Pro

The evolving threat landscape: Staying ahead of phishing attack trends

News By Jack Chapman published August 19, 2024

Key phishing trends to look out for in 2024

(Image Credit: TheDigitalArtist / Pixabay) (Image credit: Pixabay)

Email security is on cybersecurity leaders' minds. 95% of CISOs are stressed about it, and with 94% of organizations experiencing incidents in the past year, it's well justified. Phishing (predictably) tops the list of CISOs' concerns, with email giving cybercriminals a direct line to every employee.

Additionally, phishing isn't a static threat: it can't be patched away like a software vulnerability and, in an ever-evolving threat landscape, CISOs have struggled to determine who the next target will be, what threats will evade their existing defenses, and how and why they're being targeted. Gone are the days of effectively managing phishing through blocklists and telling people to look out for awful typos and complicated sender email domains; cybercriminal gangs now use an arsenal of techniques and technologies to improve their success rates in bypassing both the technical and human layers.

Jack Chapman

VP of Threat Intelligence at Egress.

Key phishing trends to look out for in 2024

In 2023, cybersecurity teams worldwide witnessed a staggering increase in QR code phishing, known as "quishing," which rapidly climbed up the list of their primary concerns. These attacks were not only prolific but also highly effective, demonstrating how cybercriminals can deftly exploit new technologies and consumer complacency at scale. In 2021 and 2022, QR code payloads in phishing emails accounted for a mere 0.8% and 1.4% of attacks, respectively. By 2023, this figure had surged to 12.4%, and it continued at 10.8% in Spring 2024. This quishing boom is anticipated to persist until most organizations implement robust defenses against this type of attack, reducing cybercriminals' returns and forcing them to utilize other tactics.

There has also been a noticeable rise in attacks that do not contain traditional payloads (such as malware attachments or hyperlinks to phishing websites) but instead rely solely on social engineering. These attacks play on the mind, manipulating emotions and engaging in deception to get victims to give up passwords, financial data, and other valuable information. 'Payloadless' social engineering attacks have increased in popularity from 5.4% in 2021 to 17.3% for the first quarter of 2024, while the use of attachment-based payloads has decreased, falling from 72.7% of detected attacks to 35.7%.

The explosion of AI we've seen in the last 18 months has made creating social engineering attacks far easier, with generative AI chatbots crafting convincing messages with a single prompt. The Egress 2024 Email Security Risk Report found that 63% of cybersecurity leaders are concerned about the use of deepfakes in cyberattacks, while 61% are worried about cybercriminals leveraging generative AI chatbots to enhance their phishing campaigns. As well as an increase in social engineering text-based attacks, 2024 has also seen a rise in the use of Zoom as the second step in multi-channel attacks. Starting with an email invitation, targets then join a video call with deepfakes of their bosses, board members, or other known contacts.

In addition to creating deepfakes and phishing emails, AI can also be used to conduct reconnaissance on targets, personalize attacks, and even automate entire phishing campaigns.

Impersonation is a frequently used social engineering technique within phishing emails, with cybercriminals aiming to hijack the trusted relationships between consumers and brands, colleagues, suppliers and customers. In the first quarter of 2024, one-fifth of attacks involved impersonation, with 77.2% masquerading as well-known brands such as DocuSign and Microsoft.

Finally, highly evasive HTML smuggling attacks are also on the increase, with cybercriminals 'hiding' an encoded malicious script with an HTML attachment, with the payload assembled postdelivery.

Enhancing defenses in an evolving threat landscape

Cybercriminals only evolve their phishing attacks for one reason: to increase their success rate. They need their attacks to get through existing detection and to be convincing enough for their targets to fall victim.

One thing all the trends mentioned above have in common: they have been developed to bypass the detection capability present in secure email gateways and email platforms' native defences. While these defenses are effective at filtering out 'known bad' attacks sent from highly suspicious domains and with previously identified malware payloads, attacks such as those that only contain text or seemingly benign HTML attachments will get through.

Consequently, organizations need to fight fire with fire and implement newer AI-powered technologies that can detect a broader range of threats.

Using AI to detect AI-enabled (and other!) phishing attacks

Integrated cloud email security (ICES) solutions are cloud-based and detect anomalies in inbound emails by combining APIs with advanced AI techniques, including natural language understanding (NLU), natural language processing (NLP), and image recognition. ICES solutions also detect obfuscation techniques, behavioral anomalies through heuristic detection, and compromised internal accounts.

An ICES solution layers on top of an email platform's native defenses and even secure email gateways (although, given the overlap in functionality between native defenses and SEGs, Gartner predicts the combination of native defenses plus ICES will replace native plus SEG). While native defenses are designed to perform email hygiene tasks and detect known threats, ICES are organizations' best defense against the increasing number of zero-day, evolving, and highly evasive attacks they're being targeted with.

