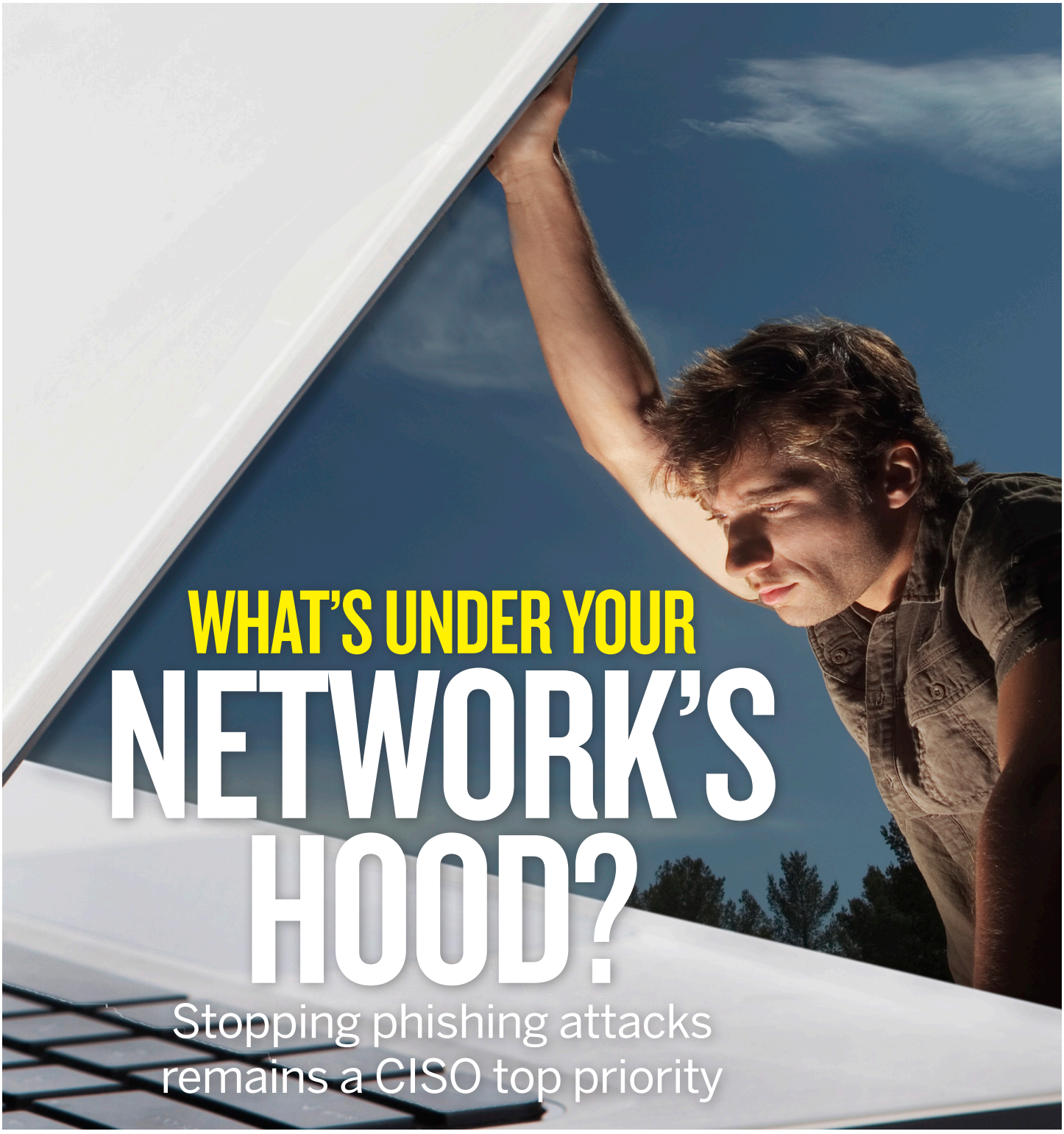

# WHAT'S UNDER YOUR NETWORK'S HOOD?

## Stopping phishing attacks remains a CISO top priority

special report

An SC Media publication

Sponsored by

COFENSE

# Phishing challenge pivots to human factors

Authentication technologies are front-burner tools to protect your network from COVID-19 pandemic email vulnerabilities. With attackers focusing on your users, common sense and technology go a long way. Scott Mace reports.

