infoblox

Threat Intel

SOLUTION NOTE

DNS-BASED THREAT HUNTING FOR UNVEILING THREATS EARLY BEFORE THEY STRIKE

FACTS AND FIGURES

- The scope of DNS is enormous. There are now 1589 top-level domains, with 200,000 new domains created every day.
- 81% of organizations experienced one or more phishing attacks in the last 12 months per CRA 2023 Global State of Cybersecurity Study
- 75% of organizations faced smishing (SMS phishing) attacks, according to Proofpoint 2024 State of Phish Report
- Lookalike domains are frequently used in phishing and spear phishing attacks. In 2022, Chinese hackers used 42,000 imposter domains in a massive phishing attack campaign, according to Hacker News.
- It's not just lookalike domains. Attackers often register domains several months in advance of being used in a broad range of attacks. One example is the Decoy Dog toolkit first identified by Infoblox Threat Intel. Many of the Russian C2 domains used by Decoy Dog were set up in advance and discovered by Infoblox back in the fall of 2022.
- Infoblox finds and blocks around 25000 new lookalike domains every week.
- **Bottom line:** There is a critical need for threat intelligence that proactively identifies these emergent domains that could be used in future attacks

CHALLENGES

Attackers love phishing because it is cheap, and all they need is one person to make a mistake and click on the link. SMS phishing attacks, commonly called smishing, have increased in frequency recently, and actors operate massive resilient smishing operations. Lookalike domains are often used in phishing and spear phishing attacks, and in 2022, Chinese hackers used 42,000 imposter domains in a massive phishing attack campaign.

While phishing and lookalike domains are a growing problem, there are other instances where domains have been registered months in advance before being used in a broad range of attacks. One such example is the recently discovered Decoy Dog toolkit, which was a set of beacons exploiting DNS to communicate with C&C infrastructure. The toolkit uses Pupy RAT, which has often been associated with nation-state actors in the past. Many of the domains associated with Decoy Dog have been active since April 2022 and were persistent and low-profile, which made it hard to discover with traditional security tools.

A different approach is needed to detect such attacks where domains are set up well in advance of launching attacks.

DNS-BASED THREAT HUNTING

DNS-based threat hunting uses large-scale DNS and analytics, to track adversary infrastructure before an actual attack starts. More specifically, it can:

- Find domains that are new to customers and categorize them as new/emergent or suspicious using metadata including Registrar, TLD Domains, SSL Certs, Name Server, Registration behavior, etc.
- Take published third party advisories, for example CISA advisories, and enhance that to find more indicators using DNS metadata. For example, in a recent CISA announcement, Infoblox found an additional 13 domains that were not in the advisory based solely on the ability to tie in DNS metadata. This greatly helped reduce a potential threat vector.

DNS based threat hunting protects against suspicious domains weeks or months before they are confirmed as malicious and used in attacks.

USING BLOXONE THREAT DEFENSE FOR PROACTIVE PROTECTION

Due to Infoblox's unique position in the query path, the solution is able to witness, analyze, and block intent to communicate, for proactive protection. Infoblox, the market leader and expert in DNS, tracks adversary infrastructure and reviews DNS logs to see suspicious activity early in the threat lifecycle when there is "intent to compromise '' and before the actual attack starts. This allows the Infoblox Threat Intel to identify new domains and lookalike domains intended for malicious use during the weaponization phase and categorize them as suspicious for several weeks or months before other security organizations/ vendors can detect them as malicious. The main reason for this delay between Infoblox's proactive suspicious categorization and other security solutions' detection is that those solutions assess the traffic behavior or content associated with those domains, which is typically only relevant once the threat is already activated.

High Risk Domains

Once the team deems certain domains as suspicious, Infoblox includes them into a feed called "Infoblox High Risk," available with BloxOne Threat Defense, to enable our customers to pre-emptively protect themselves from new and emerging threats. These are feeds with indicators for highly suspicious domains that haven't had associated malicious activity confirmed yet but show indications that they may have been acquired by threat actors as part of their weaponization phase and can be activated for malicious usage in the future. The feeds are classified into three categories:

- **Suspicious Lookalikes** - A type of suspicious domain that looks similar to legitimate domains, potentially for use in future phishing activity.
- **Suspicious NOED** - (Newly Observed Emergent Domains) - A type of high-risk, suspicious domain that has only recently been observed within customer traffic. (thus, 'emergent')
- **Suspicious Domains** - These are other domains that appear suspicious but do not fit the profile of a suspicious lookalike or NOED.

Infoblox launched suspicious emergent domains data in early November 2022, and has detected and categorized 19.4M active Suspicious indicators in CY23. This number of active Suspicious domains keeps increasing over time. Besides this high volume, another criteria of importance is the suspicious classification quality: out of the millions of domains classified as suspicious, only 0.0002% have been flagged as false positives.

This concept of blocking suspicious domains has helped Infoblox customers block early for some security advisories, including Decoy Dog and MFA attacks like Oktapus. Many of the domains associated with the Decoy Dog toolkit were already discovered and included in Suspicious Domains feeds in BloxOne Threat Defense back in the fall of 2022. So, BloxOne Threat Defense Advanced customers who had set their policy to block suspicious domain feeds have been protected against many of the C2 domains since then.

