LEADERSHIP AND PROJECT MANAGEMENT TIPS FROM AN ISLA® WINNER

InfoSecurity PROFESSIONAL

JANUARY/FEBRUARY 2018

A Publication for the (ISC)²® Membership

Whaling

Targeting Bigger Phish

(ISC)² InfoSecurity PROFESSIONAL 10 YEARS

SOC IT TO 'EM

CPAs inspire an industry-agnostic cybersecurity framework

BLOWN AWAY

Cutting down on the noise in threat intelligence feeds

TARGETING THE BIGGEST Phish

TODAY'S 'WHALING' IS BRINGING HUGE PAYOFFS FOR INTRUDERS WHO SUCCESSFULLY IMPERSONATE THOSE TOPPING THE CORPORATE FOOD CHAIN.

BY DEBORAH JOHNSON

THE EMAIL FROM THE CEO of a financial services company asked the client to pay the attached invoices and provided banking information. The company paid. It was a fraud. "They were in the hole for about £200,000."

So relates Carl Chapman, CISSP, the CISO/COO at business consultancy Crescent Bridge, Ltd. based in London, when discussing a successful "whaling" attack on a company with which he was familiar. The attacker "had effectively created a duplicate domain and impersonated the CEO to ask them to pay invoices to a fraudulent bank account."

PHOTOGRAPH BY JOHN KUCZALA

The fraud was eventually discovered "by chance," Chapman says. "Someone spotted it, something just didn't look right. They were able to recover about 75 percent of the amount."

Spear-phishing is not a new threat, but advances in techniques are revealing a more substantial threat for organizations. By more thoroughly researching their targets, these attackers can reel in a considerable payoff—sometimes millions of dollars. Security professionals call it "whaling," because of its success in impersonating much bigger "phish."

According to the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center, between October 2013 and December 2016 there were more than 40,000 domestic and international business email compromises (BEC)—how the FBI designates phishing attacks—adding up to more than US$5 billion in losses.

THE PHISHING EVOLUTION

Phishing has narrowed its focus from the earliest attempts: hackers spreading a wide net to millions of emails loaded with malicious attachments or links, usually from a financial institution, hoping a recipient would fall into the trap. With targeted phishing—spear-phishing—these bogus emails are directed to specific people, seemingly from someone they know—and likely trust.

"It is sent in a way to seem like it is coming from a particular employee," says Kevin Williams, CISO for the City of Austin in Texas. "And based on that person's job function, they craft the message to look like something they would send out. 'Oh, yeah. That's Bob. Bob's a PM. He always sends me something with a link on it.' Then click on it…."

Similarly, Geographic Solutions, a designer of web-based workforce systems based in Palm Harbor, Fla., has received its share of spear-phishing emails, says security and compliance team lead Justin Warniment, CISSP-ISSEP, ISSMP, CCSP, CISM. "We had targeted emails to our financial folks, accounting, also HR. Very targeted at our senior managers, such as directors."

And the emails don't need to be complicated. Nick Johnson, a systems administrator at FNB Bank in Mayfield, Ky., remembers two specific attempts. "They posed as a very high-level bank employee. It was a very simple email that was trying to get us to process a wire. It wasn't like it had a lot of detail to it and that's what made us look at it."

Whaling attacks are "just a continued innovation and evolution of techniques used by hackers," says Matthew Gardiner, senior product marketing manager for Mimecast, an email management and security company based in London. "Instead of pretending to be someone outside the organization, they realized they could be someone with authority inside the organization."

"They posed as a very high-level bank employee. It was a very simple email that was trying to get us to process a wire. It wasn't like it had a lot of detail to it and that's what made us look at it."

—NICK JOHNSON, systems administrator, FNB Bank

Williams adds, "The more sophisticated attacks are usually one link in a very long chain of attacks. In a phishing email posing as a city project manager, when our investigators do forensics on that employee's machine, they will usually find they were the victim of an earlier phishing attack. The earlier attack got the [victim's] name, contact list, message format—all the information that they needed to conduct their next attack. The results of the new attack will become input for the next attack, and so on."

The victims are not only high-profile, news-making organizations. Smaller businesses are impacted just as often, says Erich Kron, CISSP-ISSAP, security advocate for the security awareness training company KnowBe4, based in Clearwater, Fla. "Those companies may lose $20,000 or $30,000"—a smaller sum compared to the losses suffered by larger companies—"but it can be devastating for a company."

