The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- What is Spear Phishing?
- Effectiveness of Spear Phishing
- Protecting Yourself

Spear Phishing

What is Spear Phishing?

You may be familiar with phishing attacks. These are emails sent by cyber criminals to millions of potential victims around the world designed to fool, trick or attack them. Usually, these messages appear to come from a trusted source, such as your bank or someone you may know. The emails often have an urgent message or a deal for you that is simply too good to pass up. If you click on the link in a phishing email you may be taken to a malicious website that attempts to hack into your computer or harvest your username and password. Or perhaps the phishing email may have an infected attachment -- if you open the attachment it attempts to infect and take control of your computer. Cyber criminals send these emails to as many people as possible, knowing the more people that receive the email, the more people will likely fall victim.

Guest Editor

Lenny Zeltser is the guest editor for this issue of OUCH! Lenny focuses on safeguarding customers' IT operations at NCR Corp and teaches malware combat at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **blog.zeltser.com**.

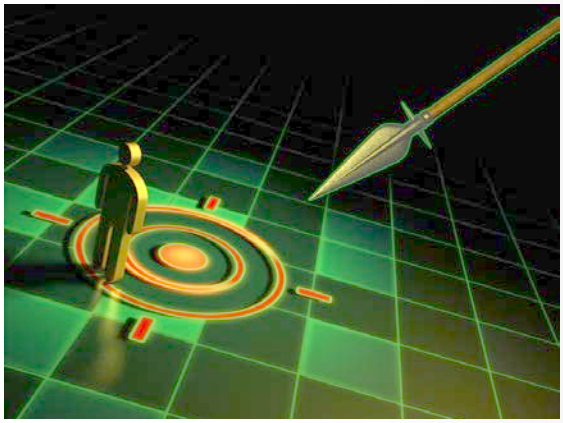
While phishing is effective, a relatively new type of attack has developed called spear phishing. The concept is the same: cyber attackers send emails to their victim, pretending to be an organization or a person the victim trusts. However, unlike traditional phishing emails, spear phishing messages are highly targeted. Instead of sending an email to millions of potential victims, cyber attackers send spear phishing messages to a very few select individuals, perhaps five or ten targeted people. Unlike general phishing, with spear phishing the cyber attackers research their intended targets, such as reading the intended victim's LinkedIn or Facebook accounts or any messages they posted to public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim to the attack.

Effectiveness of Spear Phishing

Spear phishing is used when the cyber attacker wants to specifically attack you or your organization. Instead of simple criminals out to steal money, attackers who use spear phishing have very specific goals, usually accessing highly confidential information such as corporate business secrets, plans for sensitive technology or

Spear Phishing

confidential government communications. Or perhaps your organization was targeted simply as a stepping stone to gain access to another organization. Such attackers stand much to gain, and they are willing to invest the time and effort to research their targets.



The best way to protect yourself against spear phishing is to be aware that you could be a target, limit the information you post about yourself and report suspicious emails.

For example, a foreign government may decide that your organization develops a product or technology that is key to their economic success and they begin to target you. They research your organization's website and identify three key individuals. These attackers then research the LinkedIn, Twitter and Facebook pages of those three individuals and create a complete dossier on them. After analyzing these targeted individuals, the attackers then create a spear phishing email pretending to be a supplier that your organization uses. The email has an attachment pretending to be an invoice, when in reality it is infected. Two of the three targeted individuals are tricked by the spear phishing emails and open the infected attachment, giving the foreign government total access to their computers and, ultimately, all of your organization's product secrets, which they will now produce themselves.

Spear phishing is a far more dangerous threat than simple phishing attacks, as the attackers are crafting an attack specific to you or your organization. Not only does this increase the chances of the attacker's success, but these attacks are far more difficult to detect.

Protecting Yourself

The first step to protecting yourself against these targeted attacks is to understand that you may be a target. After all, you and your organization probably possess sensitive information that someone else might want, or can be used to access another organization that is the attacker's ultimate goal. Once you understand that you could be targeted, take the following precautions to safeguard yourself and your organization:

- Limit the information you post about yourself, such as mail forums, Facebook or LinkedIn. The more personal details you share, the easier it is for cyber attackers to craft a spear phishing email that appears relevant and genuine.

Spear Phishing

- If an email that asks you to open an attachment or click a link appears suspicious or requests sensitive information, verify the message. If the email appears to come from a company or a person you know, use the contact details you already have on file to contact the sender and verify that they sent you the message.

- Support your organization's security efforts by following the appropriate security policies and making use of the security tools that are available to you, such as antivirus, encryption and patching.

- Remember, technology cannot filter and stop all email attacks, especially spear phishing emails. If an email seems a bit odd at first, read through it carefully. If you are concerned that you may have received a spear phishing email or fallen victim to spear phishing attack, contact your help desk or information security team immediately.

Special Purchase Program

Are you employed in Education or State & Local Government? Do you need security awareness training but have a limited budget? If so, now is the time to take advantage of a limited time offer through the SANS Institute. Now through July 31st, receive discounts on Securing the Human for End Users & Developers, OnDemand Courses, GIAC certifications, and NetWars Continuous. For more information, please visit:

- Educational Institutions – http://www.sans.org/renisac
- State & Local Governments – http://www.sans.org/cis

Resources

How to Avoid Getting Spear Phished:	http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304
Avoiding Social Engineering and Phishing Attacks:	http://www.us-cert.gov/ncas/tips/st04-014
Phishing:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
Common Security Terms:	http://www.securingthehuman.org/resources/sec
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis