGO

IT & Security Vendors

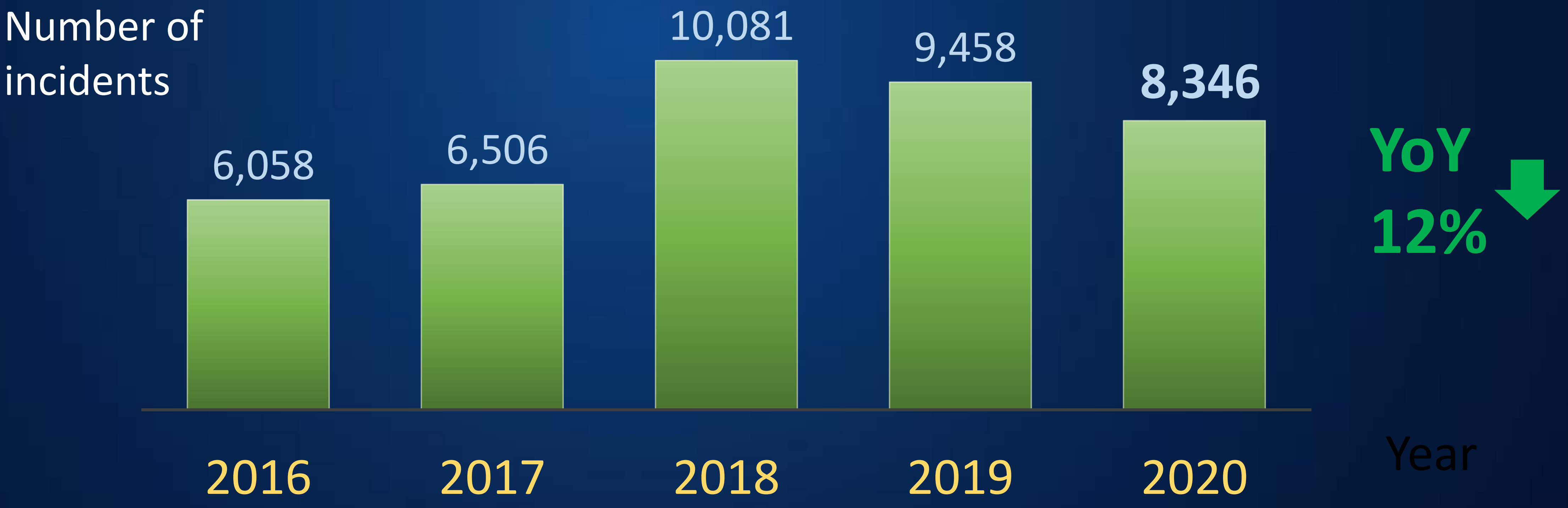
Universities

Local Security Researchers

HKCERT

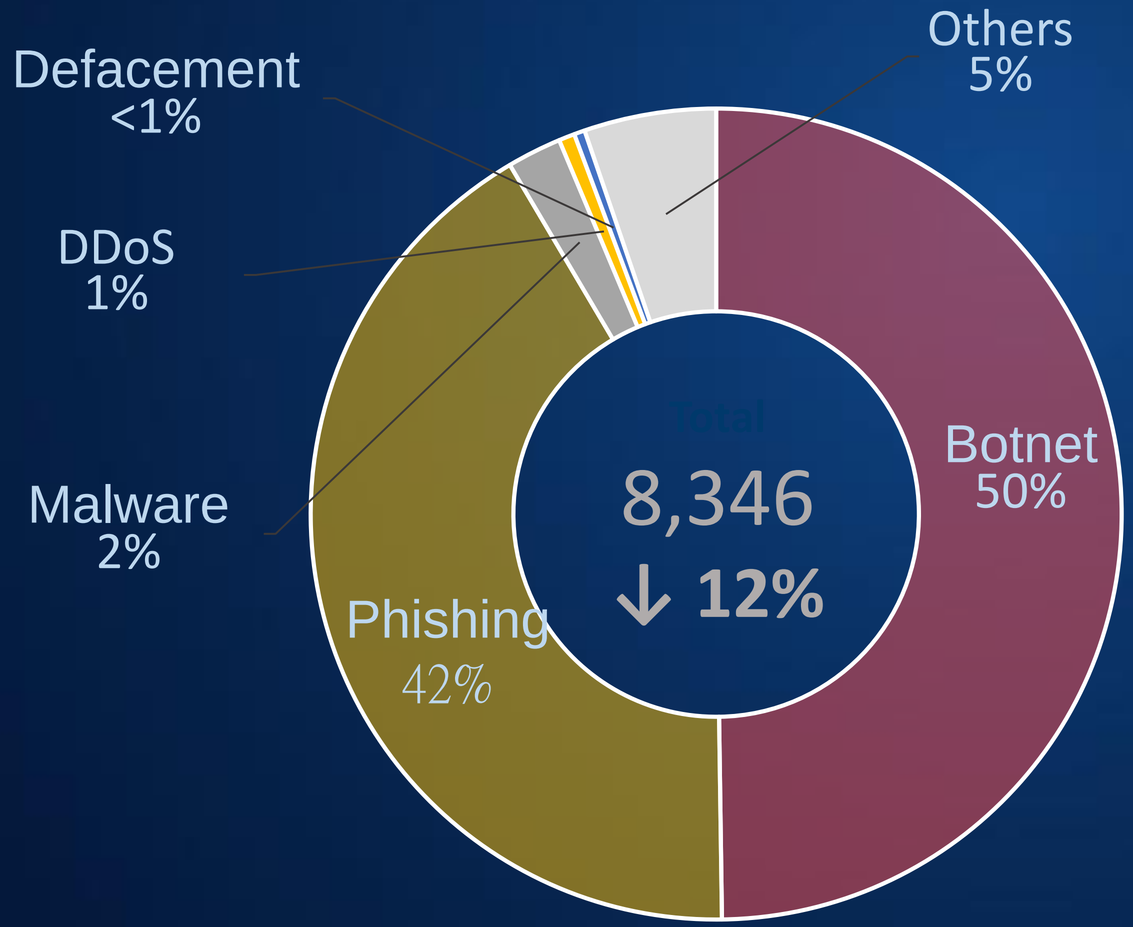
Cyber Security Outlook

HKCERT Security Incident Reports Handled



Source : HKCERT

HKCERT Security Incident Reports



Major Security Incidents

	2019	2020	Change 變化
Botnet	4,922	4,154	⬇ 16%
Phishing	2,587	3,483	⬆ 35%
Malware	1,219	181	⬇ 85%

Ransomware mainly targets the enterprises, causing a drop of personal malware cases

Source : HKCERT

Security Risks of the New Normal

Proliferated Targeted and Organised Cyber Attack

Escalated Supply Chain Attacks

Security Risks of the New Normal

Threat landscape changes along with the "New Normal"

Remote Work

Distance Learning

Digital and Contactless Payments

Tele-Medicine

Online Entertainment

Robotics

Online Shopping

Security Risks of the New Normal

Threat landscape changes along with the "New Normal"

Remote Work

Distance Learning

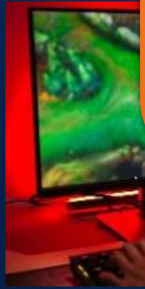
Digital and

Cor

Pa

Tele-

edicine



Entertainment

Robotics

Online Shopping

About 81% employers in Hong Kong believe hybrid work is feasible in the future; while 62% of them have plans to implement it permanently.

