Microsoft

SECURITY ENDPOINT THREAT REPORT 2019 – INDIA

Navigating the cyberthreat landscape

Cybersecurity remains a top priority in today's interconnected world. Microsoft shares trends in endpoint threats and guidance for staying cybersafe in today's evolving landscape, based on analysis of over eight trillion threat signals daily, from January to December 2019.

The research covered a total of 15 markets, which include China, India, Indonesia, Malaysia, Philippines, Sri Lanka, Thailand, Vietnam, Taiwan, Singapore, New Zealand, Korea, Japan, Hong Kong, and Australia.

EVOLVING CYBERTHREATS 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

India's malware encounter rate was 1.1 times higher than the regional and 1.8 times higher than the global average.

7th
Highest encounter rate in Asia Pacific
Ranked #6 in 2018

5.89%
35% from 2018

Malware encounter rate in India

Highest encounter rate
1 Indonesia
2 Sri Lanka
3 Vietnam

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

India's ransomware encounter rate was 2 times higher than the regional and 3.3 times higher than the global average.

3rd
Highest encounter rate in Asia Pacific
Ranked #3 in 2018

0.10%
29% from 2018

Ransomware encounter rate in India

Highest encounter rate
1 Vietnam
2 Indonesia
3 India

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

India's cryptocurrency mining encounter rate was 4.6 times higher than the regional and global average.

2nd
Highest encounter rate in Asia Pacific
Ranked #1 in 2018

0.23%
52% from 2018

Cryptocurrency mining encounter rate in India

Highest encounter rate
1 Sri Lanka
2 India
3 Vietnam

Lowest encounter rate
1 Japan
2 China
3 Australia

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

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

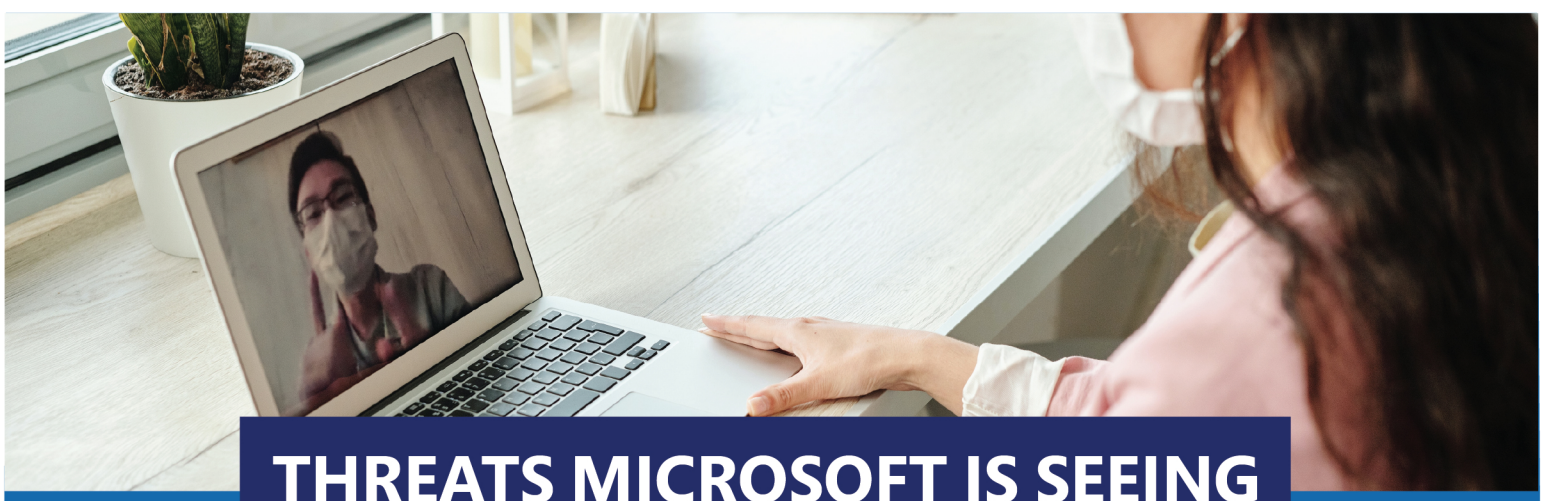
2nd
Highest attack volume in Asia Pacific
Ranked #11 in 2018

0.24*
140% from 2018

Drive-by download attack volume in India

Highest attack volume
1 Singapore
2 India
3 Hong Kong

Lowest attack volume
1 New Zealand
2 Korea
3 Philippines



THREATS MICROSOFT IS SEEING SINCE COVID-19

Many of the compromises that enabled these attacks existed 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

GUIDANCE FROM MICROSOFT

ORGANIZATIONS

DO **SAFEGUARD employees** with strong tools and infrastructure

DO **SET UP 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 suspicious messages

INDIVIDUALS

DO **UPDATE all devices** with the latest security updates

DO **INSTALL an antivirus service** on computing devices

DO **WATCH OUT for malicious or compromised websites**

DO **AVOID pirated** software

DO **RECOGNIZE** and report suspected attack attempts

DO **VERIFY all links and attachments** before opening them