



Microsoft Security Endpoint Threat Report 2019

Understanding the Threat Landscape in India

About Microsoft Security Endpoint Threat Report 2019

- ◆ 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 India

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 in India

5.89%
(↓35% from 2018)

7th

Highest encounter rate in Asia Pacific

1.1 times higher than the regional average
1.8 times higher than the global average

Malware trends in India

- ◆ India moved from 6th to 7th highest encounter rate YoY across the region
- ◆ Cybercriminals continue to capitalize on:
 - ◆ Lower levels of cyber awareness
 - ◆ High usage of unlicensed and/or pirated software, and sites that illegitimately offer free software or content



Countries with highest encounter rate

1. Indonesia
2. Sri Lanka
3. Vietnam



Countries with lowest encounter rate

1. Japan
2. New Zealand
3. Australia

RANSOMWARE

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



Ransomware encounter rate in India

0.10%
(↓29% from 2018)

3rd

Highest encounter rate in Asia Pacific

2.0 times higher than the regional average
3.3 times higher than the global average

Ransomware trends in India

- ◆ India continued to rank 3rd highest for ransomware encounter rate YoY across the region
- ◆ Cybercriminals are shifting their efforts to customized campaigns targeting specific:
 - ◆ Geographical areas
 - ◆ Industries
 - ◆ Businesses



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 in India

0.23%
(↓52% from 2018)



Countries with **highest** encounter rate

1. Sri Lanka
2. India
3. Vietnam

2nd

Highest encounter rate in Asia Pacific

4.6 times higher than the regional and global average



Countries with **lowest** encounter rate

1. Japan
2. China
3. Australia

Cryptocurrency mining trends in India

- ◆ India moved from highest (1st) to 2nd highest encounter rate YoY across the region
- ◆ Recent fluctuations in cryptocurrency value and the increased time required to generate cryptocurrency have resulted in attackers refocusing their efforts to exploit:
 - ◆ 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 in India

0.24*
(↑140% from 2018)

2nd

Highest attack volume in Asia Pacific

3.0 times higher than the regional and global average

Drive-by download trends in India

- ◆ India moved from 11th to 2nd highest attack volume YoY across the region
- ◆ Cybercriminals remain focused on stealing financial information or intellectual property
- ◆ This has resulted in India, along with Hong Kong and Singapore, recording an increase in attack volume, over 3 times the regional and 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

**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

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

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

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

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