Source: HKPC Survey (2021-Jul)

Security Risks of the New Normal

Web meeting hijack

Attacks targeting remote access and remote storage

Attacks targeting distance working endpoints

Increased phishing and ransomware attacks

Formulate Security Strategy for the New Normal

SMEs and Enterprises

- Provide WFH security guideline
- Plan for capacity resilience for remote working
- Protect remote access facilities and endpoints
- Raise user security awareness

Employees and Users

- Ensure privacy and security of working environment
- Keep business and leisure apart
- Think before connecting or entering credentials
- Report suspicious activity

Useful Guidelines

Six Security Tips for Home Office
https://www.hkcert.org/security-guideline/six-security-tips-for-home-office

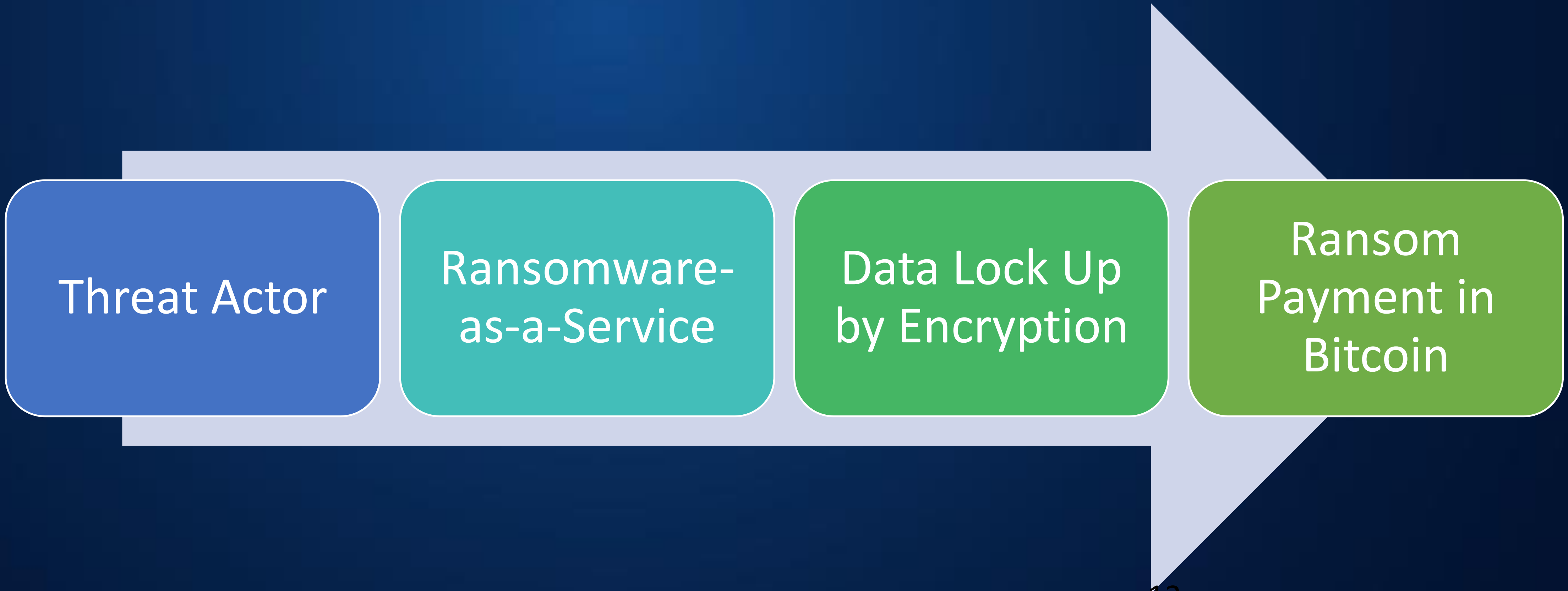
Assessing the Security of Remote Access Services Guideline
https://www.hkcert.org/security-guideline/assessing-the-security-of-remote-access-services-guideline

Ransomware

Ransomware Evolution

Traditional Approach

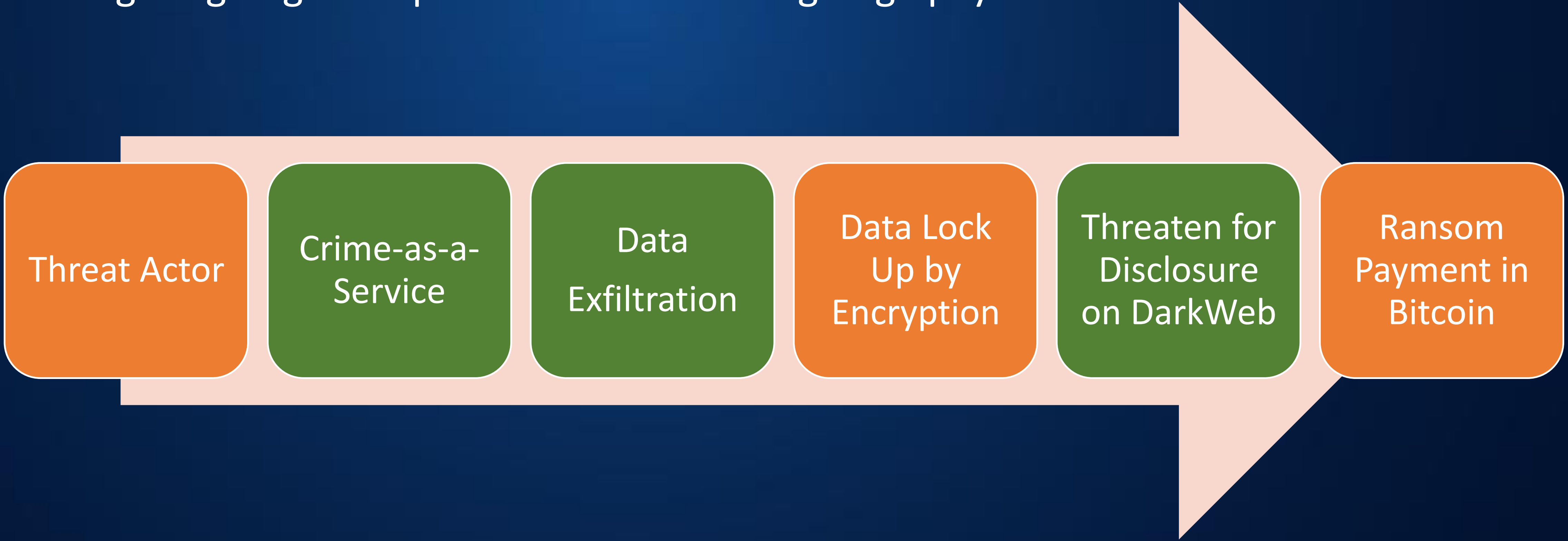
Indiscriminate campaigns spreading the malware to variety of victims



Ransomware Evolution

Evoluted Approach

- More targeted and sophisticated
- Targeting large companies and demanding huge payments



