COFENSE VALIDATOR™

Cofense Validator Case Study

Retailer Reduces Malicious Emails in Inboxes by 10% Through Optimization of Email Security

Industry: Retail – Electronics & Building Material | Organization Size: 27,000

PROBLEM

Large investments were being made in email security controls but results seemed underwhelming and significant threats were still landing in the inbox.

SOLUTION

Cofense Validator showed the efficacy of multiple configurations, leaving this retailer with clear insight into which was the right choice for them.

RESULTS

Adjustments to email security controls resulted in a 10% decrease in reported malicious email in the month immediately following the configuration changes.

PROBLEM

This retail organization was making significant investments in security yet underwhelmed at the performance of the email security controls they had in place. They needed to optimize the configuration of these controls to ensure less threats were making it through the perimeter and into the inbox of their end user employees.

SOLUTION

In partnership with this retailer's CISO, the Cofense team immediately got to work with the goal of understanding how the existing security solutions can provide a better security posture without adding budget. The technologies involved included Microsoft EOP (Exchange Online Protection) and Cisco IronPort.

Using Cofense Validator, four email accounts were set up with identical security configurations as what an employee of the retailer would have. One account would be used for each configuration profile being tested. The validation ran for a period of 3 weeks. As the name alludes, each configuration profile represents a different potential scenario for how the email security controls could be configured. A benefit of running these configurations through Cofense Validator is that you're sending the same exact content to each - enabling a true side-by-side comparison.

(cont.)

Using real, active threats identified by Cofense Intelligence, Validator sent malicious indicators to the mailbox where they were either blocked or successfully bypassed controls. For each threat that bypassed the retailer's email defense stack, Cofense Active Threat Reports were sent to their security team detailing corresponding information to help with future defense.

With the output from Validator the team was able to analyze the performance of each configuration profile to determine which was more successful in blocking the phish. This enabled this organization to make clear, data-backed decisions on configuration best practices.

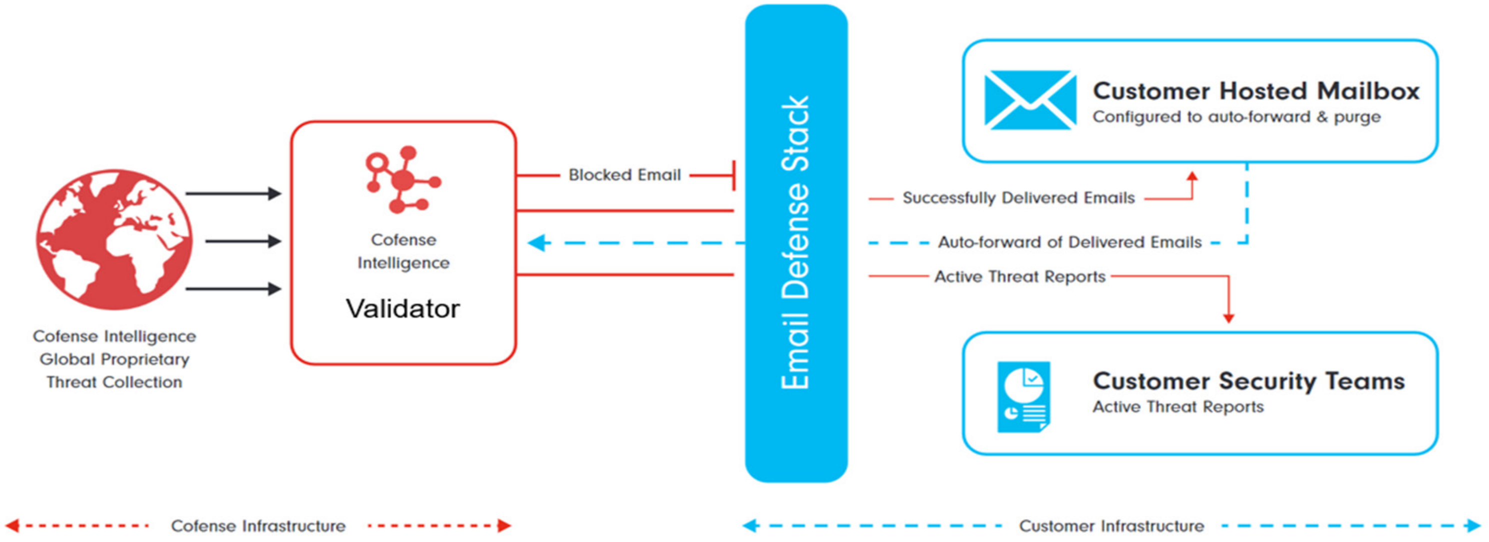

Figure 1: The above workflow illustrates the process between Cofense Validator and the customer's infrastructure. Over a period of 3 weeks, this easy to deploy solution enabled configuration changes that reduced the risk of phishing emails to this retailer.

RESULTS

Prior to sending any malicious indicators, Validator sends a series of baseline tests of benign file types to assess the basic configuration of each profile. Initial baseline results showed VBA and JNLP filetypes (among others) made it to the mailbox despite the belief that these should not have allowed based on current state configuration settings.

