RISE Enable • Protect
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

June 2017 | SECURITY.BSD.UCHICAGO.EDU | Volume 3, Issue 6

Inside this Issue:

Petya Global Ransomware Attack

On June 27, a second ransomware attack started affecting European companies and government agencies, as well as some large U.S. organizations, under the code name "Petya." This attack is similar to the global ransomware attack that occurred on May 12. So far, the University of Chicago and the University of Chicago Medicine have avoided any issues. **As we did on May 12, we are asking your help in minimizing any damage by ensuring that any Windows computers or servers you use or manage are secure**. **Detailed instructions for securing Windows computers follow this message.**

The malware exploits the same weakness from the May 12 attack, specifically a patch for MS17-010. Patches are available for Windows operating systems from Windows XP and above, and Server operating systems from 2003 and above.

Action required:

- Please review and be certain your Windows computers are patched with MS17-010.
- Backup your files on the network file share system, where they will be stored safely and are recoverable.
- If you are a victim of a ransomware attack, please notify the appropriate Information Security Office immediately:
  - BSD – security@bsd.uchicago.edu
  - UChicago – Call 2-CERT , or email security@uchicago.edu
  - UCM – Call 2-3456, or email security@uchospitals.edu

The coordinated IT security teams at the University, the Biological Sciences Division (BSD), and the University of Chicago Medicine 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. Please consult your preferred local or national news outlets for the latest information on the global impact of this attack.

Detailed instructions for securing Windows computers.

Windows 10

- Tap or click on the Start menu, followed by Settings.
- Once there, choose Update & security, followed by Windows Update on the left.
- Check for new Windows 10 updates by tapping or clicking on the Check for updates button.
- In Windows 10, downloading and installing updates is automatic and will happen immediately after checking or, with some updates, at a time

when you're not using your computer.

Windows Vista, Windows 7, Windows 8, Windows 8.1

- Open the Control Panel.
- If using Small icons view, click on the Windows Update option. If using the Category view, click on the System and Security option, then click on the Windows Update option.
- Windows Update will check for any available updates for your computer. If any updates are found, you should be able to view the available updates. It is highly recommended that you first install all important updates and service packs that are available. In some cases, you may only be able to do a few important updates or service pack updates each time, if some updates are dependent on other updates being installed first.

Windows XP and earlier

- Visit http://windowsupdate.microsoft.com.
  - For this page to work, you must view it in Internet Explorer.
- On the Microsoft Windows Update page, select the option Scan for updates. If prompted to install a plug-in, click Yes. Not installing this plug-in will prevent you from scanning for updates.
- After Windows Update has completed scanning, you should be able to view the available updates for your computer. It is highly recommended that you first install all critical updates and service packs that are available. In some cases, you may only be able to do a few critical updates or service pack updates each time.
- Although Microsoft does provide some driver updates for hardware devices, it is important to realize that they will not have all the latest drivers. You may want to consider updating the drivers directly from your computer manufacturer. See the computer drivers page for a listing of computer hardware manufacturers and a link to their drivers page.
- Note: Whenever you are prompted to reboot the computer, reboot the computer. Rebooting is an important step and in some cases may be required several times before you have installed all the Windows updates available. After the computer has rebooted, make sure to visit the Windows update page again to make sure all the files you need are downloaded.

BSD Endpoint Continuous Security Assurance

As part of the BSD Research-Centric Information Security Enablement (RISE) program, established to enable and protect the research and academic functions of the BSD, Endpoint Continuous Security Assurance is now available to your departments.

Background:

The Endpoint Continuous Security Assurance service uses IBM's BigFix for BSD IT Assets (i.e. laptops, desktops, and servers) to enable local technical support staff to ensure that devices meet organizational security requirements and reduce the risk of lost, stolen or destroyed data and institutional information that could lead to financial and/or reputational loss.

Features:

The Endpoint Continuous Security Assurance service provides the following benefits:

- It enables local technical support staff to ensure compliance with the University's and divisional cyber security policies and minimum security standards.
- It ensures alignment with our encryption requirements.
- It allows local technical support staff to install critical security patches on computers as soon as they are made available.

IBM's BigFix is a "client-based" tool. The BigFix software on the computer then communicates with the BSD's BigFix server system status updates. This information is necessary to verify encryption and associate the computer to the owner.

