HKCERT

Be Smart Online – Defend Against Extortion Attacks

Yu On NG
Security Consultant,
HKCERT

Agenda

1. Cyber Extortion

i. Ransomware

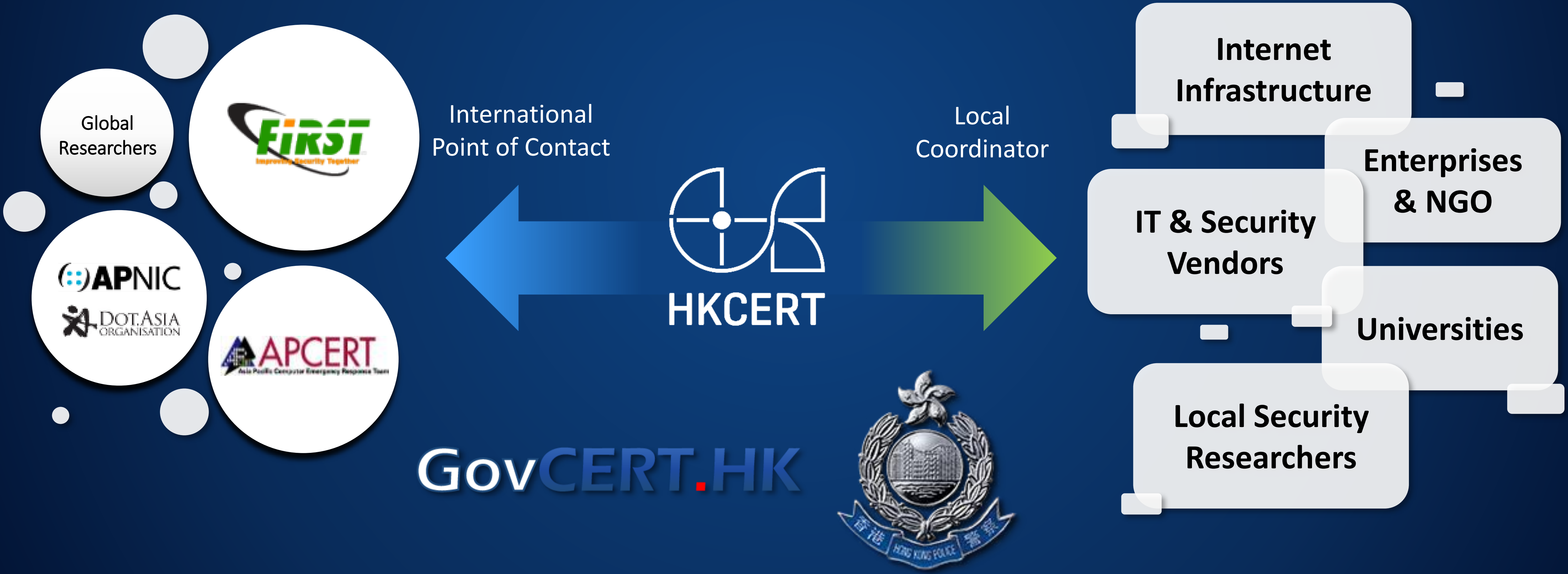
ii. Ransom Email

iii. Ransom DDoS

2. Security Advice

HKCERT acts as

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



Global Researchers

International Point of Contact

HKCERT

Local Coordinator

Internet Infrastructure

Enterprises & NGO

IT & Security Vendors

Universities

Local Security Researchers

FIRST
Improving Security Together
APNIC
DOT.ASIA ORGANISATION
APCERT
Asia Pacific Computer Emergency Response Team
GovCERT.HK
香港警察
HONG KONG POLICE

HKCERT services

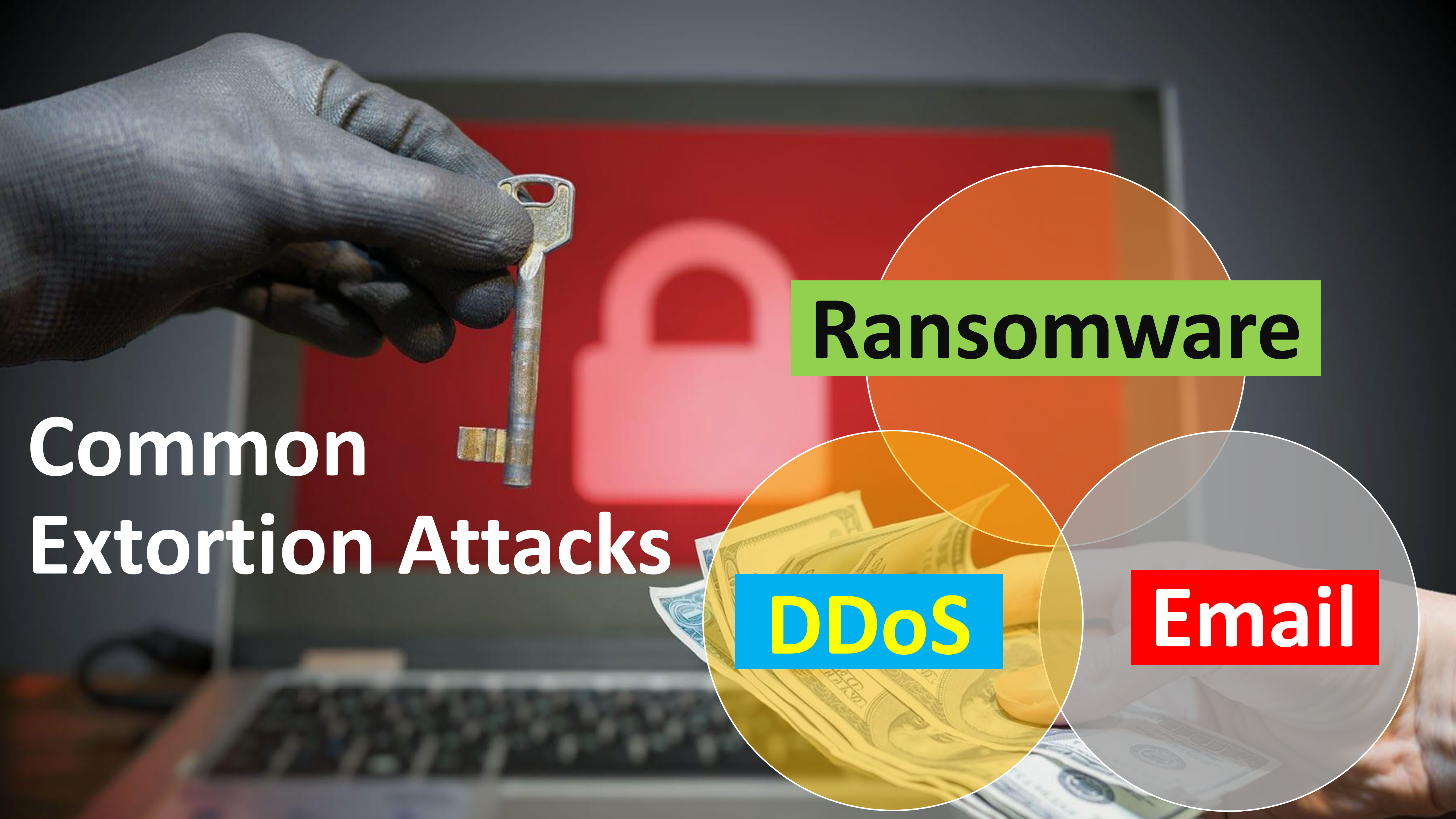
01 Security Alert Monitoring and Early Warning