Cofense helped this organization discover that Cisco IronPort IPs were on the allowed list inside of Microsoft EOP configuration on the retailer's side. In other words, Microsoft was most likely not scanning emails that first came through Cisco IronPort. And given the mail flow for almost all Configuration Profiles originated with IronPort, this enabled these to work with both Cisco IronPort and Microsoft on a workaround. So, by the end of the engagement, Microsoft was in fact scanning emails in addition to Cisco IronPort.

Overall, as Figure 2 depicts, **this retailer saw a 10% dip in malicious emails reported after Cofense Validator clearly showed which configuration changes would provide the best results.**

(cont.)

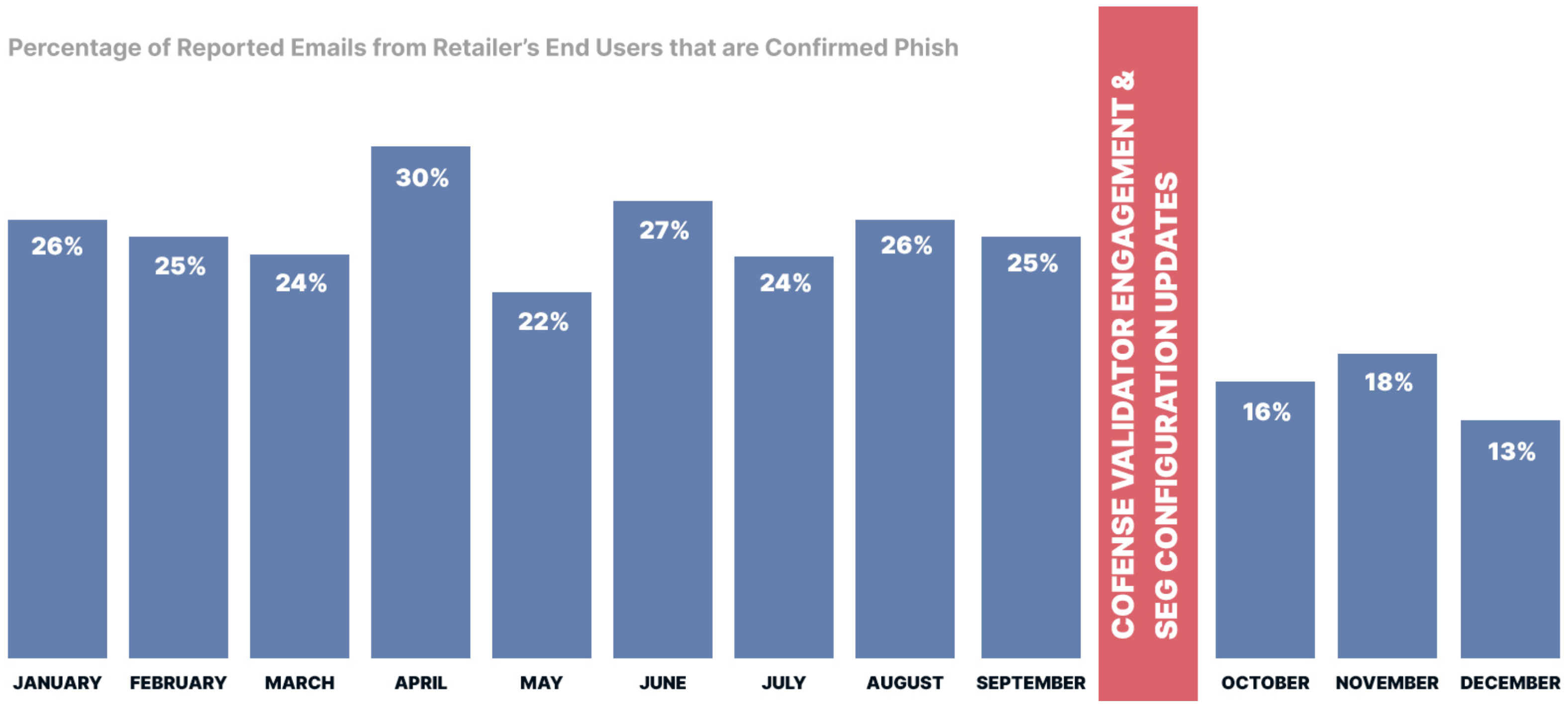

Figure 2: Prior to making configuration changes to their email security controls, this retailer regularly saw around 25-30% of their reported emails were confirmed malicious. Immediately after updating the configuration post-Validator engagement, there was a 10% drop to 15.8% confirmed malicious showing immediate impact to overall email security posture.

WHAT'S NEXT

Many malicious phishing campaigns that made it to the inbox landed in the Junk folder. But even so, given end users can interact with emails in the Junk box (and often do), the same risk can be assumed as if the attack landed in the inbox. This organization will investigate improving the Junk box rules for this purpose and a planned follow-up Validator engagement will help to confirm configuration changes made as an outcome of the first engagement.

Most of the malicious phishing campaigns that made it to the inbox were credential phishing attacks, that are difficult for email security controls to stop at the gateway. The threats that Validator showed made it to the inbox would have otherwise been automatically found and quarantined if Cofense Vision were in place at this organization. By layering in Cofense Vision, the threats sent from Cofense Intelligence that made it to the inbox would have been auto quarantined from inboxes without intervention from the internal IT/mail/security teams. This organization is currently exploring implementing Cofense Vision to help them become more efficient and lead to an even stronger security posture.

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of close to 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175