No longer just selling bait, PhishMe adds considerable tackle

Analyst: Adrian Sanabria

27 May, 2015

Security awareness products have come a long way from forcing employees to go through SCORM CBT modules designed for bank employees. Progress has required some experimentation and seen its share of controversy. Critics claim that because user awareness will never reach 100% efficacy, spending any money on it is a waste of time. PhishMe, however, is one of a few companies in this area that has shown us that enlisting rank-and-file employees as 'human sensors' can result in valuable security intelligence. Moreover, the company's products make it possible to clearly measure results, making it appear that the myth of the 'security awareness myth' can be put to bed.

The 451 Take

Detectives have long known the value of a reliable informant, so why not encourage similar relationships between users and incident responders in the enterprise? PhishMe has essentially built a product set to do this. Simulator tells you how good users are at spotting threats and grooms them to be better. Reporter allows them to exercise these skills every day with live email, and Triage adds a platform for incident handlers to act on Reporter's data in an automated manner that can also integrate with other security product investments within the enterprise. Triage, the latest addition to PhishMe's 'tackle box,' may seem like a basic connector, but it is an important addition because it allows the enterprise to integrate PhishMe data and products with other security products and completes the incident response workflow cycle within the company's offerings. It should have been a clue when Kevin Mandia joined the board of directors, but now it all makes sense – unlike most other security awareness offerings, PhishMe has more to offer than checking a compliance box or teaching users not to click malicious links; it is clear the focus is on leveraging employees to detect attacks that get by security controls.

Context

The four-year-old Leesburg, Virginia-based company has just over 100 employees by our estimation. PhishMe raised $13m in series B funding in March, contributed by original investor Paladin Capital Group and joined by new investor Aldrich Capital Partners. This brings the company's total funding to $15.5m.

Strategy

We've been hearing arguments from the anti-security awareness crowd for a while now. This group contends that, if 100% efficacy isn't feasible with a given threat detection/prevention approach, it can't provide value and we shouldn't bother using it at all. The fact that this observation applies to all security products seems to elude (delude?) this group. They also point to studies that show, while security awareness training results in fewer clicks on malicious links, given a broad enough range of targets, *someone* often still falls for the bait. 'All it takes is one' is the mantra.

PhishMe's Reporter and Triage products, and the company's product strategy in general, turn this perspective on its head. In the previous example, if we were able to successfully train a majority of users to identify phishing threats, why stop there? What happens if we enable these employees to *report* these threats?

'All it takes is one,' takes on new meaning.

Now, with the combination of PhishMe's Reporter and Triage products, a user can spot a phishing attempt, report it, and automated integrations with Web gateway or content filtering products can allow the incident response team to automatically block the threat. With this approach in place, it no longer matters if 100% of the user base spots the phish – if one person spots it and reports it, manual or automated incident response workflow has an opportunity to prevent additional employees from getting phished and deal with any employees that fell for the bait before the threat was reported. PhishMe reports initial customer results showing IR teams getting insight into phishing attacks within seconds, versus the average breach detection times of days, weeks or months we're used to seeing from industry reports. With this approach, even the smallest amounts of success in a security awareness program can now yield valuable results. All it takes is one.

Products

PhishMe's earliest products, like many other security awareness startups, revolved around training users to spot attacks. The descendant of this product, Simulator, allows customers to launch

phishing campaigns against users, educating those that are susceptible to such campaigns. Although this is becoming one of the more commodified products in this market, the opportunity to improve quality continuously keeps competition active and fresh. The need for ever-increasing quality is evident in two places: the user-facing campaigns themselves and in the data captured on user responses. Do campaigns reflect what attackers are capable of and are actively using? Are analytics on the output data useful in improving employees' ability to detect and respond to phishing threats?

PhishMe Reporter, the company's second product, was released a few years ago. Reporter consists of an email plug-in for the Windows version of Outlook, Outlook 2011 for Mac and a Chrome extension for Google Mail. These plug-ins and extensions allow users to report phishing attempts from within emails. The data from Reporter is used to build a reputational score for users over time in the Simulator product. As phishing campaigns hit the enterprise, statistics from Reporter can be used to track the success of a security awareness program. PhishMe speaks of one customer that defines success as the point where more users are reporting campaigns than falling for them – a metric easily tracked for simulations and for reported phishing emails with the company's Simulator and Triage products.

PhishMe Triage, announced at the 2015 US RSA Conference, makes it possible to create new use cases through data from PhishMe's other products. Triage combines analytics, a user interface for incident responders and standardized output to integrate PhishMe products with other security products and existing IR workflows. Triage helps prioritize threats using several techniques, including user reputation scores (one user might be more effective at spotting real threats than another), severity of phishing indicators, volume of reported email and possible phishing alerts submitted by users through Reporter. Once an email is reported as malicious, Triage analyzes the content – not just links, attachments and sender domain/IP. Analyzing the full content of the email makes it possible to detect emails that are similar, but not identical, and threats that aim to use persuasion to achieve goals rather than malicious software. This is an important distinction, as many threat detection/protection vendors tend to focus only on malware, when a significant number of security incidents don't involve malware at all.

Once a potential phishing campaign is identified and analyzed, the next step in the incident response workflow is generally to take action. Triage turns the analyzed data into a sort of internal threat intelligence by formatting results in YARA – a widely used standard for creating rules and signatures that can be used to detect and block malicious attacks. PhishMe has announced integration for various tasks with several SIEMs, sandboxes and URL analyzers. A few of these vendors include Splunk, ArcSight, FireEye, ThreatGrid (Cisco), Cuckoo and recently

Raytheon-acquired Websense. Triage also allows the security analyst to respond quickly to active threats by building rules and 'recipes.' The product has templates to assist users in building recipes.