Without letup the cyberattacks keep coming but they are not necessarily aimed at your network's protocols or software vulnerabilities — at least, not at first. Instead, they maneuver themselves into part of your corporation's most vulnerable infrastructure and manipulate your employees to fall for some email message that is not what it appears to be.

Knowledge workers encounter these hazards during every working day when they are reading and responding to email. A decade ago, the email industry developed ways to provide greater assurance of the identity of an email sender. These technologies gradually came into more widespread usage, but the opt-in nature of email technology on the internet means that adoption is far from universal; it remains so today. In addition, the lack of universal implementation of the technologies, plus some built-in vulnerabilities, make these approaches useful but hardly a silver bullet for phishing and business email compromise (BEC) attacks.

It started with great promise early during the past decade. Domain-based Message Authentication, Reporting & Conformance (DMARC) brought together such heavyweights as Google, Comcast, Yahoo! Mail, and LinkedIn to implement Domain Keys Identified Mail (DKIM), which uses an asynchronous key pair to verify that a message was sent from a legitimate user of an email address to prevent email forgery.

Sender Policy Framework (SPF), which like DKIM was codified into a standard by the Internet Engineering Task Force (IETF), detects email spoofing by evaluating the path it took, and comparing a message's originating IP address against Domain Name Service (DNS) records.

Where DMARC enforcement falls short is that it only authenticates at the time each email gets inspected. DMARC cannot make any assurances that future emails will always be authentic, says CISO John Masserini of Millicom International Services LLC, a Coral Gables, Florida, operator of the Tigo brand of cable TV and cell phone services in 14 countries in Latin America and Africa.

Criminals can stand up their own email servers that look legitimate, and that is a problem for DMARC technology. There is also an operational challenge for threatened organizations.

"If we were to lock down a lot of our email with DMARC that expressly prohibited emails from non-approved senders or non-authenticated senders, we would have a business problem," Masserini says.

The reason: Three of four email domains have yet to implement the DMARC standards, and thus get their email approved by the other one quarter. So, an organization trying to abide by them has a lot of "prohibited" emails to process, to separate legit messages from illegitimate ones.

## OUR EXPERTS: Phishing

**Joshua Bartolomie,** director of research and development, Cofense

**J. Wolfgang Goerlich,** consulting CISO, Cisco

**John Masserini,** CISO, Millicom International Services

**Branden Williams,** adjunct professor, University of Dallas

**Teresa Walsh,** global head of intelligence, FS-ISAC



**832M**

*In March 2020, some 67 major data breaches effecting 832 million data records were identified*

– IT Governance

"It's surprising because DMARC is the strongest means for an organization to control how its emails are handled across the internet," says J. Wolfgang Goerlich, a consulting CISO at Cisco. "If Acme Corp. sends me an email, and Acme Corp. has DMARC configured, I can validate that the email came from Acme Corp. and not from a criminal spoofing an Acme Corp. email address. For CISOs, DMARC provides a means of brand protection."

J. Wolfgang Goerlich, consulting CISO, Cisco

However, while DMARC identifies valid senders, but it does not validate a *specific* sender. For example, if John Smith at Acme is sending from a validated email address, a DMARC-enabled email server will accept the message. But if John Smith's email credentials have been compromised and an attacker is using his credentials to send malware through the authenticated Acme server, the message still will be accepted. Additional levels of security are required to further validate messages and payloads beyond DMARC, the experts point out.