02 Report and Response
Hotline: 8105-6060

03 Publication of Security Guidelines and Information

04 Promotion of Information Security Awareness

Common
Extortion Attacks



Ransomware

DDoS

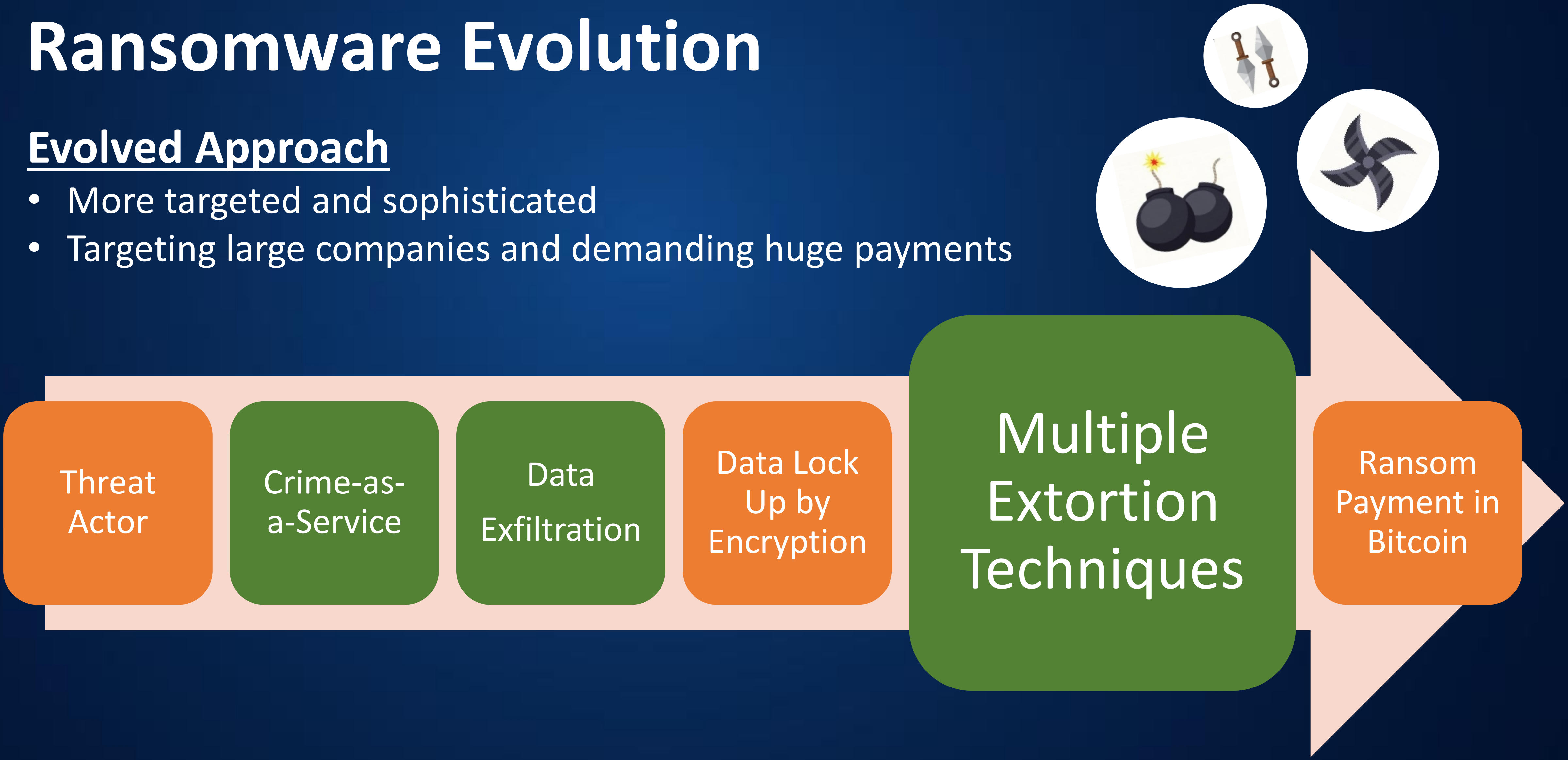
Email

Ransomware

Ransomware Evolution

Evolved Approach

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



Threat Actor

Crime-as-a-Service

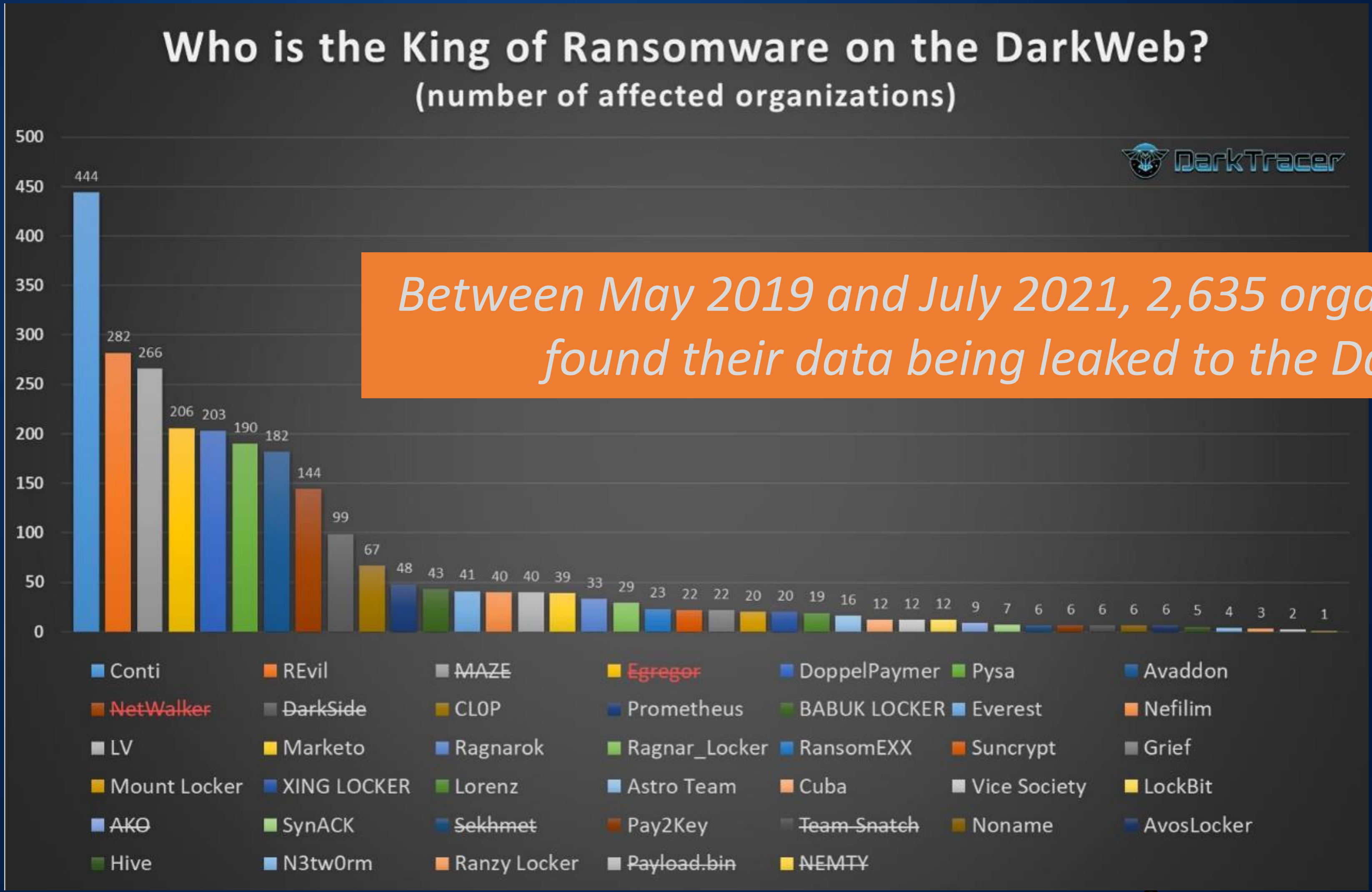
Data Exfiltration

Data Lock Up by Encryption

Multiple Extortion Techniques

Ransom Payment in Bitcoin

Sharing: Statistic on DarkWeb



Between May 2019 and July 2021, 2,635 organisations have found their data being leaked to the Dark Web

