Vade Secure
Predictive Email Defense

Expert Focus

April 2019

Brought to you by Vade Secure

Attackers' threats are more sophisticated and complex than ever before. Your defenses have to be better.

DEFENDING THE INBOX

Countering dynamic email threats

The ubiquitous email inbox is Ground Zero for the vast majority of cyberattacks. Are you doing everything you can to protect your systems and your users from the latest malware, phishing and other growing threats? Are you sure? Allen Bernard reports.

The state of email security today is not pretty. As network security continues to improve, hackers and cybercriminals are increasingly focusing on the email inbox to launch attacks. Corporate email today has become a favorite target for these cybercriminals, nationstate attackers, script kiddies looking to make a name for themselves, and all sorts of unsavory characters.

Due of the ubiquity of email, it is a popular target for cybercrooks. They see it as a way to make a quick buck by getting someone to turn over their credit card numbers, banking logins and passwords; as well as a common vector to introduce ransomware or launch long-duration, lurking attacks aimed at infiltrating an organization's hierarchy to find out who holds the keys to an organization's accounts and controls, then send targeted spear phishing emails to steal money via fraudulent wire transfers.

Historically, the perpetrators of email-based attacks generally wanted one thing: money. While many headlines focus on state-sponsored actors trying to subvert critical infrastructure or steal intellectual property (IP), 76 percent of attackers in 2017 were motivated by financial gain, according to Verizon's 2018 Data Breach Investigations Report.

"[Bad] actor motives have historically been driven by financial gain, followed by strategic advantage aka espionage. Just under 90 percent of breaches fall into these two motives, with money once again leading the charge," the report states.

Email's fatal flaw is not technical — configured correctly, layered security can catch up to 99 percent of all inbound threats, says Erik Nyberg, vice president of technology at KVC Health Systems.

It is the human in the loop that makes the remaining one percent so effective, he says. Humans are gullible. They trust first and generally only ask the hard questions later. And there is a small but not-unsubstantial sub-set of people that, no matter how many times they are told not to, they click on just about every link and attachment they receive, he notes. Stating the obvious from the attackers' perspective, cybercriminals and hackers love these people who click everything, he continues.

Even when email is outsourced to popular cloud platforms such as Microsoft Office 365, its users are still plugged into the corporate network. This gives attackers access to all manner of applications and data denied to outsiders. That could be why 93 percent of all breaches start with email, according to Verizon's report. And that stat makes it easier to understand why spear phishing and business email compromise (BECs) attacks are on the rise.

According to a research note from Konstantin Rychkov, the Prague-based research manager at International Data Corp.'s (IDC) European Security Solutions, this is one reason spear phishing and BECs attacks, also known as CEO Fraud, are increasing. In one such instance, writes Rychkov, 14 wire transfers sent over several weeks cost a company $45 million.

> “They’ll actually fake an entire email chain and then they’ll email someone in accounts payable and say, ‘Okay, I’ve discussed this with the finance director and they’ve approved this. So, go ahead and pay this invoice.’”
>
> *– Erik Nyberg, vice president of technology, KVC Health Systems*

Malware threat falls

“The big [threat today] is spear phishing,” says Nyberg. “It’s not the mass spam anymore. It’s literally someone writing an email to our accounting or HR department. It’s just one email with no weird links in it or strange language. You may even find KVC’s signature on it so it looks real. There’s just not a lot behavior to flag it. That type of spear phishing is very hard for a filter to catch because we write plenty of legitimate emails that look the same.”

Another problem that is making phishing more effective is that modern email platforms hide the email address and return path of the sender. Attackers simply bypass email filters by sending emails using only a name. While many spear phishing attempts rely on email spoofing (visible alias spoofing, cousin domains), these are still comparatively easier to detect than SP emails coming from a legitimate email account within your organization. This explains the surge in Microsoft Office 365 phishing.

“They aren’t going ‘whaling,’” says Nyberg. “They’re going after the people that have the ability to make financial or transactional decisions. The most volume lately has been using one of our executive’s name. They don’t have to use their email account.”

The top three email threats KVC faces today are attackers asking HR to reroute employee paychecks to the scammer’s account, attackers submitting fake invoices from real vendors the organization does business with, and pilfering user credentials.

