The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Overview
- Patching
- Backups
- Phishing

Lessons From WannaCry

Overview

Recently, you most likely watched widespread news coverage of a new cyber attack called WannaCry. It infected over 200,000 computers worldwide and locked numerous organizations out of their data, including hospitals in the United Kingdom. There are several reasons this attack gained so much attention. First, it spread rapidly from computer to computer by attacking a known weakness in Windows computers. Second, the attack was a type of malware called Ransomware, which meant that once it infected your computer it encrypted all your files, locking you out of your data. The only way you could recover your data was from backups or by paying the attacker a $300 ransom to decrypt all of your data. The third and most important reason this attack gained so much attention was because it never should have happened. The weakness that WannaCry attacked in Windows computers was well known by Microsoft, which had released a fix months earlier. But many organizations failed to install the fix, or were still using operating systems that are no longer supported by Microsoft. Here are three simple steps you can take to make sure attacks like WannaCry never infect your computers.

Guest Editor

Dr. Johannes Ullrich is the Dean of Research for the SANS Technology Institute. He is responsible for the **SANS Internet Storm Center**, which monitors current cyber security threats. He teaches Web Application Security (**DEV522**), Intrusion Detection (**SEC503**), and IPv6 (**SEC546**).

Patching

First and foremost, make sure your computers, mobile devices, apps, and anything else connected to the Internet are up-to-date. Cyber criminals are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to exploit them and hack into the devices you are using. Meanwhile, the companies that created the software for your devices are hard at work fixing these vulnerabilities by releasing updates. By dutifully installing these updates on your computers and mobile devices, you make it much harder for someone to hack you. That's what was so frustrating about the spread of WannaCry: the updates to fix and stop the attack had been released almost two months earlier by Microsoft. Had organizations kept their computers up-

Lessons From WannaCry

to-date, the attack would never have worked. To ensure that your devices stay current, enable automatic updating whenever possible to almost any technology connected to a network. This includes not just your computers and mobile devices, but also Internet-connected TVs, home routers, and gaming consoles (and someday perhaps even your car). If your operating systems or devices are so old that they are no longer supported with security updates, as is the case with Windows XP, replace them with new ones that are supported.

The key to protecting yourself from attacks like WannaCry is to follow three simple steps: keep your computers updated, be wary of phishing attacks, and back up your systems.

Backups

In some cases, cyber attacks like Ransomware may even infect up-to-date systems. A second way to protect yourself is to back up your data. Backups are copies of your information stored somewhere other than on your computer or mobile device. When you lose valuable data, you can recover that data from your backups. Unfortunately, too many people fail to perform regular backups, even though they are simple and inexpensive. There are two ways to back up your data: physical media or cloud-based storage. Each approach has advantages and disadvantages. You can use both approaches at the same time if you are unsure which one to use.

Physical media is devices you control, such as external USB drives or network-connected drives located in your home or office. The advantage of using your own physical media is that it enables you to back up and recover large amounts of data very fast. The disadvantage is that if you become infected with malware, such as Ransomware, it is possible for the infection to spread to your backups. If you are using physical media for backups, you should store copies of your backups off site in a secure location. Make sure any backups you store are properly labeled.

Cloud-based solutions are online services that back up and store your files on the Internet. Typically, you install an application on your computer. The advantage of cloud-based solutions is their simplicity. In addition, if you become infected with Ransomware, the infection cannot access cloud-based backups. The disadvantage is that it can take a long time to

Lessons From WannaCry

back up or recover very large amounts of data. Do not forget to consider the privacy and security of Cloud backups. Does the backup service provide your backups strong security, such as encrypting your data and strong authentication?

Phishing

Finally, bad guys are always updating and changing their methods of attack. Cyber criminals often use another attack method called phishing. Phishing is when cyber criminals send you an email that tries to trick you into opening an infected attachment or visiting a malicious website. If you do either, your computer may become infected. While WannaCry did not involve phishing, this attack method is commonly used for many other types of attacks, including most types of Ransomware. In addition, the cyber criminals who developed WannaCry will undoubtedly update their attack methods in the coming months and use new techniques, such as phishing, to infect even more computers. The key to protecting yourself against such email-based attacks is common sense. If an email or message seems odd, suspicious, or too good to be true, it is most likely an attack.

Video of the Month

Every month, we post a short, fun security awareness video that covers how you and your family can stay safe and secure online. Learn the latest simple tricks to making the most of the Internet. https://securingthehuman.sans.org/votm

Resources

What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Using the Cloud Securely:	https://securingthehuman.sans.org/ouch/2016#november2016

License