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

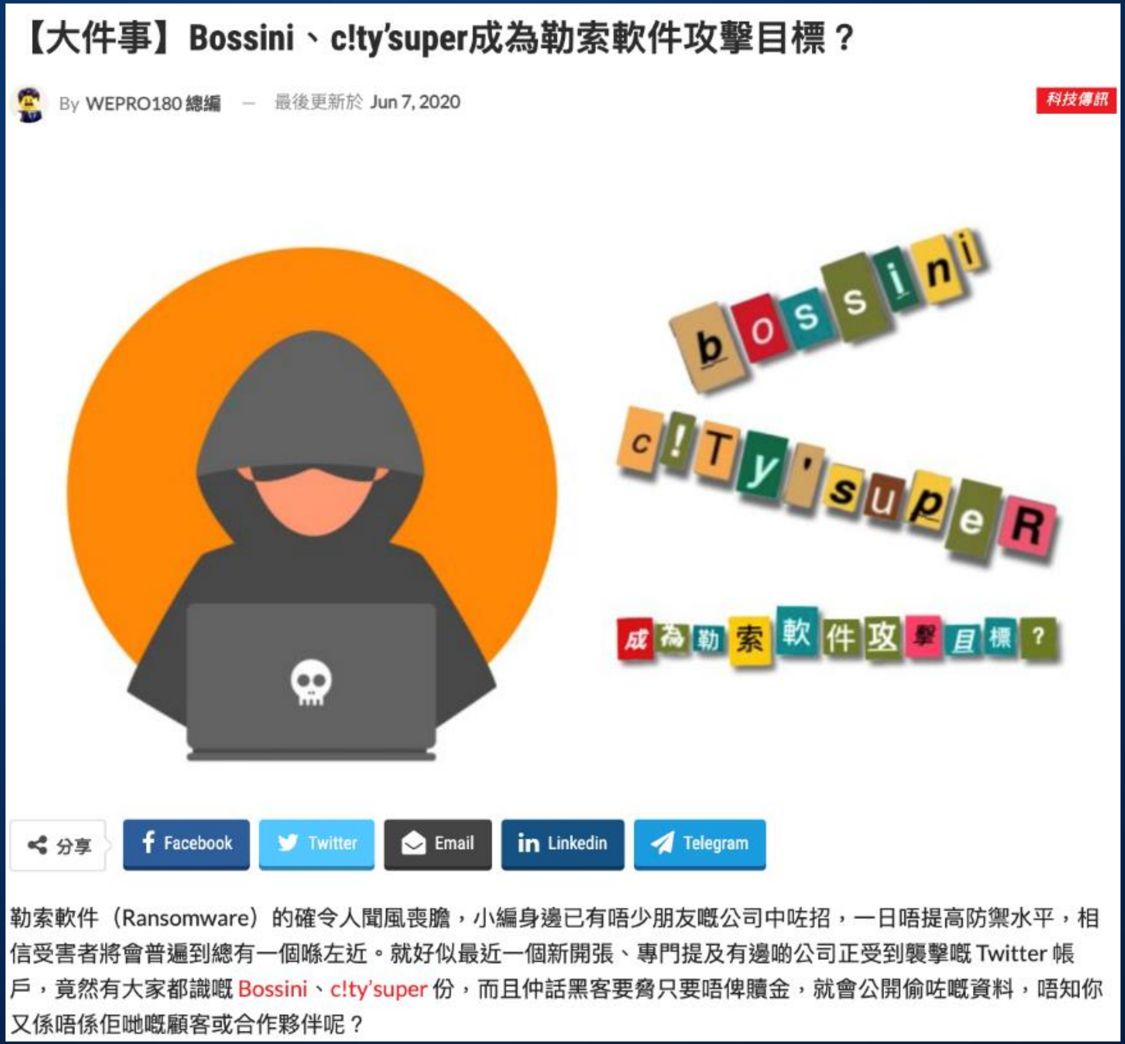
Sharing: Attack worldwide

Victims 2021

1. Critical Infrastructure **Colonial Pipeline**	**$4.4m**
2. Retail **Dairy Farm**	**$30m**
3. Manufacturer **JBS Foods**	**$11m**
4. Insurance **AXA**	**Amount Not Known**
5. Technology **Acer**	**$50m**
6. SMEs **(Kaseya supply chain attack)**	**$5m**

ource: bleepingcomputer.com, bloomberg.com, corneliustoday.com, kaseya.com and wired.com

