by Michael Bazzell

Protecting Your Organization From Computer Crime

Online fraud changes every day. We are seeing the evening news transition from reports of violent crimes to details of the latest cyberattack. Cyber criminals adapt their techniques constantly in order to always stay one step ahead of victims. Lately, most hacking groups focus on stealing a large amount of data from companies. This may be credit card numbers, login credentials, or private personal information such as Social Security numbers. The groups find it much more lucrative to put the time into stealing large databases of information instead of targeting individuals. Recent attacks, such as those against Equifax and other high-value targets, are typical of these cases. In these attacks, criminals steal the details of millions of people, causing great financial loss. However, these attacks are much less common than the smaller attacks that rarely make headlines. For every large entity that is compromised, hundreds of smaller organizations' servers are exploited.

I believe the most probable attack against smaller organizations is targeted email spear-phishing. Standard phishing has been around for many years. When you receive an email that appears to be from your bank, it is likely a phishing attack. These messages use a scare tactic to make you think that your account has been compromised, and provides an internet link that will allow you access to your account to protect your money. Of course, the link forwards to a cloned website that is visually similar to the real bank website, and the criminals hope that you provide your user name and password to gain access. As soon as you do, they access your real account and do as much damage as possible in a short amount of time. Spear-phishing takes things to a different level.

How Would I Hack You?

The following is a scenario that I would use if I were going to target a specific entity as a criminal hacker. This is based on my experience investigating these types of incidents.

I would do my homework and research the entity. I might look up current and previous hiring opportunities for a position such as computer technician or network administrator. These posts probably include a reference to the type of systems that are present, such as the operating system of your network or the type of database that is used. It is common for a recruitment post to mention required skills such as "SQL Server Administration" or "Microsoft Exchange Administration." Both of these tell me enough about your environment to start an attack.

I would then create a list of employee names that I want to target. I would do this through Facebook, Twitter and LinkedIn. In my presentations, I show how a hacker can create a list of more than 75 percent of a business' employees by scraping these social networks in less than five minutes. I would then locate a few official email addresses from the company's website in order to identify the format of all email addresses for the employees. For example, if I find Bob Wilson's email address is b.wilson@company.com, I know that Mary Johnson is m.johnson@company.com, and Tom Williams is t.Williams@company.com. I would use Excel to generate the list for me.

Now that I have the email addresses of my targets, I would generate a custom bulk message similar to the following.

Dear employee,

As you may know, our Microsoft Exchange Server was partially compromised in an early morning attack. Fortunately, all of your information is safe; however, we need you to reset your password immediately. Any accounts that have not been converted by the end of the day will be disabled. Please click the following link to update your account.

www.secure-email-server-company.com

This email would be sent from a free program that will "spoof" an email address and name to be anything desired. I

would search on LinkedIn to find the name of your computer network administrator and make the email appear to be from him or her. The shady link in the message would forward to a server that I have full access to. As soon as you log in, I have your current credentials to your email account. I would use these to access your real account and look for bank statements, company accounts, etc. I might even send a quick note to everyone in your contact list telling them that I (you) are stuck in the U.K. and need $1,000 to get a new passport. I only need one person to respond and wire me money to make it worth my effort. If this message was not appropriate for your organization, I might choose something similar to the following.

Dear employee,

As you know, we have finished the migration to the new payroll direct-deposit system. If you are receiving this message, you have not submitted the required form in order to have your paycheck deposited into your account. Please complete the attached document and return by the close of business today. You cannot be paid until this data is entered.

The attachment with this message would be a malicious DOC or PDF file that would not raise any red flags. When you open it, your machine becomes infected and I would have remote access to your data. I would send this email from the name of someone in your payroll division for that extra feel of authenticity.

Overall, these messages always contain three very specific elements:

- **Scare Tactic:** This could include a data compromise (example 1) or payroll issues (example 2).
- **Action Requested:** This could include clicking a link (example 1) or opening a file (example 2).
- **Familiarity:** This could include familiar details (your software provider) or personnel (your payroll manager).

Ultimately, I will attempt to use your username and password combination on any business websites or social networks you may have access to such as online email providers or financial websites. If you use the same password for multiple services, I compromise all of them. Every day, several employees fall for these scams.

Be extremely cautious of unsolicited email messages. If anything seems out of place, challenge the message. If it appears to be from a co-worker, call that person and verify the details. If it appears to be from a business partner, contact that entity through known valid channels and verify the information. While challenging others is often considered rude, it may save you from becoming the next victim.

Also, be careful about the content that you post online. If your Twitter account mentions your upcoming vacation to Hawaii, you are helping a burglar. If your LinkedIn account summarizes your duties at your workplace, you are helping a potential cyber attacker. If your Facebook page has photos of your child with a nickname of "Mikey," and your security question on your bank account is "What is my son's nickname?", you are really asking for trouble. Surprisingly, hackers have all of the time in the world to identify the smallest of vulnerabilities in your life.

Overall, I know that we cannot stop all computer crime. However, I truly believe that you can prevent it from happening to you. Following some general rules will prevent you from being the easiest target for a close eye on your online activity will help you avoid becoming the next victim on my incident list.