CARPE DIEM: HOW TO SEIZE THE PHISH

If every person looked closely at every email they received, phishing as a serious cybersecurity threat would be greatly reduced, if not eradicated altogether. But with today's fast-paced, multi-tasked workplace culture, it is easy for phishing emails to slip through the cracks and gain entry from even the most careful employees. This is why despite more than a decade of experience in dealing with and researching phishing, it continues to be a costly problem for corporations.

The Anti-Phishing Working Group reports a **65 percent increase in the total number of attacks in the last year, and the FBI has repeatedly confirmed that phishing is leading to multi-billion dollar losses for U.S. businesses.** With email filtering alone – which is necessary but not sufficient to defend against sophisticated threat actors – as the primary defense, many organizations are lacking the multi-faceted strategy they need to catch and stop the most advanced and dangerous campaigns.

Two recent attacks launched against DomainTools executives demonstrate both the aggressive nature of today's phishes, and the importance of the human factor in catching them. One executive received an untargeted phishing email that was clearly fake – the type of effort that most moderately aware users can easily catch. He recognized it immediately, deleted the email and moved on. No harm done. Just a few weeks later, the CFO received an email that was made to look as if it was from the CEO, and while she could identify it as a phish, it was much more carefully crafted and sent using a spoofed domain that closely resembled the company's. Fortunately, her training and attention to detail made it easy to spot the email, delete it without incident, and pass it on to the security team for further research on the attacker.

These examples show us that phishers are consistently using approaches that email filters can't detect, and that employees are the last line of defense to prevent a phish from penetrating the organization.

Houston-based Ameriforge Group Inc., suffered such a fate last year when its accountant was targeted by a phishing scam that led him to wire $480,000 into a bank account in China. More recently, we've seen highly sophisticated campaigns targeting Gmail users around the world, one of which successfully infiltrated roughly one million accounts. Electronic signature provider DocuSign confirmed that an unspecified number of customer email addresses were breached and being used for phishing attacks. The phishing emails were designed to look like they were sent by DocuSign and included attachments that would install malware if opened.

This paper will outline the various "species" of phish that are used today, their most dangerous tactics, and how organizations can build stronger, proactive defenses against them.

"These incidents are damaging in many ways. Beyond the financial losses associated with these campaigns, companies may lose customer trust and brand equity, and can face legal penalties for failing to protect sensitive customer information." – Tim Helming, Director of Product Management, DomainTools

DIFFERENT SPECIES OF PHISH

The ability to effectively seize the phish every time, and help employees become more successful at identifying and thwarting phishers starts with a clear view into the types of campaigns that are used. These can be categorized as untargeted or targeted.

UNTARGETED: AMATEUR

This type of campaign sits on a blurred line between spam and phishing. Most of the emails are caught by email filters, and those that make it through rarely fool the average user. An example is the common 419 scam, which asks recipients for a small sum of money in exchange for a larger repayment at a later date. These can be simply discarded when found, and don't merit further attention from the security team.

UNTARGETED: SOPHISTICATED

The distinction between this kind and the amateur untargeted approach is that it is designed to look more realistic and trick users into clicking on a malicious attachment or link. Often, phishers will leverage typical human behaviors – such as sending an email to ourselves – to improve the authenticity of their emails. Many of us send ourselves emails regularly, and are so busy in day-to-day work that we may or may not remember if we did indeed send a certain email. Phishers will take advantage of this to create an email that it looks just like any other. These are still mass, widespread campaigns, but can be harder to detect. Again, this type typically does not warrant much follow-up, and users can be trained to delete them and move on.

TARGETED: SPEAR PHISH

Spear phishing is targeted at a specific individual, usually to either harvest credentials, drop malware, or both. These types of attacks are often not caught by email filters and can be much more dangerous than mass campaigns. Spear phishing has been reported to cost U.S. businesses an average sum of $1.8 million annually, and these attacks often require involvement of the information security team to add safeguards against the phishers identified.

TARGETED: BUSINESS EMAIL COMPROMISE (BEC)

This type of phish is evolving quickly – the FBI's Internet Crime Complaint Center noted a 1,300 percent increase in exposed losses from these attacks since January 2015. It is also the most dangerous species as it involves spoofing the domains of a target's trusted colleagues and partners, through emails usually directed at high-ranking executives or officials with the aim to steal money or IP.

"Phishers will use social media and other online resources to research their targets to put context around these emails so they appear authentic. The Ameriforge Group incident was a result of a BEC campaign, and just one of the thousands the FBI has recorded across billions in stolen money." – Helming

PHISHING TACTICS

Phishers have many motivations. They are typically financially driven, but we've also seen targeted phishing campaigns with geopolitical or espionage intentions. A spear phishing or BEC attack could be used for any purpose aimed at stealing something of value from a specific victim. Common goals include:

CREDENTIAL HARVESTING: Campaigns trick targets into inputting their username and password into a phony login page

MALWARE INJECTION:
A phisher lures victims into clicking on a malicious attachment or link that prompts a malware download.

TAKING A SPECIFIC ACTION: Targeted, typically sophisticated emails requesting the transfer of funds or sensitive information to phishers posing as a trusted source.

While BEC campaigns have been around nearly since the birth of phishing, they have become a prominent threat in recent years. The growing number of BEC incidents and other targeted campaigns shows us that phishers are creative, motivated and will not be deterred even as mainstream cybersecurity awareness improves.

Phishers use a handful of tactics to make their bait appear real. Security professionals must take BEC attempts seriously, and unlike untargeted campaigns that can be generally ignored, view them as red flags that spur further action. When a phisher has put time and energy into crafting a believable email through any of the approaches below, the information security team must take the campaign seriously.