Sharing: Attack in Hong Kong



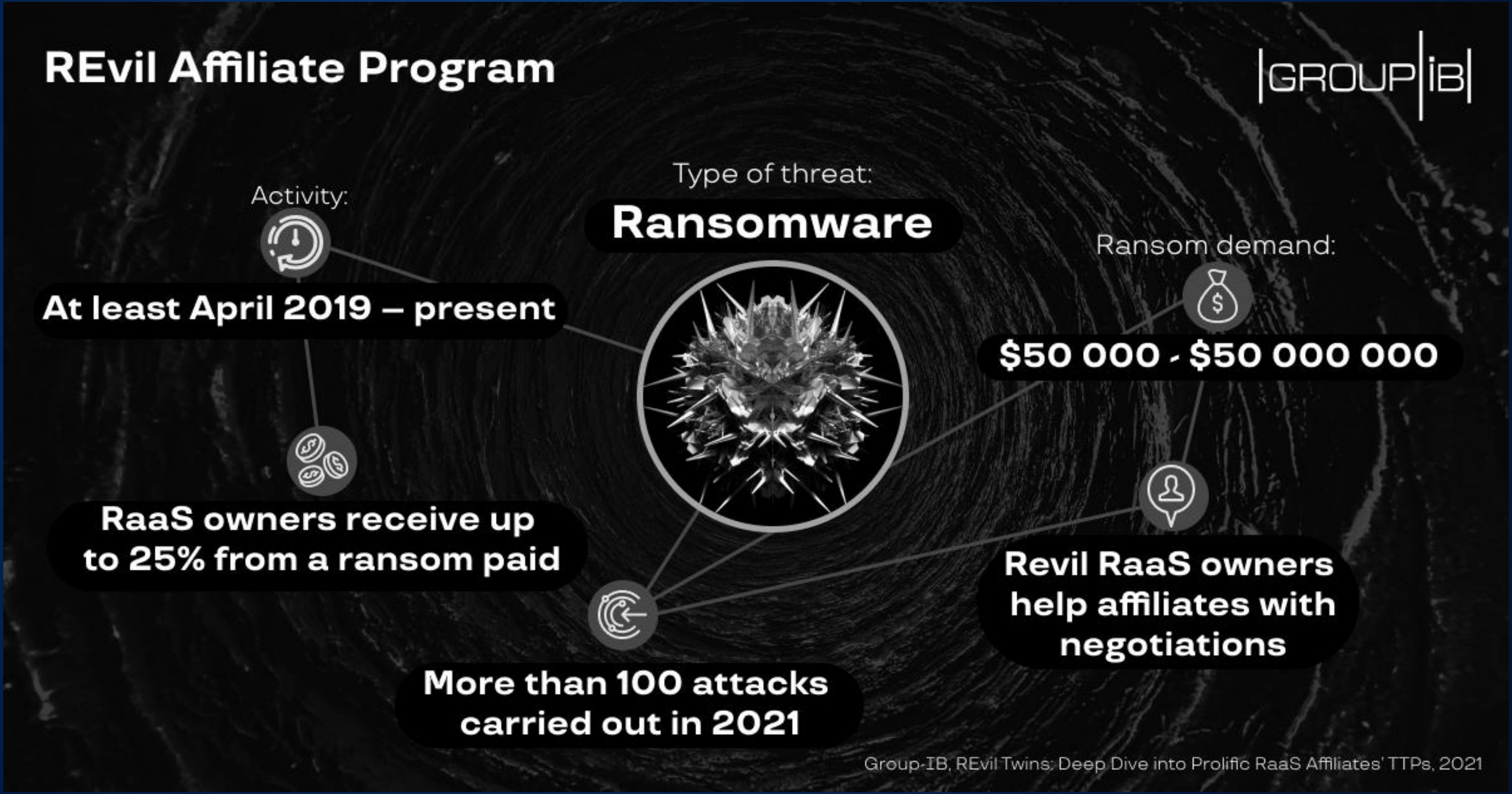
【大件事】Bossini、c!ty'super成為勒索軟件攻擊目標？

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？/

Sharing – Meet REvil RaaS



REvil Affiliate Program

Activity:

At least April 2019 – present

Type of threat:

Ransomware

Ransom demand:

$50 000 - $50 000 000

RaaS owners receive up to 25% from a ransom paid

More than 100 attacks carried out in 2021

Revil RaaS owners help affiliates with negotiations

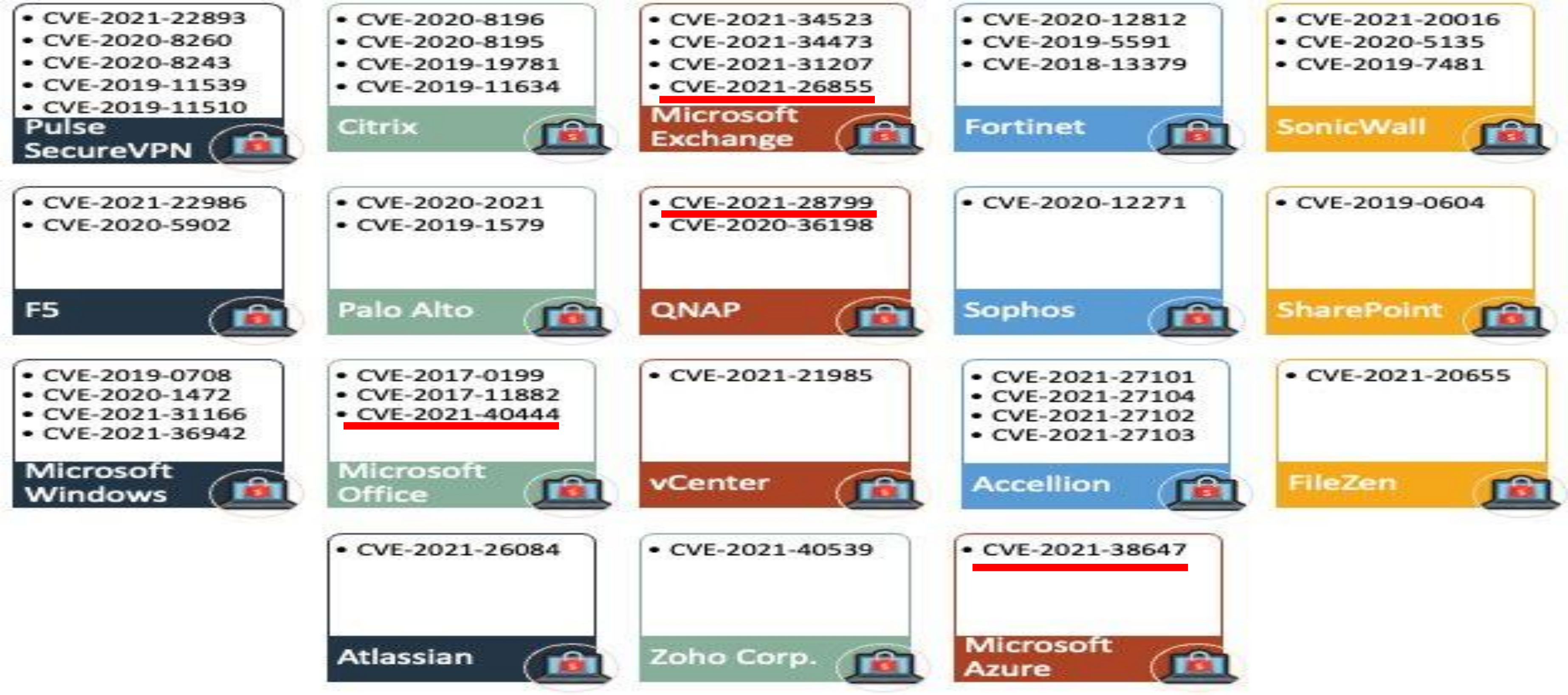
Group-IB, REvil Twins: Deep Dive into Prolific RaaS Affiliates' TTPs, 2021

urce: istockphoto.com

Major Attack Vectors

1. Phishing email (link/attachment)
2. Unsecure remote connection, e.g. RDP
3. System vulnerabilities

Vulnerabilities exploited by ransomware gang



- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8243
- CVE-2019-11539
- CVE-2019-11510

Pulse SecureVPN

- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-19781
- CVE-2019-11634

Citrix

- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Microsoft Exchange

- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Fortinet

- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

SonicWall

- CVE-2021-22986
- CVE-2020-5902

F5

- CVE-2020-2021
- CVE-2019-1579

Palo Alto

- CVE-2021-28799
- CVE-2020-36198

QNAP

- CVE-2020-12271

Sophos

- CVE-2019-0604

SharePoint

- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Windows

- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444

Microsoft Office

- CVE-2021-21985

vCenter

- CVE-2021-27101
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

Accellion

- CVE-2021-20655

FileZen

- CVE-2021-26084

Atlassian

- CVE-2021-40539

Zoho Corp.

