RANSOMWARE

Message from Delaware Chief Security Officer, Solomon Adote

Delaware continues to monitor the cyber events impacting the City of Baltimore, MD. As you'll read in this edition, the City was a victim of a ransomware attack which was initiated through a phishing attack.

This is how bad actors are taking advantage of just a momentary lack of vigilance to bring the operations of a major US city to a halt. It's been 3 weeks, $18 million spent and the city is still struggling to recover. Each of us has a responsibility to help keep our state and organizations safe and secure. I urge you to increase your vigilance while using email.

Delaware state employees should complete Securing the Human 2019 to acquire new skills that can help identify the tactics of the bad actors. **Stay alert!**

Ransomware is a cyber attack by criminals that locks the data on a victim's computer, usually by encryption. The motive is nearly always financial. Perpetrators notify victims that their computer has been infected and give instructions on paying for recovery, often in cryptocurrency, such as Bitcoin.

Individuals aren't the only target: governments, institutions, and businesses all collect personal data, a goldmine for hackers. A brute-force attack hit Colorado's Department of Transportation (CDOT). A variant of the SamSam ransomware, penetrated a temporary system being tested without full security. It is strongly recommended to secure even limited deployment or test systems. Bad actors accessing CDOT ultimately affected roughly half its IT environment: 1,300 PC's, 400 servers, and all databases/ applications.

Baltimore's incident froze computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services. Even now, a month after the attack began, many systems remain offline. The Baltimore Sun published details of a phishing email that allowed hackers inside the City network.

HELP I'M INFECTED!!

The Malwarebytes blog offers these tips for avoiding data ransom threats and recovering if you are a victim:

Rule 1: ***Immediately*** contact your Security office and/or IT department if your workplace computer is infected

Rule 2: ***Never*** pay the ransom. This is advice endorsed by the FBI. All that does is encourage cybercriminals to launch additional attacks against either you or someone else.

Solutions for ransomware infection after it happens are imperfect at best. They often require more technical skill than the average computer user has. Avoid fallout from ransomware attacks through good defenses.

Invest in a reliable cybersecurity program with real-time protection designed to thwart advanced malware attacks such as ransomware. Look for features that shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage (an anti-ransomware component).

Create secure backups of your data regularly

Use cloud storage that includes high-level encryption and multiple-factor authentication. Although you can purchase USBs or an external hard drive to save new or updated files, you must physically disconnect these devices from your computer after backing up, otherwise they can become infected with ransomware, too.

Keep operating systems and software updated

The WannaCry ransomware outbreak took advantage of a vulnerability in Microsoft software. Even though Microsoft released a security patch in March 2017, many folks didn't install the update promptly, leaving their computers open to attack. Safest method: change your settings to enable automatic updating.

Finally, Stay Informed

Social engineering, visiting suspicious websites, and falling prey to other scams are among the most common ways computers are infected with ransomware.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.