IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Cofense

To stop phishing attacks in their tracks, organizations should start by educating employees. The right approach to phishing defense turns the emails users report into valuable intelligence that helps prevent breaches.

The Value of Human Intelligence in Phishing Defense

June 2019

Written by: Frank Dickson, Program Vice President, Security Products

Introduction

Cybersecurity is an increasingly sophisticated discipline as companies struggle to avoid becoming "one of the breached." The adversary is cunning and motivated and may be an individual, a criminal cybergang, or even a nation-state.

A troubling reality is that most breaches trick the user into becoming an active enabler. Phishing, the soliciting of end users to click on a malicious link or attachment, is the attack method of choice. According to the Verizon *2018 Data Breach Investigations Report*, phishing and pretexting represent 93% of all social breaches. Email is the attack vector of choice in 96% of all phishing instances.

AT A GLANCE

KEY STATS

- » Phishing and pretexting represent **93%** of all social breaches.
- » Email is the attack vector of choice in **96%** of all phishing instances.

Equally sobering is that perimeter technology isn't a magic bullet. Email gateways and other technology defenses don't catch every phish — and it takes only one miss to inflict a financial loss. When the machines fail, what can you do? Begin by educating users to recognize and report.

Educating Users to Generate Intelligence

Phishing education or awareness programs aim to condition users to practice email safety. By learning what to look for in a malicious email, users become the last line of defense. As we'll see, they also become "human sensors," a source of rich threat intelligence.

A recent IDC Market Spotlight, *Phishing Training Evolution: Moving from Reactive to Proactive*, described effective antiphishing programs as not a single "thing" or method but an integrated set of techniques that addresses the different ways users learn. Computer-based training (CBT) provides foundational insights. How do you recognize a phish? What are the common clues? CBT also supplies context to the problem. Simulated phishing attacks are another key ingredient. They expose users to phishing tactics in a realistic setting — their busy corporate inboxes — and give feedback on performance so that people learn in real time.

In contrast to IDC recommendations, many organizations still offer phishing "testing," the equivalent to a vulnerability scan, several times per year. Vulnerability scanning is fine for machines. After all, vulnerabilities can often be patched. However, humans are not machines — we cannot be patched. Organizations must accept that the best security awareness program in the world will never deliver a zero phishing click rate. Some users will always click. Remember, the goal is to keep the threat of phishing front and center in users' minds and keep users up to date on the latest threat actor tactics, especially those used against the organization. By conditioning users effectively, you can operationalize their knowledge to better defend your organization against phishing threats.

Today, phishing education looks beyond surface-level detection to integrating users into the defense ecosystem. In a mature phishing defense program, user reporting of suspicious emails is the key metric, the true measure of effectiveness. Just because users didn't click on a simulation email doesn't mean they actively made that choice — they may not have seen or read the email. Reporting of the email is a conscious and deliberate action. It indicates how users will behave during a real attack.

Well-conditioned users, who are enabled to recognize phishing threats and empowered to report them, give security operations teams visibility into attacks they otherwise would not see. In essence, user reporting is a valuable source of threat intelligence because it is based on real attacks that have bypassed your controls and are active in your environment. Think about it. In addition to providing a last line of defense and reinforcing existing cybersecurity architecture measures, user feedback allows security professionals to "tune" existing detection measures on *real* data. Additionally, existing defensive measures become enforcement points for user-generated insights.

Equipping the SOC to Act Faster

To act on the phishing intelligence alert users provide, security operations teams must be able to cut through the noise and separate harmless spam from phishing emails. This requires automation to shift the SOC's workload from "analysis" to "action." There are three important layers:

Users with an "easy" button to flag suspicious emails reported phishing emails 11 times more frequently than those without the button.