Threat Actor

Crime-as-a-Service

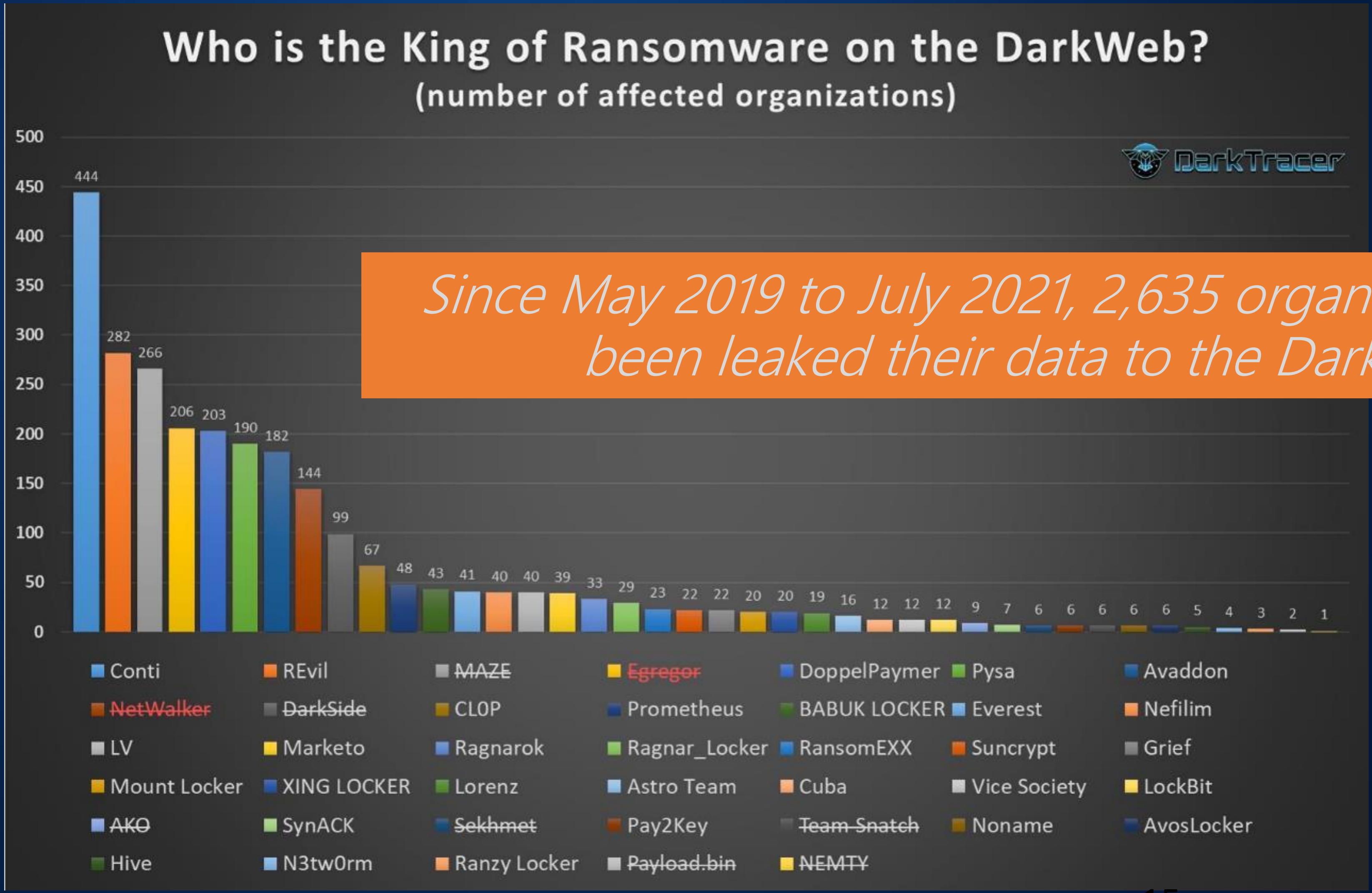
Data Exfiltration

Data Lock Up by Encryption

Threaten for Disclosure on DarkWeb

Ransom Payment in Bitcoin

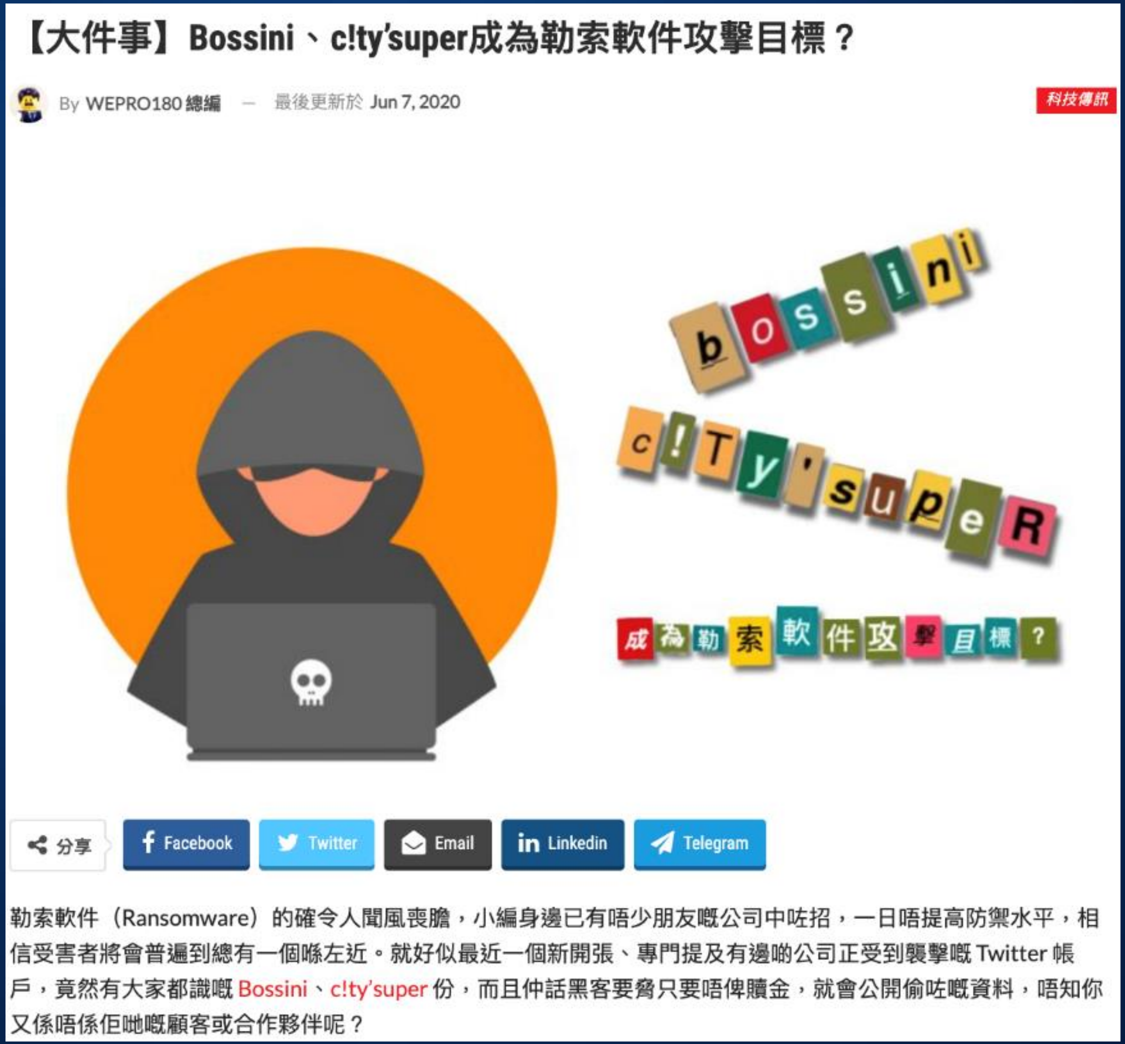
Ransomware on the DarkWeb



Since May 2019 to July 2021, 2,635 organisations have been leaked their data to the Dark Web

