Phishing, a ‘Tail’ as Old as Time in Cyber Security

ARTICLE 06.03.22 DEAN DORTON

Phishing attacks have been occurring for years. You know the story, a threat actor attempts to trick an unsuspecting user into clicking a link or malicious attachment that leads to installing malware or directs them to a malicious domain that could attempt to harvest email credentials, or further penetrate your device. The tactic is still common because unfortunately, it still works. But with the increase of organizations relying on stronger email filtering solutions and better end user awareness training programs, they are not as susceptible to some of these basic attacks. Enter the evolution of more sophisticated and clever tactics.

“But this domain is safe!”

Threat actors are utilizing clever strategies to attempt to bypass even the best email filters. One such strategy is using common, legitimate domains to host a link to their malicious site or attachment. These domains could be Google Drive, ShareFile, OneDrive, Box, Dropbox, Adobe InDesign, etc. On the surface, these services are legitimate and offer users ways to quickly share files amongst one another. This is why most reputation-based scanning used within email filters will not often categorize the initial link as malicious because it is not. The following screenshots provide an excellent example of this in action.

Initial Email Example:

https://deandorton.com/wp-content/uploads/2022/05/1.png

In this example, a threat actor gained unauthorized access to a trusted sender for the recipient. They then sent this email that included a link to open a document. Due to this being a trusted sender, the recipient opened the file because they had no reason to assume that the link was malicious. The link then led to the following:

Ind.adobe.com site hosting the malicous file:

https://deandorton.com/wp-content/uploads/2022/05/2.png

In our example, once the user proceeded to this point, they realized something was off and reported the email to the IT team; however, if they had proceeded on to the next step, they would have received the following:

Malicious Site:

https://deandorton.com/wp-content/uploads/2022/05/3.png

There it is! The true purpose of the email was to try and harvest email credentials. An unsuspecting user could have being successfully phished here and it was all because that initial email was being hosted by a legitimate service. This is not the only variety of these types of emails and certainly will not be the last, so that leaves us with more questions.

So what can we do?

There are few different strategies that can help prevent against phishing attacks:

1. **Never assume that an email is safe just because it came from a trusted sender that you communicate with regularly.** Threat actors are engaging in reply-chain attacks, where they gain unauthorized access to an account and then start replying to emails posing as the hacked user. When in doubt, contact the sender out-of-band (phone call, preferably) to verify the email.
2. **Make end user awareness training a priority.** An end user is any organization's first line of defense! A well-trained staff can bring attacks to a halt. Ensure that your users are provided with regular security training and that they are informed of the latest threats. Ensure that they are trained to review the address bar for any site that is asking them for email credentials. If it's not a Microsoft (or whatever email system you may be using) domain, then that is a red flag. It is also helpful to periodically test the effectiveness of the training by sending out phishing simulations.
3. **Utilize multi-factor authentication (MFA).** In any particular scenario, even if a threat actor was able to harvest email credentials, they would not have be able to perform any actions on objectives if multi-factor was enabled for the account. It is a cybersecurity best practice to ensure that MFA is enabled on all externally-facing systems, email being one of the highest priorities.
4. **Block uncategorized websites in your web filtering solution and/or firewall.** Threat actors spin up thousands of domains per day and these are often categorized as, "uncategorized," where filtering solutions are not sure if they are malicious or not. Blocking these outright could help stop attacks in which the malicious site is uncategorized.

If any of the tips above have given you pause and you would like to know where your security posture stands, please contact Dean Dorton's team of cybersecurity professionals for assistance.

Jordan Johnson
Cyber Security Consultant
jjohnson@ddaftech.com • 859.425.7659