





STOPPING PHISHING ATTACKS WITH RAPID SEARCH AND QUARANTINE



BUSINESS CHALLENGE

Despite the latest in Secure Email Gateways (SEGs), phishing attacks are still reaching inboxes, putting organizations at risk. While well-trained users will report a phishing attack, others won't. Unreported phish represent a risk of compromise waiting to happen.

SOLUTION BENEFITS

-  Uncover the totality of a phishing campaign across the entire messaging environment, leveraging available threat intelligence
-  Quickly quarantine suspicious emails across the entire email environment
-  Rapidly restore emails in the event of a false positive
-  Maintain privacy while enabling threat hunting



WHY SOC ANALYSTS NEED PHISH MITIGATION TOOLS

All nets have holes. Phishing threat actors are constantly evolving their attacks to bypass perimeter controls, including (SEGs). Once a phish is delivered, time is of the essence, as the first user is likely to click in 16 minutes, while an organization's best reporter will notify the phishing defense team 12 minutes later¹. Security analysts need to find Indicators of Phishing before malware can take hold or credentials are harvested.

PHISHING ATTACKS ARE HUMAN ATTACKS

Data breaches are increasingly occurring due to social attacks on humans, with 90% of these attacks coming from phishing¹. These breaches, on average, can cost an organization close to \$4M². The very nature of these attacks requires tools specifically designed to empower humans to find and mitigate these threats, quickly, efficiently, and reliably.

UNREPORTED PHISH ARE UNDETECTED THREATS

Even if an organization has an excellent culture of reporting, some phishing emails will make it to inboxes and lie there, unopened. As reports of a phishing attack come in, security analysts need the ability to find and respond to these silent threats before they are acted upon by unsuspecting users.



COFENSE VISION™

Cofense Vision provides rapid search, quarantine, and restore of phishing threats across the entire messaging environment. Using flexible queries, analysts can find even the most complex morphing phishing attacks in seconds. And, when seconds count, analysts can quarantine suspicious emails knowing that transparent restores are just a mouse-click away.

BENEFITS OF COFENSE VISION



POWERFUL SEARCH

Cofense Vision stores a copy of every email received in an off-line database designed for phish hunting. Instead of being limited to the basic search capabilities of Microsoft Exchange, Vision lets analysts search by any Indicators of Phishing, including attachment hashes and partial URLs. And integration with Cofense Triage™, our premiere phish threat analysis platform, lets analysts go from report to search in seconds.



RAPID QUARANTINE

Once the totality of a phishing attack is discovered, Cofense Vision enables an analyst to quarantine all instances of the attack across any number of connected Microsoft Exchange systems. Quarantine happens in seconds, all with a single mouse-click.



ONE-CLICK RESTORE

When an attack is suspected, analysts need to know they can take protective actions immediately while they research the threat. Cofense Vision lets an analyst restore any quarantined emails in seconds in a manner completely transparent to the user.



PRIVACY ENABLED

An organization's email communications often contain sensitive information, including data protected by privacy regulations. Cofense Vision provides detailed auditing of all search, quarantine, and restore activities. Also, analysts are not required to have high privilege access to the messaging environment to perform their duties.

¹ 2018 Verizon Data Breach Investigation Report

² \$3.92M - 2019 Ponemon Cost of Data Breach Report

