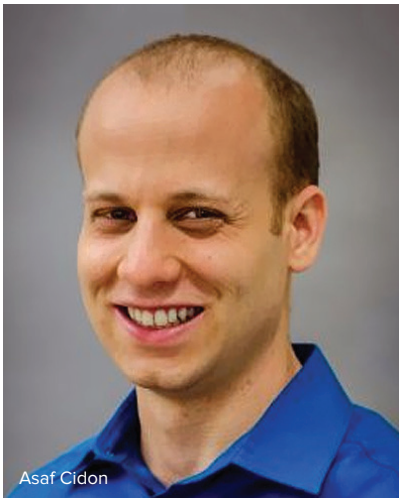
Spear Phishing: Top 3 Threats

Barracuda's Asaf Cidon on Latest Trends and Solutions

Barracuda®

ISMG
INFORMATION SECURITY
MEDIA GROUP


Asaf Cidon

Cidon is the senior vice president, email protection products at Barracuda Networks. He previously founded and was the CEO of Sookasa, which was acquired by Barracuda Networks in 2016, and worked as a software engineer at Google. He is the recipient of SC Media's 2017 Rising Star Award and holds a PhD in electrical engineering from Stanford University.

Among the top new spear-phishing threats to enterprises: Extortion. Asaf Cidon of Barracuda outlines the top three spear-phishing threats and new strategies to defend against them.

Cidon was surprised to see how quickly extortion has taken off as a prevalent threat, as outlined by Barracuda' newest spear-phishing report.

In an interview with Information Security Media Group's Tom Field, Cidon discusses:

- Insights from Barracuda's latest report;
- Why top threats are so successful;
- New defensive strategies and solutions.

Key Findings in Report

TOM FIELD: Barracuda has a new report on spear phishing. What do you find to be the most surprising findings of this report?

ASAF CIDON: This is a report that we compiled based on a ton of data that we collected through our different email security products, and even though I'm in charge of the team that actually built these products, I was actually quite surprised with some of the findings that we uncovered ourselves.

The first thing that struck a chord with me is the rise of blackmail email or sextortion emails. We're seeing that attackers are increasingly bypassing existing email defenses by sending emails that include no attachments or links and basically tell the recipients that the attacker has obtained a password to their account and wants them to send them some bitcoin or otherwise they will expose very embarrassing information about the recipient, like embarrassing photos of them or their dirty browsing history or something like that.

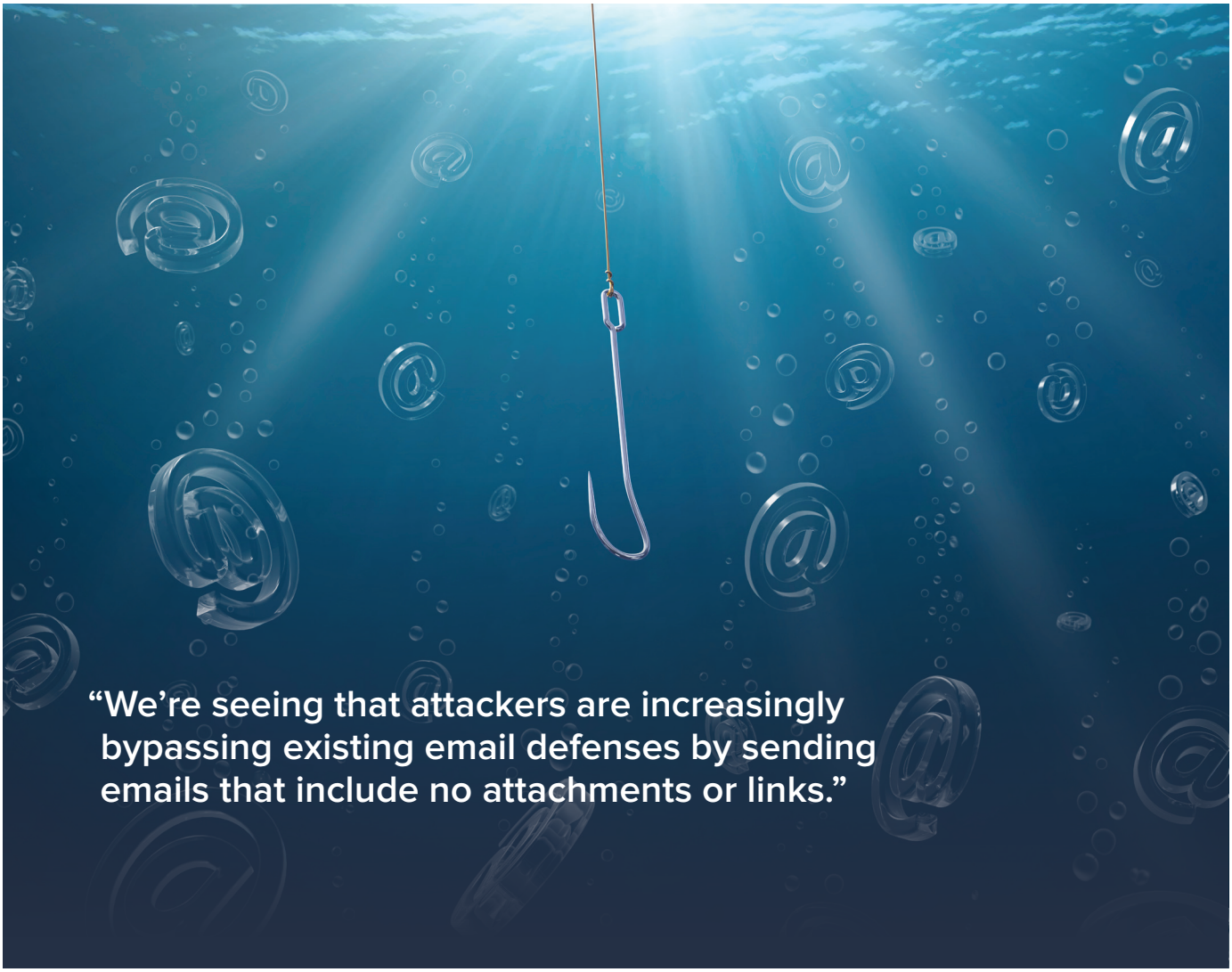
In our report, we found that actually today these attacks comprise over 10 percent of all the spear phishing. These type of attacks have gone from zero to over 10 percent … in just a matter of a few months, so that was quite striking to me.

