SO LONG, AND THANKS FOR ALL THE PHISH

An old security vulnerability continues to thrive

special report

An SC Media publication

Phishing for credentials

Phishing remains perhaps the most effective way for attackers to get inside an enterprise. Even in attacking high-level targets, phishing and more targeted "spear-phishing" schemes are the major tactics for intrusion. Karen Epper Hoffman reports.

There is an axiom that says, "Give a man a fish he eats for a day; teach a man to fish and he can feed himself forever." Cybercriminals have co-opted that to say "Give a man a fish and he eats for a day, teach a man to phish and he'll live like a king." Phishing is the bane of CISOs everywhere.

There is nary an organization these days that has not been on the receiving end of a phishing or more targeted "spear-phishing" email. The goal is collecting sensitive information, personal credentials or passwords with the intent of getting into networks to steal information, or lock it up and ransom the data and systems back to the enterprise itself.

This type of attack plays to the oft-referenced idea that the human employee typically is still the weakest link in the data security chain. And, despite the broad-based attention paid to these types of attacks, bad actors have gotten very good at social engineering targets and exploiting their weaknesses. Phishers expertly determine which buttons they need to push in these carefully crafted emails to make them seem legitimate, urgent and requiring immediate response or action from their targets. Regardless of increased awareness training, Verizon's 2017 Data Breach Investigations Report found that roughly one in 14 people will automatically click on any attachment or link they receive — and more than 25 percent of them were tricked into clicking more than once. The same report found that last year two-thirds of all malware made its way onto systems via email attachments, more than six out of 10 of which were packed in popular JavaScript attachments.

Indeed, attackers have become very sophisticated in their abilities to exploit vulnerabilities in applications such as email or messenger programs. They can bypass network security by impersonating corporate executives and by employing established social engineering techniques—often times, using legitimate code, or information about their targets, the people they are impersonating or the organization itself, gleaned from research the attackers conducted beforehand. By using these approaches, they make their phishing emails and messages or texts seem all the more real and legitimate, and they get users to divulge either credentials or data, or to take an action that permits the attacker to gather additional intelligence.

Former Rep. Mike Rogers, R-Mich., who served as chairman of the U.S. House Intelligence Committee from 2011 to 2015, speaking at the U.S. Chamber of Commerce's cybersecurity summit in late 2015, says sophisticated phishing emails are behind more than 90 percent of successful cyberattacks. And some experts peg the percentage even higher.

The Ironscales 2017 Email Security Report, based on a survey of 500 cybersecurity professionals, found that as many as 95 percent of all successful worldwide cyber-attacks started with a phishing email. In

OUR EXPERTS: Phishing

Chad Greene, director of security, Facebook

Brendan Griffin, threat intelligence manager, PhishMe

Rep. Mike Rogers, former chairman, U.S. House Intelligence Committee

Limor Kessem, global executive security advisor and security researcher, IBM Security

Phishing

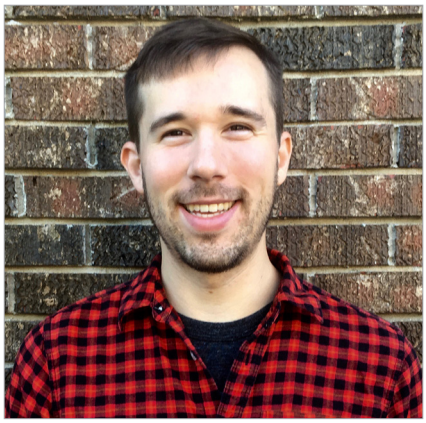
45%

Percentage increase of BEC attacks in the fourth quarter of 2016

– Proofpoint

fact, more than half of all emails are spam, and the percentage of these spam emails that carry malicious attachments is growing in leaps and bounds, according to IBM's X-Force research team.

