ESG SHOWCASE

When Humans and Machines Collaborate

Date: April 2022 **Author:** Dave Gruber, Principal Analyst

ABSTRACT: Adversaries have become adept at evading automated email security mechanisms by combining automated machine-driven attacks with an added layer of human-assisted attack intelligence. Combatting this threat requires a new approach—leveling up defenses by enabling machine and human collaboration to overcome the threat. Innovative new solutions are focusing on enabling humans to more seamlessly contribute insights that inform scalable machine defenses to stop attacks.

Overview

Email-borne attacks continue to evade security controls, despite the use of both the native email security controls provided within cloud-based email platforms and the addition of cloud email security supplement solutions. According to a recent ESG survey, 68% of organizations continue to experience email-borne attacks on a regular basis, including phishing, ransomware, and malware.[1]

Unlike other attack vectors, email provides a path for adversaries to highly personalize and diversify email content for individual targets, combining machine and human intelligence—making it extremely difficult for machine-only defenses to keep up. As attackers leverage an almost infinite number of potential impersonation actions, combined with polymorphic phishing tactics, even the most sophisticated machine-only defenses struggle to achieve complete protection. The evolving email threat landscape has resulted in 57% of organizations reporting that they believe email security is in a state of transformation and are therefore planning on reevaluating all available security controls.[2]

Fortunately, new solutions are emerging, combining the most advanced machine-based defenses with human-assisted intelligence in a tightly integrated fashion. These innovative new approaches are enabling hybrid, human/machine collaboration leading to earlier detection and increased prevention of email-borne threats. Combining technology-driven advanced analytics with human insights from users, security analysts, and a broad community of crowd-sourced human intelligence increases the velocity of intelligence-to-prevention, helping defenders keep up with this highly dynamic threat vector.

Why Machine-only Solutions are Struggling

Machine learning (ML) has become foundational to most modern cybersecurity solutions, with 38% of organizations reporting that they think email security providers should be doing more with ML to improve email security.[3] ML models are created based on the discovery of patterns of activity and translated into algorithms that can then further identify and detect variants of patterns. While a powerful tool in cybersecurity, ML models still have limitations. Models are built from

[1] Source: ESG Research Report, *Trends in Email Security*, August 2020.
[2] Ibid.
[3] Source: ESG Survey Results, *Trends in Email Security*, July 2020.

identified patterns that reflect known behaviors or activities that can be analyzed using algorithmic models. This technique enables cybersecurity solutions to identify variants of attack patterns, increasing the scope and breadth of detection.

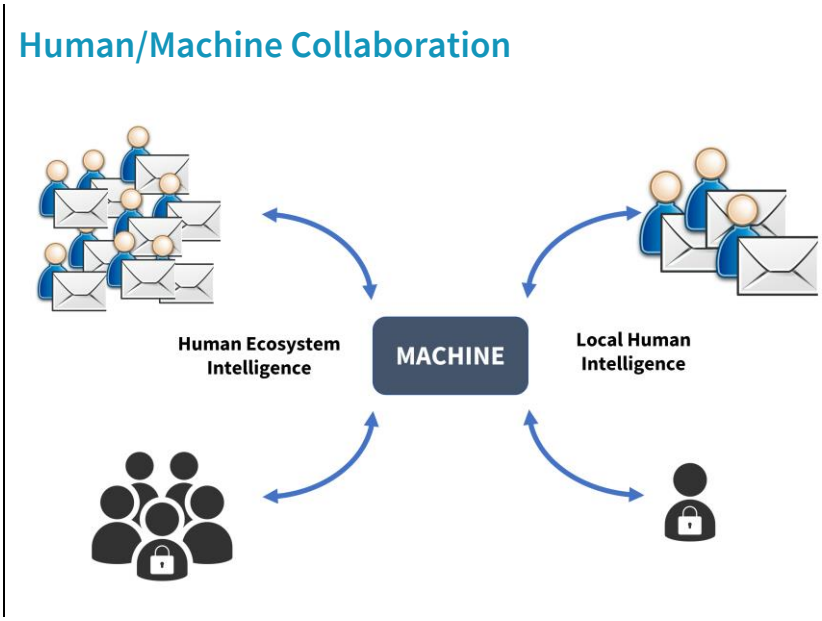
However, highly personalized, socially engineered attacks don't often follow patterns. Adversaries have become extremely adept at evading even the most rigorous, automated, ML-driven prevention tools by targeting specific individuals with fully customized and impersonated content—frequently morphing and constantly utilizing new schemes for enticing target users. While often identifiable by humans, these attack techniques are commonly missed by machine-only defense solutions.

Leveling the Field: When Machines and Humans Work Together

Because phishing, social engineering, and other popular email attack methods often combine the use of both human creativity and technology to compromise systems, building an effective defense utilizing new thinking and approaches that enable humans and machines to collaborate more effectively can increase the effectiveness of defenses.

