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**
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.

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

- **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:

- **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.

**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 Insights**
Ransomware insights and statistics: see the chart to the right to help identify ransomware activity and understand the extent to which your organization is at risk.

- Support for all HTTPS traffic encryption protocols
  - Only 71% of SaaS storage apps and 53% of SaaS collaboration apps support all HTTPS traffic encryption protocols.

**Easy Mark Attack Methods**

- **Cloud app**
  - Encrypt data at rest and in transit

**SaaS Storage Apps**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data at rest and in transit</td>
<td>71%</td>
<td>29%</td>
</tr>
<tr>
<td>Support for all HTTPS traffic encryption protocols</td>
<td>53%</td>
<td>47%</td>
</tr>
</tbody>
</table>

**SaaS Collaboration Apps**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt data at rest and in transit</td>
<td>83%</td>
<td>17%</td>
</tr>
<tr>
<td>Support for all HTTPS traffic encryption protocols</td>
<td>56%</td>
<td>44%</td>
</tr>
</tbody>
</table>

**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**

To learn more about Microsoft’s Digital Crimes Unit, or the Microsoft Security Intelligence Report, visit www.microsoft.com/sir.

© 2018 Microsoft Corporation. All rights reserved. This document is for informational purposes only.