Privacy Buzz

MAY 2016 – RANSOMWARE

What is Ransomware?

Ransomware can take different forms, but in its essence it denies access to a device or files until a ransom has been paid.

Some Facts about Ransomware:

1. Hackers use the following paths to infect a machine: phishing emails, unpatched programs, compromised websites, online advertising and free software downloads;
2. Not only can ransomware encrypt the files on your computer, the software is smart enough to travel across your network and encrypt any files located on shared network drives;
3. Typical ransomware has a 48-72 hour deadline which, once passed, causes the ransom to increase. Most ransoms start in the $100-$500 area, and once the deadline has passed it will likely increase to over $1000.
4. Once the files are encrypted, the hackers will display some sort of screen or webpage explaining how to pay to unlock the files.

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money
Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse. Read Entire Article - May 23, 2016

Is My Computer Infected?

1. You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
2. An alarming message has been set to your desktop background with instructions on how to pay to unlock your files.
3. The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files.
4. A window has opened to a ransomware program and you cannot close it.
5. You have files with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML

Ransomware Can Be Avoided By Practicing the Following Safe Browsing Habits:

1. Never click on pop-ups.
2. Ensure Operating System (OS) and browser(s) are up to date and/or patched.
3. Maintain active, up-to-date firewall software.
4. Never respond to spam emails.
5. Only open known or expected email attachments.
6. Do not click on links in emails. Always copy and paste links to a browser.
7. Avoid using a personal email account to register for random or short-term services.
8. Avoid using peer-to-peer (P2P) network programs.
9. Use a reliable site adviser, such as McAfee SiteAdvisor, to help you avoid potentially malicious sites.

If a work machine is infected, please contact the VUIT Help Desk or your local support personnel.

For more information about how ransomware works or how to protect yourself, contact VUIT Security Operations at vuit.security.operations@vanderbilt.edu