An organization that can leverage its security staff experts as well as its end-user population—both overtly and with tools that gather additional context from them—can gain an edge. Combining end-user context with the expertise of local security resources increases threat intelligence leading to increased detection. In addition, expanding beyond local end-users and security analysts to a broad ecosystem of solution users further adds intel to defenses.

By bringing this broad, human audience together, an organization can enhance machine detection with continuous human intel to strengthen defenses in near-real time. And by leveraging insights from attacks against hundreds or thousands of other organizations, solutions can gain additional efficacy across the broader community.



This defense model, in which machines and the humans across many organizations work together to more formidably thwart email attacks, is compelling. The starting point is a platform designed from the outset to blend human ingenuity and reason with the speed, algorithms, and huge data sets that machines support. Both are essential to counter the combination of human insight/innovation and technology attackers are using. Specific attention around the automation of engaging the human element is necessary to support collecting, aggregating, analyzing, measuring, and sharing valuable human intelligence with core automated security controls.

Harnessing Human Context and Intellligence

Efficient, purpose-built automation can assist in harnessing intelligence from end-users, security analysts, and the broader ecosystem.

User Intelligence

Email Users Provide Context

Human-assisted, real-time intelligence gathering can inform and strengthen automated machine defenses, while speeding detection and mitigation of emerging threats.

Providing end-users with a simple, easy-to-use mechanism to share context is paramount to engaging this audience. When machines struggle to make definitive decisions on individual emails, banners and other alert techniques can offer users an opportunity to provide additional insights that can help machines make more definitive decisions in the future. In-context interactions within the body of individual emails allow an end-user to call out questionable content, providing additional intelligence supporting machine analytics. This approach can also provide in-context security awareness training, strengthening mindful future decisions. Real-time learnings from user actions can also be cycled back into the broader solution, helping other users and organizations utilizing the same solution improve future detection capabilities.

Security Analysts and Email Administrators

Questionable email content is often escalated to security analysts or email administrators for review and action. Investigation often requires analysts to leverage other systems and information, slowing the time to resolution. Optimizing workflow, providing in-context threat intelligence, and supplying related information to support fast decision-making can reduce administration time spent while speeding resolution. Capturing and recycling intelligence from administrator decisions can further strengthen machine-led decision making.

Optimizing Escalated Emails

When machines fail to definitively make decisions, humans get involved, yet many are overwhelmed by the volume of escalations. Optimizing the investigation and decision process reduces the spread of attacks.

The Broader Ecosystem of Human Intelligence

Crowdsourcing additional inputs and information from other organizations can scale threat information collection so that the effectiveness of cyber-defenses is increased not just for one organization, but for many. When intelligence can be captured and recycled from a broad end-user and administrator audience, the overall effectiveness of the solution increases. Automating the collection and integration of real-time intelligence is the starting point, but also requires a systematic approach to validating input before it is shared with others.

Introducing IRONSCALES, a Self-learning Email Security Platform

IRONSCALES provides an email security platform that is capable of enabling advanced machine analytics to work collectively with users and administrators to strengthen email security efficacy and efficiency. IRONSCALES claims to have architected a solution highly optimized to capture and recycle intelligence from humans in near-real time and apply it to automated machine analysis to strengthen the efficacy of email security for all who use the solution.

The platform combines multiple sources of information and highly automated human/machine interaction to substantially improve protection against phishing and other email-borne threats while helping IT and security professionals work more efficiently. Key features and capabilities of the IRONSCALES email security platform include the following:

- Similar suspicious emails clustered into a single incident enables analysts to remediate clusters of related suspicious emails in a single action.
- AI-powered incident suggestions support faster investigation and remediation.

- **Automatic triage and response to employee-reported emails** reduce investigation time and strengthen protection against future attacks.
- **Auto-remediation of emails already delivered to inboxes** reduces the potential for harm when malicious emails reside in mailboxes.
- **Mobile-native, single-click incident resolution** helps security analysts and administrators work efficiently from anywhere.
- **90-day scan** back at time of integration to find existing threats hiding in mailboxes, reducing future threat.
- **Enterprise training and awareness and simulated phishing scenarios** empower end-users to become a more effective part of the defensive effort.
- **Real-world phishing exploit for actively testing email perimeter defenses with actual threats** provides critical information for the SecOps team.

The Bigger Truth

Email threats are a primary attack vector that is constantly evolving. Attacks combine the newest threat technology coupled with creative human-engineered, human-assisted attack techniques and tactics designed to evade automated controls and deceive email users.

New approaches to email security combine machine and human intelligence to level-up with the adversary. ESG recommends IT and security teams explore innovative email security solutions from vendors such as IRONSCALES to address ongoing email security challenges.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188