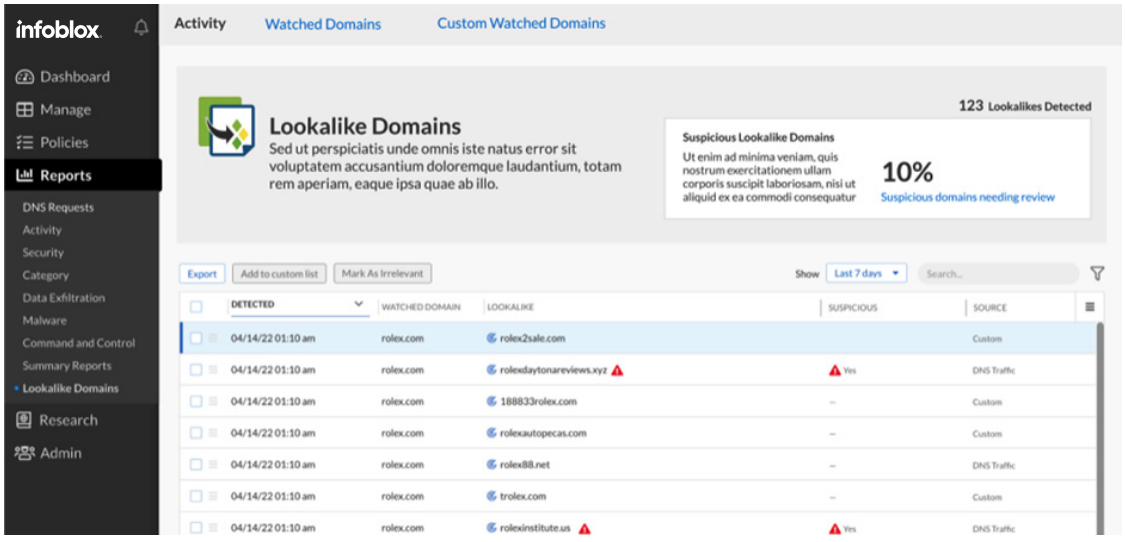
Infoblox has added 19.4 million domains in suspicious domain feeds in CY23, greatly reducing risk from future attacks.

Lookalike Domains

In addition to suspicious feeds, Infoblox customers can use the built-in lookalike domain security feature in BloxOne Threat Defense to proactively identify and stop socially engineered threats using lookalike domains in advanced targeted attacks intent on breaching the enterprise, compromising customers or damaging your valuable brand.

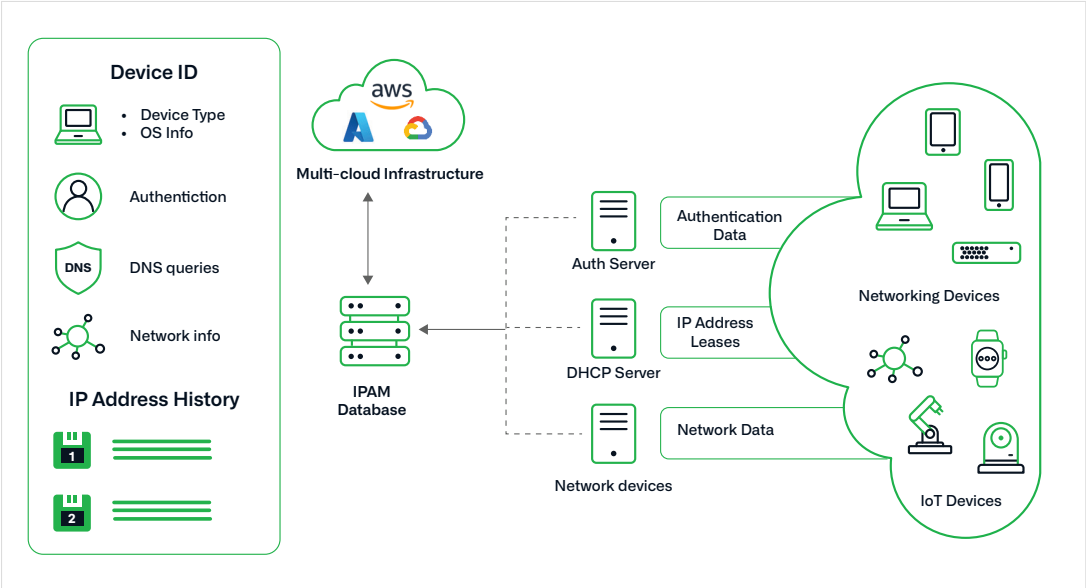
Customers can submit domains used by their own organization, supply-chain partners, or other domains that might be imitated in an attempt to trick users, partners or customers as part of a cyber attack. Infoblox then begins a continuous monitoring process for potential lookalike domains and analyzes each one's registration, activity, history, and more to assess their level of risk. These findings are presented in an interactive dashboard to help customers quickly make informed next-step decisions. And this information is continuously updated to reflect new lookalike domains or activity related to currently identified lookalike domains.

A 'take-down' service is available separately that draws on Infoblox's deep trust-based relationships and our unique position in the global IT environment to help threatened companies respond to limit their financial and brand exposure. The Infoblox Domain Mitigation Services include validation services to confirm an incident has, in fact, occurred; mitigation through coordination with major ISPs and regulators; and monitoring with reporting to better understand the threatscape and to strengthen your security. Due to our reputation for investigative diligence and quality, the average removal time in some regions can be as little as 24 hours, enabling our customers to eliminate many threats before they begin, and quickly get back to business as usual.



Easy User and Device Attribution

While blocking communications to these domains is the first step, it is equally important to get quick visibility on what devices/assets are involved in those communications. Syncing IPAM metadata with DNS provides much needed visibility to determine where the malicious queries originated in the network. Using IPAM data, it is easy to determine whether the anomalous DNS activity is coming from network devices such as firewalls, user devices, or any other type of network-connected asset. You can even define security policy based on IPAM metadata easily using Infoblox.



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

+1.408.986.4000
www.infoblox.com

Version: 20240411v1