RISE
Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

May 2017 | SECURITY.BSD.UCHICAGO.EDU | Volume 3, Issue 5

Inside this Issue:

Lessons from WannaCry

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 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 reason this attack gained so much attention was because the weakness that WannaCry attacked in Windows computers was well known by Microsoft, which had released a fix months earlier. Many organizations failed to install the fix, or were still using operating systems that are no longer supported by Microsoft. The coordinated IT security teams at the University, the Biological Sciences Division (BSD), and the medical center are taking this threat very seriously. Many steps have already been taken to mitigate this threat, and we continue proactive assessment of University, BSD, and medical center systems to look for weaknesses and monitor for signs of infection.

Here are three simple steps you can take to make sure attacks like WannaCry never infect your computers.

1. Patching

First and foremost, make sure your computer, 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 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, mobile devices, Internet-connected TVs, home routers and gaming consoles, you make it much harder for someone to hack you. 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.

2. 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. Backup 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.

- The STA-01-BSD Minimum Security Standards for Systems specify that all important data should be backed up to a BSD-approved network storage.
- Laboratory system admins must establish a regular, procedure to carry out and verify regular backups.
- Labs should document restoration procedures, and periodically execute trial restores to ensure data continuity.
- The Center for Research Informatics can help meet these standards by housing your data and preventing unauthorized access by outside parties and providing automatic backup services. For more on the CRI, visit http://cri.uchicago.edu.

3. Phishing

Finally, cyber criminals are always updating and changing their methods of attack. Cyber criminals often use Phishing which involves sending you an e-mail 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, it is the most common attack method for most types of Ransomware. If an e-mail or message seems odd, suspicious, or too good to be true, it is most likely an attack.

For more information on phishing, visit the BSD ISO website:http://security.bsd.uchicago.edu/phish.

If you have any other questions, please contact the Organizations' Information Security Office.

Department	Email
BSD Information Security Office	security@bsd.uchicago.edu
UCM Information Security Office	help@bsd.uchicago.edu
UOC Information Security Office	security@uchicago.edu

Socializing Securely

Common threats from the use of social networking include viruses, identity theft, third-party applications, and social engineering attacks. This article describes the possible threats and the implications of those threats as well as how to protect yourself by implementing security measures and following good practices when using social networking services.

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

What security implications do these sites present?

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because:

- The Internet provides a sense of anonymity;
- The lack of physical interaction provides a false sense of security;
- They tailor information for their friends to read, forgetting that others may see it as well;
- They want to offer insights to impress potential friends or associates.

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

- **Remember that the Internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.

- **Be wary of strangers** - The Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.

- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.