National Cybersecurity and Communications Integration Center

03 September 2013

Spearphishing Attacks

Spearphishing

Spearphishing is generally defined as the targeting of individuals or groups with the intent to harvest specific information or infect the targeted entities with malware. Malicious actors craft emails that appear to be from a legitimate source, often address the targets by name, rank, or title and are intended to be convincing enough to entice the target to open an attachment, click on a link or respond with information. According to a 2012 Trend Micro report[1], 94% of spearphishing emails use malicious attachments while the remaining 6% use alternative methods like links to malicious websites used to drop malware on a victim's computer or spoof a login page in attempts to steal user credentials.

Targeting

Often, it is not necessary for actors to compromise a system to gather information about a target individual or organization. Malicious actors may be interested in or angry with a person or organization and choose to make them a target. Actors can locate names, jobs, titles and personal information of individuals and their companies simply by searching the web or social media platforms like LinkedIn.[2] This information can be used in their campaigns to increase the apparent validity of their phishing messages and lower the guard of intended victims. Additionally, actors can use information gathered from one individual and apply it to another within the same organization. For instance, many companies follow standardized email naming conventions. Therefore if an attacker knows that a company uses joe.doe@company.com, they may be able to determine an individual's email address even if that address has never been posted online.

Avoid Becoming a Victim[3]

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Be wary of emails with grammar and spelling errors as these can be red flags for phishing attempts.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information including following links sent in email. Instead type the URL of the valid organization into a browser manually to ensure you do not become a victim[4]
- Check hyperlinks by hovering over them with your mouse. The true link destination should appear. If the website looks suspicious it may be a phishing email. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- Check for spoofed emails by hovering over them with your mouse. This should reveal the sender of the email. If the senders email does not appear to come from or be associated with the

received email, it may be a spoofed phishing email. Additionally, you may view message headers to determine the sender as well.

- Be mindful of suspicious attachments, especially those that include extensions such as .exe, .zip, .com, .bat. [5]
- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information). Many login pages like those of financial institutions use encryption. These sites will appear as https://. If you are logging into a secure site without https in the URL, it may be spoofed.[6]
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

Tools for Prevention[7]

- Digitally Signed E-mail (PKI)
  - Digital signatures are unforgeable, to a high probability.
  - Messages can be automatically verified by E-mail readers.
- Secure Token Authentication
  - Social engineering scams like phishing will always be possible as long as the victim knows all of the information necessary to make a transaction.
  - The user cannot accidentally divulge the information necessary to make an electronic transaction.
  - All fraud requires physical access to the token.
  - The user cannot opt to authenticate in a way that circumvents the security policy.
- Sender Policy Framework (SPF)
  - Phishing emails often forge the sending domain of the targeted institution.
  - Forces phishers to use sending domains that are not identical to the legitimate sending domain name.
- Implement Technical Controls to Prevent Use Of Embedded Hyperlinks (E-Mail)
  - Phishing attacks through deceptive URLs can be reduced.
- Implement Technical Controls to Prevent Use of Personal Webmail
  - Phishers often target the personal email account (i.e. Yahoo, Gmail, etc) of targeted Government Employees.
  - Webmail is a vector for inadvertently introducing malicious code to the Government's network.
- Active Web Monitoring
  - Spam filtering rules can be rapidly updated by vendors to block E-mail containing references to malicious sites.
- E-Mail Gateway Anti-Virus Scanning (Sandboxing)
  - Malicious code can be blocked from entering the network.
  - Gateway scanning supports rapid updates of a relatively small number of scanning nodes.
- E-Mail Gateway Content Filtering
  - Phishing attacks usually involve a malicious web site that is often active prior to transmission of the first phishing email.
  - Very effective at blocking access to known phishing sites, without waiting for an ISP to take the phishing site down.
- E-Mail Gateway Anti-Spam Filtering
  - Network users cannot always detect fraudulent E-mail that appears to be from a legitimate institution.

- Fraudulent E-mail can be blocked before the user has a chance to respond to it, stopping the attack at an early stage.
- End users do not need to install software on the desktop.

Detection and Mitigation[8]

- Log unsuccessful email attempts, both incoming and outgoing. Spear phishers often have to guess the mail format (i.e. firstname.lastname@xyz.com, lastname@xyz.com, FLastname@xyz.com, etc) therefore it is likely the mail server will reject mis-formatted emails. This is probably the first sign your organization may be targeted. By reviewing logs shortly after trigger events, it is possible to learn whether attempts are being made and thus new rule sets can be created to block the sender and alert the individual they are being targeted. Also, if it is determined an attack against an individual or group is possibly occurring, notify the individual or group to be more aware of the threat.
- Log network traffic (both incoming and outgoing), especially surrounding a possible trigger event. If a successful attack occurs, network administrators will potentially see an increase in outbound traffic soon afterwards, thus indicating compromise of the network. Diligent monitoring of inbound and outbound traffic will also provide insight into new or unexplained network traffic and allow network administrators to create rule sets to block or minimize exfiltrated data.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information).
- Take advantage of any anti-phishing features offered by your email client and web browser.

Remediating Possible Attacks

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators who can look for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft (see Preventing and Responding to Identity Theft for more information).
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

[1] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
[2] https://blog.duosecurity.com/2013/06/spear-phishing-how-attackers-use-email-to-steal-privileged-information-install-malware-make-your-life-miserable/
[3] http://www.us-cert.gov/ncas/tips/ST04-014
[4] http://www.htmlgoodies.com/beyond/security/article.php/3473221/Identifying-Spoofed-Websites.htm
[5] http://blog.returnpath.com/blog/lauren-soares/10-tips-on-how-to-identify-a-phishing-or-spoofing-email
[6] http://www.ebay.co.uk/gds/How-to-identify-Spoof-Phishing-emails-/10000000000108460/g.html
[7] Spear Phishing Prevention Strategies Created by Threat Analysis & Info Sharing Branch NCCIC/US-CERT August 23, 2013
[8] NCCIC Advisory Targeted Phishing Attacks