PRE-EMPTIVE PHISHING MANAGEMENT

Phishing scams take advantage of lapses in security awareness. They masquerade as familiar and reliable sources to convince victims that their messages are legitimate, deceive them into providing confidential and financial information, or persuade them into clicking on a link that downloads malicious software to infect their systems. Once the attempt succeeds, the attackers have an entry point into the network.

Given the steady rise and sophistication of phishing attacks, many organizations use different threat detection techniques to mitigate the risks posed by these attacks. While anti-phishing solutions filter a bulk of these attempts, they rely on known signatures to identify malicious emails. The ThreatDefend® Platform offers several capabilities that security teams can implement to submit suspicious emails for analysis and prompt reporting without having to depend on signatures.

THE GROWING PHISHING CONCERN

Phishing can give the attacker the "insider" access they need to accomplish their ultimate objective. The attacker sends emails that appear to come from trusted sources, often someone with authority seemingly within the organization itself, to trick the recipient into clicking on a malicious link or revealing sensitive information. An attacker may pretend to be one of the organization's network administrators and send an email to an employee, prompting them to log into a site to validate something. If they click on the link, the attacker can download malware onto the device, giving continued access to the organization's internal network and stealing credentials for reuse.

A Business Email Compromise (BEC) attack is a form of phishing where an attacker poses as an executive in a company (usually the CEO) and attempts to deceive employees, partners, customers, or vendors into disclosing sensitive data or, worse, transferring funds into an account.

CASE STUDY:

Criminal posing as an auditor steals money from a commodities trader.

The corporate controller received emails that appeared to come from the company's outside auditing firm with requests for wire transfers totaling $17.2 million. The initial email requested a wire transfer of $780,000, the following day for $7 million, and three days later, a final request for $94 million. The initial emails include language focusing on secrecy, urgency, and sensitivity, including:

"I need you to take care of this. For the last few months we have been working, in coordination and under the supervision of the SEC, on acquiring a Chinese company. This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations."

The controller called the auditor to confirm, using the phone number provided in the email. The criminal was ready with a person posing as an auditing firm employee to verify the requests. There was also an element of consistency between the wire requests and the company's business plans. The company had discussed the expansion into China, and they were in the middle of an audit. These factors put the wire requests and the need for sensitivity and secrecy in line with company business plans.

Combatting Phishing is Not a "Check Box" Security Item

Organizations often employ a combination of tactics to try to mitigate the risks posed by phishing. It typically starts with educating employees and implementing best practices around properly using email and not clicking on embedded (web/file) links. They also frequently use URL filters, IP blacklists, and reputation feeds to prevent connections to or from sites known as sources of attacks, including phishing.

These solutions certainly help reduce infection rates and minimize the attack noise. However, given the sheer volume of users, devices, and sites that organizations deal with, there is no way to lock emails down and prevent phishing completely. As a result, organizations must assume that phishing emails will get through and ensure they have the appropriate tools in place to monitor and identify phishing activity, which the Attivo Networks ThreatDefend® platform complements.

ATTIVO NETWORKS FOR PHISHING ANALYSIS

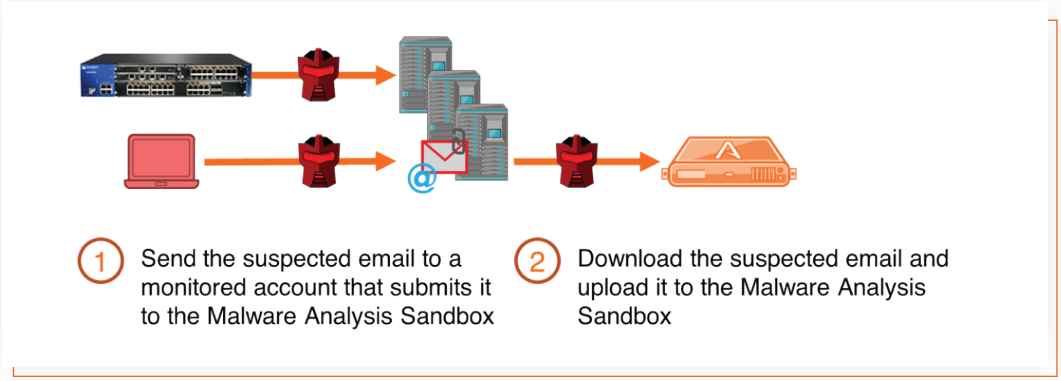
To mitigate the risks posed by phishing, organizations can leverage the Attivo Networks ThreatDefend® platform to complement their existing security processes and controls for phishing detection and analysis. The ThreatDefend® Platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform's components include the BOTsink® deception server, the Endpoint Detection Net Suite™, and ADSecure™ for Active Directory protection.