- **Reporting automation for the end user.** Users need an easy way to report — an "easy" button, if you will, to make the process of reporting suspicious emails as frictionless as possible. For example, forwarding the suspicious email as an attachment to preserve the integrity of valuable forensic information is something that a security professional would do instinctively; users, however, will struggle to see the relevance. A "report phishing" button serves as a constant reminder that the organization values user-reported emails and eliminates the issues with manual processes. An example was recently cited in which users with an "easy" button to flag suspicious emails reported phishing emails 11 times more frequently than those without the button. Reporting volume correlates to greater visibility into threats. Please note that timely user feedback important feedback is essential in maintaining user commitment and refining the quality of the crowdsourced data. The platform must acknowledge the report and subsequently provide a verdict — valid, junk, or confirmed malicious.
- **Ingest automation for IT.** Ingesting all this data manually would be a nightmare. The platform must automatically structure reporting into a data set and autofilter the straightforward conclusions: known good, known junk, and known bad. It must provide insight into the real, or potential, risk of reported emails, based on their attributes, content, or even who reported the email. It must also enable analysts to easily answer the question "Where do I need to focus first?"

» **Analytics automation for security professionals.** Successful execution on the first two points is wasted if we create needless work for busy security professionals. Of course, the platform needs an easy-to-use GUI — powerful tools that are hard to use deliver little efficacy. Integrated malware analysis tools are a must, as are capabilities to identify and prioritize potential zero-day threats. Because security information and event management (SIEM) is the foundation of many SOC operations, integration with SIEM is essential. APIs are needed to enable network, web security, and messaging security tools used as enforcement tools and to share intelligence with other analytics platforms.

Considering Cofense

Cofense is the biggest player in the phishing defense arena. Founded in 2008 as PhishMe, its former brand name, the company was the first major advocate of phishing education and awareness, a full five years before the Target breach made phishing a household name. In 2018, PhishMe rebranded as Cofense to reflect expansion from a pure educational solution to an end-to-end platform, one that uses human intelligence to stop phishing attacks, from the inbox to the SOC. Today, Cofense employs over 400 employees around the world. Among its 2,000-plus customers are over half the Fortune 100.

The Cofense technology platform offers the following integrated suite of solutions that transforms phishing education into actionable intelligence.

Cofense PhishMe

Due to the constant evolution of phishing threat actor tactics, end-user education and awareness activities should not be a one-and-done exercise. Effective phishing defense requires a network of human sensors able to identify phishing threats that have bypassed perimeter controls to be delivered to recipient inboxes. Recognition of current phishing threats requires regular and ongoing exposure to the tactics and techniques being observed in the wild and used against the organization itself. Underpinned by the Cofense Threat Intelligence, Research, and Phishing Defense Center teams, Cofense PhishMe enables organizations to simulate the real threats they face.

Cofense PhishMe Playbooks leverage automation to dramatically reduce the time it takes to configure simulations. Administrators can schedule a year's worth of simulations in just a few minutes. This allows organizations to focus on pressing matters such as the needs of specific target groups or repeat clickers.

Responsive Delivery — a capability unique to Cofense PhishMe — eliminates whitelisting issues and increases program engagement. It delivers simulation emails direct to Exchange and Office 365 mailboxes *only* when users are actively using their email, regardless of email client. Supporting robust anonymization capabilities, Cofense PhishMe is well-suited to organizations and geographies with strict privacy requirements. Comprehensive analytics enable security awareness teams to accurately measure their program's effectiveness and communicate results to organizational stakeholders.
A focus on today's real threats provides relevance and reassurance for security operations teams: The threats they are likely to face are being addressed in phishing awareness.

Cofense Reporter

Cofense Reporter is the original antiphishing "easy" button. It operationalizes phishing awareness and reporting, acting as the conduit that feeds user reports — raw data — to the SOC, where it becomes usable intelligence. Cofense Reporter is deployed as an email client add-on, providing a quick-click mechanism for end users to report suspicious emails to security operations teams and supports a wide range of email platforms and clients, including Microsoft Outlook (2007 onwards) on Windows and Mac, Microsoft Outlook Web Access, Microsoft Outlook App on iOS and Android, Google Gmail, and Lotus Notes.

When used in conjunction with Cofense PhishMe, Cofense Reporter validates simulation emails sent by the PhishMe platform. When a PhishMe simulation email is received and reported by an end user, a customizable message is displayed to reinforce the correct behavior. The reporting metric is also sent to the PhishMe platform, enabling the tracking of desired reporting behavior and overall resilience to phishing.