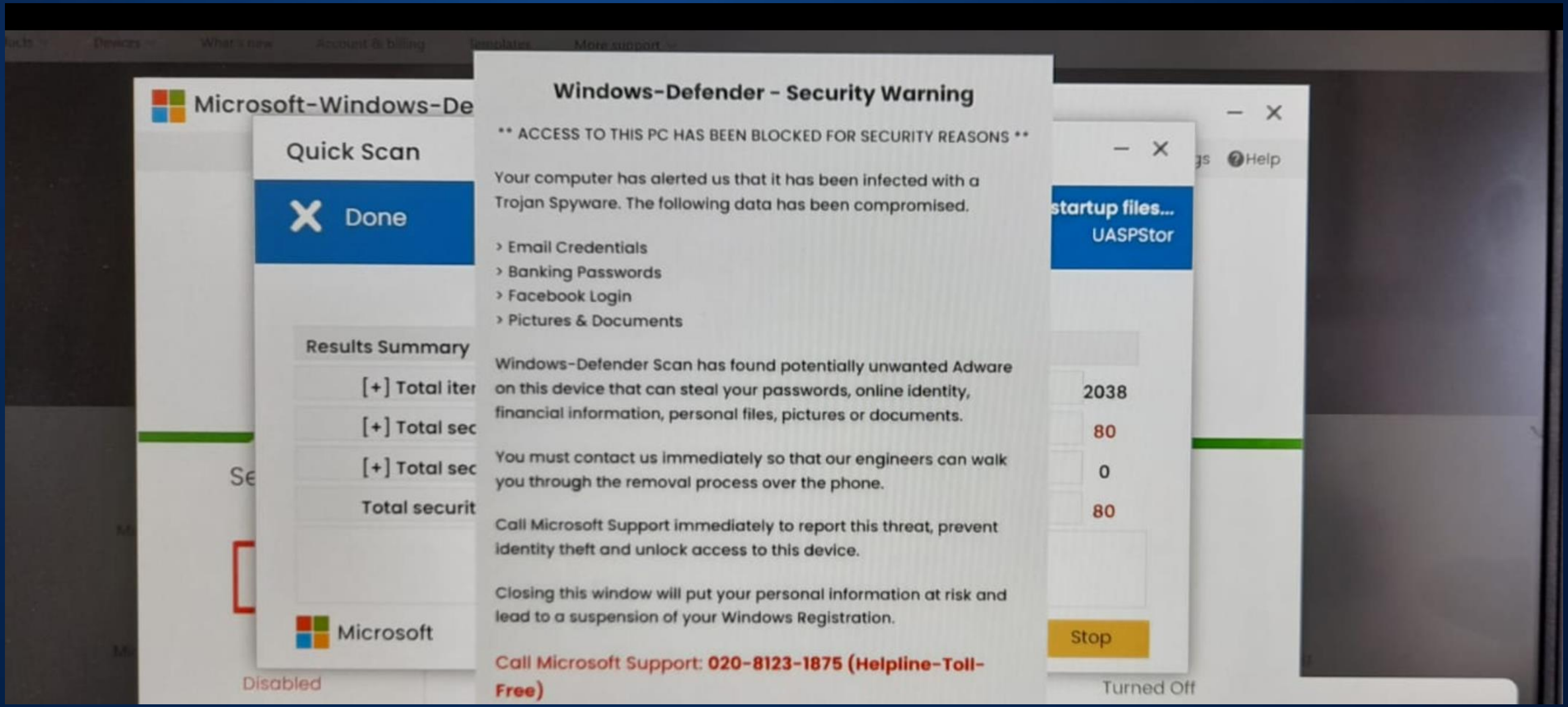
- CVE-2021-38647

Microsoft Azure

ource: bleepingcomputer.com

Major Attack Vectors

4. Tech support scam (Social Engineering with Interactive Voice Response)
5. Supply Chain Attack



Windows-Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

› Email Credentials
› Banking Passwords
› Facebook Login
› Pictures & Documents

Windows-Defender Scan has found potentially unwanted Adware on this device that can steal your passwords, online identity, financial information, personal files, pictures or documents.

You must contact us immediately so that our engineers can walk you through the removal process over the phone.

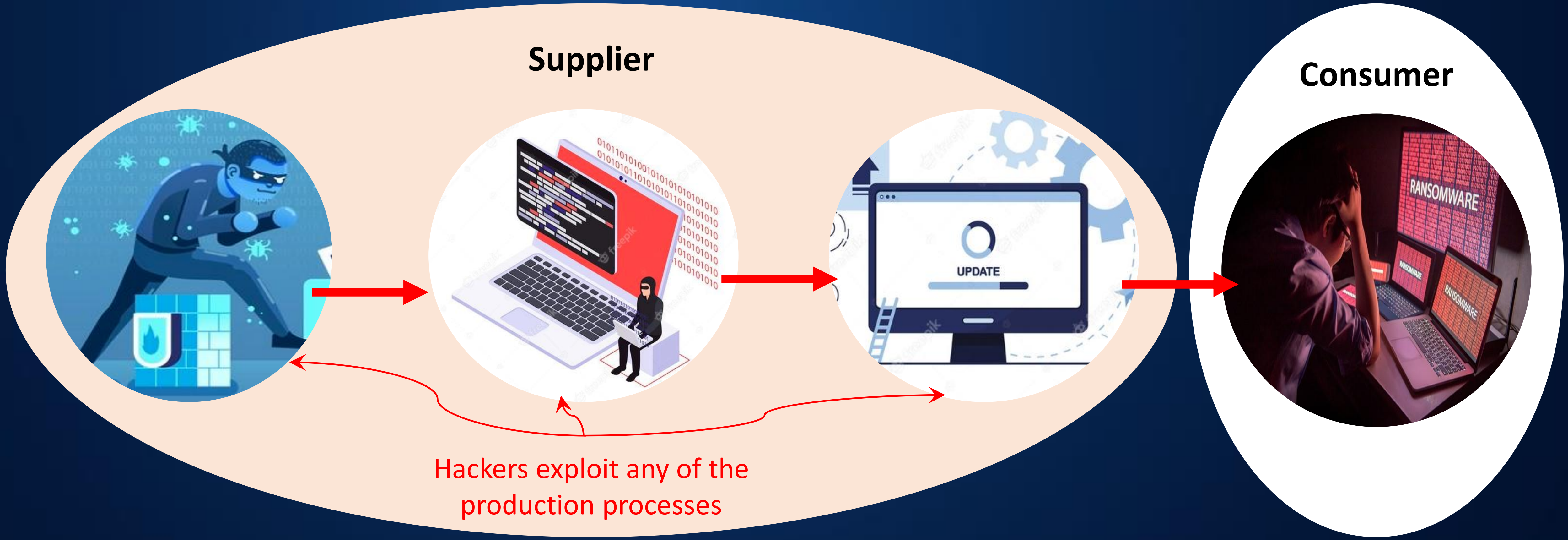
Call Microsoft Support immediately to report this threat, prevent identity theft and unlock access to this device.

Closing this window will put your personal information at risk and lead to a suspension of your Windows Registration.

Call Microsoft Support: **020-8123-1875 (Helpline-Toll-Free)**

Ransomware X Supply Chain Attacks

- Kaseya IT management tools are being compromised by supply chain attack to plant REvil ransomware to its customers



