beazley

Article

The Threat of Phishing: What Organizations Need to Know

Jad Nehmé • June 26, 2023

Phishing attacks have long been a cybersecurity challenge for organizations; today, they are responsible for more than 80% of reported security incidents. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing, which is the practice of sending emails that appear to be from a trusted sender in order to induce targets to reveal confidential information, is the most common type of phishing attack, comprising 65% of all phishing attacks.

Perhaps one of the reasons for the proliferation of these attacks is that phishing campaigns are relatively easy and cheap to conduct due to automation (for example using "Caffeine" phishing-as-a-service platform). Today, spear phishing can require manual efforts, but it is becoming easier with the abundance of personal data that is available publicly today. Tomorrow, we can expect to see automated and personalized spear phishing campaigns driven by Artificial Intelligence (AI).

The impact of a successful phishing attack can vary, from retrieving private information to deploying malware and gaining remote access. As none of these outcomes are welcome intrusions, organizations are well advised to learn how to protect themselves from a phishing attack. There are a number of techniques that should be considered.

REDUCE THE NUMBER OF PHISHING EMAILS YOU'RE EXPOSED TO

Organizations should secure the configuration of their email solution (SPF, DKIM, DMARC and SID) to block emails received from unknown or suspicious sources as a matter of policy. In addition, implementing a mail threat protection solution with features that include spam filtering, scanning links, sandboxing attachments and blocking common malicious attachment types (HTA, docm, xlsm, exe, PS1, VBS, js, etc.) is advisable.

LEARN TO BETTER RECOGNISE PHISHING EMAILS

Teach and train your employees to detect spoofed domains in websites and email addresses through security awareness and anti-phishing training (services offered by KnowBe4 and CybeReady). Domain spoofing is a form of phishing where a threat actor creates a fake website or email domain to impersonate a trusted business or individual. Typically, the domain appears to be legitimate at first glance, and the differences may be very subtle and hard to spot (a W that is actually two Vs, a lowercase R and N mimicking an M, or a lowercase L that is actually a capital I).

EXAMPLE OF DOMAIN SPOOFING

An example of a spoofed domain name is **O365.rnicrosoft.fr.** Notice the "**rn**" instead of " **m**". Another domain name with the potential to fool employees is **https://beazley.changepassword.com**. This is a subdomain that belongs to **changepassword.com** and not to **Beazley.com**. In contrast, **https://subscribe.beazley.com** is a subdomain name that belongs to Beazley.com. This can be counterintuitive, as we are used to reading sentences from left to right, but websites and domain names need to be read from right to left.

Targets may be tricked into revealing sensitive information, sending their password (and potentially MFA token), sending money, or clicking on malicious links without realizing that they are interacting with an unknown entity and/or downloading a malicious file. In addition to educating employees about this threat, adding the header "[External]" for emails received from external email addresses can help remind employees to be more vigilant about potentially spoofed email addresses.

LIMIT THE IMPACT OF A PHISHING ATTACK

Phishing emails are mostly used for two key purposes: to redirect users to spoofed websites and steal their passwords, or as a means to deploy and execute malicious code or software on users' workstations. In this case, the malware is either attached to the email itself, or downloaded from a link that is opened by the user or by a macro embedded in an attached Word, Excel or PowerPoint document.

There are several steps an organisation can take to limit the impact of a user clicking on a malicious link, or double-clicking on a malicious file. A sensible first step is to have up-to-date antivirus software and to restrict the execution of downloaded files recognized as malware. You can also block macros that attempt to execute commands on the system or open external links. Finally, having an Endpoint Dectection & Response (EDR) agent deployed with automatic remediation enabled on workstations can help detect and block new (previously unknown) malicious content from executing.

Implement security hardening and restrictions on users' endpoints such as AppLock to ensure there is no execution of scripts or unsigned software, and no USB devices can be utilized (ex. aligning to the CIS benchmark recommendations). Prevent access to the Local Security Authority Server Service (**LSASS**) process that stores users' passwords locally on endpoints by applying credential guard, reducing the number of locally cached credentials to 1, and running Lsass as PPL.

Limiting users' access rights is also key. This includes making sure that

users with access to emails do not have privilege (or administrator) access, making sure that regular users are not allowed to enrol new devices into the Active Directory, and ensuring that domain administrator accounts do not connect to workstations.

Finally, build procedures and train your IT security team to better respond to successful phishing attacks.

Isolating yourself completely from the internet, though the most fail-safe solution, is rarely an option. But with a bit of foresight, an organisation can arm themselves against phishing attacks by proactively taking responsibility for the security of their operations and their user's data. As techniques and prevention protocols change frequently, ongoing training and frequent re-evaluation of security procedures can often be an organisation's best defences.

Jad Nehmé

Client Experience Manager

beazley