DOMAINTOOLS®

PROTECTED WATERS: NO SPEARPHISHING ALLOWED

HOW TO DETECT AND BLOCK TARGETED SPEAR PHISHERS IN THE PREPARATION PHASE

Cybersecurity threats from targeted email attacks—or spearphishing—are showing no signs of slowing down. The financial damage of this type of phishing can be dire. Recent figures show that 96 percent of successful data breaches begin with email, costing an average of $7.9 million per incident.

One of the major challenges with phishing is that it's a social engineering method, not a technology-based one. Phishers are adept at tricking a victim to take an action that will compromise that individual's information, the organization's network, or both. With spearphishing, the stakes are even higher. The adversary has taken additional steps to research the target organization, its employees, social media accounts and other information, leading to the creation of a believable and highly personalized campaign.

BUSINESS EMAIL COMPROMISE: A TRICKY PHISH

Business Email Compromise (BEC) is a specialized type of spearphishing that can be especially difficult to detect with content filters. The elements of a BEC campaign are based on:

- In-depth research about a specific target
- Knowledge of the inner workings and dynamics of a specific group of employees or business associates
- Social media monitoring to tailor emails to align with real life events such as vacation or a promotion
- Use of a target's actual name and business email or well-crafted spoof

Blocking against all phishing attempts is costly, time intensive and arguably impossible. Security organizations must determine the ROI of how much they are focusing on generalized phishing. Spearphishing is far more dangerous than generalized attacks, which are often caught by email filters or discarded and/or flagged by users. Therefore, you must target the attackers that are specifically targeting you, and exploit the weaknesses in their approaches.

PHISH IN YOUR SEA

Proactively protecting your waters to keep the spearphishers out, and determining which phish to block begins with understanding the phishing lifecycle, and how spearphishing is different.

Spearphishing attempts are targeted, specific and well-crafted. The number one difference between spear phishers and other schools of phish is the upstream effort the threat actor must take when creating a campaign. This involves extensive research about your brand, to understand names and titles of employees, the hierarchy of your organization, key company partners and other unique details that will help the phisher customize an attack.

DO YOUR OWN RESEARCH

Security teams should audit all of the information that exists in the public domain about their company and employees, to gain a complete picture of what the adversary is able to learn.

While it's unlikely that security teams will be able to detect a spearphisher at the research stage, they can build a defense based on the steps that follow. These are typically the same as other phishing attempts, but with customized, targeted content designed to fool your users. Below is a step-by-step snapshot of how a spear phisher will research a target and stand up infrastructure to support the campaign.

1. **In-depth research.** Using passive DNS, domain search, name server records and other pieces of public information, sophisticated spearphishers will find out the technologies used within the company, portals, partners, employee lists, department lists, personal information on social media, etc.
2. **Spoof websites.** Using the information gleaned in the research phase, the spear phisher will determine specific brands and domains to spoof. It will register domains, and build websites that imitate the real thing.
3. **Operationalize**. Spearphishers will operationalize spoofed websites in a variety of ways, depending on their end goals. This may include drive-by malware or remote access trojans that download to the computers of any users that visit the site. Others will be designed to harvest credentials, prompting victims to enter sensitive personal, financial or other account information.
4. **Carefully craft and target emails.** Spearphishing emails can be very convincing, and will be crafted to look like they are coming from a trusted colleague or partner. If it is a BEC attempt, the email may come from a legitimate email address, rather than a spoofed one. Some are so well-designed that even vigilant users can be tricked into clicking through to a malicious site.

PROTECTED WATERS

BALANCE RESOURCES AND RISKS:

Make sure your infrastructure is set up to make the most of threat intelligence and email filters that help catch phishing attacks, so the team isn't wasting time trying to chase every potential phish. Remember, though, that filters and built-in anti-phishing capabilities are not designed to catch targeted attacks unique to your organization. Focus internal resources on combating the spearphishers, while your tools do the heavy lifting on low-level, generalized attempts.

