FORTRA™

2023 Domain Impersonation Report

Table of Contents

Introduction

In the first half of 2023, the average brand was targeted by nearly 40 look-alike domains every month. Domain impersonation is involved in a vast number of online threats. Once a look-alike domain has been created, it may be used to host branded content, redirect to third parties, engage in malicious activities and more.

The domain landscape as a whole has been tumultuous so far in 2023. In Q1, top-level domain (TLDs) registrations tied to domain registry provider Freenom were halted, directly contributing to an 80% quarter over quarter decrease of free registrations tied to phishing attacks. While a large number of cybercriminals have since shifted to paying to register look-alike domains, the volume of country-code TLD (ccTLD) abuse remains high. In fact, for the first time since reporting on domain data, Fortra saw cybercriminals favoring ccTLDs over Legacy TLDs in Q2. What's more, eight new Google TLDs were introduced to the domain pool in May, with newcomer .ZIP already associated with both credential theft and phishing redirect campaigns.

Changes to a domain record can be made at any point during its life, making it challenging to identify a threat and gather evidence for mitigation. In this report, we use data from Fortra's PhishLabs and Agari to take a look at the average volume of look-alike domains targeting brands in 2023 and the types of content they hosted so that security teams have a better understanding of how a look-alike domain may be used in an attack. For purposes of this report, a look-alike domain is defined as a domain name that is similar to a trademark or service mark. Additionally, a "brand" refers to the brand name of a company, product, or service. A single brand may be used in multiple domains that have been registered by the company.

One Brand	Four Brands
Fortra.com	Fortra.com
Fortralogin.com	Agari.com
Fortrabenefits.com	PhishLabs.com
Fortrafun.com	Clearswift.com

Brand Examples

Key Findings:

The average brand was targeted by 40 lookalike domains per month in H1

77% of look-alike domains deemed malicious hosted phishing sites

Abuse of Country-Code TLDs (ccTLDs) surpassed both Legacy and New TLDs with 46% of volume in Q2.

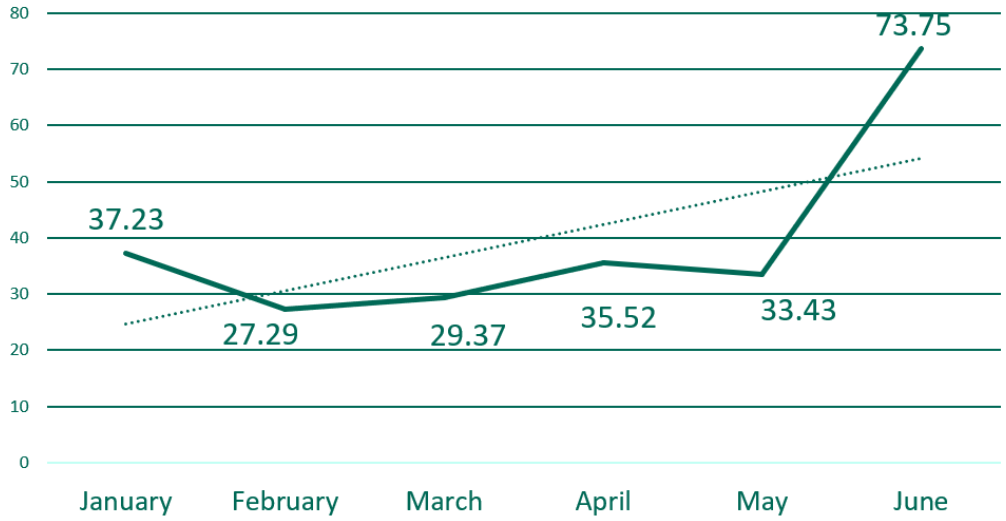
More than 62% of spoofed email display names impersonated well-known brands including Microsoft and Google

H1 Look-alike Domain Volume

Average Look-alike Domain Per Brand

In the first half of 2023, the average brand was targeted by 39.4 look-alike domains per month. The number of look-alike domains targeting brands has trended up so far this year, with anywhere from 37 to 27 look-alike domains impersonating a specific brand on any given month until June.

The volume of look-alike domains leapt more than 120% from May to June, with the average brand targeted by 73.75 look-alike domains. This growth can in part be attributed to a jump in look-alike domains targeting the technology, retail, manufacturing, and financial industries, with a significant increase specifically in attacks on a top three webmail provider. February saw the lowest average volume, with brands targeted by 27.29 look-alike domains.



How Look-alike Domains are used in Attacks

Look-alike domains may be used in a variety of ways to target a brand. In this report, we have categorized the types of content look-alike domains host into four distinct categories:

No Relevant Content: Parked Domains, Monetized Links, Content Unavailable, and Domains without Content.