As cyber-crooks make these phishing emails increasingly believable and well-researched, an Intel Security survey in 2015 found that 97 percent of people could not tell the difference between an authentic email and a well-crafted fake one. And it's not difficult to see why this cheap and effective method of cracking open an enterprise system is still so popular with newbie hackers and experienced ones.



Brendan Griffin, threat intelligence manager, PhishMe

"Phishing is a numbers game and remains effective because it's a relatively easy attack to attempt repeatedly," says Chad Greene, director of security at Facebook. "It often only requires a single person to fall for the phishing attempt for it to be successful. With persistence, an attacker will likely eventually find someone to enter his or her login credentials."

> *"Phishing is a numbers game and remains effective because it's a relatively easy attack to attempt repeatedly" – Chad Greene, director of security, Facebook*

And mobile devices are becoming an increasingly popular attack vector for these attacks as well. Newsweek recently reported that since the beginning of this year, mobile ransomware attacks—which tend to be initiated through SMS text phishing or "smishing"—are up more than 250 percent over last year.

Indeed, phishing has played a major role in nearly every global, high-profile cyber-attack in the first six months of this year. These include multiple attacks on businesses and individuals throughout Qatar (more than 93,000 attacks in the space of three months) in the Middle East and Nigeria in Africa, a phishing campaign aimed at the postal service of the Czech Republic, and multi-pronged attacks hitting U.S. and international businesses including Chipotle, Amazon, Google, Deloitte and Facebook, plus government agencies like the National Institutes of Health and the U.S. Postal Service.

Even the dreaded 2017 WannaCry ransomware onslaught, which is believed to have affected nearly a quarter of a million people in more than 150 countries, likely started with phishing, security researchers believe. And savvy phishers are going yet another step further, using other recent, high-profile cyber breaches and offline-related tragedies as a means to trick otherwise wary employees and individuals with their pleas. In late September, the Federal Trade Commission alerted the public that scammers were pretending to be agents of Equifax to collect sensitive personal information from people already worried about their leaked data. Other recent scams have preyed on the charity of businesses and consumers who want to help or donate to people affected by the recent spate of 2017 hurricanes, including Harvey and Irma.

Limor Kessem, global executive security advisor and a cyber security researcher for IBM Security, agrees that this form of social engineering continues to remain popular because "it preys on human emotion and impulse to act" by crafting emails that might "scare the reader into opening an urgent message from their bank, threaten that an account has been disabled, or reward readers with fake tax refunds, supposed rewards from popular retailers, or reduced prices for something they need." And, for employees in particular receiving a supposedly "urgent"

54%

More than half of the 350,000 security professionals surveyed said they expect a successful cyber attack against their company within a year

– Crowd Research Partners

invoice, notice from a tax authorities, salary file, money transfer request purportedly from a C-level executive, or a notice to pick up a parcel that could not be delivered would likely trigger an immediate action or response, she adds.

Changing Language, Changing Landscape

When it comes to phishing, fraudsters use timing, trends, and technical modifications to make their phishing attacks work better, Kessem continues. "We can see seasonal trends with phishing, mostly around tax time and the holiday season, but phishers prey on users whenever a popular subject arises, like major sporting events, or news about something that affects the entire nation," she says.

Kessem adds that phishers rely on a variety of established methods that they shuffle to keep evading spam filters and detection. Some examples from recent campaigns feature different site redirection schemes, serving malicious URLs from within benign productivity files, wrapping up malware payloads in multiple layers of different file formats, and registering numerous fake domains to serve malicious content and malware, she adds.

Limor Kessem, global executive security advisor, cyber security researcher, IBM Security

Facebook's Greene has similar experiences. "The threat landscape is always changing and the cybercriminals are always looking for ways to look more legitimate and increase believability," Greene says. "Over time, the language used in lure emails has become more polished and often lacks the grammatical or spelling errors that were easy giveaways in classic phishing lures."