PATROL THE WATERS

Rather than waiting for these targeted emails to hit the network, security teams can get ahead of the spear phishers and proactively block emerging campaigns. The most effective way to do this is to investigate suspicious domains, and learn as much as possible about the spear phisher's infrastructure and techniques.

Using DomainTools PhishEye and Iris Investigation Platform, security teams can go upstream in the phishing lifecycle and take action while campaigns are still in the preparation phase.

HERE'S HOW

Containing more than 97 percent of the known internet, and hundreds of millions of domains, PhishEye provides security teams with a deep database designed to detect domains that spoof a keyword. Teams can search for and monitor terms that correspond to their brand and industry. The tool will provide a summary report of registered domain names that associate to those keywords. It also provides lists of domains spoofing well-known brands with their associated Risk Scores. When new domains matching the monitored terms are registered, PhishEye will send a notification so the security team can examine them.

WATCH NEW DOMAINS CLOSELY

Be sure to keep an eye on all of the domains your organization is resolving, paying special attention to the newest sites, or sites that are visited by only one or a small handful of users. This is a valuable starting point for uncovering potentially dangerous sites and phishing campaigns.

- PhishEye also provides a Proximity Score, which shows whether the domains are related to any sites that have been blacklisted or reported as malicious.
- These results can be ported into a variety of platforms, including Iris, which helps map the adversary infrastructure. Starting with known indicators, Iris will help uncover connected infrastructure of campaigns targeted at a specific company or brand.
- Building from a flagged phishing email, suspicious domain or other indicator, teams can enrich the data with background information from DNS, Whois and other records. Iris will offer guided pivots for investigators to look further into key pieces of information. This helps to answer questions such as: what themes occur between the related domains? Are there red flags such as high Risk Scores? What attributes exist on the sites that might indicate their nature?

WATCH NEW DOMAINS CLOSELY CONT.

- With this information, teams can compare the findings to logs and information captured in the SIEM system to see whether any pieces of the connected infrastructure had touched the network in previous attempts. This gives a sense of the dwell time and other attacker behaviors. All of this provides intelligence to build into the defense rules for blocking.
- Further monitoring of the related infrastructure deepens the intelligence. Investigators can observe what else the phisher is doing, find patterns and build a detailed profile of the adversary.
- Exporting reports from the investigation makes it easy to share important information with other investigators on your team, business units, leadership, partners and the broader industry.

PIVOT ON PHISHY INFORMATION

By following pivots, teams can find a wealth of information related to a single indicator, ultimately exposing everything about a malicious, targeted campaign. Practicing these techniques on generalized phishing attacks will improve the team's investigative efficiency and sophistication, so they are well-prepared when a spear phisher enters their waters.

PHISH AS PHORENSICS

A single phishing email contains key pieces of threat data that can be used to learn more about an adversary. Even one data point can help break open a campaign that wasn't otherwise visible. Use the phish you've caught as phorensics to:

- Maintain an aquarium of phish for observation
- Map the infrastructure behind caught phish
- Infer their intents and methods to uncover other related or similar threats
- Understand their methods for targeting

CONCLUSION

Spearphishing is here to stay. Bad actors have vast resources for researching and targeting specific organizations. Their tactics are becoming more and more sophisticated all the time. Even in the face of dedicated and skilled adversaries, security teams can protect their waters and keep the spear phishers out. Leveraging filtering and intel feeds, and investing in robust user education to protect the perimeter is essential. But as important as these steps are, they are not enough. Deep analysis and investigation into campaigns and phishy domains, and the connected infrastructure behind them, will provide an important boost in aligning your defenses against the threats that are unique to your organization.

> "Rather than waiting for these targeted emails to hit the network, security teams can get ahead of the spear phishers and proactively block emerging campaigns. The most effective way to do this is to investigate suspicious domains, and learn as much as possible about the spear phisher's infrastructure and techniques."

ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at http://www.domaintools.com or follow us on Twitter: @domaintools.