Branded Content: Domains hosting content related to an organization including logo or industry.

Redirects: Domains redirecting to third party or competitor websites.

Malicious: Domains hosting content associated with phishing, counterfeit, cryptocurrency, or malware.

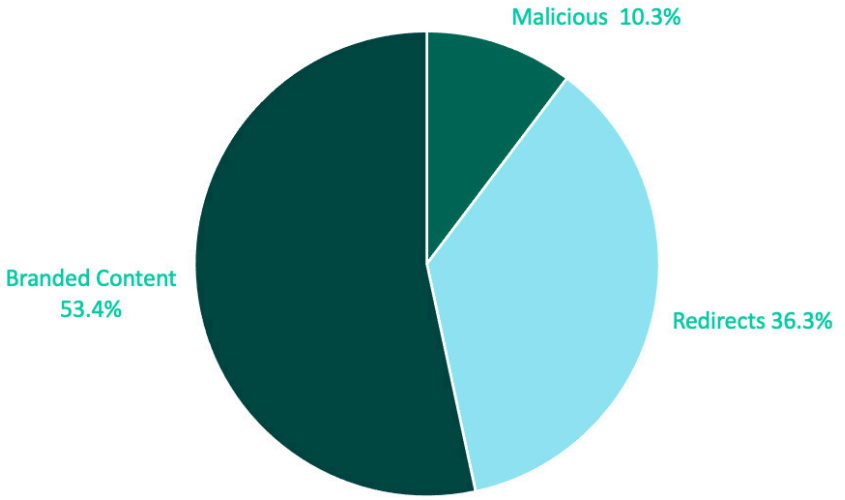
In the first half of 2023, 86% of look-alike domains hosted No Relevant Content. This means that while the domain itself displayed attributes identical or similar to a brand, it did not host offending content or was used only to serve ads. While a look-alike domain categorized as No Relevant Content was at its most benign at the time of writing this report, it should be noted that content can change at any point and may require mitigation.

Top Look-alike Domain Threat Types

Branded Content, Redirects, and Malicious Content are considered the three categories of threats hosted by look-alike domains.

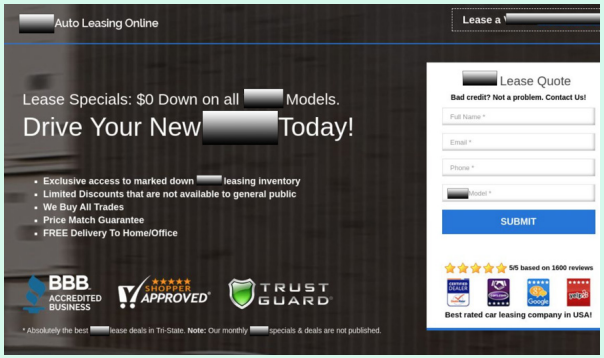
In the first half of 2023, most look-alike domains hosted Branded Content, with 53.4% of volume.

The second most common means of using a look-alike domain was redirecting to a third-party website or competitor site. Redirects made up just over 36% of threat volume. Malicious activity came in third, with 10.3% of look-alike domain volume.

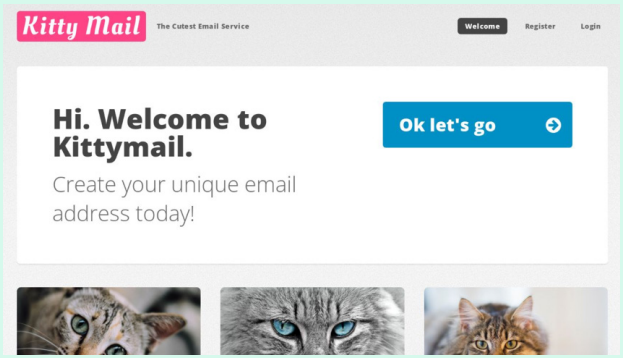


H1 2023 Look-alike Threat Types

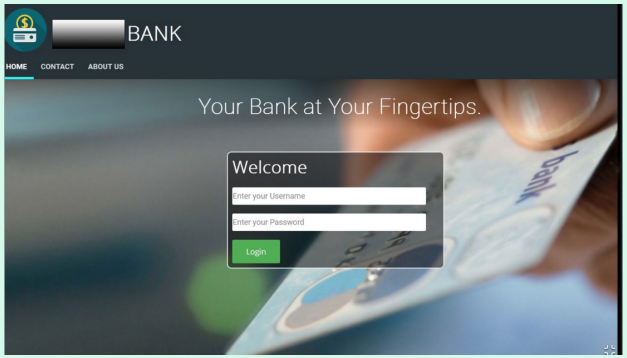
Below are examples of each category.



