Attivo NETWORKS®

Pre-Emptive Phishing Management

Phishing scams are designed to take advantage of lapses in security awareness. Masquerading as a familiar and reliable source, phishing scams convince victims that their messages are legitimate and deceive them into providing confidential and financial information, or to click on a link that can download malicious software that target vulnerabilities in applications installed on their systems.

Given the steady rise and sophistication of phishing attacks, many organizations are trying different threat detection techniques to mitigate the risks posed by these attacks. This paper will cover why phishing is one of the top cyberattacks occurring today, the impacts of phishing, how it works, and the steps an organization can take to protect their employees and assets from these attacks.

The Growing Phishing Concern

Phishing attacks are on the rise. The IBM Threat Intelligence Index found that phishing emails increased in volume by 4x in 2016. Additionally, the IRS reported that W-2 phishing emails increased 870% in 2017. And no organization is safe. 76% of organizations reported being victims of phishing attacks in 2016[1].

Phishing is attractive because, when successful, it can give the attacker the "insider" access they need to accomplish their ultimate objective. The attacker simply sends an email(s) that appears to come from a trusted source, which is often someone with authority within the organization itself, and then tries to trick the recipient into clicking on a malicious link and/or revealing sensitive information. The success of these exploits depends on the recipient trusting the source and believing the validity of the request being made.

For example, 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 may download malware (including spyware) onto their device, which gives them persistent access to the organization's internal network, as well as capture login information for that user, for subsequent reuse.

[1] https://info.wombatsecurity.com/state-of-the-phish

The Anatomy of Phishing Attack

A phishing attack is typically made up of multiple phases:

1. Planning. An attacker decides which business to target and then collects intelligence on that business, such as employee, customer, or partner names, titles, and e-mail addresses. Similar to a spammer, they will often use mass-mailing and address collection techniques.
2. Setup. The attacker will create methods for delivering the message and collecting the data they are looking for from their targets. This will generally involve setting up e-mail addresses and web pages.
3. Attack. The phisher will then send a phony message that appears to be from a legitimate source (often from within the targeted organization), attempting to engage individuals into disclosing confidential information about themselves and other sensitive/financial information, such as account or credit card numbers.
4. Identity Collection and Theft. The attacker will record the information they collect on web pages or popup windows so that they can use it to make illegal purchases, commit other forms of fraud, or launch other attacks.
5. Fraud. The phisher will then execute their "end game," using the information they've gathered to steal, disrupt, or commit fraudulent activities. In most cases, the victims are unaware of these activities until they are notified by a financial, law enforcement, or other organization that is suspicious of the activities that are occurring.
6. Repeat. The phisher will evaluate the successes or failures of the completed scam and, in many cases, begin another attack cycle.

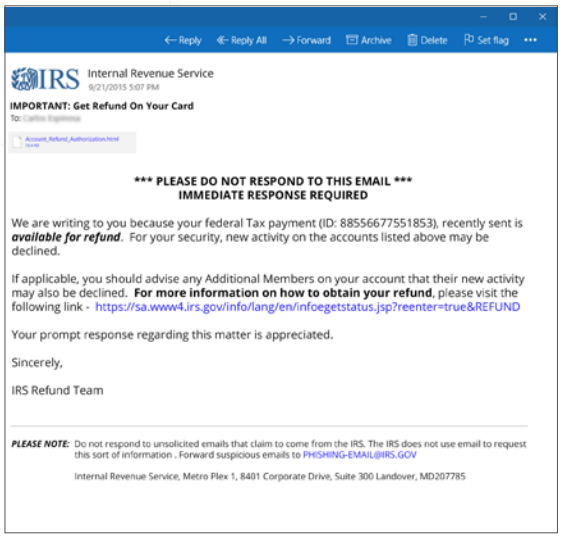
An Example—Phishing in the Wild

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. In the three years between October 2013 and December 2016, BEC scams accounted for more than $5 billion in losses[2].

Scenario: Auditor Asks for Payment for Acquired Business Victim: Controller at Employee-owned Commodities Trader

The corporate controller received emails that appeared to be from the company's outside auditing firm with requests to transfer millions of dollars to a Chinese bank. Three wire transfers were requested and sent for a total of $17.2 million. The initial email instructed a wire transfer of $780,000, the following day a request was emailed for $7 million and three days later a final request was received for $9.4 million. The initial emails include language focusing on secrecy, urgency, and sensitivity, including:

"I need you to take care of this. For the last 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."



