Webinar Series: Cybersecurity for your business

Emerging cyberthreats and the role C-suite members play in protecting the business in the COVID-19 era

Abbas Kudrati
Chief Cybersecurity Advisor
Cybersecurity Solutions Group
Microsoft Asia

Harry Pun
Cybersecurity Executive
Cybersecurity Solutions Group
Microsoft Greater China

Microsoft

Hong Kong Cyber Threat Landscape

Shifting Sands – Trends in Cybersecurity

Microsoft

What’s Old is New Again

Our data shows that these COVID-19 themed threats are retreads of existing attacks that have been slightly altered to tie to this pandemic.

We’re seeing a **changing of lures, not a surge in attacks.**

Malicious URLs

Each day we see and processes more than 18,000 malicious COVID-19-themed URLs and IP addresses

Swapping malicious URLs on a more frequent basis in an effort to evade machine learning protections

11th

Highest encounter rate in Asia Pacific

Ranked #11 in 2018

2.28%

↓ 34% from 2018

MALWARE

Hong Kong’s malware encounter rate was 2.3 times lower than the regional and 1.4 times lower than the global average.

Highest Encounter Rate	
1	Indonesia
2	Sri Lanka
3	Vietnam

Lowest Encounter Rate	
1	Japan
2	New Zealand
3	Australia

Source: security endpoint threat report 2019

Microsoft

MALWARE

Code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network

Malware encounter rate across Asia Pacific

5.34%

(↓23% from 2018)

1.6 times higher than the global average

Countries with highest encounter rate

1. Indonesia
2. Sri Lanka
3. Vietnam

Countries with lowest encounter rate

1. Japan
2. New Zealand
3. Australia

Malware trends in Asia Pacific

Cybercriminals remain focused on attacking countries with:

- Lower levels of cyber awareness
- High usage of unlicensed and/or pirated software, and sites that illegitimately offer free software or content

Beyond Phishing

Top Observations

Vulnerable Internet-facing network devices

Brute forcing RDP servers

Credential theft and lateral movement (Mimikatz, Cobalt Strike)

Wide range of ransomware payloads

9th

Highest encounter rate in Asia Pacific

Ranked #8 in 2018

0.02%

↓ 71% from 2018

RANSOMWARE

Hong Kong's ransomware encounter rate was 2.5 times lower than the regional and 1.5 times lower than the global average.

Highest Encounter Rate	
1	Vietnam
2	Indonesia
3	India

Lowest Encounter Rate	
1	Japan
2	New Zealand
3	Australia

Source: security endpoint threat report 2019

Microsoft

RANSOMWARE

Malicious software that disables a device or its files until the attacker is paid a ransom

Ransomware encounter rate across Asia Pacific

0.05%

(↓29% from 2018)

1.7 times higher than the global average

Countries with highest encounter rate

1. Vietnam
2. Indonesia
3. India

Countries with lowest encounter rate

1. Japan
2. New Zealand
3. Australia

Ransomware trends in Asia Pacific

Even with a slowdown in ransomware encounters, cyber attackers are shifting their efforts to customized campaigns targeting specific:

- Geographical areas
- Industries
- Businesses

Human-Operated Attacks are Different

Automated Attacks

Often enter via phishing

Rapid deployment

Human-operated Attacks

Enter manually

Long game; dormant

Hands on keyboards

Human-Operated Ransomware Attacks

Common Attack Techniques

- Initial entry through misconfigured or outdated Web servers
- Credential theft and escalation of privilege
- Deployment through commodity malware infection
- Human-operated lateral movement
- Finding and exploiting poor security controls
- Disabling security controls

10th

Highest encounter rate in Asia Pacific

Ranked #9 in 2018

0.02%

↓ 71% from 2018

CRYPTOCURRENCY MINING

Hong Kong’s cryptocurrency encounter rate was 2.5 times lower than the regional and global average.

Highest Encounter Rate	
1	Sri Lanka
2	India
3	Vietnam

Lowest Encounter Rate	
1	Japan
2	China
3	Australia

Source: security endpoint threat report 2019

Microsoft

CRYPTOCURRENCY MINING

Malware introduced into an unsuspecting user or organization's machine(s), which then uses the machine's computing power to mine cryptocurrency

Cryptocurrency mining encounter rate across Asia Pacific

0.05%

(↓64% from 2018)

On par with the global average

Countries with highest encounter rate

1. Sri Lanka
2. India
3. Vietnam

Countries with lowest encounter rate

1. Japan
2. China
3. Australia

Cryptocurrency mining trends in Asia Pacific

Recent fluctuations in cryptocurrency value and the increased time required to generate cryptocurrency have resulted in attackers refocusing their efforts to target markets with:

- Low cyber awareness
- Low adoption of cyber hygiene practices

Microsoft

3^{rd}

Highest attack volume in Asia Pacific

Ranked #8 in 2018

0.24*

↑ 60% from 2018

DRIVE-BY DOWNLOAD

Hong Kong's drive-by-download attack volume was 3 times higher than the regional and global average.