Branded Content targeting a global automotive manufacturer



Look-alike domain redirecting to an email provider



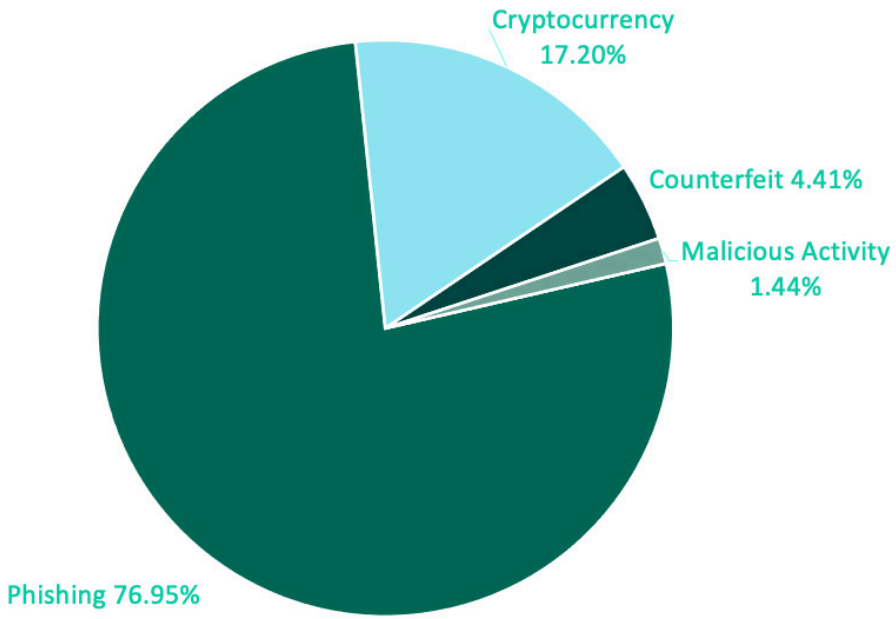
Look-alike domain hosting phishing content

Malicious Content

Fortra divides Malicious Content hosted by look-alike domains into four categories:

- Phishing Content
- Cryptocurrency Scam
- Counterfeit Site
- Malicious Activity or, the possibility of malware on the page

In H1, Phishing made up the lion's share of Malicious Content, with more than three quarters of overall volume within the category. Cryptocurrency Scams were the second most common, with just over 17% of activity. Counterfeit Sites contributed to only 4.4% of volume and Malicious Activity such as malware represented only 1.4%.



H1 Types of Malicious Content

Top-Level Domain Abuse

The top-level domains used in phishing campaigns fluctuated widely in H1. While TLD abuse can be inconsistent from quarter to quarter, the first half of 2023 saw a move away from commonly seen free registration providers, to new and paid TLDs within the top ten.

In Q2, half of the top ten abused TLDs were new to the group, with many seeing dramatic changes in volume. Notably, multiple TLDs within the top ten are clearly capable of misleading targets if used in conjunction with a brand or industry-related URL. New gTLDs .APP and .SHOP are two examples of TLDs demonstrating large jumps in abuse that, if used in phishing attacks, would be ideal choices in targeting a technology company or retail brand.

Taking a look at TLD types, for the first time since reporting on TLD data, ccTLDs made up the majority of abuse, with nearly 46% of overall volume. The ccTLDs among the top ten were .PL, .CO, .ID and .FR. While all four ccTLDs showed a quarter over quarter increase from Q1, .PL and .FR jumped considerably, with .PR growing nearly 250% and .FR a sizable 700%.

Legacy gTLDs were abused 18.5% less than they were in Q1, making up 41.7% of volume. While Legacy gTLD .COM declined 8.5% over Q1, it remained the most abused TLD over all others. Legacy TLD .ORG also saw a decline, moving from the second spot in Q1 to the 7th in Q2.

TLD	TYPE	% PHISH	% CHANGE QOQ
.COM	Legacy gTLD	35.11%	-8.48%
.NET	Legacy gTLD	2.44%	+65.1%
.PL	ccTLD	2.35%	+246%
.INFO	Legacy gTLD	2.16%	+42.2%
.CO	ccTLD	2.06%	+17.2%
.APP	New gTLD	1.91%	+206%
.ORG	Legacy gTLD	1.90%	-45.8%
.ID	ccTLD	1.65%	+57.0%
.FR	ccTLD	1.31%	+699%
.SHOP	New gTLD	1.20%	+387%

New TLDs contributed to just over 12% of abuse in Q2, with .APP and .SHOP jump to the sixth and tenth spots, respectively. This is due to a 206% quarter over quarter increase for New TLD .APP and 387% increase in .SHOP.

