Phishing

A simplified walkthrough on how phishing campaigns are often orchestrated, and possible defences.

Netscylla Cyber Security Ltd
GB 10571639

Address:
Telecom House,
125-135 Preston Road, Brighton,
East Sussex,
United Kingdom, BN1 6AF

Introduction

Phishing is usually described as a social engineering type of attack where attackers attempt to trick normal (or even expert) users into performing an action they would not normally commit. However, phishing can sometimes be a little more complex. Instead of the social engineering style attacks of eliciting information from a target. It is now usually combined with technology, obfuscation and malware; what may appear to be a normal action from the user's perspective; such as opening an invoice, receipt, postal-order, invitation, or brochure – but is actually the first stage of attack on the network.

Phishing emails can hit any organisation, the end-goal is not necessarily theft of information or theft of monies. Attackers can install malware, pivot through though your systems to commit further crimes and fraud, or even utilise your resources to generate crypto-currencies at your expense.

Attackers could just randomly target you for an easy win, or it could be a structured attack where they are attempting to compromise the supply chain, and your organisation is on one of many paths that may lead to the compromise of their target.

Phishing can be sub-categorised into three terms:

- Mass phishing – attacks that are perceived as randomly spraying or brute forcing your user base.
- Spear phishing – attacks that are targeted against specific people in your organisation, these could be obtained through OSINT, or easy pickings from other online leaks.
- Whaling – attacks targeted towards board members, and chief officers of the company.

Why Phishing works

"Give a man a phish he eats for a day, teach a man to phish and he eats for live!"

(Modified version of an old English proverb, used throughout the phishing community).

Phishing is often successful because its exploits the human condition. People are often under pressure to deliver quick results, or people wish to be considered good-natured, being a team player or being helpful. Phishing attacks can play off both: they attempt to manipulate a targets instinct to make them feel good about themselves – instilling a positive attitude, so that the target is unaware of the disguised nature of the attack; or equally they can play off a targets fears – the impact of stressful situations, possible repercussions, and ultimately trouble.

About this paper

Netscylla is a practitioner of red-teaming and phishing, phishing is by far the one of the easiest and preferred methods to penetrate a company. We will cover some of the approaches, that consider at a high-level some of the defences against suspicious emails and these types of attacks.

Step one: Through the attackers looking glass

The Attack

When an attacker has decided to target your company, they first go after your domain records by using a DNS service. DNS records hold the information and addresses about your organisations digital footprint, from these records an attacker can deduce possible protections, and location of your servers, and what number of different services you offer. Think of it as your company's public phonebook for the internet. It contains web-site addresses, mail server addresses, phone server addresses and may contain email addresses of your system administrators.

Websites are often analysis (or 'scraped') for their digital content which may contain usernames and email addresses that can easily be harvested by a technically competent attacker, and used in further phishing and social engineering attacks.

Reconnaissance is always the first step of the attack. If an attacker can detect a number of protections they may immediately give up, in favour of finding easier targets. In this context, we could say that deterrence has won over the attacker. However, a persistent attacker will always persevere.

Defence Considerations

Consider the amount of information you have published about your company on the World Wide Web?

- Your websites:
    - Be mindful of your website content? Can you minimise it? Are all those contact details necessary? Should you publish information about your partners, suppliers, clients?
- Third Parties:
    - What are your corporate policies involving employees disclosing where they currently work on social media sites?
    - What are your policies on using corporate emails on forums or group sites?
- Your DNS records:
    - Are you disclosing too much information?
    - Do your records contain security mechanisms/standards that you adhere to?

Step two: Attacking mail servers

The Attacks

Mail relaying

If your mail server has been misconfigured, it may allow mail relaying. This is like gold for attackers as in addition to targeting your organisation, they can now masquerade as your organisation and hide behind a mask of anonymity and attempt to attack other organisations.

Also, because open mail relays offer no means of authentication they are additionally vulnerable to spoofing.

Spoofing

When E-mail was created in 1972[1] there was no real security built into the protocol or exchange of email between servers and organisations. An attacker can create their own mail server, and simply pretend to be one of your servers, we call this type of attack spoofing.

But E-mail spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. E-mail spammers and phishers often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

The Defence

Mail relaying

Check with your mail administrators that mail relaying has been disabled.