Supplier

Consumer

Hackers exploit any of the production processes

source: HKCERT

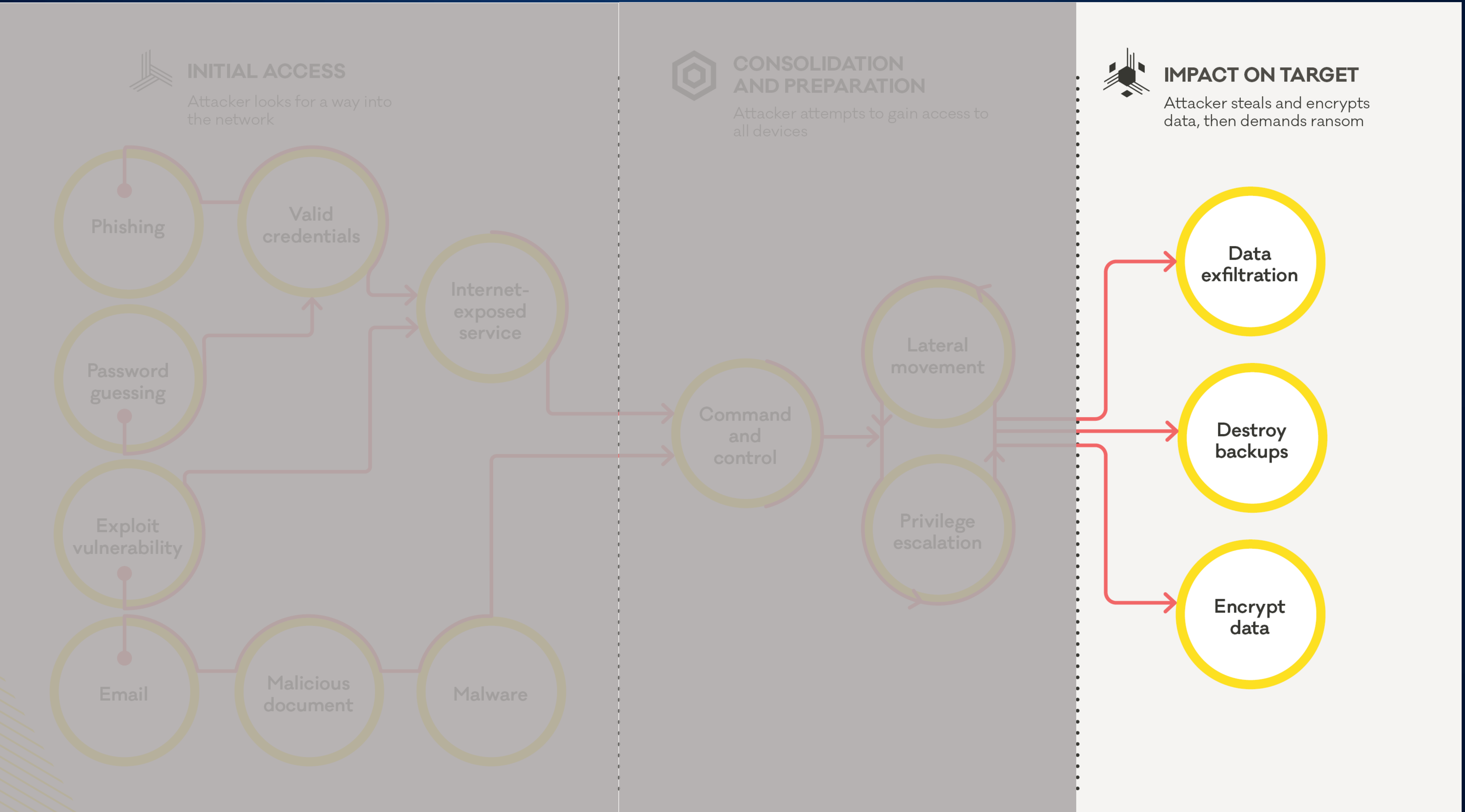


Image source: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

More and More New Extortion Methods…

Contacting Victims’ Customers and Partners

DDoS Extortion

Short Selling Victims’ Stock

Disruption Critical Infrastructure Systems operated by Victims

Email Extortion

Extortion Techniques

Claims that …

- Have stolen your password
- Know everything about you
  - Photos of you doing something embarrassing
  - Take over your webcam to record video
- Or hold your organisation data
  - Stolen from company server

Threaten you …

- Disclose your contact

Demand for …

- Demand for ransom payment

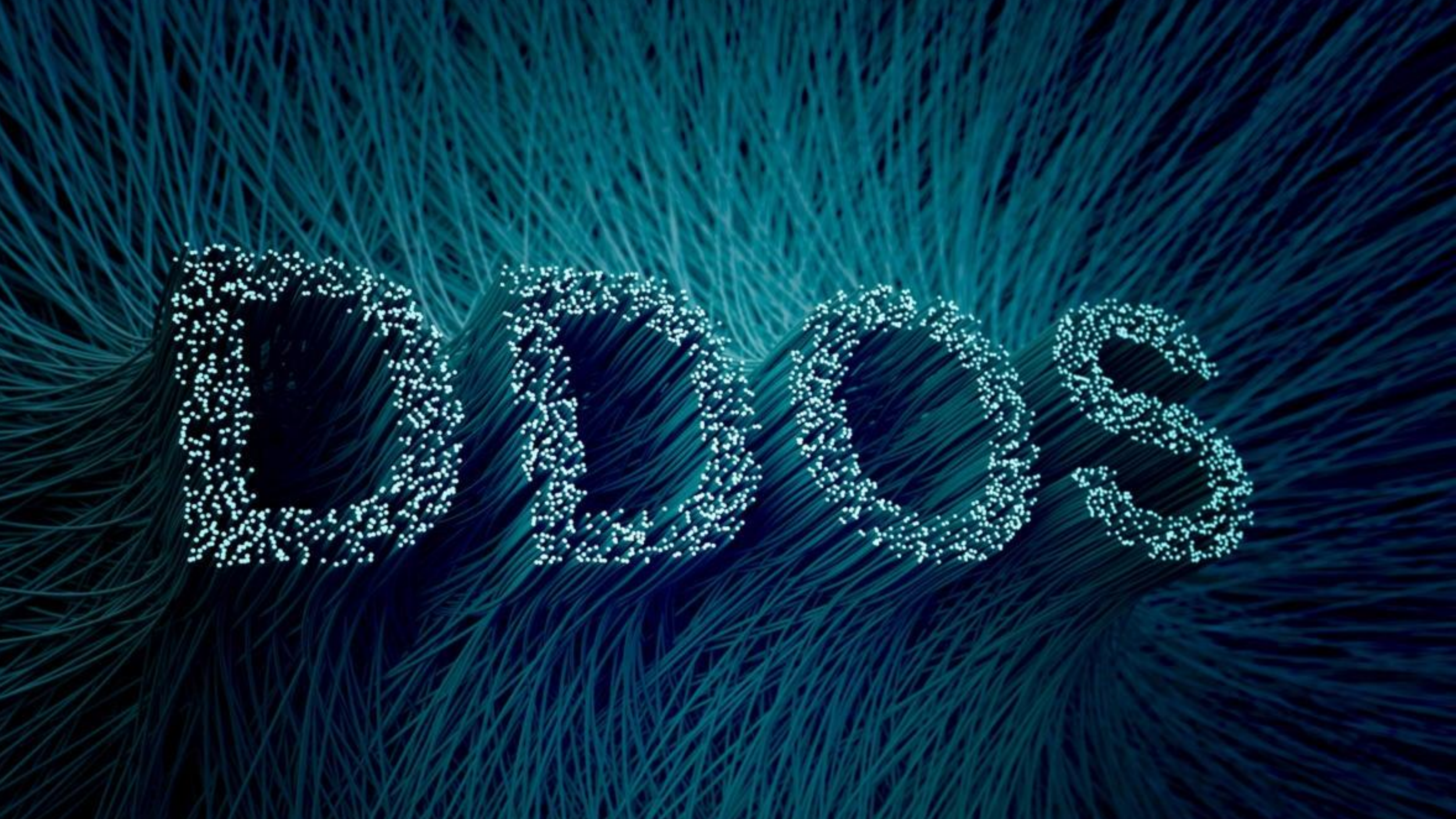
Threat Actor Techniques

True (probably)

- Buy your information on darkweb
  - Information may be leaked due to data breach of online systems
    - In 2014 Yahoo had been stolen 500 millions passwords
- Make up a story which fear you most, e.g. about personal matters

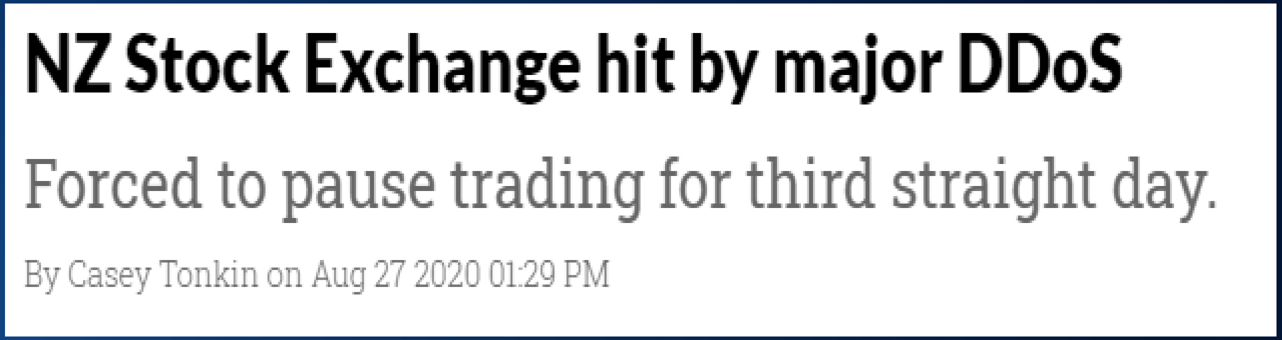
False

- Hack your computer or plant malware
- Hold photo / video of you
- Hold your organisation data
- Hold your contact list