[2] https://www.ic3.gov/media/2017/170504.aspx

The Controller called the auditor to confirm, using the phone number provided in the email. The criminal was ready with a person in place posing as an employee of the auditing firm to confirm the requests. There also was an element of consistency between the wire requests and the company's business plans as the company had been discussing the expansion into China and they were in the middle of an audit. These factors put the wire requests and the request for sensitivity and secrecy in line with company business plans[3].

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 the proper use of email and the practice of clicking on embedded (web/file) links. They also frequently use URL filters, IP blacklists, and reputation feeds to try to prevent connections to or from sites that are known to be the source 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 are dealing with, there is really no way to completely lock down and prevent phishing. As a result, organizations need to assume that attackers are already in the network and ensure they have the appropriate measures in place to monitor and identify phishing activity. This is where Attivo Networks can help.

Attivo Networks for Phishing Protection

1 Send suspected email to dedicated account

2 Download susptected email and execute in Sandbox

To mitigate the risks posed by phishing, organizations can leverage the Attivo Networks ThreatDefend™ Deception and Response Platform as a complement to their existing security processes and controls for phishing detection and analysis.

Attivo Networks Pre-Emptive Protection

To prevent a phishing attack from being successful, organizations can use the ThreatDefend Platform which is comprised of the BOTsink® Malware Analysis Sandbox (MAS), that analyzes suspicious emails that employees receive, and the ThreatStrike™ endpoint suite, which simplifies email evaluation submission.

[3] https://guardianananalytics.com/wp-content/uploads/2016/06/BEC_True_Stories.pdf

1. Submissions can be made directly into the BOTsink MAS through the ThreatStrike EP suite, which provides a simple-to-deploy Outlook plugin that enables questionable emails to be sent to a dedicated phishing email account that is monitored by the BOTsink engagement server.
2. Once an email is placed in the folder, the BOTsink MAS will run extensive attack analysis on the email in question to understand exactly what it is designed to.
3. The MAS will extract and scan any files and execute any links to assist in determining the ultimate intent of the attacker.
4. The solution also provides analysis reports on any network connections, registry access, process and file activity, as well as delivering screenshots of the emails execution, so organizations can see exactly what they are facing.

Attivo Threat Detection: Identifying Attacks Inside the Network

If a phishing attack is successful, the attackers will find their way into the network via an infected machine or by reusing stolen credentials. They will then conduct reconnaissance activities to map the network looking for assets to compromise. With deception deployed in a network, attackers are lured to engage with a deceptive asset which is indistinguishable from production assets. When they do, the BOTsink engagement server will detect the attacker and engage them so that it can analyze their actions.

