IronSights

Advanced Protection Against Business Email Compromise (BEC)

Overview

Organizations around the world now face unprecedented challenges preventing, detecting and responding to modern and more sophisticated phishing attacks, such as business email compromise (BEC) and sender impersonation. Standards like DMARC are not well adopted since they very hard to implement and are effective only against specific types of phishing attacks such as exact domain spoofing.

With more than 500 businesses being targeted per day by BEC attacks, what can businesses do to protect their inboxes from this increasing threat vector?

IronSights an Advanced Mailbox-level Anomaly Detection takes a “bottom-up approach,” using machine learning algorithms in the mailbox itself to create a fingerprint in conjunction with common past communication habits and trusted relationships to proactively combat impersonation and spoofing emails in real-time.

Key Business Benefits

1.

Prevent email spoofing and impersonation emails, such as display name and domain look-alikes in real-time.

2.

Reduce risk of financial loss from business email compromise (BEC) attacks.

3.

Assist busy and unsuspecting employees at recognizing and reporting phishing attempts through InMail banner alerts.

The Need for Advanced Email Authentication

The email protocol was not designed with security in mind, and there is no authentication mechanism in place whatsoever.
However pseudo-authentication is now possible using ‘sender fingerprinting’, an advanced machine learning based technology that can identify the true identity of a sender. This technology was designed and built to answer a simple, yet very complicated question:

Who is sending me what?

- The “Who” equates to the real identity of the sender
- The “What” stands for the content and the context of this communication

How Does IronSights Protect Against BEC?

IronSights is an Advanced Mailbox-level Anomaly Detection module that protects company's employees from business email compromise (BEC), email spoofing and impersonations attempts by dynamically learning their mailbox and communication habits.
IronSights fingerprinting technology takes into account factors like implementation level (no/full/partial) of DMARC/SPF/DKIM, sending IPs, normal communication context and others in order to create a unique fingerprint for each sender, any deviation from the norm will be detected immediately.
Using machine learning algorithms, IronSights also continuously studies every employee's inbox to detect anomalies based on both email data and metadata extracted from previously trusted communications.

Why IronSights

- Advanced Protection against impersonation and spoofing
- Identify and prevent against BEC attempts and email phishing messages with or without active payloads
- Harden existing email spoofing protection and impersonation detection that DMARC and secure email gateways cannot provide
- Improve trust and confidence in end users while reducing business disruption

Features

- Sender fingerprinting
- Advanced mapping of trusted external and internal senders
- Inbox behavioral analysis
- InMail banner alerts to flag anomalies in the mailbox

Deployment

IronSights is available as a quick and easy two-click deployment for Office365 and G Suite in the cloud, on premise, or hybrid, with no MX records changes required.

Other Products

IronShield

IronTraps

Themis

IronSights

Federation

IronSchool

IRONSCALES

For more information
visit our website at www.ironscales.com
and follow @ironscales on Twitter
Contact us at contact@ironscales.com

Headquartered in Tel Aviv, Israel, IRONSCALES was incubated in the 8200 EISP, the top program for cyber security ventures, founded by Alumni, the Israel Defense Forces' elite intelligence technology unit.