DDoS

Ransom DDoS

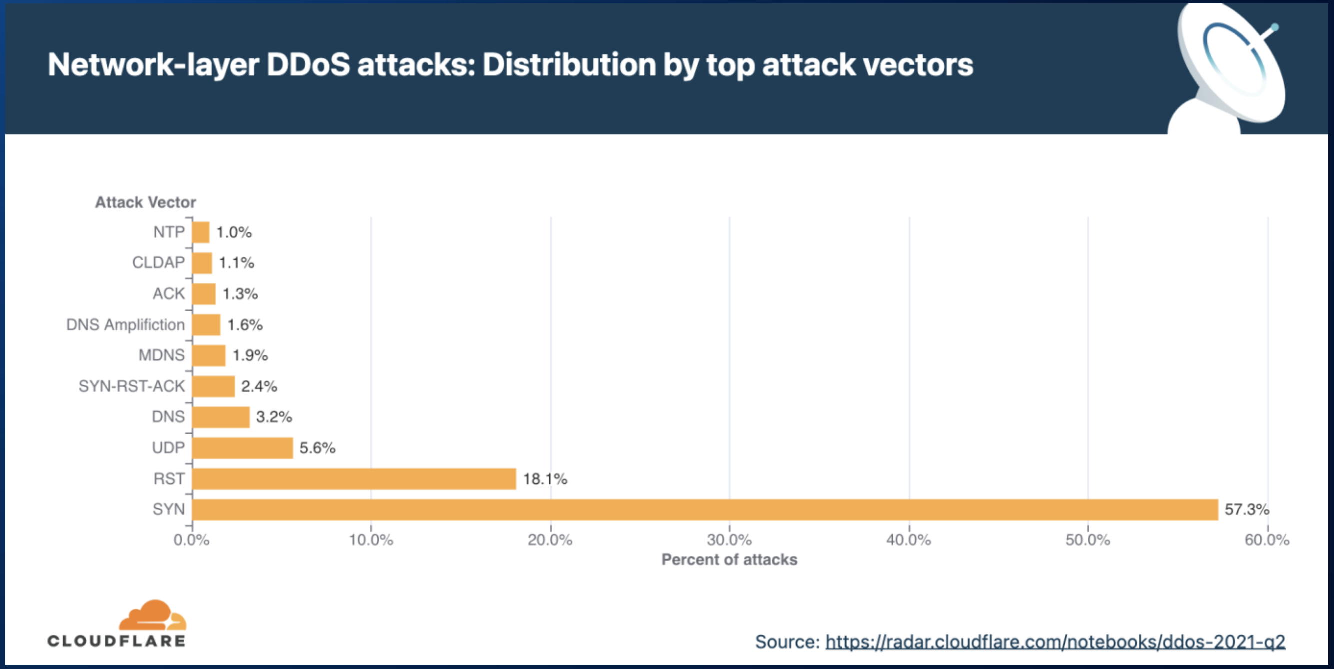
- Huge **scale** and long **duration**
- Highly organised and sophisticated
- Targeting **Financial** and **Retail** Sectors



NZ Stock Exchange hit by major DDoS

Forced to pause trading for third straight day.

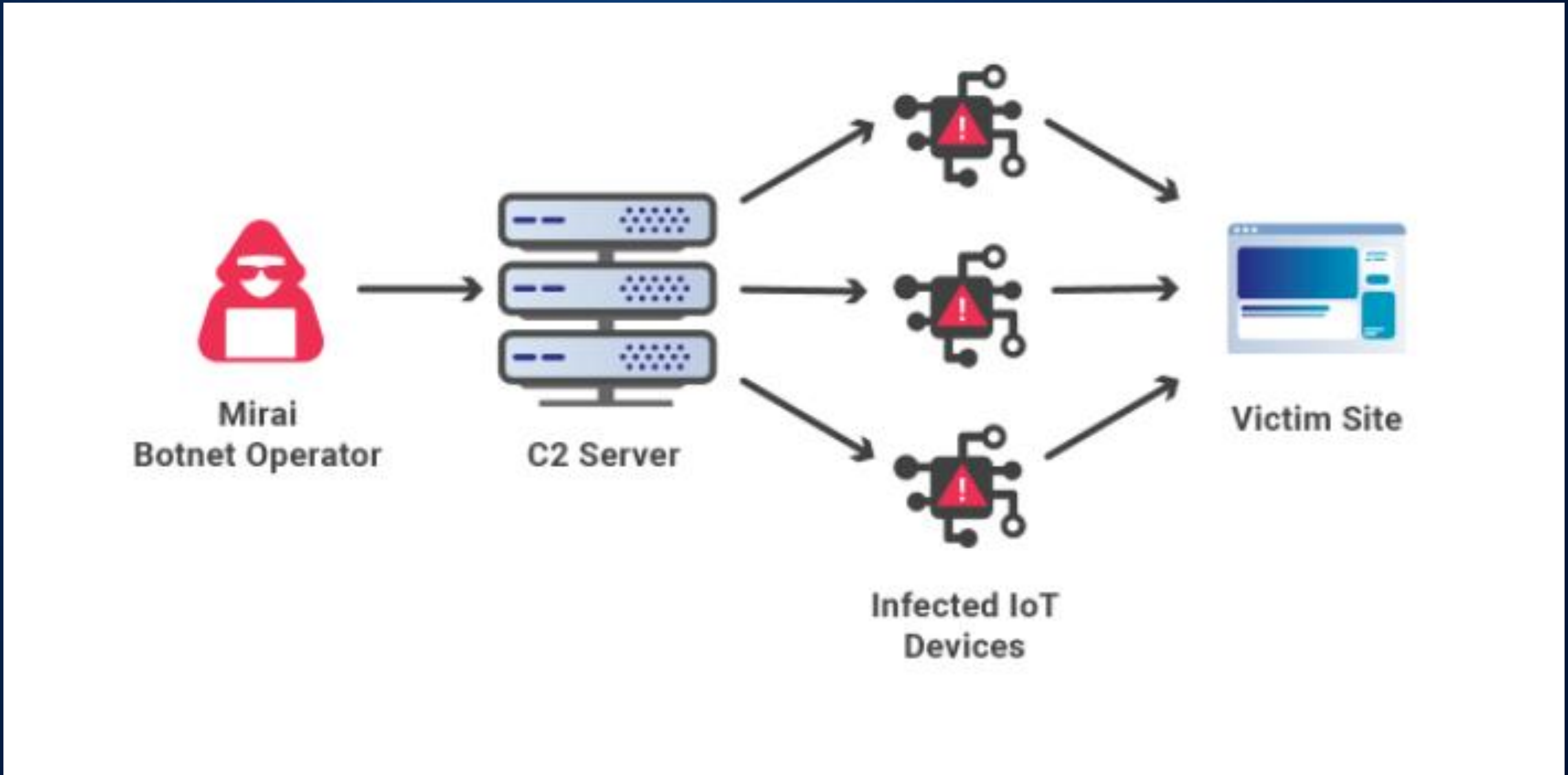
By Casey Tonkin on Aug 27 2020 01:29 PM



Network-layer DDoS attacks: Distribution by top attack vectors

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

Threat Actor Techniques



source: cloudflare.com

	Ransomware	Ransom Email	Ransom DDoS
Victim	🏢 👤	👤	🏢
Chance of Occurrence	☠☠☠☠☠	☠☠☠☠	☠☠☠
Impact	☠☠☠☠☠	☠☠☠	☠☠☠☠
Detection / Identification	☠☠☠☠☠	☠☠☠	☠
Prevention / Mitigation	☠☠☠☠☠	☠☠☠	☠☠☠☠
Time to Recover	☠☠☠☠☠	☠	☠☠☠☠

source: cloudflare.com

Security Advices

- Cyber extortion is not an IT problem
- It is a human criminal problem
- Plan, detect and response are the keys

Ransomware

1. Protect ALL endpoint devices
    1. Patch regularly
    2. Anti-virus keep up-to-date
    3. Monitoring
2. Offline backup regularly
3. Segmentation, e.g. network, access control, IT/OT, backup
4. Multi-factor authentication
5. Incident response

source: istockphoto.com

Paying Ransom or Not?