> "If we were to lock down a lot of our email with DMARC that expressly prohibited emails from non-approved senders or non-authenticated senders, we would have a business problem."
>
> *– John Masserini, CISO, Millicom International Services*

"Because DMARC relies on the DNS infrastructure, it does have its own set of vulnerabilities that a sophisticated attacker can take advantage of to make a bad email look good," says Branden Williams, an adjunct professor at the Satish & Yasmin Gupta College of Business at the University of Dallas in Texas. Still, Williams says, "it is a great first line of defense and every CISO should be making decisions on inbound email for their firms using this technology."

Millicom's approach was integrating its email system with its security operations center (SOC), as well as a third-party real-time threat intelligence system to scan the links presented in incoming mail. If a link was flagged, it was replaced with links that redirect email users to proxy URLs, away from threats.

"Think about the sheer volume of email even small companies receive," Williams says. "In order to do this effectively, you would either need to whitelist URLs, or be able to create a virtual 'detonation chamber' for every URL to see what it does. You are correct to call that a Sisyphean effort." For instance, he points out that maintaining a URL whitelist has difficulty scaling up.

"If you have a proxy that's updating signatures or domain lists on a daily basis, those domains come up and are gone before even the next iteration of updates end up at the proxy," Masserini says. "So, relying on either network-based control or an endpoint control, while it's absolutely there, it can't be the only solution these days."

Three areas for securing emails are before the email gets to the recipient, at the point the recipient decides to act on the mail, and one after the recipient takes action. "Before a potentially malicious email even gets to the end users, in addition to DKIM, a strong email security system applies a combination of heuristics to identify and stop suspicious emails," Goerlich says.

He suggests that security teams also consider email message encryption for protecting sensitive messages and high-risk recipients.

**10**

*The Virgin Media UK database was left publicly available for 10 months from 2019 to 2020. 900,000 records were affected*

– IT Governance

"This is really all about really quickly identifying who is reporting bad or suspicious links, and really trying to figure out who they're impacting and how bad they are," Masserini says.

### On-prem vs. cloud

Email security vendors are incorporating machine learning into their products, searching for suspicious patterns, down to very slight misspellings in a sender field, or invisible characters embedded in an email domain. "That's the kind of stuff where the automatic decisioning of machine learning is playing a key role," Masserini says.

Even if a user clicks on a bad link, layers protecting security of the affected enterprise applications can also play a role. "The number one way criminals break in is by logging in with stolen credentials," Goerlich says. "It makes sense to prioritize email security. But the number two cause of breaches is criminals exploiting vulnerabilities in the applications we host."

## *Most breaches* are not detected by tech

Most email-based data breaches end up being detected by means other than technology, says Joshua Bartolomie, director of research and development at Cofense, during a recent SC Media 20/20 webcast tilted "What's under your network's hood."

"Some definitely were" detected by tech, he says, "but a lot of them were from an employee notifying the security ops team or an incident response team."

Employees often are alerted to a potential data breach because something did not look right — such as a web site that did not look like the user expected — or a feeling that something they clicked on might have stolen their credentials. Or, perhaps, their computer has been acting strangely since they opened a particular email attachment.

Phishing threats continually evolve, and today security teams are seeing a lot of new threats related to the COVID-19 outbreak. One such email warns recipients that a supposed infection has taken place in their area and offers to tell the recipient that more information is available if they click on a link in the email.

Business email compromise (BEC) is not new, but it continues to trigger breaches, even though it comes in the form of emails with no links and no attachments, Bartolomie says. "A lot of it is just, 'Hey, I need to talk to you, but I can't get to the phone. Ping me when you get back to your desk," Bartolomie says. "It's just starting a conversation."

Artificial intelligence is sorely challenged to find those BEC emails among the vast flow of messages companies receive. "An average organization of 10,000 people ingests on average a million emails a day," he says. "I would not put all your eggs in one basket, whether it's AI or not AI."

As with most security threats, he recommends a defense-in-depth strategy.

Bartolomie also has advice for those migrating email services to the cloud. "Some of these cloud services have some great back-end tooling," he says. "Make sure you know what it is so that you have the licensing, so they're turned on, and able to be used by somebody who knows how to use them."