This past year has seen a sharp increase in the number of business email compromise (BEC) scams, like CEO fraud, according to Symantec's 2017 Internet Security Threat Report. CEO fraud is where a bad actor pretends to be the chief executive or another top executive to get the CFO or accounts payable department to put through a wire transfer or release confidential or valuable information to the bad actor. BEC scams alone have cost enterprises more than $5 billion between October 2013 and December 2016, according to the FBI.

This past year has also seen a huge uptick in W-2 phishing scams, aimed at getting organizations to turn over sensitive tax document information based on a fraudulent email purported to be from the Internal Revenue Service, or from a high-level executive at the organization requesting payroll or HR information. Tax phishing emails jumped 870 percent in 2017, according to the IRS Return Integrity Compliance Services.

Given most employees' fear of running afoul of the IRS, these phishing scams tend to have a 25 percent success rate, according to the IRS. In a 2017 press release aimed at warning employers about this onslaught, Tamara Powell, acting director of the IRS Return Integrity Compliance Services, called these attacks "one of the most dangerous email phishing scams we've seen in a long time."

Greene says that in these more sophisticated attacks, "it's not unusual for there to be an intermediate target who is only being phished to compromise his or her account and send the next lure to the 'real' target. Once the intermediate account is compromised, the lure can be added to an existing email threat using real content in the proper context to be believed."

And while attackers are aiming high with more up-market spear-phishing, many are taking more of a shotgun approach, phishing often and aggressively to as many targets as they can. In other words, cyber-criminals are aiming both high and low in their attacks, going after quality and quantity, potentially big payoffs as well as smaller ones, in effort

53%

Percentage of US companies that said it took 2 or more days to recover from a cyberattack

– Hiscox Cyber Readiness report

Ransomware questions become more complex

The complex web of mitigating, preparing for and responding to ransomware threats is becoming all the more tangled for enterprises, as they wrangle with concerns around ethics, business case, and a changing security and technological infrastructure.

That is the over-arching message from Brendan Griffin, threat intelligence manager for the intelligence operations group at PhishMe, when he discussed existing and emerging issues around ransomware during an SC Media 20/20 webcast in October. Griffin's comments during the webcast, dubbed "Know Your Ransomware Enemy," offers insight into the growing challenges of responding to ransomware demands and advice on what enterprise IT security teams can do to better protect themselves, their customers and their sensitive data.

Given that the people behind these ransomware scams are not always acting in good faith and honesty, Griffin's take on the issue of whether or not enterprises should pay the ransom to their attackers or not — if this presents the cheapest and easiest way to regain access to their locked down data, or if these bad actors can even be trusted to follow through with turning over control, comes back to making an educated business decision.

Griffin points out that for hospitals, government agencies or enterprises that manage crucial infrastructure and utilities, "the stakes can be much higher for not paying the ransom. Lives are on the line there." For these organizations, there are also ethical questions surrounding how they handle ransomware demands, "and that's why ransomware has such a grip on some entities," Griffin adds. "It's not just about the cost, but how long we can [ethically] delay the services we provide."

In many cases, Griffin says, organizations typically consider their ransomware response based on the technical issues, and not the business case — the impact of downed or delayed services, or missing data that would need to be replaced, and the ultimate cost of that data being exploited by cybercriminals.

He points out that often the simplest (and the best) means of mitigating ransomware attacks is through basic changes in protocols and procedures, such as putting through a phone call to the CEO or the CFO to confirm an urgent wire transfer they supposedly requested by email. "Any request for a wire transfer should go through a particular process," Griffin says. "Information security is spilling over, beyond technical, into other parts of the business which may have been seen as isolated from worrying about these things before."

To the issue of using backups after a breach, Griffin says that while the conventional thinking is that making regular backups of corporate data and networks is the best way to defend the enterprise in the event of a ransomware attack, savvy cyber-criminals often anticipate this approach, and will lock up network backups and restore points as well. "There's a risk in relying on backups too much," he notes. "Nothing should be on the network that you cannot afford to lose." For mission-critical data and systems, he recommended a separate air-gapped system.