“They’ll actually fake an entire email chain and then they’ll email someone in accounts payable and say, ‘Okay, I’ve discussed this with the finance director and they’ve approved this. So, go ahead and pay this invoice,’” says Nyberg.

The industry term for this is pretexting, a lie used primarily in social engineering attacks to obtain privileged data. It can be used, for example, to establish a relationship with someone in order to lure them into a false sense of security. Once trust is established, the attacker asks for funds to be transferred or that sensitive information such as account numbers and passwords be disclosed.

Two other problems facing KVC, and many other organizations today, are mobile devices and remote offices. When employees are behind firewalls at its Olathe, Kansas, headquarters, Nyberg says, their inboxes are protected by multiple firewalls, as well as email security software from Vade Secure. So, if the email filters do not catch the phishing website, the firewalls should, he says.

“Maybe the firewall happened to catch a phishing website earlier,” he adds. “In an official KVC office, there’s another chance we can catch something that we lose when [employees] leave the office.”

One thing Nyberg has not seen is an increase in malware coming in via email attachments. This is backed up by Verizon’s findings. Since its peak in 2014, email-borne malware is down significantly. While the stratospheric rise of ransomware has slowed somewhat; malware, while still a significant threat due to its destructiveness, is actually not all that pervasive.

“We analyzed 444 million malware detections across approximately 130,000 organizations and the median organization received 22 or less pieces of malware per year,” Verizon’s report states.

“[We] use supervised classification AI and machine learning algorithms and deep learning that uses computer vision to detect phishing attacks and to detect [infected] images.”

– Sebastien Goutal, chief science officer, Vade Secure

The AI factor

Advanced email protection systems increasingly rely on artificial intelligence (AI) and machine learning to remove the human from this loop by automating the entire detection and remediation process. Once these systems recognize a threat has slipped through, instead of simply alerting someone in IT, they track down and remove suspected emails from user inboxes, quarantine them, and then alert IT to the threat once it has been neutralized.

Because email has a significant human element, it is important to have layers of security. Vade Secure’s approach is that users need to be protected against unknown and dynamic threats. And for this, they need to have multiple layers of protection powered by AI to ensure a predictive defense and also remediation.

Archiving, encryption, and other defensive technologies should be among the additional layers — not replacing but augmenting the security built into Office 365. AI provides the first line of security, then these additional security measures are layered on top, whether from Microsoft or another security provider.

AI and machine learning offer CISOs the ability to go deeper into a potential attack than simply analyzing each email as it comes in. It is a two-step process, but the first step of process has three components, Sebastien Goutal, Vade Secure chief science officer says — Anticipate, Decimate, Remediate.

AI gives the system the ability to anticipate what is coming next. “You block from the first sample if the filter is looking for the behavior of the attack,” he says.

The next step is decimate — you can detect live what your engine is missing. Because no security is 100 percent effective, he says, you need to react very fast when this happens. He likens this to how telecommunications companies such as Comcast protect their users. “All emails go through their filters. When people say an email is junk, their system learns from this. They use AI and machine learning to do this.”

The final step is remediate. “Let’s say the attack is so well built it gets through. That happens every day. The AI system needs to identify its own mistakes and fix it.”

To accomplish this you need to have to ability to clean up the email boxes, he continues. On Office 365, for example, administrators will have ability to clean up all mailboxes from all the phishing emails their filters missed.

The second part of the process is the ability to connect AI to their Office 365 systems to clear the mailboxes in real time, since normally there is not only one user getting a copy of a phishing email. The identification and remediation process can be conducted on the first phishing email the system identifies, but then AI — with the assistance of heuristics that look at the behavioral aspect of the emails — then can replicate the decontamination process on all similar phishing emails sent to users automatically.

“[We] use supervised classification AI and machine learning algorithms and deep learning that uses computer vision to detect phishing attacks and to detect [infected] images. That is common,” Goutal notes.

“The way threats are evolving it reminds me of a marketing drip campaign,” says Jonathan Goldszmidt,

“Where we see the biggest issue now is in spear phishing and the sophistication is phenomenal.”

– Gunter Bayer, CIO, vCloud

senior technology consultant and managing partner at smartIT, a managed security service provider (MSSP) in New York City.

“If someone was in sales, every day of the week they would do different types of targeted emails and progress them … with the goal of getting a successful sale,” he says.