Automating inspection of employee-reported phishing emails to elevate threat-hunting

capability

Abuse mailboxes have been a standard part of anti-phishing defenses for years, providing employees with a mechanism to report 'abusive' emails (whether spam, phishing, or other), and a way for security analysts to triage them.

They've also become incredibly noisy, which negatively impacts their value. More phishing attacks and spam are getting through traditional detection and filtering systems, so people are generally reporting more. There's also a high margin of error when people report emails: on average, 85% are false positives.

Traditional abuse mailboxes require manual review, with a security analyst investigating each reported email in turn. This is a significant drain on analysts' time and can severely limit their threat-hunting capability. Even when real threats are found, administrators can spend up to 30 minutes investigating and remediating the threat by coding PowerShell scripts, another manual task which is also proven to be unreliable with polymorphic attacks and evolving phishing campaigns.

AI-powered abuse-mailbox functionality can be delivered as part of an ICES solution to automate the inspection of all reported emails and the remediation of phishing threats, including subsequent emails within an ongoing campaign and polymorphic attacks. This can cut analyst investigation time by 98%, significantly reducing response times and enhancing detection accuracy.

Additionally, centralized threat intelligence and complete visibility enable security teams to quickly understand threats across the organization, as well as give them the opportunity to manually review all automated processes.

Personalized security to empower the human element

Personalized security that adapts to each employee's behavior and the changing threats they face is always going to be more effective than one-size-fits-all. This includes both technical controls and the training someone receives.

This approach requires aggregating data from across an organization's cybersecurity ecosystem – something cybersecurity vendors have traditionally not been very good at enabling. We also produce behavioral analytics, threat feeds, and product telemetry, but we tend to keep them siloed in our systems. Each dashboard provides its source of truth – and security analysts are left with fragmented views, a lack of visibility, and the, again, manual task of piecing together holistic insights.

However, through native bidirectional APIs, cybersecurity products can share data and intelligence, with a single dashboard offering deep, hyper-accurate insight into human risk. By aggregating data from multiple sources, organizations benefit from instant visibility that far exceeds what's on offer from independent systems.

This data can also be used to dynamically adapt security controls across each integrated product, automatically tightening them if risk increases with changes in the threat landscape or an individual's behavior. It can also be used to ensure people are better prepared for the real threats they face.

The Egress 2024 Email Security Risk Report found that 100% of organisations carry out security awareness training (SAT), however very few (only 9%) tailors it to each employee. Three-quarters (74%) use the default out-of-the-box programs or tailor them to their organization as a whole; only 19% deliver SAT that reflects the department or team someone works in.

SAT is most effective when it is relevant and timely, enabling employees to easily recall what they've learned. If, for example, an employee has suddenly started receiving an influx of impersonation-based phishing attacks, they will be best prepared if they've sitting training modules on these types of attacks.

By sharing insights from email threat intelligence with an SAT platform, it's possible to auto-enroll employees in the most relevant training programs and phishing simulations, automatically adapting to give them the best defense in their personal threat landscape.

It's time to adapt

The old ways aren't enough in today's threat landscape. Cybercriminals don't sit still: when one attack type or payload fails to yield the expected

returns, they move on to the next. With advancements in AI and a booming crime-as-a-service ecosystem, this evolution is easier than ever.

To work in cybersecurity, therefore, means a never-ending battle. But just as the tools and technologies that cybercriminals have at their disposal have changed, so have ours, especially regarding human risk management and email security. By improving defenses and efficiency through the ways listed in this article, cybersecurity teams can adapt to changes in the threat landscape and stay one step ahead of the hackers targeting their organizations.

We've featured the best business VPN.

This article was produced as part of TechRadarPro's Expert Insights channel where we feature the best and brightest minds in the technology industry today. The views expressed here are those of the author and are not necessarily those of TechRadarPro or Future plc. If you are interested in contributing find out more here: https://www.techradar.com/news/submit-your-story-to-techradar-pro

---

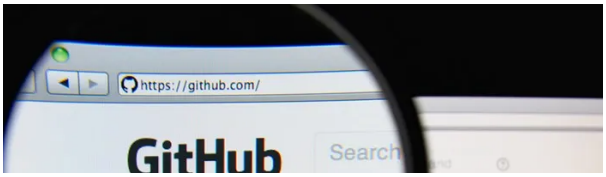
Jack Chapman

Jack Chapman, VP of Threat Intelligence, Egress.

TOPICS

MALWARE

LATEST ARTICLES



1 **GitHub Enterprise Server has a critical security flaw, so patch now**

2 **Get one of the best party**

speakers around at its lowest ever price

3 **'We're working on it': The Rings of Power season 3 hasn't been confirmed yet, but the Prime Video show's creators have an update on its development**

4 **iCloud is now way more popular than Apple TV Plus and Apple Music – here's why that's controversial**

5 **New Mint Mobile deal gets you five lines for the price of one**