SOLUTION NOTE

COUNTERING PHISHING, BECs, AND OTHER EMAIL-BASED RISKS THROUGHOUT THE KILL CHAIN

MODERN EMAIL SECURITY RISKS

In today's interconnected world, email is still a critical communication channel for individuals, government agencies and corporate organizations. Because of this global dependence, email also remains a primary entry vector for cybercriminals looking to exploit vulnerabilities and gain unauthorized access.

Unfortunately, threat actors have become more focused on larger enterprises as mass market phishing attacks, like fake 'PayPal' emails, have become much less successful, and their methods have shifted to a rise in 'spear-phishing', BEC (Business Email Compromise) and other, more targeted attacks. Even ransomware attacks typically start with an email. The impact on organizations has been devastating in several areas:

1. **Financial Losses:** Successful attacks can result in direct financial losses due to fraudulent transactions, ransom payments, lawsuits, and regulatory penalties.
2. **Operational Disruption:** Malware introduced via email can disrupt operations, halt critical processes, and compromise proprietary or other sensitive data.
3. **Brand Damage:** Breaches erode trust, tarnishing the victim's reputation. Clients, partners, and stakeholders lose confidence, affecting long-term relationships.

FACTS & FIGURES

- 70% of all attached files or links containing malware in 2023 were not blocked by network border protection services.[3]
- Business Email Compromise (BEC) attacks nearly doubled in 2023.[1]
- 36% of all data breaches involved Phishing.[1]
- An estimated 3.4 billion malicious emails are sent every day.[2]
- 8 out of 10 organizations had at least one individual who fell victim to a phishing attempt.[3]
- Phishing makes up 44% of social engineering incidents.[1]
- Blocking threats at the DNS layer can reduce EDR and FW alerts by 50%.

WHY EMAIL THREATS REMAIN SUCCESSFUL

To counter advancements in email and malware security, threat actors have become masters at hiding their malicious intent from email, firewalls, EDR, DLP, and other security measures. In 2023, 70% of attached malware or links were able to bypass border defenses[3] with the help of attacker strategies such as:

1. **Target Research:** Investigating the targets — people, organization, technology, key events, etc. — to help threat actors find the most effective messaging, timing and other 'social engineering' factors to increase the chance of success.
2. **Cutting Out 'Clues':** Develop custom email content for the victim to ensure believability and use links with 'Lookalike' domains to help them appear legitimate.
3. **Minimizing Function Code:** The embedded or linked malware should do very little, typically designed to just 'download' the next malware component, making it look like any other cloud app requesting an update.
4. **Taking Small Steps:** After the initial 'downloader' code is in place, connect with C2 (command and control) and dynamically download more small components as directed, each designed to perform limited functions such as pen test and exploit tools. Keeping code small and succinct reduces the chance of detection.
5. **Orchestration Attacks:** Using massive attack infrastructures, coordinate the execution of innocent-looking code modules from multiple locations to avoid detection, and dynamically update modules to improve or change their function.

DETECTING THREATS THAT OTHERS MISS

The key weakness in modern email attacks is an increasing dependence on many stages of communication throughout the attack. From the first connection request to install a 'downloader' to the final stages of stealing data or receiving a key to begin ransomware encryption, the attack must reveal its true intent to DNS. Threat Actors cannot disguise or lie to DNS about the desired destination for any communication. So, they build large, complex architectures using thousands of domains to make coordinated communications appear more random, unconnected, and less suspicious. In one case, a Chinese-based phishing campaign used 42,000 domains.[4]

Combining Domain level information with DNS and other threat intel, Infoblox proactively identifies these architectures, offering customers protection against malicious domains months before they pose a real threat. This makes DNS-layer security a great complement to other defenses that may offer their own unique detection capabilities, such as spam filtering or malware analysis. But malware delivered via email is effectively evading gateway and endpoint defenses up to 70% of the time[3] using a variety of methods, including encryption, tunneling, Domain Generation Algorithms (DGAs), and Lookalike domains. Luckily, none of these approaches can fool DNS.

And while this is good news for better detection of threats in email, it also provides an additional layer of defense across the threat lifecycle. For example, if an email attack were to successfully install a 'downloader' using a vulnerability in an email client or other third-party cloud app, every subsequent communication gives DNS another opportunity to identify malicious behavior and stop an attack before it can reach a successful conclusion.

BLOXONE® THREAT DEFENSE FOR PHISHING… AND MORE

Email is just one of the many critical applications we depend on daily, and they all depend on DNS. Infoblox BloxOne Threat Defense is a comprehensive DNS Detection and Response (DNSDR) solution that can detect threat activity that other solutions miss and stop attacks before they occur with hunted, pre-campaign DNS threat intel to disrupt attacker supply chains.