With the explosion of the Internet of Things devices in enterprise settings, the ransomware challenge is likely to get more difficult before it gets easier. "Once [ransomware] reaches the Internet of Things, it becomes harder to redress the issue," Griffin says. Many of these IP-controlled machines might not have security built in directly and they are not designed with vulnerability patching in mind. "This will introduce a whole new aspect [of ransomware] and new challenges for security professionals."

— KEH

55%

Percentage of companies in the US that say they have cyber insurance

– Hiscox Cyber Readiness report

to get access to information or entry into corporate systems wherever they can. At least two-thirds of the time (67 percent), corporate employees are victims of spoofing and impersonation, but they can often fall prey to branded or seasonal attacks, according to the IronScales report.

There are also simply more cyber-crime and black-hat hacker groups actively targeting businesses than there were in the past, according to Kessem. "Malware groups that operate banking Trojans, for example, are more focused on businesses in search of heftier amounts of money to steal," she says, adding that Dridex, TrickBot and Qakbot were all Trojans that preyed almost entirely on business and corporate banking customers.

Chad Greene, director of security, Facebook

School of Phish

Phishing is a problem that is both technical and human in nature, so it is not surprising that the likely solutions to mitigate the problems associated with the risk and impact of phishing attacks, especially on more high-value targets, need to incorporate both technology and human training, the experts agree.

Kessem believes the real issues with phishing "begin and end with the human factor. Without proper education and awareness, employees will remain the weakest link no matter what sort of tools and technology are being used." To combat these concerns, she recommends that CISOs opt to launch an effective awareness campaign across the organization to help keep the potential of phishing in their employees' minds by providing recurring and visual reminders about common risks, best practices, and the importance of security to the organization.

Greene points out that Facebook is a contributor to and member of the FIDO Alliance, which is aimed at developing standard and interoperability for authentication technologies. Such technologies could help stem the tide of these fraudulent emails, messages and texts. In addition, Greene adds, the giant social media network has implemented two-factor security keys that can provide users with the options of two-factor identification and thereby mitigate the misuse of stolen passwords.

Education about phishing and online scams has become a part of many organizations' toolkits, and law enforcement and industry regulators including the SEC, the IRS, and the FTC post advice on their web sites, she adds. Kessem believes that every organization should plan and implement their own customized educational process about online threats, and follow best practices from NIST, ISACs (Information Sharing and Analysis Center) and other organizations in order to standardize security practices.

"Role-based training should be provided to users across the organization, from the C-suite to accounting, HR, the IT staff, administrative workers, and any other group, to ensure that each employee understands the risks, their potential exposure in their specific role, and ways to respond if ever they suspect an issue," Kessem adds. "Security policies and standards should be clear and communicated to all employees. Then have them sign a document outlining their own responsibility to uphold those standards on the company's infrastructure and equipment." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

7.14%

One in 14 people were tricked into opening an infected link

– Ironscales

Sponsor

PHISHME

PhishMe is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today's top attack vector — spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process. PhishMe's customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

For more information, visit us at phishme.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
CUSTOM PROJECTS COORDINATOR Samantha Lubey
samantha.lubey@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@haymarketmedia.com*

WANT TO LOWER YOUR
MALWARE THREAT?

UP YOUR PHISHING DEFENSE.

OVER 90% OF MALWARE ATTACKS, INCLUDING RANSOMWARE, START WITH PHISHING. PhishMe helps you train employees not to take the bait. Condition users to recognize and report phishing, plus arm incident responders with PhishMe Triage and PhishMe Intelligence—let them hunt down threats smarter, faster, better. It's human-focused, automated, holistic phishing defense.

LEARN MORE:

Download PhishMe's 2017 "US Phishing Response Trends Report"

DOWNLOAD NOW

PHISHME®