What is spear phishing?

Spear phishing can be defined as a phishing method that targets specific individuals or groups within an organization. While phishing tactics may rely on shotgun methods that deliver mass emails to random individuals, spear phishing focuses on specific targets and involve prior research.

How to setup a spear phishing campaign?

Step 1: Research

If you target individuals, you need to start some information gathering. A good source are social media profiles or articles or job descriptions.

Examples:

If a target posts something about his private activity like visiting a music concert, you could send a phishing email where you invite the person for a free backstage pass for the next concert. If you know the person works in support, you could adress the target with a specific salary statistics download for support people in similar positions. The goal is to find something, that could motivate the user to click.If you happen to see on Facebook or Linkedin friends of the target, you can also refer to those people in your first contact attempt. The scenario creation is the most important step.

Finding a scenario should relate to the actual risks

The attack configuration depends primarily on who you want to test (department/role), how much "inside information "* the hacker may have, and what risk you want to address. For example, consider that HR staff face different risks than IT staff or finance staff. HR is constantly receiving resumes that could contain dangerous code. The IT department has more technical freedom to download or even install software. And finance people may be vulnerable to attack if they are presented with financial data in Excel format.

In the context of risk, you naturally want to test scenarios that could also be a problem for your own organization. In this respect, attack simulations where you recreate a Netflix, Paypal or Amazon phishing attack are irrelevant: One's own organization may not care if an attacker gets hold of an employee's Netflix login data. It may be annoying for the employee, but it doesn't reflect a threat scenario for internal company data. In addition, the employee may also experience phishing aimed at private services as an invasion of privacy and will question the value of such an attack.

Regarding the risks, the technical aspect is also very important: one should take only those scenarios which can pose a threat from a technical point of view. If every user surfs with a company computer, which has an updated browser, then clicking on a link will not endanger the organization's data. Thus, hyperlink attacks would not be a real threat scenario. And if every employee can get to the company's webmail access only via 2FA authentication, just phishing Windows logins doesn't make sense. The hacker would not be able to do anything with the login data. Only if you recreate a fake 2FA page and successfully phish the user, you have created a realistic threat scenario.

There are different types of phishing scams. Some are fairly generic attacks, where hackers send generic bulk emails (which aren't necessarily bad) to various organizations and hope someone falls for

their scam. In more specific attacks, the scammer first researches their targets on social media and other public outlets, then creates tailored attack scenarios for those specific individuals or departments based on the information gathered. Example: If the company publicly announces that a new CEO is coming on board, the hacker could create a fake message from that potential CEO welcoming all colleagues and asking them to familiarize themselves with the upcoming organizational changes summarized in an attached document with a macro. So before you plan a scenario, ask yourself what type of attack you want your simulation to cover: the specific, investigation-based, or generic?

If you decide to use a more complex scenario, you should always strive to create credible content. If your campaign includes a fake email from your finance department, make sure you use appropriate language, terminology, names, etc. So, don't post fake bank account verification requests when sending an email from your IT staff, for example. Also, don't forget to keep the fake party in the loop before you launch the campaign.

Please download a few ideas for spear phising tests

here

.

Step 2: Phishing Attack

Build trust first

The actual attack could be launched in multiple steps. LUCY offers something called double barrel attack, where you first initiate the communication and build a trust relationship before the actual attack happens. Example: If you plan to send an email to HR about a new HR portal that gets introduced, you might first want to send an announcement ahead without any link like "Hi, This is to inform you that on date XXX we will launch the new HR portal and we selected you as test user. Stay tuned!". The double barrel attack can be fully automated. If you want to communicate with the target interactively, you could also use the mail manager.

Make it customized

Make sure you use petsonalized greetings, a mail footer that is realistic and if you have multiple targets, use the variables that LUCY offers. Using the example above you could setup an email that looks like this:

"Hi %name%, This is to inform you that on %time("Y/m/d H:i:s", "6880")% we will launch the new HR portal using the link https://company.com/hr and we selected your department %division% as a test case. Stay tuned!".

Spoof the Domain with typossquatting If the client uses example.com as a domain, you could reserve a domain like example.services or examples.com or portal-example.com as a typosquatted domain. If you are curious what possible domains are available, check out External Link. You can the register the domain through LUCY in the domain API.

Make it difficult A difficult template relates to your own organization and/or spoofs a known sender and domain. The message content could reflect any internal email sender, such as your support team, HR, or another department. Depending on the scenario, you can clone the relevant website, change the domain, and test whether users would fall for the copy. For example, if you're using a Citrix or Cisco VPN portal, you could invent a scenario where you ask users to enable access to a new portal

using their Windows credentials.

Make it perfect! If you ask to login on a page, make sure the page has the look and feel from the target company. One possibility is to clone an existing client page and then add a login to that page using the LUCY editor. Make sure you also create a trusted SSL certificate with LetsEncrypt. To give the email also a professional touch, you could buy a Smime certificate (e.g. https://comodosslstore.com/email-identity/email-certificate?) and add it to the campaign.

Test! Before sending the email, do a test run! Newly reserved domains often end up in SPAM as they have no reputation profile yet.