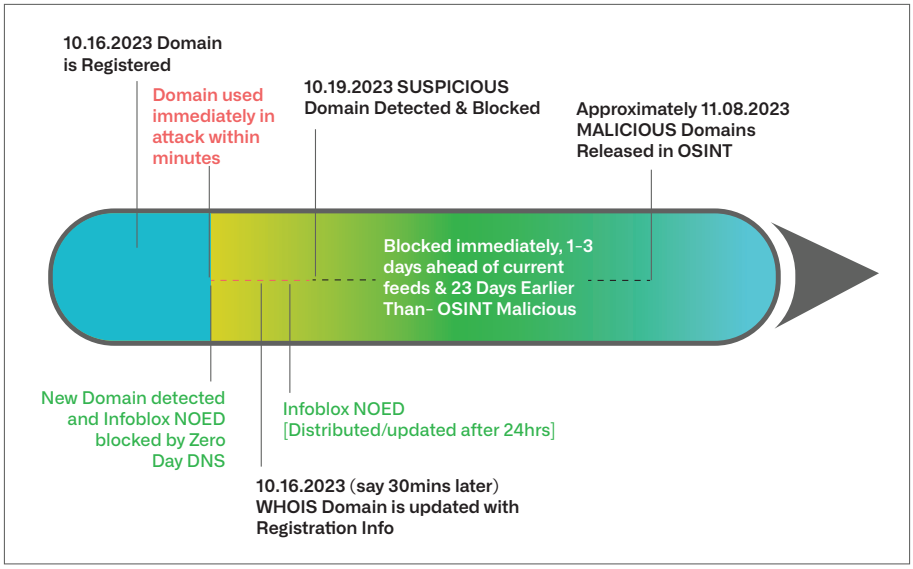

Figure 1: Timeline showing a phishing campaign domain and when it gets blocked with Zero Day DNS™

Intelligent ecosystem integrations uplift the effectiveness of other security tools, and automation capabilities help reduce manual workloads. Plus, Infoblox's unique AI-driven analytics help SOC analysts cut through the noise of alert overload so they can quickly focus on what matters most by taking action with insights that reduce MTTR, raise the ROI of existing security tools and elevate overall SecOps efficiency.

KNOW WHICH EMAIL THREATS MATTER MOST

Email threats comprise the largest portion of all cyber threats which, in turn, means they can easily produce more security alerts than any other threat type. So, the SOC must filter through mountains of alerts every day in an attempt to identify and prioritize what can be ignored, what requires a response and everything in between. Even today's most advanced SIEMs require a great deal of time and expertise to filter, sort, eliminate, and otherwise manipulate the data to extract something meaningful. So Infoblox has built in decades of DNS expertise and threat intelligence into our BloxOne Threat Defense solution in the form of a platform called "SOC Insights."

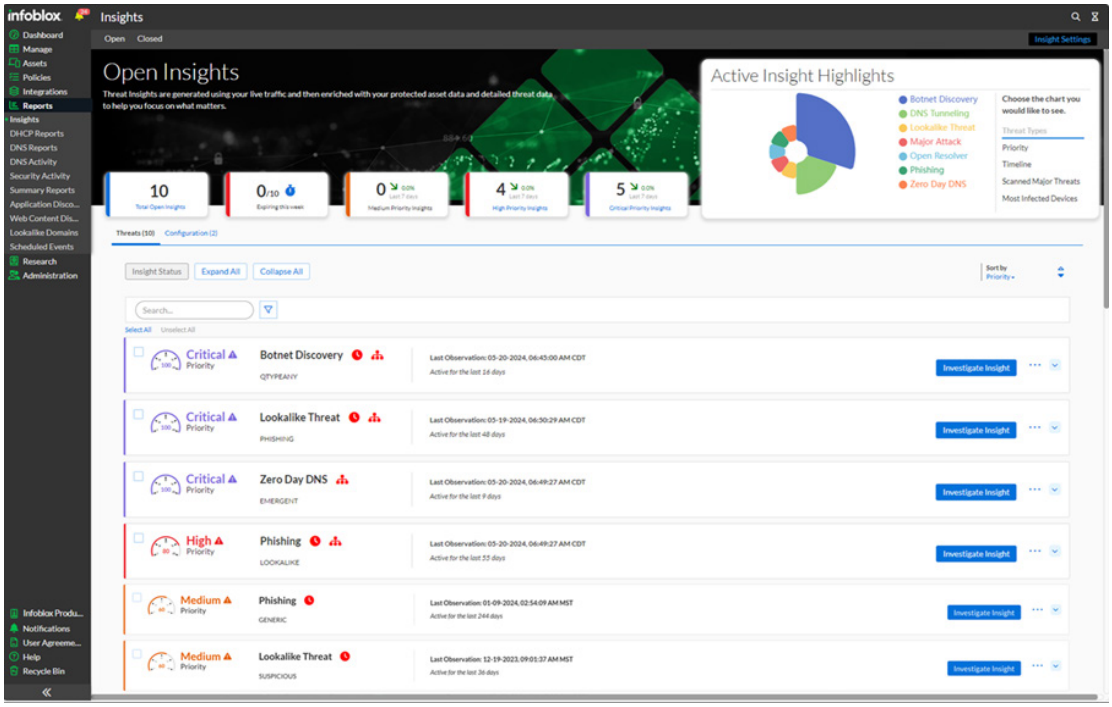

Figure 2: The SOC Insights console displays a short, manageable set of 'Insights' after applying AI-driven analytics to hundreds of thousands of events along with related network, ecosystem and DNS Threat Intel data.

SOC Insights serves as a platform to apply advanced machine language and unique AI-driven analytics to turn vast amounts of event, network, ecosystem, and unique DNS Threat Intel data into actionable insights. It improves SecOps efficiency by identifying related events and other data and grouping and organizing available information under various 'Insights.' This makes it easy for analysts to make quick decisions on where to start and provides one-click access to an investigation portal to put relevant data at their fingertips. This eliminates much of the time wasted just collecting information related to an event from multiple tools so analysts and responders can immediately begin the work that demands someone of their expertise and experience.

1 "Verizon 2023 DBIR Report", Verizon

2 "51 Must-Know Phishing Statistics for 2023", Luke Irwin, itgovernance.co.uk

3 "2023 Phishing Infographic", CISA

4 "China-Based Campaign Uses 42,000 Phishing Domains", Infosecurity Magazine

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240531v1