[Blog post/mailing list]

Some Notes about the Current Ransomware Attack

You may have seen reports this past weekend about the worldwide ransomware attack known as WanaCrypt0r or WannaCrypt. A few people have asked me about this so here are some basics:

What is ransomware?

Like all malicious software, ransomware is designed to attack computer systems. Typically ransomware will sequester your computer and encrypt your files until a ransom is paid to the attackers. It may be delivered via an infected email attachment, a hijacked website, or a USB drive. In this case, the infection appears to be delivered directly through computer networks, which is one reason it has spread so quickly. It's important to understand that while the main attacks have been occurring in Europe, the U.S. is not invulnerable so prevention is our best defense.

Am I protected?

This particular ransomware infection attacks Windows systems through a known vulnerability which was patched by Microsoft in March for Windows 10, Windows 8.1, Windows 7, and Windows Vista. If your computer is set for automatic updates, you will be protected. If you are not sure if your computer is set for automatic updates, please email me and I can help you to configure it.

If you are still using Windows XP or Windows 8.0, Microsoft has issued a patch which you can download and install here:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

What can I do generally to protect against ransomware?

As with all malicious infections, ransomware is constantly evolving. This attack is targeted at Windows and so the following steps are directed primarily at Windows users. Those of you who are Mac and Linux users are also vulnerable to ransomware so some

of these will apply to you as well. Be aware that there is no method of protection that is 100% secure. Nevertheless, we can aim for the best protection possible. My recommendations:

1. Ensure your computer is set to automatically download and install security updates. Windows 10 does this automatically; for other Windows versions, follow these instructions.

2. Set up periodic backups of your drive or at least your important directories, so that you can restore them in the event of a ransomware or other malware attack. This is not just about malware, a simple hardware failure can result in data damage or loss (yes this has happened to me!). There is a debate about whether cloud backup (e.g. DropBox) or local backup (e.g. an external drive) is better. My opinion is that they both have merit but you should pick what is easiest for you to manage and just get started. If you're not sure about any of this, email me and we can talk further.

3. Install and configure an anti-malware application that can monitor your computer. Windows has Windows Defender built-in so set it to scan your machine regularly. Also, consider third-party applications like Malwarebytes.

4. If you are on your own home network, activate and configure your computer's firewall. Windows has a built-in firewall and you can check its status.

5. If someone sends you an email attachment that you didn't ask for, check with them BEFORE you open it, to make sure they really sent it. Attachments are common vectors for ransomware. The same holds for unsolicited emails with links to websites you are unfamiliar with. This is the basis for most phishing attacks.

6. Social media posts are also common vectors for ransomware and other malware attacks. Think carefully before clicking on links or embedded images, especially if they are forwarded to you from someone else.

Good security is built in layers, so please consider all of these steps as you secure your computer and data. It is important to remember that the individuals and groups who create these attacks are counting on you to behave naively and expose yourself to their attacks. By following the above precautions, you can stay safe and smart online.

NCSA statement about attack
https://staysafeonline.org/about-us/news/ncsa-statement-on-the-ransomware-attack
CERT statement about attack
https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported
Information about the March 2017 security patch:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Microsoft guidance for this attack
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/