Source: https://twitter.com/darktracer_int/status/1416026018452672513/photo/1

Ransomware Incidents in Hong Kong



【大件事】Bossini、c!ty'super成為勒索軟件攻擊目標？

By WEPRO180 總編 — 最後更新於 Jun 7, 2020

勒索軟件（Ransomware）的確令人聞風喪膽，小編身邊已有唔少朋友嘅公司中咗招，一日唔提高防禦水平，相信受害者將會普遍到總有一個喺左近。就好似最近一個新開張、專門提及有邊啲公司正受到襲擊嘅 Twitter 帳戶，竟然有大家都識嘅 Bossini、c!ty'super 份，而且仲話黑客要脅只要唔俾贖金，就會公開偷咗嘅資料，唔知你又係唔係佢哋嘅顧客或合作夥伴呢？

Source: https://wepro180.com/tech-news/【大件事】bossini、ctysuper成為勒索軟件攻擊目標？/

More and More New Extortion Methods…

Contacting Victims’ Customers and Partners

DDoS Extortion

Short Selling Victims’ Stock

Disruption Critical Infrastructure Systems operated by Victims

Paying Ransom or Not?

AXA cyber-insurance policies in France (2021-May)

- Insurance company AXA stop reimbursing ransom payments for ransomware victims in France

Tax deductible in U.S. (2021-Jun)

- The ransom payments made in ransomware attacks may be tax deductible, just like the other traditional crimes, such as robbery or embezzlement

Sophos State of Ransomware 2021 Report

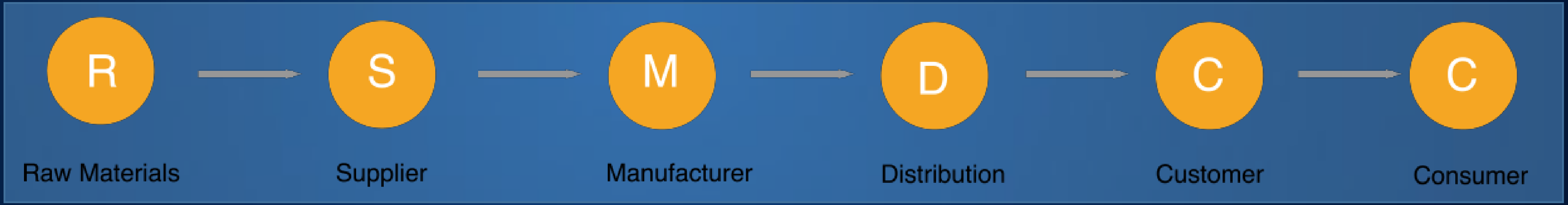
- **32%** victim companies will pay ransom in 2021, higher than **26%** in 2020
- On average, only **65%** of data can be restored after paying the ransom

Source: https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

Supply Chain Attack

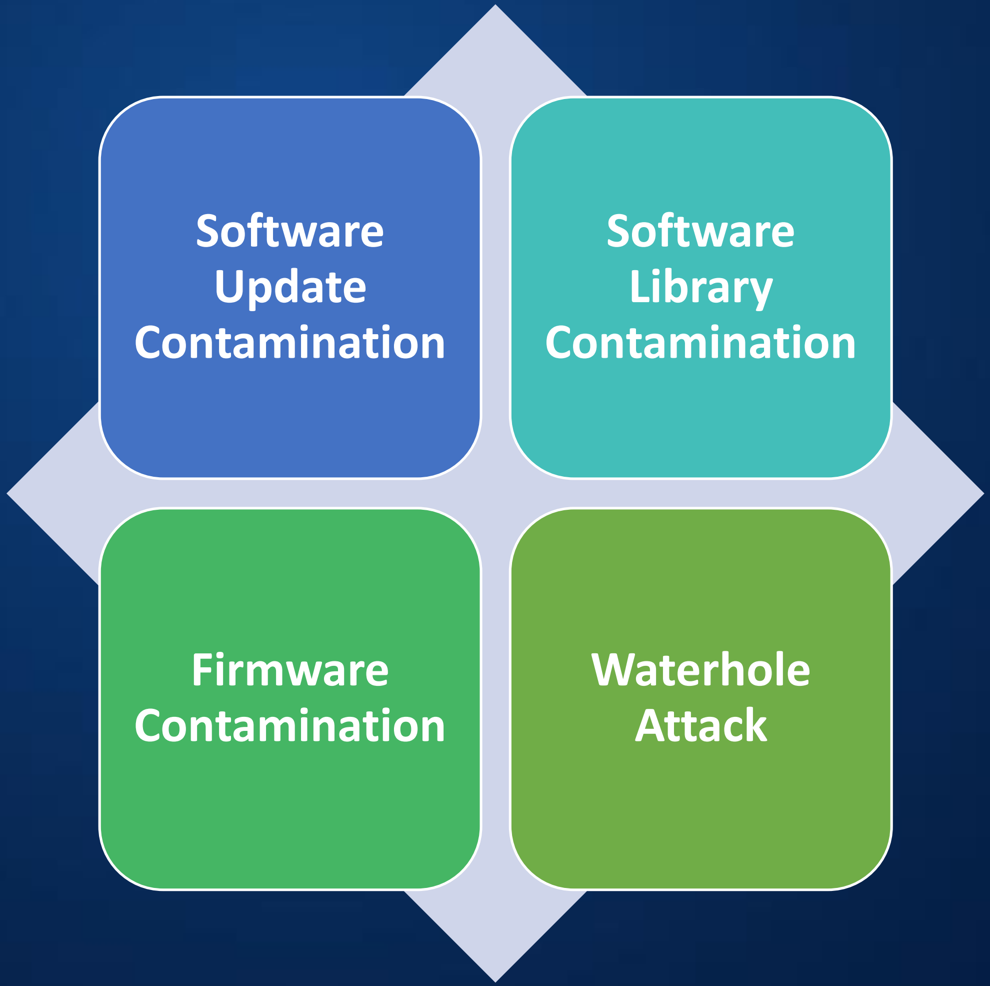
What is Supply Chain Attack?

A basic diagram of a supply chain network



Attackers target weak points in the supply chain to launch their initial attacks.