BigFix does not collect any personal data (email, calendar events, contacts, personal files, etc) from computers. Only the minimum inventory information about the computer will be gathered to ensure the device upholds the BSD minimum security standards.

Computers used for BSD science, academics and administration related business should be setup with the BigFix client software by your departmental IT Custodian.

For more information about the BSD's Endpoint Continuous Security Assurance service, visit http://security.bsd.uchicago.edu/bigfix-endpoint-management/. Send any questions and feedback about this new service to security@bsd.uchicago.edu.

The Wi-Fi Snooper

Wireless networks are convenient, but they are also inherently insecure. Hackers can easily snoop insecure wireless networks to steal confidential data and/or your personal information. Please read the following story about how student Jennie Parker narrowly escapes a cyber security incident.

Jennie Parker loved her new neighborhood coffee shop. When she needed to get out of the noisy, distracting environment of the laboratory and knuckle down on writing her thesis, it was the perfect retreat. Good espresso, comfy seats, friendly staff, and best of all, free Wi-Fi. The place was so chill, you didn't even have to ask for the password!

Across the coffee shop sat another regular visitor, staring deeply into his laptop. Max liked the cafe's password-free Wi-Fi too, though for completely different reasons. Using software he found on the internet, he could easily access all of the information sent to and from computers on the Wi-Fi. He could eavesdrop on the Internet connections from cafe shop patrons and screen information they sent. The place was crowded this afternoon, Max thought, and it promises to be a fruitful visit.

After staring at a blinking cursor for several minutes, Jennie decided she needed a break. Her roommate's birthday was coming up, and she needed to pick out a present soon. Maybe something from the yarn shop that just opened up downtown? Jennie went to their website, picked out some gifts, and was ready to enter her credit card, when she noticed something strange. Shouldn't there be a lock icon next to the site address in the browser?

Jennie heard somewhere that you shouldn't trust a site with your information if it was only "http," not "https." Oh well, so much for the yarn, she thought, and picked out a book from Amazon instead.

When Max noticed the woman at a nearby table pull out her credit card, he paid special attention to the Internet connection information popping up on his screen. Spotting the web address for a store, he was pretty sure a credit card number was soon to follow. But he winced when the user switched to an https site -- the subsequent data was encrypted, and thus impossible for him to crack. Not this time.

Back to work on her thesis, Jennie realized she would need to reference some data on her lab server. Dang it, she thought, I'm not ready to head back to the craziness of the lab just yet, and navigating to the server address from the cafe just brought up a forbidden access error. Then she remembered the BSD VPN, a "virtual private network" to create a secure connection to the BSD network.

By entering in her BSD user name and password (on a https site, she noticed), Jennie could access her data remotely and feel confident about its privacy. Relieved she didn't have to head back to her office just yet, she cheerfully ordered another coffee and dug back into her thesis.

Max perked up when he noticed some interesting traffic to university sites from the IP address he was watching for credit card information. Now he dug

through the packets looking for passwords -- one slip, and he could access all of the user's private information and e-mails. But again he was foiled, as encrypted data showed up once again. "I guess people at this cafe are getting smarter," he thought, closing his laptop and sulking out the cafe door.

Preventative Measures

- To connect to a wireless network, you must first select the network you want to connect to. There are often multiple networks to choose from in crowded or public places. However, always be careful which networks you connect to. Cyber criminals can create counterfeit or fake wireless networks designed to harm or monitor everything you do. To protect yourself, always be sure you are joining a trusted Wi-Fi network. Otherwise, you have to assume that devices on non-trusted networks can scan, probe or hack any other device connected to that network. By making sure you only connect to trusted wireless networks, you protect yourself against these and other attacks.

- When working remotely, use the BSD's VPN (Virtual Private Network) to connect when using a wireless network other than the UChicago's. Visit http://security.bsd.uchicago.edu/bsdvpn/ to learn more about the BSD VPN. If your department is not currently participating in the BSD VPN, you can use the University's cVPN at https://cvpn.uchicago.edu/.

- Finally, make sure your laptop and mobile devices are using is the most current version and has the latest patches and software. In addition, be sure your encryption software is installed and you have anti-virus

What to do if you become aware of an information security incident? Contact the BSD ISO Team via email at security@bsd.uchicago.edu.