KNOW YOUR ENEMY

According to Verizon's 2017 Data Breach Investigations report, which analyzed 42,068 incidents and 1,935 breaches from 65 organizations in 84 countries (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/), 51 percent of breaches involved organized criminal groups. And these groups are smart, says Kron. "These people are very intelligent—[operating as] businesses more than individuals. We've seen in some of these ransomware strains where they offer tech support. You can chat with them to get them payment."

And just like legitimate organizations, says Mimecast's Gardiner, they find partners. They host "attacks in data centers that will look the other way if you pay them. They split the money the way any company would with those they do business with. 'I'll provide you a ransomware as a service platform if you give me 40 percent of your take.' The key takeaway is: Don't think about it as some random hacker."

Ultimately, says Crescent Bridge's Chapman, "it's actually really simple: It's very cheap to do. Once you undertake that type of attack successfully in one business, then maybe it's an opportunity to do it again and again."

SOME OF THE WHALERS' LURES

The internet and social media have come together as a malicious hacker's dream. The information available online

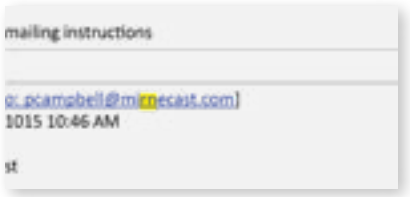
coupled with some knowledge of a specific business can give an attacker all he or she needs, warns Chapman. "A financial services organization that has less than 50 people, it's quite likely they're not going to have all of the services, like payroll and invoicing, they're not going to do those things in-house. They're going to do them externally. If you're able to identify, say—I'll use LinkedIn as an example—C-level individuals at your target business and you can see that they are connected to a managing director of a small payroll business you probably have most of the information you need to perpetrate that crime."

The FBI issued a clear warning in its May 2017 alert: "The subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment."

Social media isn't the only place for data mining. Open-source intelligence provides a raft of valuable information, says KnowBe4's Kron. "You have corporate filings and information like that. Even the company's website has a lot of great information. For example, if an organization is getting ready to do an IPO or a product release, that's great information the bad guys can use to target the executives."

With information from public filings and social media, hackers can create an extremely personal email, says Cory Deeter, director of cybersecurity operations and IT compliance for Finish Line, a retailer of sports shoes and clothing based in Indianapolis. "One example I [saw] was an email sent to a CFO from a supposed close college friend. The email referenced college nicknames for one another and included a malicious attachment."

Domain and email spoofing is another tool in the whaler's tackle box—and even cybersecurity specialists are not immune as Mimecast's Gardiner relates. "We're mimecast—m-i-m-e-c-a-s-t dot com. They sent it from mirnecast.com [m-i-r-n-e-c-a-s-t]; the 'rn' looks like 'm' to the casual viewer *(see image, below)*. They could send email from that domain as if it were our CEO, in fact, trying to get our CFO to send off money."



Mimecast was not alone in this type of whaling attempt. Proofpoint, a security and compliance company based in Sunnyvale, Calif., investigated attempted email intrusions at more than 5,000 large enterprises in Q4 2016. The investigation revealed that two-thirds of those attacks used spoofing.

TALES FROM THE DEEP

SIX WAY TO STOP WHALING ATTACKS

Educate and inform employees.

Use simulations—staged whaling messages—to detect organizational weaknesses.

Make faking messages difficult by using unique identifiers.

Tap technology using gateway protections such as DMARC, DKIM and SPF.

Stay alert through monitoring services.

Rethink procedures for email authentication and financial transfers.

Source: https://www.mimecast.com/resources/infographics/Dates/2016/8/infographic-tales-from-the-deep/

ESCAPING THE WHALER'S HARPOON

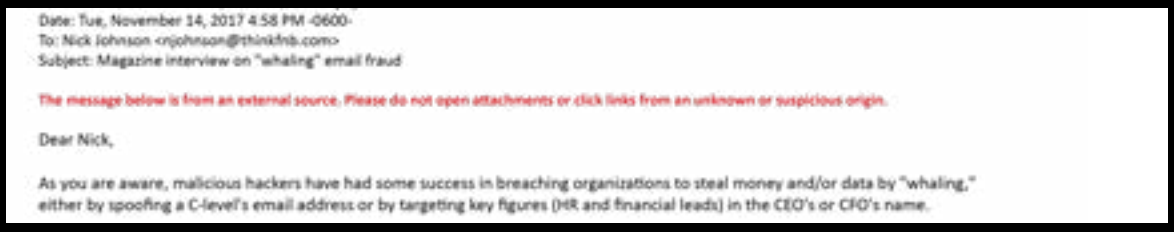
Just as the whalers have the lures and tricks, cybersecurity professionals have their own toolbox.