Spoofing

To prevent spoofing of your corporate domain, consider implementing at least one but preferably all of the following anti-spoofing controls:

- SPF – Sender policy framework, effectively whitelists the servers permitted to send mail from your domain.
- Sender ID – (Or SPF 2.0) Microsoft's own implementation of SPF.
- DKIM – Implements signed SMTP headers through the use of digital signatures, to prevent mail spoofing and masquerading.
- DMARC – a policy that uses SPF and DKIM, and how violations of the policy should be reported. Useful for detecting alerts when an attacker attempts to spoof your domain.

More information on protecting emails and these technologies can be found here.

[1] http://www.nethistory.info/History%20of%20the%20Internet/email.html

Step three: Targeting Users

The Attacks

Phishing emails can be crafted in a variety of ways: from beautifully crafted HTML designs, to simple plain text. There are also two common attack strategies: phishing URLs to websites that will attempt to trick targets into disclosing credentials; and payloads – malicious attachments that they want to trick targets to execute.

Email Format

HTML mails carry slightly more danger, as content can be easily manipulated and obfuscated to disguise malicious links and rename and disguise executable files to appear as benign media files.

Plain text emails can be unappealing and ugly to users, due to the lack of style, fonts and images. However, this format forces the attackers to properly construct their emails, as obfuscated links can easily be detected by automated technology. Some attackers prefer to send mail as plain-text often to evade anti-spam and some security gateways. Instead of using obfuscated URLs, they attempt to use typo-squatted domains and email attachments to lure the targets.

Attachments

Usually phishing e-mails contain attachments, depending on your e-mail security gateways and filtering technology, you could receive: executable files, documents with malicious macros, malformed documents that trigger a known exploit and PDFs that contain malicious code. These files are often referred to as ‘droppers’ or ‘stagers’ and contain the first piece of malicious script/code. These malicious files will then attempt to download further code in an attempt to compromise the user, before leveraging the users access and privileges to attack the domain or surrounding infrastructure.

The defence

Automated tooling

Endpoint protection can help minimise some threats, but the usual downside to this approach is that they are signature based; an advanced and determined attacker can manipulate their exploits and malware to evade detection.

Examples of endpoint protection:

- Anti-Virus
- Anti-Malware
- IDS/IPS
- Security Gateways
    - Prevent the downloading and executing of attachments
    - Filter malicious URLs and HTTP links
    - Automatically filter known phishing sources
- Anti-Malware DNS servers
    - Consider the use of DNS services that actively block known botnet and phishing domains.

User awareness and training

User training and awareness; helping users to get into the habit of utilising some quick and simple checks, can help defend against a lot of simple attacks. Attackers often have bad spelling, grammar, inappropriate greetings or signatures. On occasion attackers often make a few more mistakes like including the wrong fonts, images or corporate logos.

Users should always spend 5 seconds to query and briefly scan an email for obvious phishing attempts:

- Is the email from an expected contact?
    - Does the senders email address look unusual?
    - What happens when you hover the mouse pointer over the sender's email address, is it the same or is it different?
- Is the email body well-structured and formatted?
    - Are there any grammatical or spelling mistakes?
    - Are any company logos present, are they correct?
- Does the email reference you directly? Is your name correct?
- Is the email trying to get you to open a URL?
    - What happens when you hover the mouse pointer over the URL, is it the same or different?
- Does the email ask you to open an attachment or copy and paste a command?

Reporting Phishes

Reporting phishes can also be a great help in early detection and eradication. Empower your users with a simple capability to report suspected phishing attempts. This could be a simple button in the mail client toolbar or an easy to follow process? Early detection, aids a faster response which can mean the difference between a successful and failed attack.

Fast and effective eradication means that compromised user accounts can be suspended for a minimal amount of time and the business can resume normal operations with minimal impact. Intelligence about malicious internet addresses can be added to filtering software to block and prevent additional incoming spurious email, or other cyber-attacks.

Conclusion

Phishing is an attack strategy that will always be used by attackers.

There is no magic shield, or product that can stop all phishing attempts. That one phishing mail that slips through your net of security could be the start of a much larger incident or possible breach. Therefore, earlier detection, analysis and eradication of phishing campaigns is one of the key areas of successfully defending against cyber-attacks.

Hopefully, we have outlined some of the attacks and defences to increase your understanding on phishing, and this paper can help you build out a multi-layered defence that can help reduce the risk of a phish successfully penetrating your organisation.