While insignificant in volume, newly released Google TLDs .ZIP and .DAD were detected hosting phishing content in June, with two known incidents attributed to .ZIP in Q2 and eighteen associated with .DAD.

Email Domain Spoofing - Imposter Type

In addition to look-alike domains, cybercriminals also forge email sender addresses without actually registering the impersonated domain, otherwise known as domain spoofing. In domain spoofing attacks the brand is not impersonated by the domain itself, but rather the display name.

The most three most common domain spoofing types are the following:

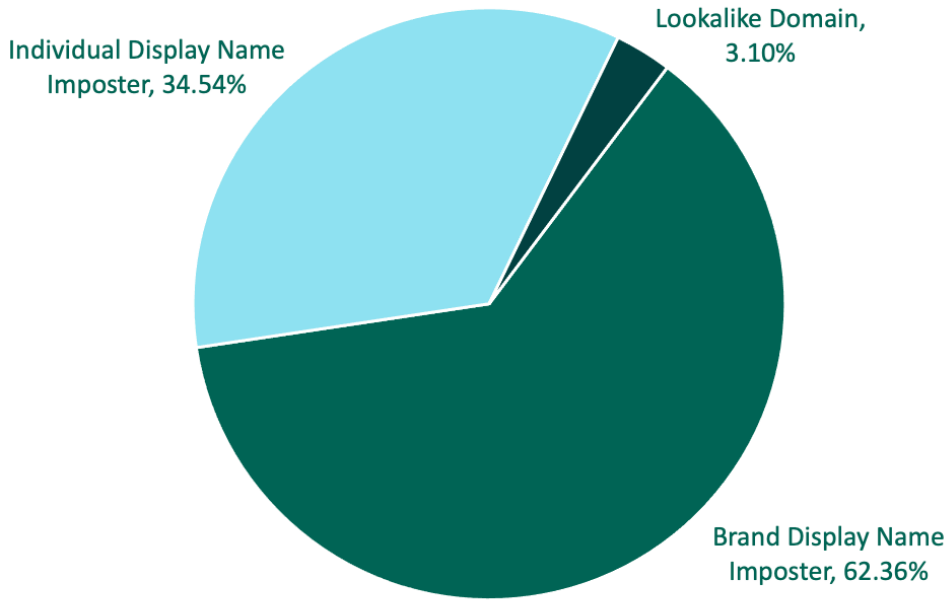
Brand Display Name Imposter - The email address is irrelevant. The attacker is relying on the fact that most mail clients only display the name portion of the From: header to impersonate a well-known brand.

Look-alike Domain - The attacker uses an email domain that is similar to the actual domain of the organization they are trying to impersonate.

Individual Display Name Imposter - The email address is irrelevant. The attacker is relying on the fact that most mail clients only display the name portion of the From: header to impersonate an individual.

In this report, we took a look at the volume of email spoofing attacks during the last month of Q2. At this time, display names impersonating a well-known brand such as Microsoft or Google made up 62.36% of attacks.

More than 34% of domain spoofing attacks were manipulated to appear as though they came from a specific individual such as a member of a corporate team or third party vendor.



Email Impersonation Attacks by Imposter Type

Conclusion

Domain impersonation is a key component to the success of online threats. Understanding how a look-alike domain might manifest and the type of content it may host is critical to early detection and removal.

In H1 2023, the average brand was targeted by 40 look-alike domains per month. This number is trending up as we move into the second half of the year. The most popular way to use a look-alike domain is to host Branded Content, which may include material related to a brand including logo or industry.

Look-alike domains hosted malicious content more than 10% of the time in H1, with Phishing representing the bulk of attacks. Cryptocurrency scams came in second, with just over 17% of volume.

In Q2, multiple TLDs were new to the top ten after increases in abuse doubling, tripling, and more for a handful of New and ccTLDs. Country-Code TLDs representing the majority of all TLD types for the first time, with 46% of overall volume.

Cybercriminals impersonated brand names most when launching email attacks, with more than 62% of display names masquerading as a well-known brand. High-ranking individuals or third-party vendors came in second, with 34.4% of volume.

The ways in which a domain can be manipulated are vast, and their ability to be modified for malicious purposes can occur at any point during its life. Gaining visibility into the behavior of a look-alike domain is the only way to identify suspicious behavior and remove the threat. In order to adequately minimize the impact of a look-alike domain, security teams should proactively monitor for new and suspicious domains and gather evidence that will justify rapid takedown.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-0823-gd-vm-r1