RANSOMWARE 101 - AUGUST 2017

A CRASH COURSE IN DEFENDING YOUR DATA

WHAT IS RANSOMWARE?

Ransomware is the term for malware (malicious software) that prevents or limits a user from accessing his or her files by locking them down, a practice commonly referred to as encryption. The only way to unlock the encrypted files is to pay ransom, usually in the form of Bitcoins, an online digital currency. Ransomware started by preying on individuals, but more recently has become a huge threat to even the largest organizations too. And if you think these schemes are being ran out of somebody's mom's basement, think again. These attacks are increasingly coming from very large, very organized crime rings that are business-oriented, tech savvy, and looking to you to help them cash in on their efforts.

HOW DO THEY GET IN?

Unfortunately, ransomware can hit in a variety of ways, but as with most crimes on the internet, the most popular avenue for attack is through spam emails that contain malicious links or attachments. Other successful methods include security exploits in vulnerable software, legitimate websites that have malicious code injected, and internet traffic redirecting to malicious websites.

WHAT MAKES RANSOMWARE SO EFFECTIVE?

One reason – fear. Ransomware operations succeed because they capitalize on fear, which could ultimately force the user to do something irrational…like paying the ransom. Maybe the fear you'll lose your job because you lost important documents to ransomware is unthinkable. Perhaps getting locked out of your system, never to open your files again, is too much to bear. Or maybe being indicted for potentially embarrassing browsing habits or unwanted public exposure makes you compelled to pay. Whatever the case may be, fear is what keeps the ransomware train on the tracks.

HOW DO YOU DEFEND AGAINST IT?

The Ransomware threat is as real as it gets, but paying shouldn't be an option if at all possible, as paying the ransom does not necessarily guarantee that victims regain access to their locked files. The best thing you can do for yourself is back up the important data on your computer to either an external hard drive, The Cloud, or both! That way, you can restore all of the files that were encrypted by the ransomware without paying the ransom. Below are some other tips to make sure you don't get caught up in the ransomware web in the first place:

- Avoid opening unverified emails or clicking links embedded in them.
- Make sure you have strong passwords that vary across all systems, software, and devices you use (Remember, the longer the password, the stronger the security!).
- Make sure all of your software, including antivirus, is up to date with the latest security patches installed.
- Adjust your browser's security and privacy settings for increased protection.
- Did we mention you should back up your files to The Cloud or an external hard drive?!? Yeah, it's that important!

REPORTING THE INCIDENT:

If you do find yourself in the middle of a ransomware situation, reporting is key. In addition to notifying your local police department, victims should immediately report any ransomware attempt or attack to the FBI at the Internet Crime Complaint Center, www.IC3.gov.

866-BANTERRA (226-8377)
Banterra.com MEMBER FDIC

Banterra®