Malware poses risks in the form of impaired usability, data loss, intellectual property theft, monetary loss and even emotional distress.

- **MARKETS WITH HIGHEST ENCOUNTER RATES**
  1. Indonesia
  2. Philippines
  3. Vietnam

- **MARKETS WITH LOWEST ENCOUNTER RATES**
  1. Japan
  2. Australia
  3. New Zealand

Cryptocurrency Mining

Attackers seeking illicit profits have increasingly turned to malware that lets them use victim’s computer to help them mine cryptocurrency coins.

- **MARKETS WITH HIGHEST ENCOUNTER RATES**
  1. India
  2. Sri Lanka
  3. Indonesia

- **MARKETS WITH LOWEST ENCOUNTER RATES**
  1. China
  2. Japan
  3. Australia

Ransomware

While individuals and organizations are becoming more intelligent in dealing with ransomware, it continues to be a significant threat in Asia Pacific.

- **MARKETS WITH HIGHEST ENCOUNTER RATES**
  1. Indonesia
  2. Vietnam
  3. India

- **MARKETS WITH LOWEST ENCOUNTER RATES**
  1. Japan
  2. Australia
  3. New Zealand

Drive-by Download (DBD)

Attackers are exploiting vulnerabilities in webpages to direct users to compromised sites that can secretly infect users even when they do not attempt to download anything.

- **MARKETS WITH HIGHEST DBD PAGES**
  1. Taiwan
  2. Malaysia
  3. Indonesia

- **MARKETS WITH LOWEST DBD PAGES**
  1. New Zealand
  2. Japan
  3. South Korea

Cybersecurity Best Practices

### FOR ORGANIZATIONS
1. **Prevention:** Preventive controls increase the cost of attacks for cybercriminals and prevent cheap, effective cyberattack techniques.
   - **Cloud Backup:** Use cloud storage services to automatically backup important data.
   - **Access Control:** Implement network segmentation and exert caution when granting application permissions.
   - **Cybersecurity Education:** Educate employees on safe cyber practices and maintain robust IT policies.
2. **Detection & Response:** Leverage cloud technology to limit attackers’ access to data and help security operations better respond to attacks.

### FOR INDIVIDUALS
1. **Cyber Hygiene:** Use anti-virus solution and keep software and operating systems updated.
2. **Genuine Software:** Avoid using pirated software and only use software from trusted sources.
3. **Password Management:** Use a strong password for each account and change them regularly.
4. **Backup Personal Files:** Backup photos and other important personal data on a trusted cloud storage platform.
5. **Stay Vigilant:** Activities where personal information will be transmitted should only be done on the users’ own devices, on a trusted network.

Get the full Microsoft Security Intelligence Report Volume 24 here: [www.microsoft.com/sir](http://www.microsoft.com/sir)