The BOTsink® server includes a function that converts one of the engagement servers into a Malware Analysis Sandbox (MAS). The MAS provides a portal for security teams to upload suspicious files for analysis, but it can also analyze suspicious emails, including their attachments and embedded links.

- Users can submit suspicious emails directly to the BOTsink® MAS through a simple-to-deploy Outlook plugin that forwards suspicious emails to a dedicated phishing email account the BOTsink® server monitors.

- Once the user submits the email, the MAS executes any attachments and follows any links to download the files for execution and analysis.

- The solution also provides analysis reports on network connections, registry access, processes, file activities, disk writes, payload drops, and other activities. It captures screenshots as the attachments and payloads execute, so organizations gain a greater understanding of the threats they face.



Post-Phishing Threat Detection

If a phishing attack is successful, the attackers needs to break out from that system to infiltrate the rest of the environment. To do this, they steal locally stored credentials, query Active Directory (AD) for sensitive or privileged accounts and object, conduct reconnaissance activities to map the network looking for assets to compromise, and then move laterally. The ThreatDefend® platform denies, detects, and derails these activities with its deception and concealment capabilities.

The Attivo Endpoint Detection Net™ (EDN) Suite anticipates methods attackers will use to break out from infected endpoints and ambushes their every move with deceptive lures, bait, and misdirections. EDN complements existing endpoint security solutions by closing detection gaps and identifying attackers early so that they cannot further infiltrate the network. It does this by hiding and denying access to critical files and data to detect and prevent discovery, lateral movement, and privilege escalation activity, and finds attack paths that adversaries can use to move between systems.

The EDN Deflect function alerts on attacker reconnaissance as they scan for ports and services on systems to exploit and redirects both inbound and outbound connection attempts to decoys for engagement. The EDN Deflect function makes every endpoint a part of the deception fabric, obfuscating what they look like from the network

to disrupt attackers attempting to move laterally. The EDN Deflect function enables native isolation of infected systems to limit their communications to the decoy environment, thus limiting the damage they can do by quarantining them away from production systems.

With the Attivo Networks ADSecure™ solution, organizations gain AD security without interfering with production Domain Controllers. The solution identifies unauthorized AD queries and returns fake object information to misdirect attackers into a decoy environment. The mere act of attacker observation triggers an alert on unauthorized activity, while the deceptive objects serve to disrupt automated attack tools. Additionally, the solution gathers Tactics, Techniques, and Procedures (TTPs) and company-specific threat intelligence to accelerate incident response.

The Attivo BOTsink® solution provides a comprehensive network-based defense for accurate alerting of threats in on-premises, cloud, remote, and OT environments. Deceptive systems that appear identical to production devices and decoy documents provide early detection of in-network threats. A high-interaction environment safely collects adversary intelligence and automates analysis and incident response. Machine-learning makes deployment and operations simple and scalable. Over 30 native integrations automate isolation, blocking, and threat hunting.

CONCLUSION

There appears to be a never-ending battle against phishing attacks and, despite comprehensive education programs, employees still make mistakes and click or download when they shouldn't. The Attivo ThreatDefend® Platform improves efficiency in submitting and analyzing suspicious emails, significantly reducing the time and resources necessary to identify and stop them. Additionally, if a phishing attempt succeeds, the ThreatDefend® Platform turns the entire network into a maze that tricks attackers into revealing themselves while denying discovery, lateral movement, privilege escalation, and data-gathering activities. Organizations that deploy the ThreatDefend® platform gain pre-emptive and post-compromise defenses against phishing attacks, elevating their security posture, increasing efficiencies, and mitigating lapses that lead to phishing compromises.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides innovative cyber deception and attack lateral movement detection solutions for combatting today's advanced threats and ransomware attacks. Delivering a superior defense for revealing and preventing insider and external threat activity, the Attivo ThreatDefend® Deception Platform offers scalable protection, detection, and data concealment and access denial solutions for endpoints, Active Directory, and network devices. It provides comprehensive coverage and attack path visibility for user networks, data centers, clouds, remote worksites, and specialized attack surfaces. It streamlines incident response with forensics, automates attack analysis, and includes third-party native integrations. The company has 130+ awards for technology innovation and leadership. www.attivonetworks.com