ANALYST BRIEF
Sponsored by: IRONSCALES

Phishing attacks are a continuing challenge for security teams. Attacks are overwhelming in number and constantly changing. Even with AI tools to help, organizations need to share the responsibility of security with their users.

Email-Based Attacks Require Human-Augmented AI Security

August 2022

Written by: Jennifer Glenn, Research Director

Introduction

Phishing continues to present a significant cybersecurity challenge to the modern enterprise. This is due in part to the fact that email — and more specifically email addresses — is a pervasive identifier across the business. Email addresses are often used as usernames and other methods of authentication to access critical applications and resources. For would-be attackers, email addresses provide a broad attack surface and multiple vectors for infiltrating the organization, including phishing, business email compromise, and credential theft.

Traditional email security solutions, such as secure email gateways (SEGs), are often the first line of defense against the onslaught of attacks. They can find and stop a good portion of the known phishing attacks. However, most of these technologies are signature based, which means attacks must get through an organization's defenses, be investigated/analyzed, and then be reverse engineered into signatures that are then pushed out to the machines. The problem is that a huge volume of "unknown" attacks can still potentially bypass an organization's defenses.

While the volume of unknown attacks is one problem to contend with, another — perhaps more challenging — issue is keeping up with attack trends. As previously highlighted, a broad surface area with multiple options for compromise means attackers can continuously change their methods to avoid detection. Social engineering ploys combined with business email compromise are becoming common. These emails appear to be from a supervisor or trusted source asking for money to be transferred or gift cards to be purchased. There are no links or attachments to trigger the defenses — only text and intent. It is much harder to detect and discern attacks in these scenarios. As a result, security teams are still spending a significant amount of time investigating and addressing these types of attacks.

Benefits and Considerations

No email security solution can eliminate threats entirely, but a modern email security platform can significantly reduce the amount of time and resources that security teams are devoting to investigating phishing and email-borne attacks. To better manage these advanced types of attacks, many email security organizations are incorporating artificial intelligence (AI) and machine learning (ML) into their technologies. Adding AI can help alleviate some of the burdens of investigating phishing attacks — but it's not a foolproof approach. Just like attackers rely on the human element to advance their attacks, defenders must also rely on human augmentation to improve their email security initiatives.

Organizations should consider an email security solution that offers the following capabilities:

- **Security awareness training.** Security awareness training includes instructional videos, documents, and random test emails that aim to educate users on what phishing emails look like and how to spot them. Security awareness is intended to assist the security team by putting some of the responsibility for protecting the organizations into the hands of the users, helping them identify potential threats or even risky behaviors. This is an important component of an email security solution as email is one of the most user-centric technologies.
- **Crowdsourced intelligence.** The next logical step in adding the human element to attack prevention is making it easy for users to report what they see. Self-service reporting offers two benefits. It helps users apply what they've learned in training while relieving some of the burden from the security team. However, it also serves as a "risk alarm" when combined with the intelligence and context from other users submitting similar information.
- **Behavior-based anomaly detection.** While slightly different from the previously mentioned components, behavior-based anomaly detection is inherently about human behavior and spotting activities or wording that is out of character, out of line, or simply not typical. It is essential not only for training AI to spot these eccentricities but also for identifying social engineering attempts and those harder-to-spot attacks that rely on malicious content.

Organizations looking at email security platforms should also consider other adjacent technologies that are used in tandem with, or in place of, email, such as collaboration platforms (e.g., Microsoft Teams, Slack) as well as project management tools with collaboration (e.g., Trello, Jira). Often these tools integrate with email and can be exposed to the same types of attacks, so they need to be included in the overall initiative.

Conclusion

Digital transformation and hybrid work are changing the enterprise landscape for the better. While the benefits are clear — productivity gains, better innovation, and improved efficiencies — these changes are also increasing the number of access points that need to be managed and secured. To be effective in reducing the impact of cyberincidents, security teams will need to offload/share some of that security responsibility.

In many cases, ML and AI technologies are used to automate detection and response, but they are not infallible. Human users are the last line of defense against cybercompromise. To shore up the human element of attack prevention, organizations need training and self-service reporting of suspected phishing attempts or other types of attacks, and their AI and other defense tools need to understand how humans act and react in order to function more effectively.

About the Analyst

Jennifer Glenn, *Research Director*

Jennifer Glenn is Research Director for the IDC Security and Trust Group and is responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies such as messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

About IRONSCALES

IRONSCALES' mission is to offer the most powerfully simple email and messaging security and training platform to help make organizations safer, together. For more information, please visit www.ironscales.com today.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com