PhishMe's Simulator and Triage products can be deployed on bare metal hardware, as virtual appliances or in a SaaS model, where they are hosted by PhishMe in the cloud.

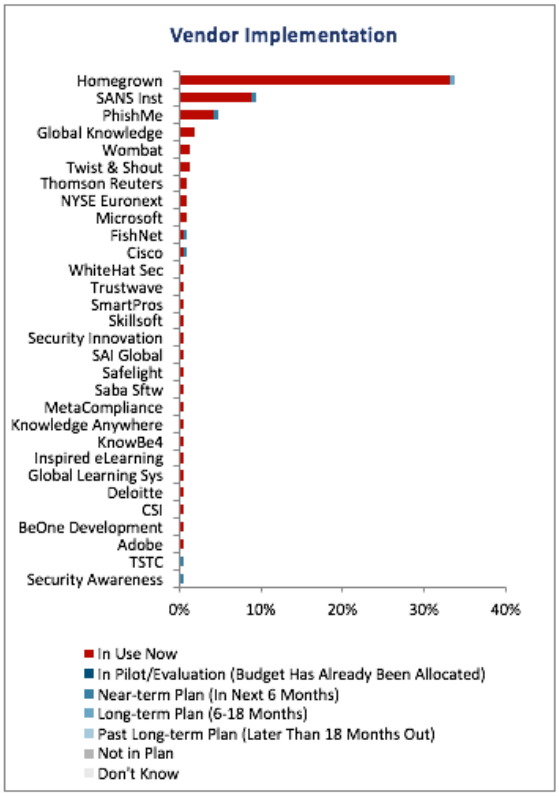
Competition

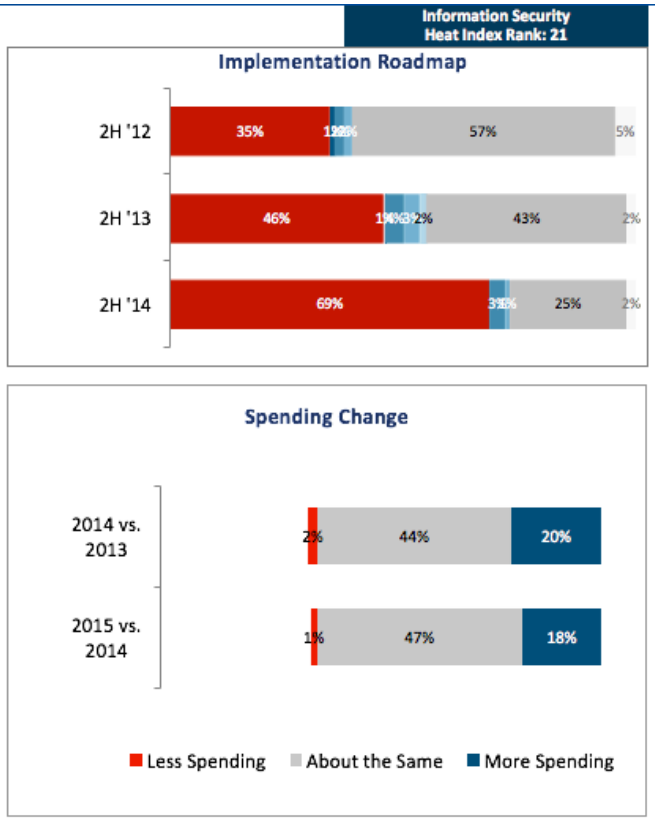
PhishMe's competition falls into a few categories: Basic user training, training with metrics/analytics baked in and vendors going after phishing infrastructure. The company most commonly competes directly against security awareness offerings, which include vendors like PhishLabs, Security Mentor, SANS Institute, MediaPro, Inspired eLearning, Security Innovation, PhishLine, KnowBe4 and The Security Awareness Company.

Wombat Security is probably the closest to PhishMe in terms of expanding beyond just user training and simulating phishing attacks. The company has a product similar to Reporter in beta trials.

The concept of finding and shutting down phishing infrastructure before the campaign can be launched is an interesting approach being explored by Risk IQ and Area 1 Security.

Looking at data collected by TheInfoPro, a service of 451 Research, PhishMe is consistently the second most popular commercial security awareness offering.





Left Chart, n=214. Top Right Chart: 2H '12, n=200; 2H '13, n=205; 2H '14, n=214. Bottom Right Chart: 2014 vs. 2013, n=212; 2015 vs. 2014, n=212. The 'implementation' charts use the same legend.

Source: Information Security – Wave 17 | © 2014 451 Research, LLC. www.451research.com

SWOT Analysis

Strengths

PhishMe's Reporter and Triage products push security awareness into new territory, and the company has a significant head start on its competitors.

Weaknesses

It is possible a large number of organizations will continue to do the bare minimum with security awareness, seeking only to 'check the compliance box.' This brings the continued growth of this market into question.

Opportunities

With PhishMe now delving into the incident response world, the key opportunities are in integrating and automating workflows with other vendors and products that PhishMe customers may already own.

Threats

There are a large number of vendors in the security awareness space, and although PhishMe technologically exceeds most of them, a large number of customers may be more interested in the approach that's *easiest* rather than the one that's the *most effective*. The very broad and versatile offerings at SANS highlight this effect.