Forms of Supply Chain Attacks



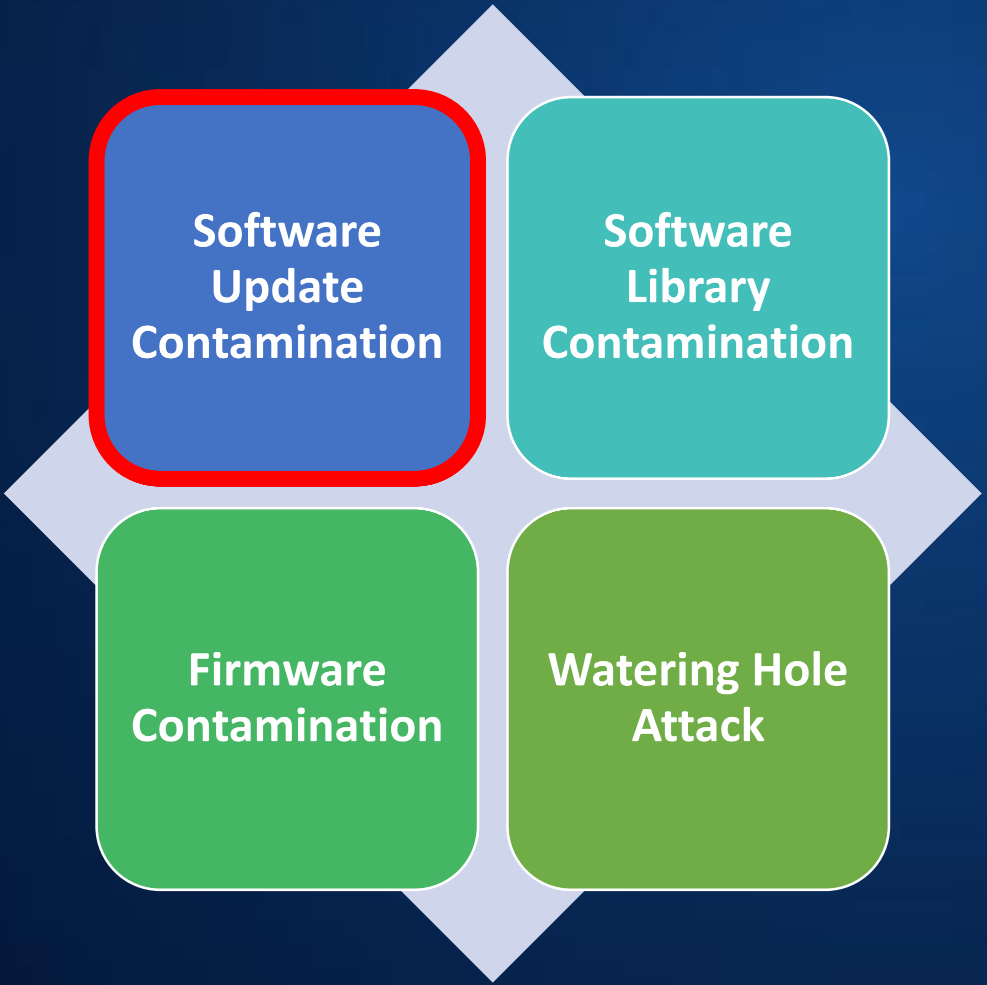
Software Update Contamination

Software Library Contamination

Firmware Contamination

Waterhole Attack

Forms of Supply Chain Attacks



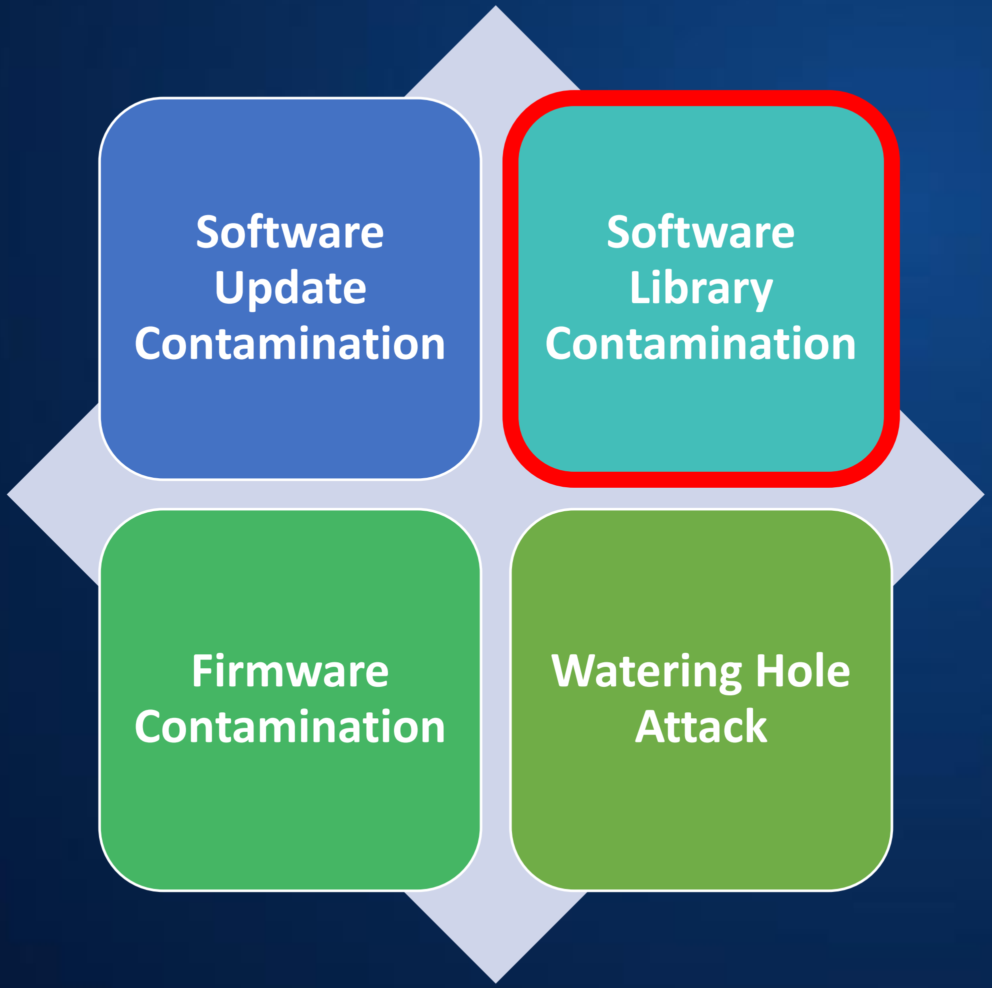
By compromising the software update mechanism, an attacker may lure the victim install a compromised software from a trusted supplier.

solarwinds

Trojan in Solarwinds Orion software (2020-Dec)

- Affected 18,000 customers
  - Over 425 of Fortune 500
  - Top 10 US Telcos
  - US military and government departments