Cybercriminals who rely on email as their weapon of choice have adopted similar tactics. Like pretexting, the goal is to establish enough of a relationship with the target (in this case, someone in accounts payable with check writing authority) to gain a level of trust based on familiarity.

But unlike pretexting, there is the added element of gaslighting, the phenomenon where someone is told so often that what they see or hear is not real, they begin to believe it.

If the target of this type of attack sees a request often enough, it will begin to seem legitimate, the thinking goes, and they will act on the request.

Because of the nature of his business, Goldszmidt’s inbox is under constant attack by hackers looking to get not only the keys to smartIT’s kingdom but its clients’ as well. That is why, as a reseller and user of Vade’s offerings, the company makes sure all sent email, including from and to internal inboxes, runs through Vade filters, he says.

Because malware-laden attachments today are often blocked by DNS servers, whitelisting domains, and email filters sandboxing suspicious content, attackers are starting to play the long game by using BEC attacks and insider attacks, says Gunter Bayer, CIO at vCloud, an MSSP and Vade partner in Ireland.

Over the past year, he notes, ransomware attackers said, “‘We’ve got in to lock your stuff up. Give us X amount and you get your stuff back — maybe.’ Now, it’s more of a long-term play where they phish for smaller amounts more quickly,” he says.

“Where we see the biggest issue now is in spear phishing and the sophistication is phenomenal,” Bayer continues. “The other big thing we see is businesses getting phished from the inside. The CFO [and] the IT department — they usually get phished from the inside because they do know a lot more about the sophistication of phishing.”

The rise of Office 365

Like thousands of other businesses over the past few years, KVC has moved its 1,700 employee inboxes to Office 365.

According to IDC’s “Email Security: Maintaining a High Bar When Moving to Office 365,” #EMEA44752219, January 2019, Office 365 accounts for almost half of all cloud inboxes. By 2022, the firm says, most inboxes will be cloud-based. This gives Microsoft a huge share of that $6 billion market. It also makes Office 365, already a prime target, even more attractive to attackers looking to break into corporate networks.

“Such standardization around the platforms of choice inevitably leads to increased interest from cybercriminals and greater risks associated with careless deployments,” says IDC’s Rychkov.

Even with Office 365 security add-ons such as Exchange Online Protection (EOP) or Advanced Threat Protection (ATP) enabled, phishing, spear phishing, and zero-day attacks still get through.

It does not help that there is a worldwide industry today supplying

> “I can’t imagine if I didn’t have AI or threat intelligence security what it would look like because Microsoft’s intelligence suite just doesn’t block enough.”
>
> *– Chris Ichelson, founder, HTG 360*

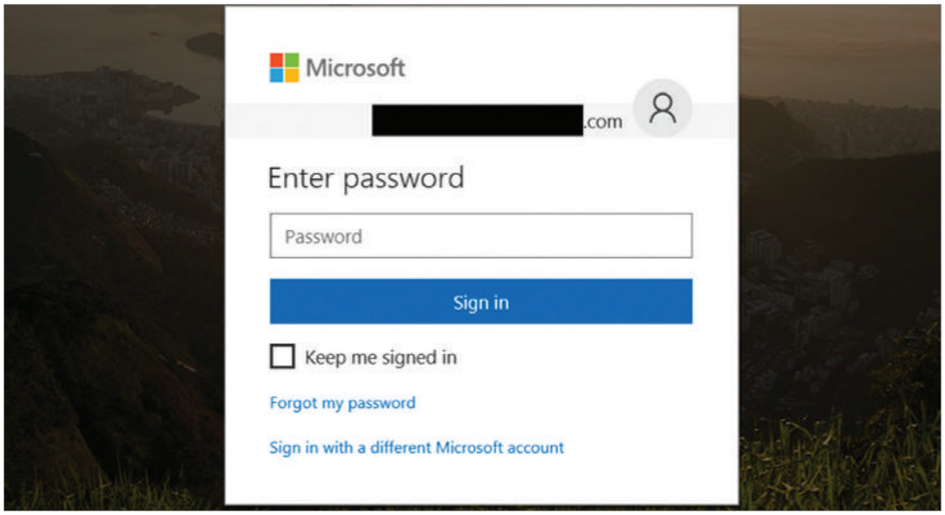
hackers with all the tools, support, and customer service — including money-back guarantees — they need to succeed in breaching Office 365.

