Staying Sharp on Security

Takeaways from the Microsoft Security Intelligence Report

Microsoft regularly aggregates the latest worldwide security data into the Security Intelligence Report (SIR), unpacking the most pressing issues in cybersecurity. Here are some highlights from SIR, Volume 22, which covers January to March 2017:

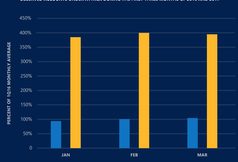
Cloud threat intelligence

The cloud has become *the* central data hub for any organization, which means it's also a growing target for attackers.

Compromised accounts

DEFINITION:
Attackers break into the cloud-based account simply by using the stolen sign-in credentials of a user

ANALYSIS:
A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services.



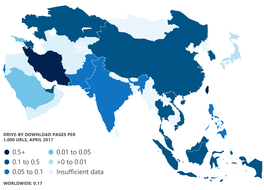
Cloud-based user account attacks have increased 300% from last year, showing that attackers have found a new favorite target.

Drive-by download sites

DEFINITION:
A website that hosts malware in its code and can infect a vulnerable computer simply by a web visit

ANALYSIS:
Attackers sneak malicious code into legitimate but poorly secured websites. Machines with vulnerable browsers can become infected by malware simply by visiting the site. Bing search constantly monitors sites for malicious elements or behavior, and displays prominent warnings before redirecting to any suspicious site.

Taiwan and Iran have the **highest** concentration of **drive-by download** pages.



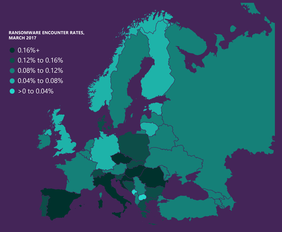
Endpoint threat intelligence

An endpoint is any device remotely connected to a network that can provide an entry point for attackers—such as a laptop or mobile device. Since users interact with an endpoint, it remains a key opportunity for attackers and a security priority for organizations.

Ransomware

DEFINITION:
Malware that disables a computer or its files until an amount of money is paid to the attackers

ANALYSIS:
Ransomware attacks have been on the rise, disrupting major organizations and grabbing global headlines. Attacks like WannaCry and Petya disabled thousands of machines worldwide in the first half of 2017. Windows 10 includes mitigations that prevent common exploitation techniques by these and other ransomware threats.



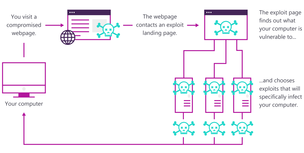
Ransomware disproportionately targeted **Europe** with **Czech Republic, Italy, Hungary, Spain, Romania,** and **Croatia** being the top six countries with the **highest encounter rates**.

Exploit kits

DEFINITION:
A bundle of malicious software that discovers and abuses a computer's vulnerabilities

ANALYSIS:
Once installed on a compromised web server, exploit kits can easily reach any computer lacking proper security updates that visits the site.

Many of the more **dangerous exploits are used in targeted attacks** before appearing in the wild in larger volumes.



Takeaways and checklist

The threats and risks of cyberattacks are constantly changing and growing. However, there are some practical steps you can take to minimize your exposure:

Reduce risk of credential compromise by educating users on why they should avoid simple passwords, enforcing multi-factor authentication and applying alternative authentication methods (e.g., gesture or PIN).

Enforce security policies that control access to sensitive data and limit corporate network access to appropriate users, locations, devices, and operating systems (OS).

Do not work in public Wi-Fi hotspots where attackers could eavesdrop on your communications, capture logins and passwords, and access your personal data.

Regularly update your OS and other software to ensure the latest patches are installed.

Stay on top of all the latest information in cybersecurity, gleaned from Microsoft's worldwide intelligence.

Read more and download the full Security Intelligence Report at microsoft.com/sir

Microsoft