July 11, 2017

Three Hack Attacks that Banks Are Watching (And What They're Doing About Them)

Cybersecurity experts around the world track threats minute-by-minute and it's a constant battle against new and evolving threats. Last month the "WannaCry" ransomware attack was the largest of its kind on record and affected millions of computers, even crippling portions of the U.K. healthcare system.

For the banking industry, the financial livelihoods of organizations and individuals are at risk – high stakes for cybersecurity experts and a top target for hackers around the world.

Here are the top three hack attacks that the cybersecurity community sees as most threatening to the banking industry:

- **Attack Type: Micro-Targeting**
  Highly sophisticated cybercriminals have moved on from emails blasts, instead preferring to target specific geographic regions and even individual companies and executives. In some cases, the American Bankers Association (ABA) has reported that hackers have broken into bank business customer accounts and impersonated members of their management to steal money and data. In other cases, retail customers are scammed into thinking that a relative is in jeopardy and needs money.

  What Banks Are Doing About It:
  Banks are adopting highly secure email applications to protect both inbound and outbound internet communications. Bankers are also educating their customers on threat actors' tools, tactics and processes. Recommended approaches to prevent micro-targeting attacks also include data categorization so that access to information is restricted as part of network structure as well as through personnel security including strict enforcement of password policies and limiting high priority accounts. Banks can also use log analysis to detect patterns and create countermeasures to help prevent attacks.

- **Attack Type: Highly Sophisticated Phishing**
  "Click on this link" emails containing hidden viruses aren't what they used to be. These days, savvy hackers are creating highly realistic, but fake websites and email campaigns that mimic bank web properties. Often, the hacker-created versions are nearly identical to those they're impersonating – including login screens and detailed sets of data fields.

What Banks Are Doing About It:
To provide customers with confidence they are on an authentic website, banks are now using Domain Name System Security Extensions (DNSSEC). Additionally, Transport Layer Security (TLS), more commonly known as encryption, ensures confidentiality and integrity of communications and transactions over the internet. DNSSEC and TLS are two of the mandated security requirements for .BANK domains. .BANK domains also include verification at the time the name is registered and periodic reviews to confirm the identity of the domain owner.

- **Attack Type: Ransomware**
  Ransomware is an increasingly common method for hackers looking to launch a mass attack. In 2016 alone, losses from ransomware were well over $1 billion according to the ABA. Cybersecurity experts say ransomware attacks come in many forms which range from email phishing, to popup windows, to downloadable software. As noted above, "WannaCry" is a recent example of this type of attack.

  What Banks Are Doing About It:
  Ransomware attacks require many defenses including customer education, staying current on software patches from vendors and data segmentation and backups. It's hard to stop all ransomware and having a sound backup process can provide a quick recovery from this and other types of attacks.

Beyond these specific hack attacks, banks are working hard to combat a rapidly changing cybercrime landscape. "Sheltered Harbor" is a new initiative that adds a significant layer of protection for the financial services industry. Banks that opt into the program maintain account information in secure, distributed storage that allows them to quickly rebuild their customer data following an attack as part of their security protocol. In an environment of near-constant cyber threats, it's one more tool in a growing arsenal for the banking industry.