ISMG INFORMATION SECURITY MEDIA GROUP

PHISHME

Proactive Defense Against Phishing

PhishMe's Robinson on Phishing Kill Chain and How to Build More Effective Defense

Phishing Trends

Tom Field: Lex, as we head toward 2018, what are some of the predominant phishing trends that you see, and how do you see behaviors in business processes being exposed by these attacks?

Lex Robinson: I'd like to break that down into a couple of areas. First is by taking a look at the types of attacks that we're seeing and then separating that from a malware discussion about what we're predominantly seeing. And really by types [of attacks], what you continue to see is that the predominant types of attacks are still URL-based, and then you get into an attachment base and then you're seeing an increase in the BEC [business email compromise] style of compromise.

Now within that, from a malware family perspective, you're still looking at Office macros, remote access Trojans, ponies and those types of things. But if we stay up at the top level and take a look at how we're being attacked or how some of those things are being modified by those coming after us, what you're really seeing with the attachments in Office macros are attacks against business processes themselves**.** So it's showing, at some level of recognition, that advanced persistent threats or other malicious actors recognize [that] we're using attachments a lot in emails - so they're coming after that. So that is a business process that's under attack.

And when you look at BECs continuing to be what they are and the cost continuing to grow over time, what you're really looking at there is another business process and behavior style of attack rather than [an attack] against technology. So what that's beginning to point us toward is not just that attackers are going to go past technology, it's that they're specifically doing that against what they recognize as common business process moving forward.

Proactive Defense

Field: You have described organizations being caught up in what you describe as a testing mindset where they're constantly testing their employees to how susceptible they are to phishing attacks. How can they shift from this testing mindset to a true proactive defense?

Robinson: The first level of that is really beginning to take on the role of an attacker, or an attacker's mentality and balance that against the way that we've chosen to respond to phishing threats or attacks over time. What I mean by that is an attacker is going to test you for weaknesses, and then they're going to come after you and exploit [those weaknesses]. So we should be doing the same thing. To stop

at a testing point, saying, “I'm going to do a penetration test and identify a problem” isn't enough for us. We actually have to take action against it.

For descriptive purposes, I'll liken this to our own health and the way that we take care of ourselves if we identify that we're unhealthy. We smoke too much. We eat too much. We do some of these other things and we do nothing to actually adjust, meaning: “Maybe I need a better diet plan or a better exercise plan.” [If I do not] actually put that into practice, then I'm not actually taking any action to prevent some sort of unhealthy condition later on. The same is true for our networks and how we address this particular problem with phishing and other cybersecurity concerns.

Setting Priorities

Field: How can people become an active element to this proactive defense?

Robinson: This is really around prioritizing cybersecurity in the same way that we do physical security. If we look at the way we've thought about cybersecurity over the years, we have virtualized within our minds and we've separated that from how we behave and how we act online very differently than how we do with physical security. So that's really the first step of it is prioritizing that for people and then empowering those people with some technology and some training to begin to recognize and report and become a part of that defense.

The Phishing Kill Chain

Field: Lex, talk to me about the “phishing kill chain” that you've developed at PhishMe. How does that map to this proactive defense we've been discussing?

Robinson: The kill chain that we've developed is really a slight modification to what currently exists, which is the attack kill chain that most people in cybersecurity are familiar with today. What we've done is simply filled the gap for what we've recognized as a sweet spot for when an email is delivered all the way to a user.

At this point, we've passed all of our technology controls. We've passed all of those security perimeter controls and so forth. But we still have an opportunity to get left of breach if we're going to utilize our associates, our employees and other people in the process go get left of breach and that's really accomplished through inserting a few other steps prior to an exploitation occurring or prior to the exfiltration of data. And that is really incorporating the notion of reporting and then [conducting an] analysis of that reporting so that we can then mitigate

before a breach occurs.

Simple Solutions

Field: Lex, talk to me a little bit about simple solutions—the ones that organizations can deploy against phishing and really be effective.

Robinson: There are a couple of levels here. One is all of your standard technology: your firewalls, email gateways, pre-fetching and scanning technologies. Those still need to be in place for us and those are fairly straightforward and effective for what they catch. Beyond that, what we need to be doing is really developing human defense and developing our associates and employees as intelligence data collectors for phishing, going back to this idea of see something, say something—recognition, reporting and then analysis of those.

Now in addition to that, when we start talking about what we want to invest in, one of the key steps that's a part of the kill chain and something simple that people can get after is baselining and understanding their own organization. Where are my technology gaps that I need to fill? What are the knowledge gaps and process gaps that I need to check on for security? This is simply taking the first step that any attacker would take—understanding my own environment and then filling those gaps in wherever that investment needs to be.

How PhishMe Can Help

Field: How is PhishMe helping organizations to respond to the latest phishing variants, and to have a proactive defense?

Robinson: That incorporates a couple of areas in terms of end-to-end solution development of human defenses, which is really what we're targeting. And we're doing that with a series of products and solutions modeled against that phishing kill chain and really empowering companies to do it.

Products like Simulator and Reporter are there to help you develop human defenses and human resources in that recognition and reporting capability itself. So if we want to run an anti-phishing program, we want to identify where we have weaknesses, a program run with these solutions can allow you to do that. On the back end of that, where the rubber really meets the road for us, has been with a Triage product where we're intaking all of that collected intelligence and doing an analysis and a prioritization of what needs to be addressed and then producing a result that allows organizations to go out, quarantine emails, apply rules to firewalls, all of those sorts of

things. Incorporated in that is our Intelligence product, which then feeds our ability to design better programs and to ensure that what we're finding is what needs to be targeted in real time.

On top of those products, we offer professional services for running anti-phishing programs for folks that may not be familiar with it as well as managing triage services for organizations that may not have the resources required or the expertise required to take in all of that data and then analyze it and develop an appropriate response.