SPOOFED COMPANY DOMAIN

There are various ways that phishers construct URLs to spoof a domain so it appears to be coming from someone within the company. Below are a few examples of how a phisher may construct a URL to look like the real thing:

Typos of the domain name

`DOMAINTOO1S.COM`

Affixes with properly spelled name

`LOGIN-ACCOUNT-DOMAINTOOLS.COM`

Properly spelled subdomains of a garbage domain:

`DOMAINTOOLS.ACCOUNT-LOGIN-293774.COM`

EXPLOITING THE BUSINESS ECOSYSTEM

Many companies have a handful trusted partners, such as suppliers or contractors, with whom they communicate every day. Sophisticated phishers may exploit these relationships by spoofing partner domains. If an employee is accustomed to sharing sensitive information – such as schematics for a new product or important financial information – with a certain partner via email, they may easily be tricked into sending that information to a phisher posing as that partner.

RESEARCH

The extent of research a phisher conducts before launching a targeted campaign is an important indicator of how dangerous the threat really is. If a phisher is sending a spoofed email from the CEO to the CFO, they may first look at the targets' social media profiles to determine recent information about those parties' whereabouts and activities. They may reference other associates by name, recent vacations taken or other personal details. This level of context and personalization around the email makes it difficult for the victim to recognize it as fake.

"It is essential for organizations to take action on these types of attempts. A phisher that is motivated to put extensive resources into a campaign is likely to continue casting the line until a successful catch is made." – Helming

APPROACH AND DEFENSE

It may seem impossible to remain one step ahead of the steady stream of phish swimming into the organization. Sophisticated companies that are successfully dealing with these challenges take a holistic approach that includes a strategic combination of people, training, email filters and other technology to bolster defenses. To be truly effective, efforts must include extensive employee training that builds security into the company culture, proactive monitoring and use of caught phishes as forensic artifacts.

TRAINING:

Cybersecurity – and phishing in particular – is largely a human problem. Therefore, the most effective solution starts with people, and building security in as part of the company culture. Awareness is improving, but generally, most employees require ongoing training, incentives and reminders that they are an essential part of maintaining security. Gamification of training processes that make learning about threats fun, along with positive reinforcement for successfully identifying incoming threats, is for many organizations the best way to ensure long-term participation from employees. Organizations should offer rewards for employees that catch real or training-based phishing emails without clicking on them.

PROACTIVE MONITORING:

Domain spoofing is at the root of BEC campaigns, and organizations will see a much higher rate of success in thwarting these attacks if they do proactive domain monitoring. In the massive Anthem data breach in 2015, hackers used the domain we11point.com – a spoof on Anthem's former company name, Wellpoint – to launch targeted attacks that tricked employees into entering their internal corporate credentials, which gave the attackers a foothold inside the protected network. Proactive domain monitoring could have enabled Anthem to identify and block this domain proactively, before the breach succeeded. This type tracking is an emerging anti-phishing tactic that adds to an organization's overall defense.

DomainTools PhishEye software was created for this purpose, providing ongoing monitoring that locates existing and new domains that spoof legitimate brand and product names so that organizations can block them before they are used for targeted phishing, and take investigative actions against the phishers behind them. This makes it possible to seize the phishes that spoof their brands and those of trusted partners. PhishEye alerts you of new domain registrations and provides useful insights about them such as a registrant details and a risk score. It uses algorithmic generation of typos, prefixes, suffixes and exact string inclusions to find the widest variety of relevant domains.

USING PHISHES AS FORENSIC ARTIFACTS:

Once a sophisticated phish is caught, the next important step is to act upon intelligence within it to learn more about the threat actor. DomainTools recently did some investigating on the emails associated with a widespread phishing campaign aimed at leading consumers to phony, malicious lending site pages. Leveraging the sender URL as a forensic artifact led to the discovery of 87 connected domains that were all blacklisted as dangerous. With DomainTools investigative tools, the domains, their registrant and additional malicious infrastructure associated with them were all uncovered in just 10 minutes. In the hands of an organization's security team, this information would be critical in arming against incoming phishes and looking for additional suspects.

Researching the domain an attacker used and learning more about the infrastructure behind the campaign makes it much easier to block all related domains in email filters and set up a targeted monitor for future action from that phisher. Such action can be doubly important in the case of targeted campaigns, where the attacker uses domains and IP addresses specifically to attack a specific victim. In such cases, the infrastructure is not likely to appear on blacklists, since no other organization will detect and report the campaign to blacklist providers.

CONCLUSION: CONTINUOUS ANTI-PHISHING

Employees are often viewed by information security teams as a liability, especially as so many cyberattacks result from employee negligence or misconduct. As demonstrated in the examples at the beginning of that article, it is possible to flip that belief on its head and leverage employees to strengthen security. With a deep-rooted culture of security, employees can become an organization's strongest line of defense and the eyes and ears constantly on the lookout for new threats.

Consumers are becoming wiser about personal cybersecurity threats and this heightened awareness is beginning to translate to the workplace. Still, attackers are strengthening their tactics and inventing new ways to trick people all the time. With well-trained employees that understand their important role and the impact sound security has on the health of the organization, it is possible to keep pace. The addition of technology that monitors domains and ongoing phishing activity is the final piece that rounds out a sustainable and continuous security strategy that can stay ahead of the threats.

"Seized phishes are important artifacts that allow security teams to spin up forensic processes that bolster overall cybersecurity intelligence and help align defenses against specific attacks. The combination of proactive monitoring and quick response to attacks is critical, especially when phishes slip past trained employees." – Helming