As with other security issues, remind employees to look for things in email that don't look right, and to speak up when they find them. "Go into it with your eyes wide open," Bartolomie says. "Know that there's going to be gaps, but try to account for them, and the best way is with education and training."

— SM

**75%**

*Percentage of healthcare information that is not encrypted*

– Ponemon

CISOs, therefore, should implement security that increases visibility into both cloud and on-premise-based applications, identify and reduce vulnerabilities within application stacks, and address regulatory and compliance requirements.

One advantage of switching to cloud-based services is the access management tools they provide, Williams says. "For example, you can easily turn on multifactor authentication and mandate it for all your users, where doing something like that on-prem can get tricky and be difficult to manage," he says.

**Branden Williams, adjunct professor, University of Dallas**

Finding a strong security solution to the authentication problem and getting it approved by senior management are entirely different skills. One way to explain this to an executive decision maker is to use the analogy of money. "Ask them how they would protect money that they store on site and they would likely use words like vault or safe," Williams says. "That's on-premises. Now ask them how they would protect money they own but cannot see. That illustrates the problem."

> "Because DMARC relies on the DNS infrastructure, it does have its own set of vulnerabilities that a sophisticated attacker can take advantage of to make a bad email look good."
>
> *– Branden Williams, adjunct professor, University of Dallas*

Moving from purely technological remedies, one method to ensure email is not the easiest attack vector for criminals is to tighten up policies and procedures, as well as updating documentation accordingly to explicitly detail the fundamental and advanced security controls being implemented.

For example, organizations have known for years that there was a lag time between when an employee is terminated, and when that employee's access to organizational email and other network resources is subsequently blocked. A common example would be an employee let go at the end of the day on Friday, but the IT team is not informed until the following Monday morning. In this example, the separated employee — or an attacker pretending to be that former employee — would have two full days of access using the old credentials.

"We have spent the better part of the last 18 months going through a massive user access cleanup and automation process," Masserini says. His organization can now terminate user access very quickly, "within hours of getting the word from HR."

At the heart of such capabilities is a robust identity management system spanning email and other enterprise application access. "It is incredibly complex," Masserini says. "There are nuances to every organization that really make it a winding road for deployment. But the return on investment on getting it done, across dozens of machines with the push of a button, are worth it."

## Testing, 1, 2, 3

Ultimately, CISOs return to that most vexing of email security challenges: training employees not to click on suspicious links or files. A standard antiphishing exercise today in common use is for the IT department to send out its own emails to employees, emails that appear to be legitimate but are, in fact,

**#1**

*The data that is most likely to be encrypted is payment-related data*

– Ponemon

simulated phishing messages that might lead the employee to visit what could be a compromised web site.

"Phishing simulations are a critical part of training our users to be more skeptical," Williams says. "They can have negative impacts, but firms should turn them into training opportunities. And if your simulations are getting low click rates, say under 10 percent, your simulations are not real enough."

**John Masserini, CISO, Millicom International Services**

Masserini likens these tests to the vulnerability tests IT departments run regularly on their network infrastructure. "It's really about education and awareness," he says. "Yelling at people or people getting in trouble because they clicked on the link has never been a successful awareness methodology. It's always about making them better, especially if you can relate it to stuff they do at home."

Creating a security culture is one of the primary roles of the CISO. Part of that culture, experts agree, is creating an environment where users identify potential phishing attacks and report them to IT. When users click on the attacks and allow the attackers in, the attackers win. The goal of user training is to reduce that number of wins sufficiently that the profit from sending out phishing attacks is reduced so that the attackers stop those attacks.

## Show us the money

Although the industry will continue to push current best practices such as DMARC and other authentication methods to combat phishing, there is one more industry-wide effort to make phishing attacks less financially profitable: finding and closing the bank accounts attackers use.

Sometimes the holders of such accounts have no idea what the true purpose of the accounts is for — to move money quickly from the targeted, defrauded firm to other accounts held by the criminals themselves. These account "mules" are recruited by criminals on the pretext that they are simply being compensated a nominal fee to help move money around.