For Geographic Solutions, Warniment says finding a security awareness training partner, as well as enhancing email security software, has made the company stronger. One key element in training—phishing campaigns. "We target certain users, groups of users or the entire company." Does anyone ever fail? "Oh, yeah. The end user is the weakest link when it comes to IT security and clicking on a malicious link."

EMAIL ALERTS

FNB Bank uses a "transport rule" in its email to alert recipients of potential danger. "A transport rule that we set up for email that comes from outside the bank into the bank, it appends a message at the top of the email that says this is a message from an external source and it has some additional warnings in there about do not open attachments or click links from an unknown or suspicious origin."

—NICK JOHNSON, systems administrator, FNB Bank



Date: Tue, November 14, 2017 4:58 PM -0600
To: Nick Johnson <njohnson@thinkfnb.com>
Subject: Magazine interview on "whaling" email fraud

The message below is from an external source. Please do not open attachments or click links from an unknown or suspicious origin.

Dear Nick,

As you are aware, malicious hackers have had some success in breaching organizations to steal money and/or data by "whaling," either by spoofing a C-level's email address or by targeting key figures (HR and financial leads) in the CEO's or CFO's name.

Finish Line has also staved off whaling attempts using a combination of approaches, describes Deeter in an email. "We leverage multiple technologies to identify suspicious emails and provide ongoing training for our users. Most importantly, our executives have a keen awareness that they are targets of these types of attacks and they remain vigilant."

Mimecast's Gardiner agrees with the multilayered approach, but sees technology as the strongest component. "It's about having automated controls to try to minimize your dependence on people to always do the right thing, which is hard because people don't always do the right thing. And you have to build up caution in people's minds. You also have to have the process not be dependent on just one email to go wrong. And if you do all these three things really, really well, then you'll be pretty safe from these attacks."

"People are it. They are almost your first and last line of defense," declares FNB's Johnson. The bank has an extensive user awareness program for all employees and focuses on what Johnson calls the "90/10 rule—they're 90 percent of the equation and all of our technology is 10 percent. But," he adds, "if they don't have a buy-in, if you have people actively subverting you from inside and clicking on things they shouldn't click on or going to places they shouldn't go to, then you are not going to get any results."

Williams, in Austin, sees the security challenge through the lens of a public entity. "I think we're better insulated because the CEO just can't come down and tell you 'cut a check. Pay that man right now.' On the other hand, we have a civic obligation to offer things like public Wi-Fi at municipal locations, parks, city hall. We also have to create things

ONE COMPANY'S PROCESS

"We, like many other large companies, utilize a multilayered approach to determining whether an email is safe.

- A typical flow routes emails through a spam detection engine that evaluates a myriad of factors, such as sender reputation, volume of mail coming from that IP address or sender and heuristic indicators of message content. Any attachment to those emails then goes through a virus scanning tool.
- Attachments are then run through another tool that executes the attachment in a sandbox environment to determine if there are behaviors of the file that indicate it could be malicious.
- Assuming it passes those checks, the email then passes to another provider who runs similar tests. If the message and the attachment pass all these checks, then it appears in the user's inbox."

—CORY DEETER, director of cybersecurity operations and IT compliance for specialty retailer Finish Line

to facilitate the public, things like council agendas, websites to take your utility payments or to schedule park space, and things like that. We need to take extra caution, take steps to isolate them from other aspects of the network, and isolate the user interaction where the data may be stored."

NO END GAME

It's widely recognized that perfect security does not exist. There's also agreement that it's going to take enlightened vigilance, ongoing training and the continual improvements in email security software to protect both organizations and individuals.

"The attackers will always shift," warns Matthew Gardiner. "If email gets sufficiently locked down—which is imaginable, it's possible—they'll pivot to something else: IoT compromises or looking for vulnerabilities in web-deployed systems that haven't been patched…."

"The industry is bleeding from a thousand paper cuts," Erich Kron says. "The big ones make the front pages but little ones happen constantly, over and over and over again. They go unreported because there's shame—it could ruin your reputation to say you fell for a phishing attack, that you 'had a breach.' So a lot of companies won't even report that this happened. They'll just eat it and hope for the best." ■

Learn More

Whaling: Anatomy of An Attack
https://www.mimecast.com/resources/ebooks/dates/2016/5/whaling-anatomy-attack/

U.S. Federal Bureau of Investigation – Internet Crime Complaint Center
https://www.ic3.gov/default.aspx

DEBORAH JOHNSON *is managing editor of* InfoSecurity Professional.