SOLUTION NOTE

Protect Your Network, Brand and Customers with Custom Lookalike Domain Monitoring

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

SUMMARY

Generating convincing lookalike domains using sophisticated homograph or homoglyph techniques has been refined through years of attacks impersonating popular brands and the largest governments. As your employees, customers and other users have become more accustomed to checking for the "true" URL behind embedded links, cybercriminals are turning to lookalike domains to better fool their victims in efforts involving impersonating any organization or brand.

Lookalike domains support malicious impersonation efforts through social media, email, fake web pages and other approaches. And while the risks to consumers may be more obvious, these techniques can support a wider range of threats to employees. For example, employees can be targeted through communications and fake web content pretending to be from a popular local restaurant, a business partner or any organization that your business frequently interacts with or controls.

This solution note reviews the risks posed by innovative lookalike domain use, the complex techniques used to create effective lookalike domains and the capabilities of the Infoblox BloxOne™ Threat Defense Advanced solution to proactively mitigate risks to your network, customers and brand.

Recent Changes to the Threat Landscape

Most cyberattack techniques are initially developed to support attacks involving the Fortune 1000 or large governments. Once refined and typically automated, those techniques are ready to be adapted for use against any businesses and governments with valuable assets.

However, the expanded use of lookalike domains has accelerated as the effectiveness of randomly generated or other less convincing URLs has declined, partially due to user education efforts among the general population about attack methods. Today, people are more suspicious than in previous generations and will check links embedded in an email, social media and mobile messages before clicking on them. As a result, cyberattacks are increasingly using lookalike domains sufficient to pass the cursory examination many people now make.

In parallel with this improvement in people's behavior, cybercriminals are having less success with traditional attack campaigns, often involving the most popular brands. In response, cybercriminals are now applying lookalike techniques to attack customers and employees connected to any brand that promises a return on a minimal investment.

The use of lookalike domains to attack an organization's customers is fairly obvious, as is the negative impact on your brand. But while employees could be attacked using a corporate domain lookalike in an official-looking communication, this approach is less effective on an audience who frequently interacts with the legitimate sites and is more likely to spot an impersonation. So attackers are more liable to impersonate someone employees are doing business with. A broad, company-wide email attack could pretend to be a special offer from a restaurant, health club, or other local business popular among employees. A highly targeted attack could use a tailored message and lookalike domain of a legitimate business partner, the company bank, a supplier or HVAC service, for example.

Human-Targeted Attack Components

Site Content	URL Path	Domain Name
• Rip-off copy • Modified copy • Malicious code or forms	• Compromise existing paths • Lookalike paths • Long, obfuscated paths	• Hacked domains • Lookalike domains

Figure 1: Human-targeted site attack components

A New Layer of Social Engineering

Attacks using sites crafted to appear legitimate, human-targeted sites have three components that must all appear genuine to be effective (Fig. 1).

- **Site Content:** It may be a modified copy of an existing, legitimate site or creatively crafted for a specific purpose. The content may change over time as the attackers update their attack or repurpose the site for a new attack. Unfortunately, site content is rarely available for security analysis until the time of the attack.
- **URL Path:** Attackers may be limited in what they can do, depending on the level of access they have on the compromised system hosting the malicious site content. But they only need enough access, and creativity, to present a credible URL path to support the ruse.
- **Domain Name:** Cybercriminals may use the domain name of a compromised system or register a custom, lookalike domain name. To support more targeted attacks, they increasingly use lookalike domain names designed to appear legitimate under a typical user inspection. Luckily, this component of an attack is almost always available for analysis by security teams.

Character Substitution

Many people are aware of simple substitutions available to create lookalike domains such as using the numeral 1 to replace a capital i (I). But more than 136,000 Unicode characters are used to represent common domain name letters and symbols in 139 modern and historic scripts, such as Latin, Cyrillic, Greek, Ukrainian, and even Cherokee. Many of these character substitutions could be detected under close inspection. But, as with optical illusions and magic shows, the human eye tends to see what the mind expects to see. While surfing the web, few people will realize that “YAHOO” is not the same as “YAHOO”.

To understand the scope of the challenge, consider the number of character substitutions possible for “Infoblox”. Using only five character sets, the number of reasonable character replacements ranges from 5 (for f) to 16 (for i). This provides 92 alternative domain names by replacing only a single character of “Infoblox”. By replacing multiple characters, the number of possible permutations grows to over 829 million.

Multi-character substitution techniques also present opportunities to replace letters like m with the letter r and the letter n or the letter w with two of the letter v as in:

rnicrosoft.com

vvalmart.com

When the content with the link appears to be from a recognized brand, the substitution is not easily recognized by someone who expects to see the letter m or w.

Complex Domain Name Manipulation

It has been many years since business owners launching a website discovered that “all the good domain names are gone!” As a result, people have become accustomed to some rather complex and hard-to-read domain names involving multiple words, often with liberal use of dots (.) or dashes (-).

Legitimate applications intend to make it easier for customers to access a service without entering a path. Unfortunately, for various reasons including a lack of standardized application of this technique on legitimate sites, the result has only made it easier for cybercriminals to create malicious lookalike domains to support attack efforts such as:

- paypal-security-services[.]com
- facebooksecurelogin[.]com
- confirm-apple-billing-infoconnect[.]com

Another popular application of this technique is to embed the target domain name as a subdomain or a part of the domain name. This technique is used legitimately, which makes a malicious application more difficult to detect. Notice the double use of “.com” in the first example:

- apple-id-com[.]com
- account.paypal.co.uk.rlsg4[.]com
- facebook-com.ugu[.]pl

Character substitution techniques do not work with the top-level domain (TLD) because substitute characters would not be considered valid. However, using an alternative TLD like “.net” rarely raises concerns. Even substituting “.cn” for “.com” may be easily overlooked.

KEY CAPABILITIES

Other BloxOne Threat Defense Advanced security capabilities enable you to:

- Secure every connection, regardless of device or location, across physical, virtual and cloud infrastructures
- Slash incident response times by two-thirds through real-time sharing of security event information
- Spur the performance of SOAR platforms through rich network context and aggregated threat intelligence data
- Significantly reduce the burden on strained perimeter defenses
- Make threat analysts 3x more productive and gain a single pane of glass for incident review with complete forensic data
- Block DNS-based data exfiltration and malware activity by shutting down communication channels used by malware, domain generation algorithms and dozens of other threats

Protecting Your Brand and Customers

Infoblox provides lookalike domain defenses, designed to address threats abusing popularly targeted brands like PayPal. The Custom Lookalike Domain Monitoring is an additional service for BloxOne Threat Defense Advanced customers, allowing them to submit their organization's own domain, or domains frequently visited by or controlled by the organization for lookalike protection. The Infoblox Cyber Intelligence Unit (CIU) will determine high-risk lookalike domains for initial assessment and monitoring. Customers are notified of suspicious activity related to these lookalike domains for visibility and as an advanced warning to help the organization avert a potential network breach or customer threats.

For more information on Infoblox BloxOne Threat Defense, visit: https://www.infoblox.com/ThreatDefense

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com