Highest attack volume	
1	Singapore
2	India
3	Hong Kong

Lowest attack volume	
1	New Zealand
2	Korea
3	Philippines

Source: security endpoint threat report 2019

DRIVE-BY DOWNLOAD

Unintentional download of malicious code to a device when the user visits a website, aimed at exploiting vulnerabilities in web browsers, applications, or even the operating system

Drive-by download attack volume across Asia Pacific

0.08*

(↓27% from 2018)

On par with the global average

Countries with highest attack volume

1. Singapore
2. India
3. Hong Kong

Countries with lowest attack volume

1. New Zealand
2. Korea
3. Philippines

Drive-by download trends in Asia Pacific

Cybercriminals remain focused on stealing financial information and intellectual property.

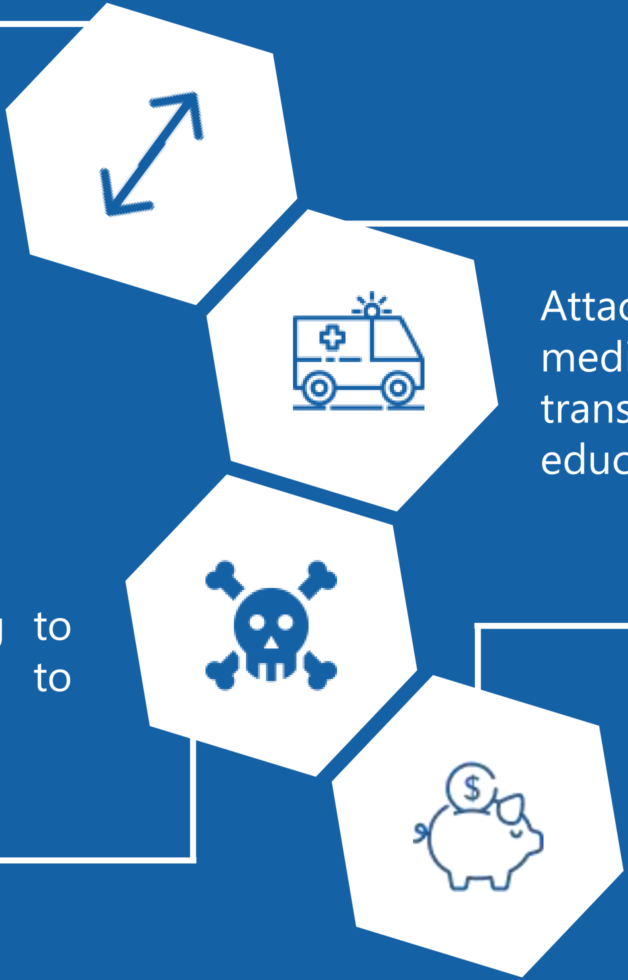
This has resulted in key financial hubs recording the highest attack volumes in 2019.

**The Security Endpoint Threat Report records the average volume of drive-by download pages detected for every 1,000 pages indexed by Bing.*

The Impact of COVID-19 on Cybersecurity

Microsoft

Threats Microsoft Is Seeing Since COVID-19



Many of the compromises that enabled the cyberattacks occurred earlier. Multiple ransomware groups have been accumulating access and maintaining persistence on target networks for several months

Attacks have affected aid organizations, medical billing companies, manufacturing, transport, government institutions, and educational software providers

Attackers had been silently waiting to monetize their ransomware attacks to maximize financial gains

The attacks all used the same techniques – credential theft and lateral movement – culminating in the deployment of a ransomware payload of the attackers' choice

Microsoft

Five Lasting Security Implications of the Pandemic

Security has proven to be the foundation for **digital empathy** in a remote workforce

Everyone is on a **Zero Trust** journey

Better **threat intelligence** comes from diverse data sets

Cyber resilience is fundamental to business operations

The end of **bolt-on security**

Recommendations from Microsoft for Staying Cybersafe

Businesses and individuals are encouraged to adopt the following best practices for cybersecurity

Guidance for businesses

- **DO:** Safeguard employees with strong tools and infrastructure
- **DO**: Turn on multi-factor authentication (MFA) as employees work from home
- **DO:** Include end-to-end encryption on trusted applications for audio/ video calling and file sharing
- **DO:** Guide employees on how to identify phishing attempts and distinguish between official communications and suspicious messages

Guidance for individuals

- **DO:** Update all devices with the latest security updates and ensure that an antivirus service is included
- **DO:** Watch out for malicious or compromised websites and avoid pirated content
- **DO**: Recognize and report suspected attack attempts
- **DO:** Verify all links and attachments before opening them

Microsoft

Microsoft

Q&A

Please type in your question at the chat pane.

Microsoft