Forms of Supply Chain Attacks



Software Update Contamination

Software Library Contamination

Firmware Contamination

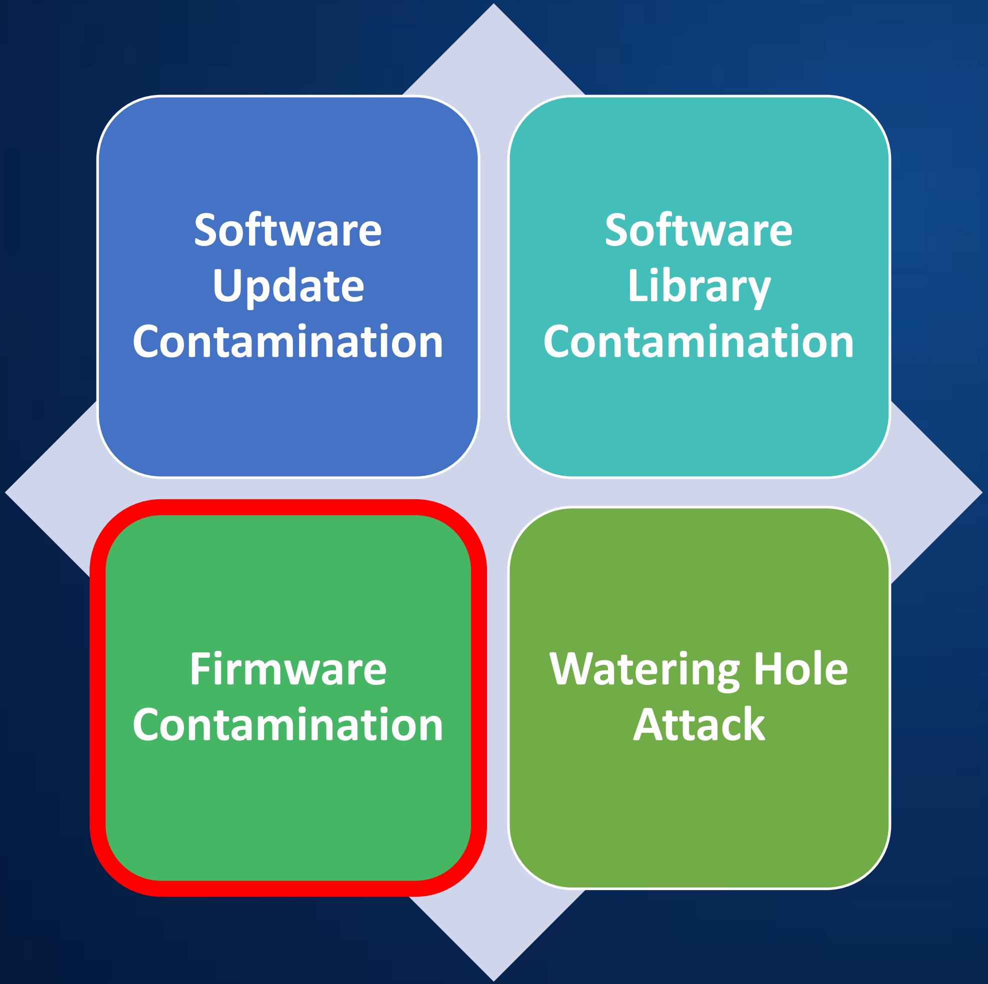
Watering Hole Attack

Software Library Contamination attack happens through the third-party code that software developers use in their projects.

Typosquatting attack was found in PyPI (2021-Mar)

- 3591 new packages were uploaded to Python Package Index
- The packages name had **similar name** of another popular packages
- These packages may involve malicious code

Forms of Supply Chain Attacks

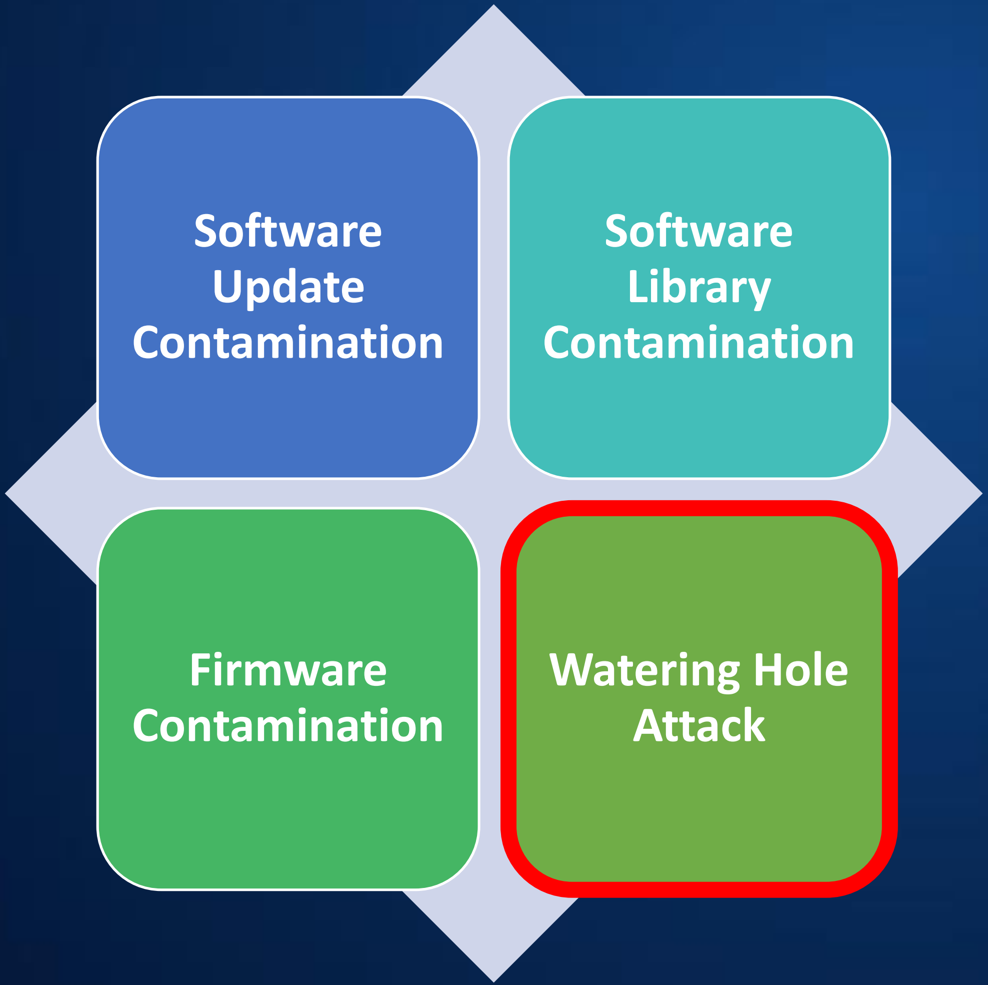


Firmware contamination is difficult to detect because pre-loaded firmware coming with devices is at a lower level than the operating system.

Vulnerable firmware in the supply chain of major server manufacturers (2019-Jul)

- Two serious vulnerabilities in **baseboard management controller (BMC)** firmware used by Lenovo, Gigabyte, Acer and other manufactures.
- An attacker with administrative rights could exploit some of these vulnerabilities to trigger arbitrary code execution.

Forms of Supply Chain Attacks



Software Update Contamination

Software Library Contamination

Firmware Contamination

Watering Hole Attack

In Watering Hole Attack, an attacker poisons a website frequently visited by victims. Victims trusting the website were prompted to download.

A watering hole attack on a Hong Kong Website (2018-Mar)

- An embedded Adobe Flash file that can exploit the Flash Player vulnerability CVE-2018-4878, was added on the home page of a Hong Kong Telecommunications company website.
- A successful exploit on this flash vulnerability can lead to arbitrary code execution.