Another interesting nugget from this report is we found a lot of these spear-phishing attacks were actually launched from personal, free email services like Gmail, which I found surprising just because you'd think that those types of email addresses would get blocked pretty easily by the mail services like Office 365 or Gmail itself. But in fact, the reason attackers are using these free email services is they actually have a really high reputation because they're considered to be legit mail senders. And so attackers are taking advantage of their reputation in order to launch some of these attacks.

Other Prevalent Attacks

FIELD: Asaf, you've talked about these extortion attacks. That's one of the three prevalent threats you're seeing today. What are the other two?

CIDON: Blackmail is the fastest new rising threat. Another one is what we call a brand impersonation. This is really the classic targeted phishing attack. These attacks involve impersonating, let's say, DocuSign or Dropbox or Outlook telling you that you have some



problem in your account and asking you to sign in to see what the problem is and then harvesting credentials of employees. That’s still, by far, the most prevalent type of attack.

And then the third category is employee impersonation, which is also called business email compromise or CEO fraud. These are the types of attacks where the attackers are impersonating someone specifically in the organization – like the CEO, for example, or a manager – and trying to get the recipient to take some action, such as send a wire transfer for an impending payment to a supplier, for example.

Failed Defenses

FIELD: These attacks have been publicized pretty well. Security leaders certainly know about them. Why, then, do they remain so successful?

CIDON: They remain successful because the majority of existing defenses really fail to stop them, and the reason for that is, because, you know, we call these attacks spear phishing and so, the word “spear” explains why these attacks are getting through. And so they’re highly targeted effectively.

The same emails are not being sent to tens of thousands of people. The attackers are actually targeting someone very specific in the organization, and so they tailor the email to the specific recipient. A really good example of that is in these blackmail emails, the attackers will include a stolen password of the recipients that was exposed in one of these major breaches to demonstrate to the recipient that the attacker has been able to hack the account.

Because they’re highly targeted, something like just a spam filter won’t stop them. And then on the other hand, while these attacks don’t really contain any obviously malicious signals – they don’t have malware or ransomware – it’s hard to catch them. Oftentimes they’re just a piece of text that would seem relatively innocent to an email filter.

New Defenses

FIELD: So you pointed out why traditional controls are unsuccessful at stopping these threats. What new defensive strategies and controls do you recommend?

CIDON: We recommend a multilayered approach to stopping these attacks. The first line of defense is still email security. But you really

> "It's really important to make sure that your employees are trained and can recognize these attacks."

want to look at AI-powered email security. Traditional email security filters just look at a very fixed set of keywords or they try to map out reputations of various domains. But these types of approaches really don't work well against these types of targeted attacks.

And so what we've built at Barracuda is an artificial intelligence-based solution that actually learns the unique communication patterns of each organization and then understands them to identify when an anomalous email comes in.

If you know what a normal email looks like in a context of specific organization, if an irregular anomaly comes in, you'll be able to identify it a lot better. So that's the first step.

Another really important step is to actually have security awareness training. Employees are the last line of defense, and oftentimes, executives might get phished even not just on their corporate email but they could get phished via SMS or via their personal inbox. So it's really important to make sure that your employees are trained and can recognize these attacks.

There are a variety of ways to do that. It starts with simulating exactly these types of attacks against your employees and seeing if they fall for them. If they do, explain to them the tell-tale signs to look for. But it also involves having training videos, certifications and even SMS-based phishing simulations on the more advanced side.

And finally there's general security hygiene, including multifactor authentication using strong passwords, ideally with a password manager. All of these steps help reduce your cyber exposure in general, and particularly against email-borne attacks.

Barracuda's Role

FIELD: What are you doing at Barracuda to help organizations do a better job detecting and responding to the threats you've outlined for me today?

CIDON: Spear phishing has been at the forefront of our attention at Barracuda. We were the first company to start developing effective solutions for spear phishing. So that started with an AI-based product Barracuda Sentinel. It's our fastest growing product.

Sentinel is taking email security to a whole new level. Not only can it automatically stop and detect spear-phishing attacks, but it's even able to detect and stop attacks like account takeovers, which is the next evolution of spear phishing where these attacks are actually originating from within a compromised employee mailbox.

We also developed and recently launched a solution called Forensics and Incident Response. If an attack did take place, it allows you to actually go back retroactively, investigate who are all the employees that received the attack, see whether they clicked on any of the links and be able to retroactively remediate and delete those emails. The next step of this is to block that attack on the network and make sure that nobody clicks on any of these things going forward.

And we acquired a company called PhishLine, a leader in security awareness training. Security awareness training is an extremely important piece of the puzzle in protecting against targeted attacks.

PhishLine has been fully integrated with our email security offerings. At this point, we can confidently say that we have the most comprehensive and deep solution in the market to prevent spear phishing. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io