Cybersecurity Threats You Should Know About in 2018

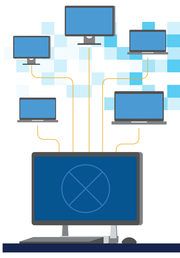
Read the Microsoft Security Intelligence Report, Volume 23 for a full account

Every year, Microsoft collects security and threat intelligence from their global network and compiles the trends into the Microsoft Security Intelligence Report. To keep up with the always evolving landscape, the Security Intelligence Report provides a thorough analysis of security threats and how to best mitigate the top attack types.

The report investigates three main topics:

- Botnets
- Easy Mark Attack Methods
- Ransomware

Botnets



Bots are programs that allow attackers to infect and take control of computers, and botnets are a network of those bots controlled by command-and-control (C&C) servers. On November 29, 2017, Microsoft's Digital Crimes Unit tackled a leading botnet that infected more than 23 million IP addresses: Gamarue. Find out more in the full report.

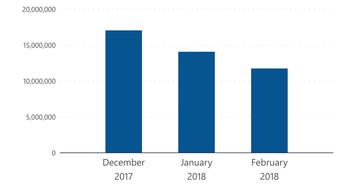
Microsoft analyzed over 44,000 malware samples that revealed Gamarue's sprawling infrastructure.

1,214
domains and IP addresses of the botnet C&C servers

464
distinct botnets

80+
associated malware families

Infected devices per month (after Gamarue disruption)



SECURITY RECOMMENDATIONS

Use solutions that apply advanced machine learning to detect Gamarue and other types of malware.

Easy Mark Attack Methods

With advancing security solutions, hackers are more apt to go after easy targets through social engineering and are constantly evolving their tactics for maximum efficiency. Here are two examples of low-hanging fruit; read the report for more.

Phishing

Broad-based phishing and spear phishing both rely on what's most often cited as security's weakest link: people. Phishing can take many shapes, including:

- Email links and attachments
- Domain spoofs
- User impersonation
- Domain impersonation
- Links to fake SaaS apps

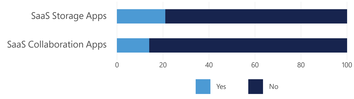
180,000,000–200,000,000
Approximate number of phishing emails Microsoft detected each month, over three months (November 2017 - January 2018).

Cloud apps

Cloud app adoption is rising to support business productivity, but a lack of security infrastructure could be inadvertently compromising data.

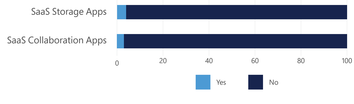
Encrypt data at rest and in transit

79% of SaaS storage apps and 86% of SaaS collaboration apps do not encrypt data both at rest and in transit.



Support for all HTTP headers session protection methods

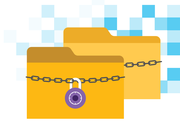
Only 4% of SaaS storage apps and 3% of SaaS collaboration apps support all HTTP headers session protection.



SECURITY RECOMMENDATIONS

For phishing, train employees on identifying and reporting suspicious links to cut off attacks before they can do damage. For visibility into and control over all cloud apps usage across the enterprise, use a cloud access security broker (CASB) security solution.

Ransomware



Ransomware infects and encrypts files (and sometimes entire disks) to prevent access until a ransom is paid—and there's no guarantee victims will regain access.

Ransomware made a real-world impact in 2017, bringing down critical services like hospitals, transportation, and traffic systems. Here are few of the unprecedented and devastating ransomware families responsible for the 2017 attacks:

- WannaCrypt
- Petya/NotPetya
- BadRabbit

SECURITY RECOMMENDATIONS

Backup your data so it can be recovered in case of a ransomware attack.

Outbreaks of Various Ransomware Families

May 2017
WannaCrypt infects over 230,000 computers — the largest ransomware attack ever.

June 2017
Petya/NotPetya attack uses the same exploit as WannaCrypt but harnesses additional methods of spreading, making for perhaps the most complex ransomware in 2017.

October 2017
BadRabbit poses as an Adobe Flash update on compromised websites, and spreads through compromised usernames and passwords.

DOWNLOAD THE FULL MICROSOFT SECURITY INTELLIGENCE REPORT, VOLUME 23 FOR MORE SECURITY INSIGHTS.

www.microsoft.com/sir

Microsoft