Microsoft’s Security Endpoint Threat Report comprises insights derived by analyzing data from January to December 2019.

Data comes from diverse Microsoft data sources, including 8 trillion threat signals received and analyzed by Microsoft every day.

The report also includes Microsoft’s guidance on navigating cyberthreats during COVID-19.

This report covers insights from the following Asia Pacific markets:

- Australia
- Japan
- Singapore
- China
- Korea
- Sri Lanka
- Hong Kong
- Malaysia
- Thailand
- India
- New Zealand
- Taiwan
- Indonesia
- Philippines
- Vietnam
Evolving Cybersecurity Threats in Asia Pacific
MALWARE

Code developed by cyberattackers, 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
RANSOMWARE

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

Ransomware trends in Asia Pacific

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

- Geographical areas
- Industries
- Businesses

**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
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
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
**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.
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

<table>
<thead>
<tr>
<th>Guidance for businesses</th>
<th>Guidance for individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DO:</strong> Safeguard employees with strong tools and infrastructure</td>
<td><strong>DO:</strong> Update all devices with the latest security updates and ensure that an antivirus service is included</td>
</tr>
<tr>
<td><strong>DO:</strong> Turn on multi-factor authentication (MFA) as employees work from home</td>
<td><strong>DO:</strong> Watch out for malicious or compromised websites and avoid pirated content</td>
</tr>
<tr>
<td><strong>DO:</strong> Include end-to-end encryption on trusted applications for audio/video calling and file sharing</td>
<td><strong>DO:</strong> Recognize and report suspected attack attempts</td>
</tr>
<tr>
<td><strong>DO:</strong> Guide employees on how to identify phishing attempts and distinguish between official communications and suspicious messages</td>
<td><strong>DO:</strong> Verify all links and attachments before opening them</td>
</tr>
</tbody>
</table>