Tackling Supply Chain Attacks

1. Put third party security management in place

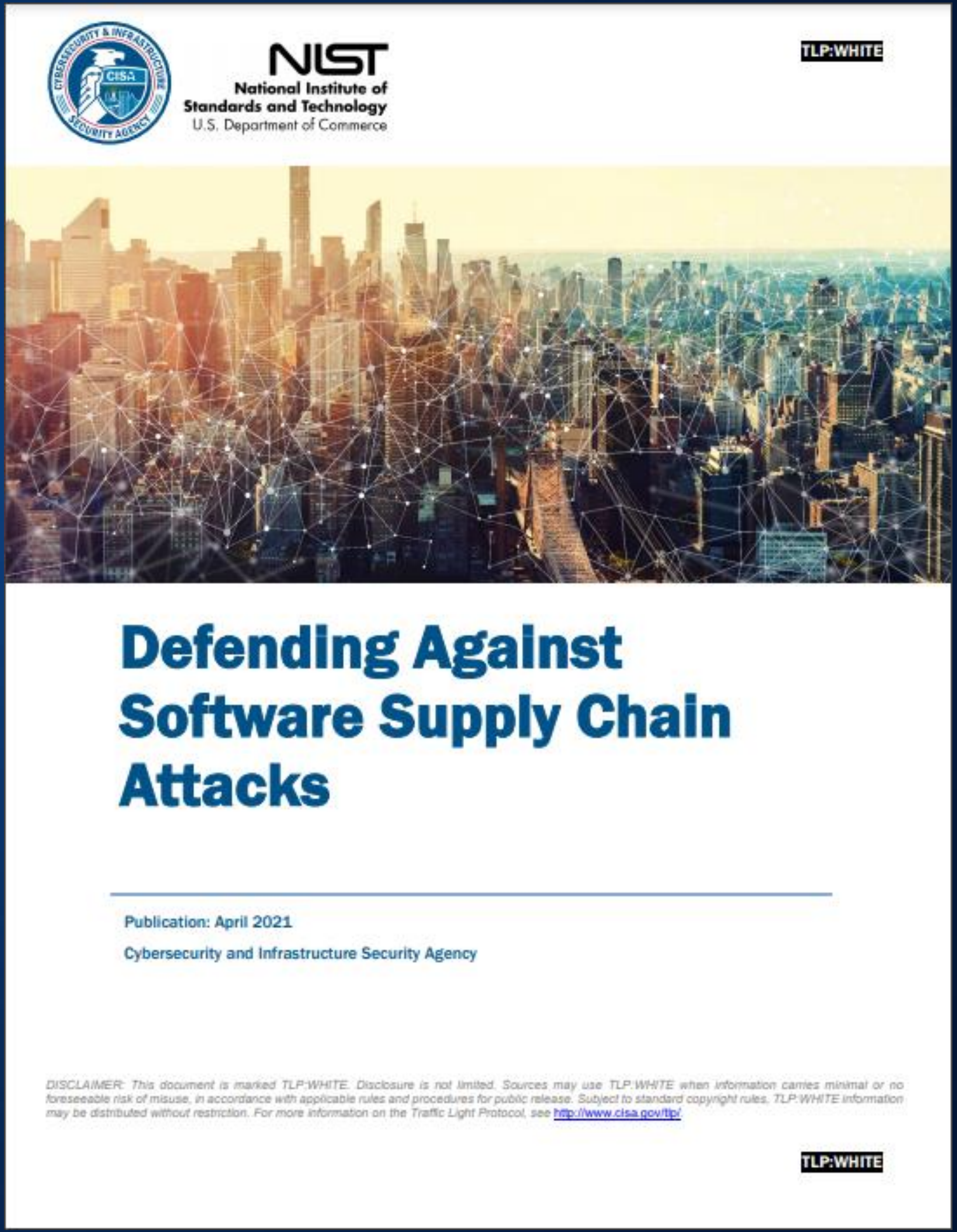
- Put third party security into security policy.
- Purchase only from authorized suppliers.
- Put in place controls in contracts.
- Employ network separation and restrict access of partners to enterprise network.
- Test third party software and updates before deployment

Tackling Supply Chain Attacks

2. Require service providers to implement security measures in service provision

- Provide contact points for incident reports.
- Provide transparency to clients of their security controls related to the service provision.
- Provide proof of authenticity and integrity to delivered software and patches.
- Give timely notification of the cyber incidents and the critical vulnerability of their products and services.
- Attend the company-side security awareness programme

Defending Against Software Supply Chain Attacks
- CISA
(ǎóǎá – Apr)



TLP:WHITE

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Defending Against Software Supply Chain Attacks

Publication: April 2021

Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules. TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

