SOLUTION NOTE

LOOKALIKE DOMAIN MONITORING PROTECTS YOUR NETWORK, CUSTOMERS AND BRAND

Proactively stop socially engineered threats using lookalike domains in advanced targeted attacks intent on breaching the enterprise, compromising customers, or damaging your valuable brand.

A GROWING LOOKALIKE THREAT

From large volume, broad-spectrum consumer-level attacks to highly targeted spear phishing, Business Email Compromise (BEC) and other enterprise threats, lookalike domains have become key components to help adversaries counter both human and technical defenses. They can impersonate your brand, employees, supply chain or other trusted partners with devastating results.

While first used almost two decades ago, threat actors continue to innovate new ways to apply lookalike domains in new types of attacks. Using adversary-in-the-middle (AitM) techniques, they increasingly attempt to trick employees into thinking they are interacting with the company's real network during authentication.

Today, attackers use lookalike domains in SMS messages, phone calls, direct messages on social media, emails, and QR codes. Most recently, attackers targeted multi-factor authentication (MFA) due to its growing adoption by everyone from gamers to digital currency marketplaces, wallets, and exchanges, such as the attack on Coinbase in early 2023. Lookalikes have become an integral part of every major cyber threat.

A GROWING LOOKALIKE THREAT

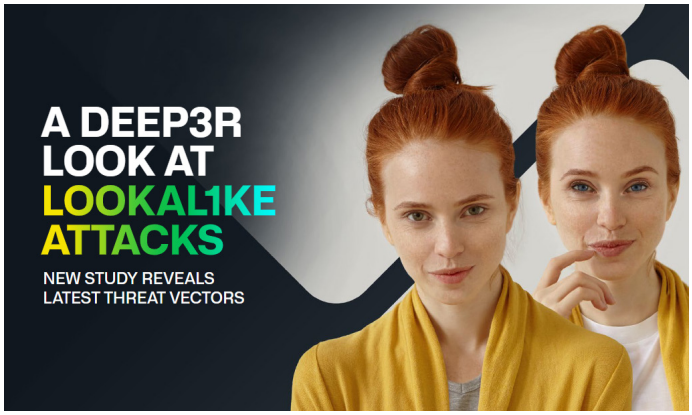

Figure 1: Infoblox Threat Intelligence shared surprising research data on the escalating risk of Lookalike domains.

FACTS & FIGURES

Other BloxOne Threat Defense Advanced security capabilities enable you to:

- Over 300,000 lookalike domains were detected in just over one year
- Combosquatting domains are now 100X more common than Typosquatting
- 200,000 new domains are created every day
- More than 1,600 domains were used in 2023 to imitate official MFA services
- 60% of combosquatting domains are active over 1,000 days
- Beyond using .com, there are 1,588 other TLDs for attacker abuse today
- DNS is used in 92% of cyber attacks

PROTECTING YOUR BRAND AND CUSTOMERS

Defending against enterprise lookalike domain threats requires a different approach than that used for more consumer-grade, mass-market attacks. With Infoblox Lookalike Domain Monitoring, customers manage their own custom list of the domains they are concerned could be used against them, their employees, or their customers. Infoblox Threat Intelligence then monitors global registrars, ISPs, actual DNS activity and more to identify potential high-risk lookalike domains against the customer's monitoring list and begin initial assessment and monitoring. The Lookalike Domain Monitoring interface gives customers visibility of identified, high-risk lookalikes and risk profile data, which helps the organization make informed decisions that can proactively avert a potential network breach, customer compromise, or damage to the organization's reputation and brand.

Lookalike Domain Monitoring is available separately and is included with a subscription to Infoblox's industry-leading DNS Detection and Response (DNSDR) solution, BloxOne Threat Defense Advanced. These solutions license customers to identify an initial set of custom domains to be monitored for high-risk lookalikes. Customers wishing to have more domains monitored for these risks may purchase additional licenses in increments of 100 domains.

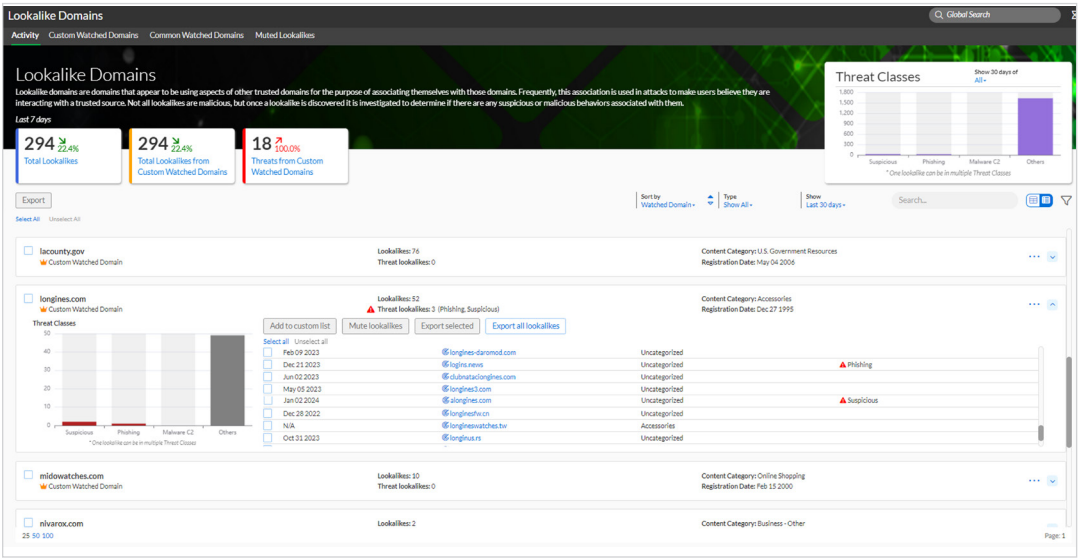

Figure 2: Easily review high-risk lookalike domains to understand the levels of risk they present

STOPPING INTERNET FRAUD FROM ABUSING LOOKALIKES

Infoblox offers 'Domain Mitigation Services' to help customers quickly take down domains that pose a risk to their organizations or customers. We apply Infoblox's proprietary blend of investigative skills, automated techniques, and industry relationships to resolve issues with industry-leading SLAs measured in hours, including data theft, site spoofing, and other cyber incidents swiftly and with discretion.

For more information on Infoblox Domain Mitigation Services, check out https://insights.infoblox.com/resources-datasheets/infoblox-datasheet-infoblox-domain-mitigation-services

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: 20240125v3