“It is very profitable as a hacker to go after [Office 365],” says Goutal. “They can even test their emails by getting an Office 365 email account and sending it to that account until it gets through. Then they send out to everyone.”

According to Vade’s in-house research, Office 365 is now the most impersonated brand when it comes to phishing attacks that use spoofed webpages and login popups to fool users into entering their data, displacing PayPal. That says a lot about the security of Office 365 and the value of breaking into it. Also, once a hacker successfully bypasses the defenses of just one account, in theory, they can use that same attack to gain access to tens of thousands of other Office 365 email accounts and the millions of inboxes that represents.

“I get a lot of clients that think Microsoft [security] is enough,” says Chris Ichelson, founder of Scottsdale, Ariz.-based HTG 360, an MSSP and a Vade reseller.

“I’ll just be honest with you … it’s just not enough. I run three email security solutions today and I still get phished. I can’t imagine if I didn’t have AI or threat intelligence security what it would look like because Microsoft’s intelligence suite just doesn’t block enough,” he notes.



Microsoft

[redacted].com

Enter password

Password

Sign in

□ Keep me signed in

Forgot my password

Sign in with a different Microsoft account

Despite the high-quality graphics and Microsoft logo, this image is a splash screen for a phishing site, according to Vade Secure.

One of the reasons Office 365 is such a big target is it still relies too much on reputation- and signature-based defenses, says Goutal. These work well for the spam and broad-based phishing attacks they were designed to stop, he says, but struggle with spear phishing and zero-day exploits such as new malware posing as a non-executable file embedded in a Word document or PDF file.

The dynamics of dynamic threats

The shift to Office 365 and other cloud-based business email platforms such as Google’s G Suite underscore the ever-changing nature of the email threat. Not that long ago, the proverbial Nigerian prince was the main threat to email users. No more. Today, the experts tell us, organized criminal groups and state-sponsored attackers pose far more serious and sophisticated challenges.

> “Such standardization around the platforms of choice (such as Office 365) inevitably leads to increased interest from cybercriminals and greater risks associated with careless deployments.”
>
> – *Konstantin Rychkov, research manager, IDC*

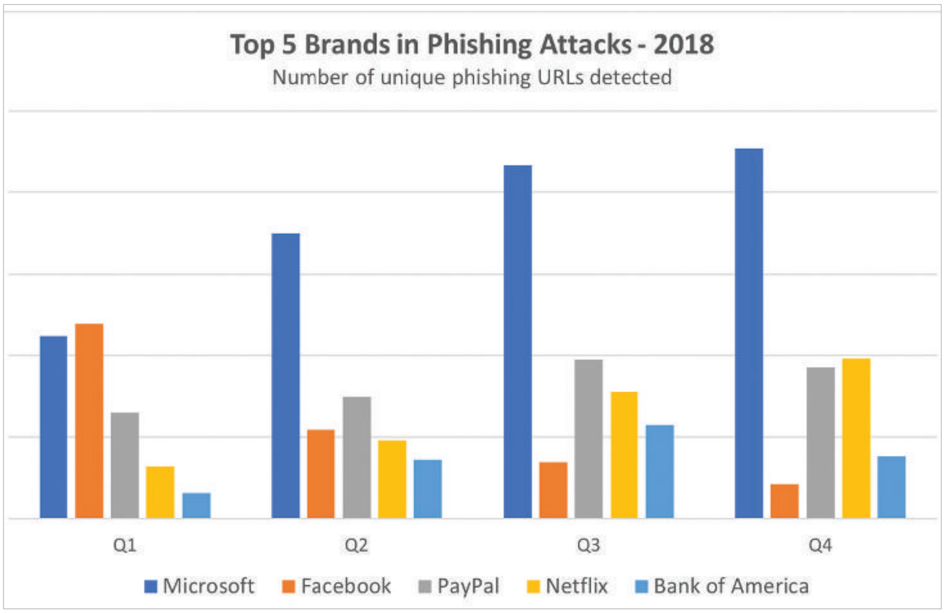
And it is not just Office 365 or Google that are at risk; all email users are subject to dynamic email threats. Nor does company size matter. It is often thought that small businesses were too small to be much of a target for spear phishing. Not so. These businesses are prime targets for a variety of reasons. Not only do SMBs have email contacts and vendors lists that cybercriminals can leverage to escalate and expand their attacks, they also can be targets for small-dollar thefts. Also, small businesses typically lack the resources or have in-house knowledge to spot BECs, for example, making them prime targets.