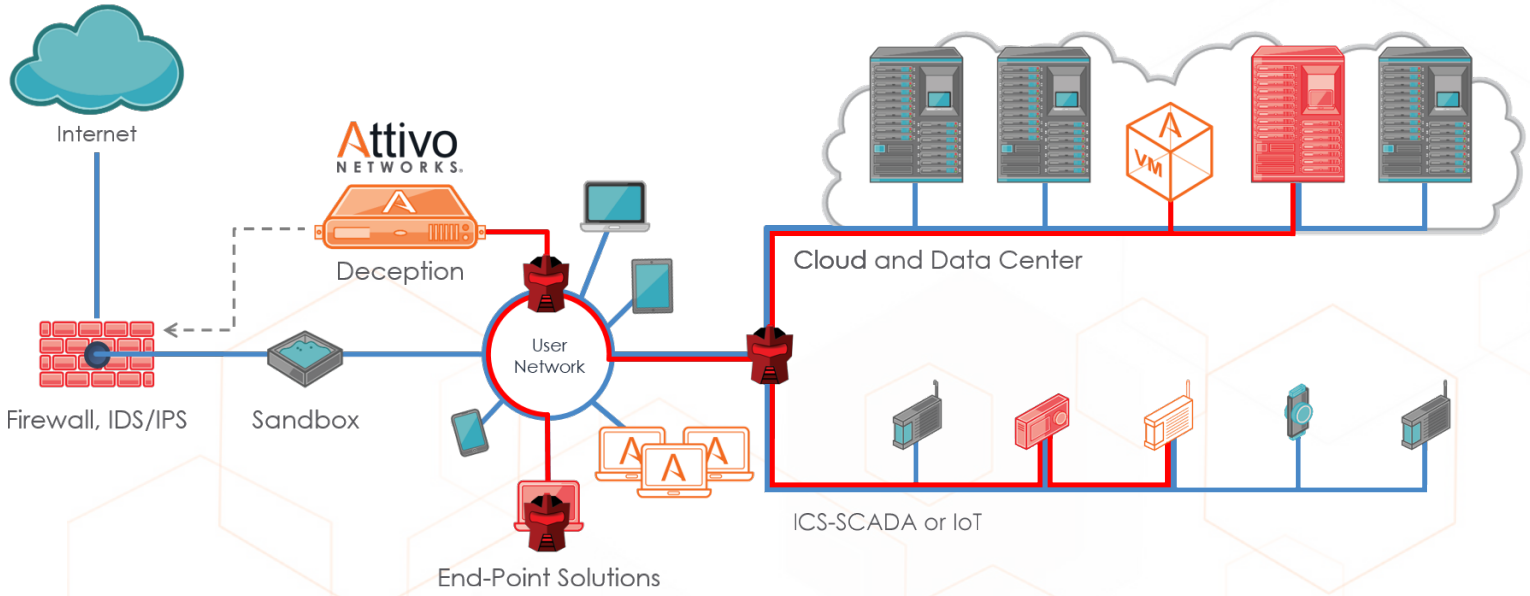
The BOTsink solution has an Attack Threat Analysis (ATA) engine that safely records and alerts on attacker activity while simultaneously responding to the attackers. As the attacker engages with the deception environment, the ATA analyzes the activity, correlates events, and raises alerts.

The platform only alerts on confirmed attacker activities that have interacted with the decoys and is not dependent on signatures or behavioral analysis, eliminating false positives, as well as false negatives. Furthermore, evidence-based analysis substantiates the alerts that the BOTsink solution can use to automate in blocking an attacker, isolating an infected system, and threat hunting so that a company can verify that it has eradicated the threat from the network. The BOTsink solution also generates output in Mandiant IOC, PCAP, and STIX formats to allow easy information sharing and attack analysis. The BOTsink outputs forensic information that includes details on infected IP addresses and C&C addresses so that security teams can promptly address the external aspects of the incidents, while also using information such as SHA1 hashes for internal threat hunting to identify additional victims. The information will also provide the details to understand what phase in the "Kill Chain" the attacker was executing.

Organizations seeking to improve incident response can add the ThreatOps solution, which creates repeatable incident response playbooks and, through 3rd party integrations with prevention systems (Firewall, NAC, End-point, SIEM), can automatically block and quarantine attacks; expediting response actions and preventing the attack from continuing to spread through the network. Organizations can customize the ThreatOps environment to match their environment and policies so that, based on aggregated attack information, organizations can make faster and better-informed incident response choices.

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, removing hours of manual work from the process. Additionally, if a phishing attempt succeeds, the ThreatDefend Platform places decoys and lures throughout the environment, turning the entire network into a trap that tricks attackers into revealing themselves. The BOTsink Solution, through integrations with 3rd party security tools, facilitates attack information sharing and automates steps in the incident response process further strengthening a company's overall security defenses.



About Attivo Networks

Attivo Networks® is the leader in deception technology for real-time detection, analysis, and accelerated response to advanced, credential, insider, and ransomware cyber-attacks. The Attivo ThreatDefend™ Deception and Response Platform accurately detects advanced in-network threats and provides scalable continuous threat management for user networks, data centers, cloud, IoT, ICS-SCADA, and POS environments. Attivo Camouflage dynamic deception techniques and decoys set high-interaction traps to efficiently lure attackers into revealing themselves. Advanced attack analysis and lateral movement tracking are auto-correlated for evidence-based alerts, forensic reporting, and automatic blocking and quarantine of attacks. For more information visit www.attivonetworks.com