2021 Cyber Hot Topics: Ransomware

From the desk of
Michael Aliperti
MS ISAC Chair

In response to the pandemic, many end-users are now working from home instead of commuting to their business locations. Homes are being used as business offices, and computers and networks are being shared by family members. Families are taking classes, doing homework, and surfing the web in addition to performing business functions.

The data created may be stored locally or in the cloud. Backups may not happen until the device is returned to the office or the end-user manually backs it up. This new environment is ripe for cyber-attacks.

The Perils of Ransomware

Ransomware is one of those cyber-attacks that are on the rise. Ransomware is a type of malware that is normally delivered through a phishing message. The phishing message entices the reader to click on a link or open an attachment. When the recipient falls for the phish, the process of infecting the device is started. It initiates a connection back to the attacker's device to receive instructions for encrypting the device.

Once the encryption is completed, the user is locked out of their data and the device. At this point, a ransomware note is displayed and a ransom is demanded in cryptocurrency (i.e. Bitcoin) to regain access to their data and their system.

Protect Your Family, Data, and Devices

So, what does this mean to you? How can you protect your family, data and devices from these cyber attackers? Here are some best practices for cyber hygiene that can help protect you from becoming a victim of ransomware:

- Don't open any emails from someone you don't know or that you aren't expecting to receive.
- Don't click on links in messages.
- Avoid opening attachments in messages. Download the attachments and scan them for malware before opening.
- If it sounds too good to be true, it probably is. Don't give away any personal information that could allow an attacker to compromise your devices or steal your identity.
- Install anti-virus/anti-malware software on your device and keep it up to date.
- Apply patches to all applications and the operating system as they become available.
- Don't browse suspicious sites. Cybercriminals count on users mistyping the name of a legitimate site. These sites are made to look like the legitimate site but are used to deliver malware to the device.
- Don't respond to pop-up windows instructing you to call a number for support. Attackers use this method to steal your personal and credit card information. Once you allow them to remotely access your device, they will install additional malware on your device instead of removing it.

What to Do if You Get Infected with Ransomware

- Don’t respond to a ransom note on the screen. Paying the ransom does not guarantee that you will gain access to your data and/or your system. The attackers will normally request payment in a form of cryptocurrency, like Bitcoin, that can’t be traced. Once the ransom is paid, your money is gone.
- Seek professional assistance. Contact your employer’s IT security department and/or law enforcement to allow them to trace the source of the infection.
- Using a separate non-infected device, change passwords on all accounts that were accessed from that device.
- If you provided the attacker with personal and/or credit card information, put a fraud alert on your account at the three major credit reporting bureaus (Experian, TransUnion, and Equifax). This should prevent the cybercriminal from using your information to open new accounts in your name. If credit card information was provided, contact your credit card company to report it to their fraud department. They will normally issue you a new credit card number and shut down the old account to prevent it from being used fraudulently.