At KVC, Nyberg says he has seen small attacks where scammers spoofed the email of an executive and then asked a field office to buy some iTunes gift cards. The scammer then asks that, since they are away from the office, if the employee could just send them the cards’ ID numbers. That’s the end of it. The attackers net a few hundred dollars in iTunes gift card numbers.

“When you’re talking worldwide actors ... what they make in a day or week or a month [is very little], it might be worth it,” says Nyberg. “If somebody’s making $5 a day and can knock off $300 in gift cards, that’s a big day. I don’t think there’s a target that’s too small anymore.”

What makes even these small-time attacks so hard to stop is the vast array of techniques attackers deploy to defeat email filters. Here are just a few:

- They hack vendor and partner systems and then work their way into the primary target posing as someone from that organization
- They use white letters on a white background or zero-font print to fool email filters into thinking the content is unique, even though the human readable text (the socially engineered phishing language) is nearly identical email to email
- They target individuals and then cyberstalk them via social media so they strike at just the right moment with a BEC attack



Vade Secure’s in-house research identified the top five phishing URLs. Of note is that Office 365 has replaced PayPal as the number one target for phishing attacks.

“Dynamic threats exist because of one reason: The email protection market relies on just two technologies – fingerprint and reputation.”

– Adrien Gendre, chief solution architect, Vade Secure

- They embed scripts into pictures (called a “stegosploit”)
- They short-circuit two-factor authentication by creating phishing pages that actually pass the user through to the real webpage once they have entered their credentials so the user is none the wiser
- They insert legitimate URLs into emails that are actually “time-bombed” so once email passes the filter it redirects the URL to a phishing website

Some of these approaches are new, some tried and true. The only sure thing is these exploits will continue to evolve.

Countering dynamic threats

“Dynamic threats exist because of one reason: The email protection market relies on just two technologies — fingerprint and reputation,” says, Adrien Gendre, Vade chief solution architect. “These are reactive technologies.”

Vade takes a layered approach to email security by first developing an overall sense of the user, he says. Proprietary processes match the style and technical indicators of each email someone sends to their profile. Behavioral analysis examines everything from file names and header fingerprints to the code and commands embedded in attachments.

To counter the ever-evolving, polymorphic threats, organizations need to employ a multi-layered approach that identifies and blocks unknown threats — even the ones that originate from inside an organization — before they reach the users’ inboxes.

No preventative technology is 100 percent effective; the next layer allows IT systems administrators to remove malicious emails using automation.

Cybersecurity threats are evolving daily. Cybercriminals, often working for organized crime syndicates, constantly evolve their technology and their tactics to bypass defenses. To them, this is easy money — an almost victimless crime that is certainly a whole lot safer than shaking down business owners or robbing banks.

Because criminals will not stop, better technology to detect unknown targeted threats, combined with tools and processes for dealing with threats that slip through, are essential. Both technologies leverage AI and thus have a greater chance to quash an attack than less robust and flexible technologies.■

Vade Secure
Predictive Email Defense

Vade Secure helps SMBs, enterprises, ISPs and OEMs protect their users from advanced cyberthreats, such as phishing, spear phishing, malware, and ransomware. The company's predictive email defense solutions leverage artificial intelligence, fed by data from 600 million mailboxes, to block targeted threats and new attacks from the first wave. In addition, real-time threat detection capabilities enable SOCs to instantly identify new threats and orchestrate coordinated responses. Vade Secure's technology is available as a native, API-based offering for Office 365; as cloud-based solutions; or as lightweight, extensible APIs for enterprise SOCs.

For more information, visit www.VadeSecure.com and follow the company on Twitter @VadeSecure.

Vade Secure
Predictive Email Defense

FROM INBOX ZERO TO INBOX HERO.

Protect your Office 365 users with AI-based predictive email defense

No MX changes, invisible to hackers

Detect unknown, targeted attacks

Block phishing, BEC, insider threats

Vade keeps 600 million users worldwide safe

www.vadesecure.com