January, 2017
Volume 12, Issue 1

Looking Forward: 2017's Top Threat Prediction

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

We wish you, your colleagues, and your families a happy and prosperous new year! As we look back on the past year's challenges, we also look ahead to which cybersecurity challenges will hold prominence in 2017. The Center for Internet Security (CIS) posted a Twitter poll asking respondents to choose which of the four listed threat areas would be the biggest cyber threat in 2017. The Internet of Things (IoT) took the top spot as biggest threat by a large margin. This shouldn't be a surprise given some of the prominent cyber attacks of 2016, including one which temporarily stopped some users from accessing popular websites such as Twitter, Spotify, and Amazon, were bolstered by compromised IoT devices.

Here are some quick primers on why these are threats to everyday users, and how you can work to protect yourself out there in the connected world.

Internet of Things (IoT): Our top polling threat, the Internet of Things is comprised of everyday objects and household items that are connected to the Internet. Examples include smart TVs, routers, smart thermostats, and smart home devices among many others. Although convenient, these devices often come out of the box with very few security features, little to no security support, and often remain in use with default passwords in users' homes. As a result, these compromised devices can be used to attack others, slowing your Internet access and possibly preventing access to popular sites like Twitter, Amazon, and Spotify etc. When purchasing and using IoT or connected home devices, be sure to change the default passwords that come pre-loaded on the device to strong and unique ones of your choosing, and also keep up-to-date on patches and updates as they become available. Basic recommendations for creating a strong password are to use at least 10 characters including uppercase and lowercase letters, numbers, and symbols. Further information on setting a strong password is available in the guide linked at the end of this newsletter.

Data Dump Re-use: With the number of high profile data breaches the past year at well-known organizations, this will continue to be an important area of concern moving forward. Cyber criminals sell or publicly post stolen usernames, passwords, social security numbers and other personal information. Unfortunately, many people tend to re-use the same login credentials between many of their accounts

due to the difficulty of remembering multiple passwords. This can allow cyber criminals to take their stolen credentials and attempt using them to access their other online banking, shopping, and other accounts. Users should follow the linked guide below to create and protect strong, unique passwords to avoid this type of compromise.

APT: Advanced Persistent Threat (APT) refers to cyber threat actors operating for or on behalf of nation-state governments like Russia and China, who are looking to compromise, steal, change, or destroy information for the purposes of espionage, disruption, or destruction. State and local governments, critical infrastructure, Universities, and the employees of all of these entities are targeted by this threat. Users can reduce the risk from this type of threat actor by using strong and unique passwords, regularly patching their computers and devices, and thinking twice before opening suspicious emails/attachments or clicking links. More information on suspicious emails is located in the guide linked below.

Ransomware: Ransomware is a form of malware that aims to block a user from having access to their own systems, commonly by encrypting the infected computer's files against the owner's will. Once access is blocked, the ransomware then requests money (a ransom) in order to restore access. Cyber criminals are commonly spreading this particular malware through malicious email attachments. This highly prevalent form of malware can be mitigated by keeping your systems and anti-virus software patched and up to date with the most recent versions. Additionally, be wary of suspicious emails and do not open attachments or click on links from untrusted sources.

Consider some of the cyber threats out there as you go forward into 2017, and consider these tips for protecting you and your devices. Have a safe and happy new year, both on and off-line!

- **How to create and protect strong passwords:**
  https://www.us-cert.gov/ncas/tips/ST04-002

- **Identifying suspicious emails and phishing scams:**
  https://www.us-cert.gov/ncas/tips/ST04-014

- **For our previous newsletter discussing keeping safe with your new devices:**
  https://msisac.cisecurity.org/newsletters/2016-12.cfm

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™