Finding and shutting down these accounts is one legal deterrent banks can use to fix this problem. For example, a cybersecurity company can act as an agent to lure in fraudsters who reveal the identity of the accounts used by mules. The company then forwards lists of these accounts to the Financial Services Information Sharing and Analysis Center (FS-ISAC), a cyber and physical threat intelligence analysis and sharing platform for the global financial industry. By sharing this data, all companies that share the ISAC's threat intelligence feed can benefit from the data pertaining to the threat and take actions to avoid becoming a victim.

> "The number one way criminals break in is by logging in with stolen credentials."
>
> *– J. Wolfgang Goerlich, consulting CISO, Cisco*

Experts agree that in order to make ISACs most effective, companies need to share such threat data, even if they have fallen victim to it. By sharing they can help others avoid the attacks, making the attackers less effective and profitable.

Perhaps prompted by the FS-ISAC's own 2018 phishing attack, the group recently enhanced its security efforts. "The bank has to investigate," says Teresa Walsh, global

**20%**

*One in five Europeans have experienced identity theft fraud in the past two years*

*– Finanso.se*

head of intelligence at the London-based FS-ISAC. When unusual banking activity is noticed, a bank employee might ask: "Why is this fraudulent money coming into the customer's account?"

> "Individual legal teams within the banks sometimes say, 'We can't share this information; it's too sensitive. We, as an FS-ISAC, try to help our members overcome challenges that they have."
>
> – Teresa Walsh, global head of intelligence, FS-ISAC

By comparing details with suspicious accounts with other banks that are part of FS-ISAC, a member bank can determine if the account has indeed been used for fraud, and make sure that none of the banks' customers have sent or will send money to that account.

Part of FS-ISAC's effort is to educate people who unwittingly act as mules, letting them know they are participating in illegal activity that can permanently mar their career or life. "A lot of this is just struggling to reach what we call 'left of the kill chain,'" Walsh says.

So far, the nascent operation has collected more than 2,000 of these bank accounts. And FS-ISAC, through its industry clout, is making a difference. "Individual legal teams within the banks sometimes say, 'We can't share this information; it's too sensitive,'" Walsh says. "We, as an FS-ISAC, try to help our members overcome challenges that they have." Pull quote (start at Individual..)

Time will tell if FS-ISAC's efforts reduce the number of fraudulent accounts in use. "We are providing a month-on-month stack analysis for our members so they can self-determine if their controls are being successful to prevent mule account creations at their banks," Walsh says. ■

---

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

*If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at (347) 480-1749, or via email at david.steifman@cyberriskalliance.com.*

**>75%**

*More than three of four US households will have a voice-assisted speaker by 2025. Such virtual assistants can get hacked using ultra-sonic waves*

– Atlas VPN

Sponsor


Cofense®,the leading provider of intelligent phishing defense solutions, is uniting humanity against phishing. The Cofense suite of products combines timely attack intelligence on phishing threats that have evaded perimeter controls and were reported by employees, with best-in-class security operations technologies to stop attacks faster and stay ahead of breaches.

*More information is available at www.cofense.com*

Masthead

EDITORIAL
**SPECIAL PROJECTS EDITORIAL DIRECTOR**
Stephen Lawton
*stephen.lawton@cyberriskalliance.com*
**SPECIAL PROJECTS COORDINATOR**
Victor Thomas
*victor.thomas@cyberriskalliance.com*

SALES
**VP, PUBLISHER** David Steifman
(347) 480-1749 *david.steifman@cyberriskalliance.com*
**VP, SALES** Matthew Allington
(707) 651-9367 *matthew.allington@cyberriskalliance.com*


IS YOUR EMAIL GATEWAY
REALLY SECURE?
Cofense sees phishing threats in environments protected by "secure" email gateways every day.
What's YOUR Plan to Stop Them?
COFENSE
Find out how we can help you catch the phish in your inbox and avoid a breach.
cofense.com