It's Phishing Season: How to Prevent Your Company from Getting Speared

By: David Newell, Chief Executive Officer, Loptr LLC
Kristopher Meier, President, Station 28, LLC
Edward O'Keefe, Director of Application Development, ABC-Amega, Inc.

Editor's Note: The subject phising and the financial damage it can cause for companies was brought up at the CRF Open Forum in Chicago in August 2016. CRF thanks ABC-Amega, Inc. for offering this article.

Forbes magazine reported in May that "people are often the weakest link in the security chain." The problem posed by contributors Steve Culp and Chris Thompson is that cyber criminals target fallible humans to get around investments in technical and physical security systems.

We recently heard a story that turns that idea on its head. Perhaps people can be the strongest link instead!?

Last month, a firm of about 150 employees was targeted with a spear-phishing attack *(Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.)* The attackers sent an email with a bogus invoice attached to nine different employees. Each phish was unique, with different text and filenames to evade detection, and the phishers personalized the messages with names and titles.

Unfortunately, one target, who works with invoices every day, didn't realize this one was fake.

After clicking to open the Microsoft Word attachment, a malicious macro exploited a zero-day vulnerability *(A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it)*, which bore into the computer. With a foothold on the system, the attacker's software reached out to "command and control" (C&C) servers *(command and control (C&C) infrastructure consist of servers and other technical infrastructure used to control malware in general, and, in particular, botnets)* in four different countries to try to make a connection. Once connected, the code started downloading additional applications to the computer's hard drive.

At this point, you can only imagine the worst happening: encrypted files being compromised on the victim's computer and shared drives, hackers gaining access to customer credit card data – panic-evoking stuff! Instead, the attack abruptly stopped. A member of the IT team rushed into the victim's office and unplugged the network cable.

The quick resolution wasn't luck. The company had focused on security improvements over the previous year.

The firm brought in consultants to help design its security program, establish controls, scan its networks, put monitoring systems in place, update and patch, share training and awareness, and it ran through table-top exercises to test out its processes. It took hard work to reach the point where the company could quickly identify and contain an attack. One of its practices was now a "post-mortem" review, where the firm analyzes an event to learn and, when needed, make improvements. As a result, the company's IT team mapped out the attack which we shared above.

The spear was carefully aimed.

Though only one person opened the malicious email attachment, the phish was targeted to nine different people at this firm. As it turned out, the nine names and titles came from one of many sites that harvests and sells personal information on the Internet. One name and title were incorrect in a unique way that made it clear which website was the source. An intriguing twist was that the site listed two additional employees who did not receive phishes. Both were members of the technology team. It appears the bad guys took the time to filter out IT staff who might be more likely to spot an attack.

The email messages all purported to deliver invoices, but each was slightly different. Each malicious attachment was also different. Those differences appear to have helped the malware bypass the firm's gateway anti-malware. (The company switched products to add attachment sandboxing after this attack, and it updated its configuration standard to disable Word macros.) The team checked mail server logs to identify other recipients of the phishing attack, confirmed that none of the other eight had clicked the attachment, and removed the messages.

The firm's intrusion detection system (IDS) didn't detect the attack. Because the firewall blocked traffic to "risky countries", it took several tries for the malware to find a C&C server it could reach. The firewall logged those attempts and successful connections to download more software to a centralized server but, like the IDS, the log monitoring software hadn't registered an attack. The company's anti-virus software only triggered on one of the additional malware downloads, reporting that the system had successfully quarantined a file.

©2016 Credit Research Foundation

How did IT (literally) pull the plug on this attack so quickly?

The person who opened the malicious attachment realized it was bogus and, instead of brushing it off or worrying about getting in trouble, quickly notified the IT department by following the protocol of submitting a trouble ticket via the company's ticketing system and by personally finding an IT representative in the office. As a result, an IT staffer immediately checked the anti-virus logs and raced to the victim's office.

Again, the swift response wasn't luck. In addition to conducting annual awareness training sessions with all employees, each week the firm's IT team rotates a new "digital poster" with a simple security awareness message on every computer's login screen. These reminders reinforce security practices that every workforce member should know. About 35% of the messages focus on reporting potential incidents to IT.

The secret to effective security reminders is three ingredients: simplicity, variety, and policy. For a little extra impact, add humor.

Make your reminders simple. Don't use a lot of words. Deliver your message in five seconds as a worker logs in or walks down a hallway. Vary the backgrounds and format of your reminders, and rotate and refresh your reminders regularly. And mix in policy. That doesn't mean you have to quote your policies, but consider the policies you want your workforce to follow and focus on the key policy statements that apply to everyone in your organization. Topics like good passwords, reporting possible incidents, protecting data, preventing loss or theft, and using encryption are examples. And, seriously, mixing in some humor, pop culture references, or unexpected formats (for example, haikus) can draw and keep attention. If you can get your workforce to look forward to your next information security awareness message, they are paying attention.

How should you deliver awareness messages? Continuously rotate new messages on digital signage platforms. Print small posters and place them on bulletin boards and cubicle walls. Place digital images on login screens, backgrounds, or screen savers. Send reminders by email. Post them on your intranet.

When the company completed its post-mortem review after the attack we've described, they reasoned that the critical control that stopped this attack quickly was an awareness poster. A person paying attention to reminders had halted an attack that two anti-virus systems, IDS, a firewall, logging, scans, and patching couldn't stop.

People *can* be the strongest link in the security chain!

©2016 Credit Research Foundation