Cofense Triage

Cofense Triage gives security operations teams a platform to automate the phishing incident response and remediation process. When suspicious emails are reported by end users, they are received by Cofense Triage and clustered into campaigns with a matching payload and given a risk score. Initial assessment of these emails by the Triage Noise Reduction Engine cuts through the noise of known false positives. It uses a commercial-grade spam engine to aid in identification of email types such as known marketing, transactional, spam, scam, or phishing emails. A malware blacklist feed also identifies emails that contain known malware.

A regularly updated and extensive rules catalog (supporting both YARA and a simple-to-use Cofense Triage rules format) matches on email attributes from the header, content, and attachments. Once again underpinned by the Cofense Threat Intelligence, Research, and Phishing Defense Center teams, rules identify the newest threat actor tactics and techniques and known threats in the wild. Security operations teams can easily create custom rules to identify specific threats or attributes; for example, those that verify that emails appearing to come from trusted third parties actually do. The use of Reporter Reputation and Status enables Cofense Triage to prioritize reported emails and campaigns based on a user's previous threat reporting accuracy — essential to identify zero-day attacks.

Integration with third-party threat analysis tools including VirusTotal (a subscription to VirusTotal is included with the Triage license) and sandboxes provides valuable referential information and context to analysts. Automated actions can be configured within Cofense Triage through playbooks to categorize, process, and respond to emails matching defined criteria. For example, the platform will automatically respond to the user-reporters when they report known good emails, eliminating one more task for overburdened SOC teams and allowing them to focus on the clusters presenting the greatest risk to the organization.

Cofense Vision

Once a threat has been reported by an end user and confirmed by security operations teams, the clock is ticking. It's essential that all recipients of the attack campaign be identified and the threat removed from their mailboxes. Optimized for email threat hunting and removing the need for privileged rights to the email environment, Cofense Vision puts advanced email threat hunting capabilities directly in the hands of the SOC.

Hosted within the customer environment, Cofense Vision is typically configured to receive emails after filtering by a secure email gateway. Once the emails are received, they are indexed and stored for fast threat hunting. Ad hoc searches can be run for specific email attributes through the UI or via API. Tight integration with Cofense Triage enables security operations teams to hunt for emails that match a specific Triage cluster directly from the Cofense Triage interface — including finding morphing campaigns where attributes such as sender and subject differ for each recipient.

Once threats are found, they can be quarantined with one click, reducing exposure time and the chances of compromise or breach. The ability to un-quarantine previously quarantined emails enables SOC teams to make risk mitigation decisions quickly and safely and restore messages if they later prove benign.

Comprehensive auditing of search and quarantine actions ensures that compliance requirements are met.

Challenges

The effectiveness of a phishing detection platform powered by human intelligence is a function of the tools around it. Even the best intelligence, if not properly leveraged, "spoils" quickly. Integration is the key; therefore automated APIs for the following are a must:

- SIEM
- Firewall
- Messaging security
- Web security

Additionally, user-reported phishing data requires organizational commitment. A platform is a great component, but commitment by users across the organization is equally vital. People and process are critical for success.

Conclusion

Augmenting existing security measures with human phishing intelligence is an important way to prevent breaches, but it isn't easy. It requires a platform to consume reports from users, quickly and effectively, and turn them into actionable intelligence. When this is done correctly, it creates value. When it is done incorrectly, it squanders human bandwidth, generating tedious work for end users, manual work for the IT/help desk and, worse, mind-numbing work for time-constrained security professionals. The scarcity of cybersecurity and IT professionals makes users a precious asset — one that cannot be wasted.

Although it may appear self-evident, the key to success is thorough planning, selecting a good platform, obtaining management and organizational support, and continually refining processes. IDC would advocate placing a special emphasis on planning.

About the Analyst

Frank Dickson, *Program Vice President, Security Products*

Frank Dickson is a Program Vice President within IDC's Security Products research practice. In this role, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

MESSAGE FROM THE SPONSOR

About Cofense

Cofense is the evolution of PhishMe, which was founded in 2008. In 2018, PhishMe was acquired by private equity and rebranded Cofense to emphasize the company's movement from providing a pure phishing training solution to an end-to-end platform for employee-sourced phishing attack intelligence. Today, Cofense employs over 400 employees around world provide phishing training and integrated anti-phishing intelligence. Among its 2,000-plus customers, Cofense includes over 50 of the Fortune 100 companies.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.