SOLUTION NOTE

infoblox

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 <u>Coinbase</u> in early 2023. Lookalikes have become an integral part of every major cyber threat.

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

A GROWING LOOKALIKE THREAT



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

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, <u>BloxOne Threat Defense</u> 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.

kalike Domains					Q. Global Search	h
rity Custom Watched E	omains Common Watched Doma	ins Muted Lookalikes				
	8				A STATE AND A STATE AN	THE R.
ookalike Do	maina				TI I OL Ste	w 30 days of
					Inreat Classes All.	
			ose of associating themselves with those domains. Frequently, t is investigated to determine if there are any suspicious or malic		ke users believe they are 1.800	
7 days			o investigated to determine in the end of any suspected of mane		1,200	
7 adys					900	
294 ×2.4%	294 ×	18 700.0%			100	
tal Lookalikes	Total Lookalikes from	Threats from Custom			0 Suppicious Phishing Malwa	re C2 Others
otal Lookalikes	Custom Watched Domains	Watched Domains			Suspicious Phishing Malwa "One lookalike can be in multiple Three	
port				Sort by	Type Show Search	E
				Watched Domain	show All+ Last 30 days+	
All Unselect All						
lacounty.gov			Lookalikes: 76		Content Category: U.S. Government Resources	
👑 Custom Watched Dom	nain		Threat lookalikes: 0		Registration Date: May 04 2006	
Iongines.com Custom Watched Don Threat Classes	ain		Lookalikes: 52 Threat lookalikes: 3 (Phishing, Suspicious)		Content Category: Accessories Registration Date: Dec 27 1995	
50			Mute lookalikes Export selected Export all lookalikes			
40		Select all Unselect all				
40		Feb 09 2023	S longines-daromod.com	Uncategorized		
30		Dec 21 2023	& clubnataciongines.com	Uncategorized	A Phishing	
20		May 05 2023	© longines3.com	Uncategorized		
10		Jan 02 2024	& alongines.com	Uncategorized	▲ Suspicious	
10		Dec 28 2022	@ longinestw.cn	Uncategorized		
0 Suspicious	Phishing Malware C2 Othe	N/A	@longineswatches.tw	Accessories		
	plike can be in multiple Threat Classes	Oct 31 2023	Conginus.rs	Uncategorized		
midowatches.com Custom Watched Dom			Lookalikes: 10 Threat lookalikes: 0		Content Category: Online Shopping Resistration Date: Feb 15 2000	••• ~
Custom Watched Don	1411		THEOR FOUNDMENTS: V		Keiten einen menst Len 15 Tonn	
			Lookalikes: 2			
nivarox.com					Content Category: Business - Other	

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 <u>https://insights.infoblox.com/</u> resources-datasheets/infoblox-datasheet-infoblox-domain-mitigation-services

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

O.

+1.408.986.4000 www.infoblox.com

 \mathbb{X}

© 2024 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

Version: 20240125v3