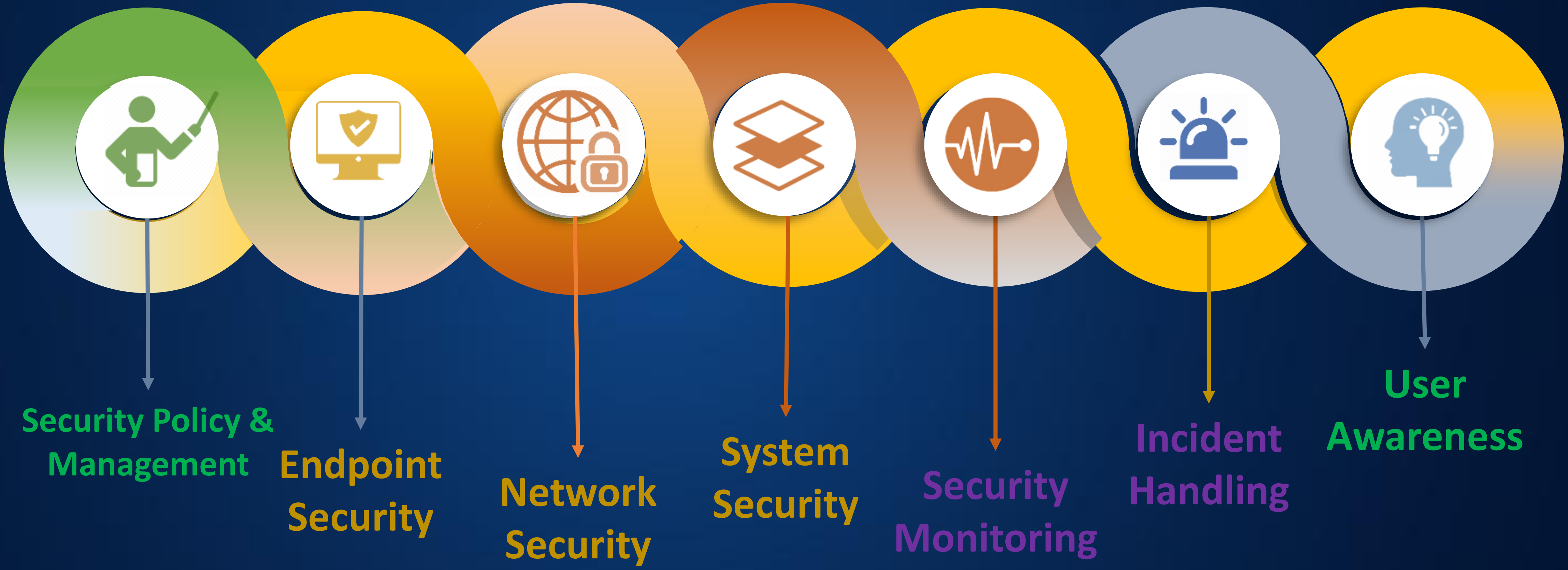
TLP:WHITE

Source: https://www.cisa.gov/publication/software-supply-chain-attacks

Security Advices

Conduct the Self-Assessment

HKCERT - The Seven Habits of Cyber Security for SMEs



Security Policy & Management

Endpoint Security

Network Security

System Security

Security Monitoring

Incident Handling

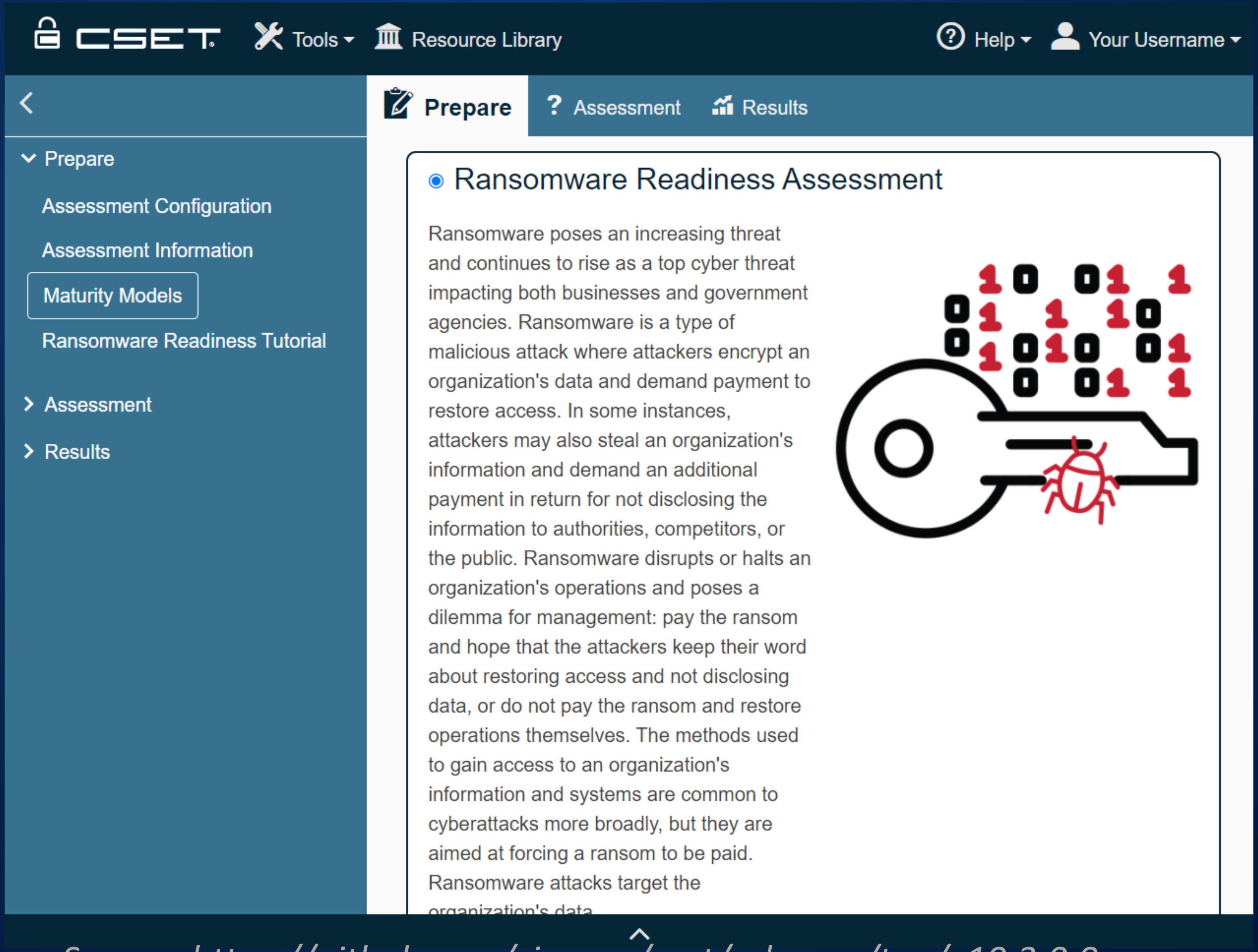
User Awareness

Best Practices ✚ Self-assessment List

https://www.hkcert.org/security-guideline/seven-habits-of-cyber-security-for-smes

HKCERT

CISA - Cyber Security Evaluation Tool (CSET®) Ransomware Readiness Assessment (RRA)



● Ransomware Readiness Assessment

Ransomware poses an increasing threat and continues to rise as a top cyber threat impacting both businesses and government agencies. Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. In some instances, attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. Ransomware disrupts or halts an organization's operations and poses a dilemma for management: pay the ransom and hope that the attackers keep their word about restoring access and not disclosing data, or do not pay the ransom and restore operations themselves. The methods used to gain access to an organization's information and systems are common to cyberattacks more broadly, but they are aimed at forcing a ransom to be paid. Ransomware attacks target the organization's data

Source: https://github.com/cisagov/cset/releases/tag/v10.3.0.0

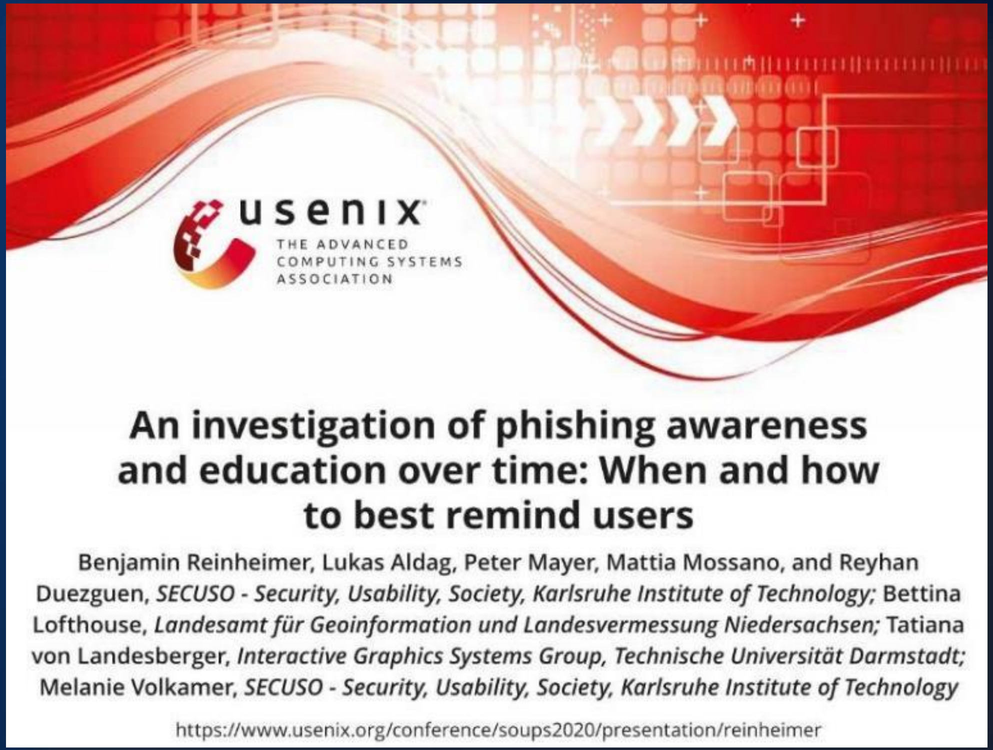
Compliance with Cyber Security Standards

ISO/IEC 27001 provides the requirements for an information security management system (ISMS). It is a management system designed to place information security under management control.

Image Source: Info Comply

Build Human Firewall

- **Organize Cyber Security Awareness Training**
  - Awareness training need to retrain after six months
- **Build a Strong Culture of Security**
  - Business units take accountability
  - Staff used to use alternative communication channel to verify transaction requests
  - Staff stay vigilant to unsolicited email and website
- **Develop Metrics on Security Awareness**
  - Regular cyber security drill exercise



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

An investigation of phishing awareness and education over time: When and how to best remind users

Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, and Reyhan Duezguen, *SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology;* Bettina Lofthouse, *Landesamt für Geoinformation und Landesvermessung Niedersachsen;* Tatiana von Landesberger, *Interactive Graphics Systems Group, Technische Universität Darmstadt;* Melanie Volkamer, *SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology*

https://www.usenix.org/conference/soups2020/presentation/reinheimer

Survey on Phishing Drill Effectiveness

Source: https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf

HKCERT Cyber Security Initiatives 2021

“Hack me if you can” animation series (Jan – Apr)

HKCERT

(1) 遙距工作及視像會議安全攻略

(2) 雲端保安要做足 確保資料無漏出

(3) 釣魚攻擊要小心 不明電郵咪亂開

(4) 5G和物聯網保安

Thank you

Hong Kong Productivity Council
香港生產力促進局
HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org