HKCERT Advice:

DO NOT pay the ransom

Sophos State of Ransomware 2021 Report

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

Ransom Email

1. Keep calm, DO NOT open attachment
2. Change password of compromised account
3. Raise **Security Awareness**, e.g. keep update of latest security information

How to find latest security information and trend ? Such as

1. Latest threat and attack method
2. Security advisory

Ransom DDoS

1. Advance Planning
   - Minimise exposure
   - Implement DDoS protection solution

2. **Swift Response**
   - Automate alerts

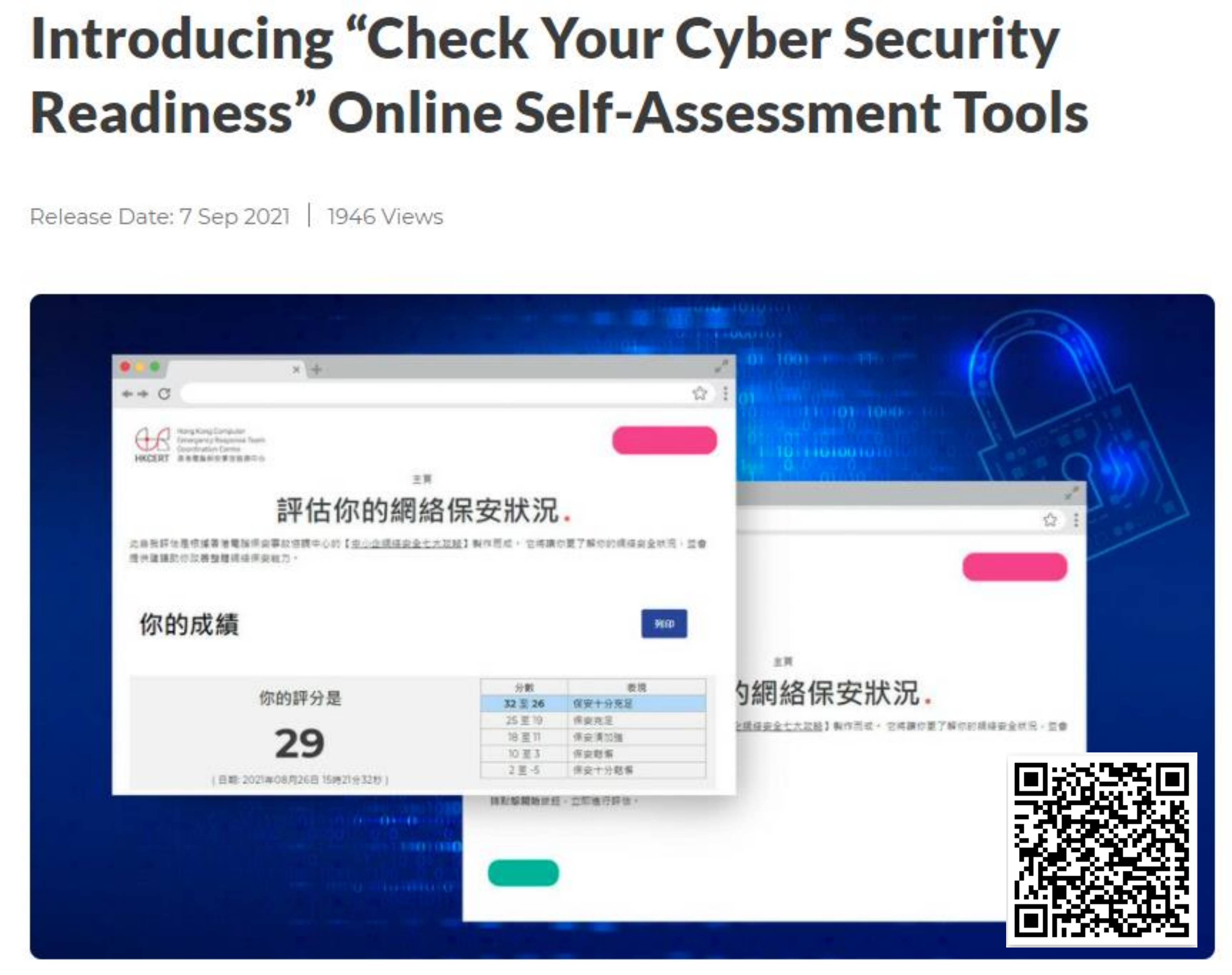
source: freepik.com

Assess your Cyber Security Readiness

HK … Es

Security Poli…
Manageme…

User
…areness



Introducing "Check Your Cyber Security Readiness" Online Self-Assessment Tools

Release Date: 7 Sep 2021 | 1946 Views

Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港電腦保安事故協調中心

主頁

評估你的網絡保安狀況。

此自我評估是根據香港電腦保安事故協調中心的【中小企網絡安全七大要點】製作而成，它將讓你更了解你的網絡安全狀況，並會提供建議助你改善整體網絡保安能力。

你的成績

列印

你的評分是

29

（日期: 2021年08月26日 15時21分32秒）

分數	表現
32 至 26	保安十分充足
25 至 19	保安充足
18 至 11	保安須加強
10 至 3	保安薄弱
2 至 -5	保安十分薄弱

主頁

…的網絡保安狀況。

請點擊開始按鈕，立即進行評估。

Build Human Firewall

HKCERT
由 Hkcert HK 發佈 · 4天 ·

【資料外洩注意!!】Fortinet SSL-VPN 設備爆發大型資料外洩事故

最近有黑客係網上公開咗87,000 個Fortinet SSL-VPN 設備嘅用戶登入名稱同密碼，相信係啲設備未有做足保安更新，畀黑客有機可乘，利用保安漏洞CVE-2018-13379竊取出嚟。被公開嘅相信係啲儲存喺設備上嘅本地VPN帳戶，而香港亦有部份設備中招，HKCERT已經聯絡受影響機構跟進。如果大家都有用 Fortinet SSL-VPN 設備但仲未更新修補呢個漏洞嘅話，請即時 take以下 action 補救：

1. 立即更新設備嘅軟件/韌體 (有關漏洞 CVE-2018-13379 ，可參考我哋於上年 12月 發佈嘅Blog，連結喺下面) ; ..... 查看更多

HKCERT
143 followers
2w •

【Patch Vulnerabilities in Remote Acces
Remote Storage Now】
...se

Patch Vulnerabilities in Remote Acces
Remote Storage Now

8

Hong Kong Computer Emergency Response Team Coordination Centre
香港電腦保安事故協調中心

Centre for coordination of computer security incident response for local enterprises and Internet Users

Facilitate information disseminating, provide advices...

Learn more

www.hkcert.org
8105 6060
hkcert@hkcert.org

Security Advice

https://www.youtube.com/user/hkcert

CTF 2021 Challenge

香港網絡保安新生代 奪旗挑戰賽

- An **online jeopardy** competition for **cyber security knowledge and skills**
- **Open, tertiary** and **secondary groups** competitions will be held in **Nov**
- **Fabulous prizes. Check out at** 👉 **https://ctf.hkcert.org**
- Online **workshops** will be arranged for preparation