BOLSTER AI

MAY 2026

Leveraging AI and Automation to Stop Typosquatting Attacks

Top Level Domain Expansion Expands Attack Surface for Cyber Criminals

By Bolster AI Research Team

Table of Contents

I. Executive Summary

Safeguarding corporate assets is an ongoing challenge. Typosquatting has emerged as a major problem — one that top management may not recognize but can significantly damage a brand. Criminals use it to install malware, steal sensitive personal and financial information, and hold computers hostage.

The only possible way to address the problem is through artificial intelligence and automation. However, most fraud detection systems only solve a piece of the problem, offer rudimentary learning models, and are largely manual processes with no automation.

In response, Bolster AI developed the industry's most accurate algorithm with a false positive rate of 1 in 100,000. Its system takes down over 99% of fraudulent sites within 24 hours — all without requiring manual intervention.

As ICANN expanded Internet naming domains, problems rose. Today, there are more than 1,500 generic Top Level Domains, and the number continues to increase. This creates a huge attack surface resulting in about 50 million users falling victim to typosquatting ruses every year.

1,400+
Generic top level domains

50M+
Users victimized annually

1 in 100K
False positive rate

99%+
Takedown rate <24 hours

"Preemptive domain registration is an economically unfeasible defense strategy. AI-based monitoring and automated takedowns cost only a fraction of defensive registration."

—Bolster AI Research Team

II. New Top Level Domains Widen the Attack Surface

Hackers rely on domain name missteps to tarnish brands

For every action there is an equal and opposite reaction. As the Internet grew, ICANN began releasing what grew to more than 1,500 new generic Top-Level Domains (gTLDs). The influx provided organizations with much-needed web addresses but also became home to hackers who carved out lucrative businesses in typosquatting.

Typosquatting (also known as domain squatting and URL hijacking) is registering, trafficking in, and using an Internet domain name in bad faith. Human beings make mistakes, and hackers leverage them — setting up fraudulent sites with names very close to legitimate ones.

In Q2 2025, Bolster AI examined nearly ten million suspicious domains. Only 29% used legacy .com domain names — a 25% drop from 56% seen in 2019. gTLDs such as .info, .ru, and .link emerged as popular domains for typosquatting attacks.

Why TLDs Matter

- 1,500+ gTLDs — 5x more than 10 years ago
- Each new TLD creates more attack variants
- 29% drop in .com phishing — shift to new gTLDs
- Criminals adapt faster than manual defenses

Common Typosquatting Patterns

Typo Type	Example
Different top-level domain	.cm vs .com
Addition to end of domain	domains.com
Hyphenation	do-main.com
Vowel/consonant insertion	domaiin.com
Vowel/consonant swap	domian.com
Subdomain period break	domain.domain.com

In one case, criminals created a fake Reddit site using reddit.co instead of reddit.com, complete with an illicitly-acquired SSL certificate — giving visitors the impression of a legitimate, secure site with a green lock icon.

III. MX Records & Business Email Compromise

New sophisticated TLD-based typosquatting email scams targeting partners and employees have emerged. The bad guys send phishing emails from their bogus primary domains — complete with A records and MX records configured to appear legitimate.

The MX record essentially weaponizes the domain for Business Email Compromise (BEC). The criminal creates a malicious domain that mimics a legitimate email source, allowing them to bypass many advanced email security products.

Executives are more likely to open these messages. In some cases, mail reaches executives during business hours featuring urgent requests — such as paying an outstanding invoice immediately. Busy individuals often take only a cursory look and fall victim to the attack.

Example of an A-record

Domain	`business.com`
Host Name	`mail`
IP-Address	`11.22.33.222`

MX-Record Example

Domain	`business.com`
Mail Exchanger	`mail.business.com`
Priority	`10`

Why This Works

MX records give fraudulent emails the appearance of authenticity. The volume and consistency of customer-reported messages show how effectively attackers have embedded fraud into everyday digital interactions.

IV. Humans Cannot Stop Typosquatting Attacks

The primary challenge is one of scale. A six-letter domain has 12,000 different variants on common TLDs alone. It is impossible for a brand to defensively register all of these domains, nor can they be monitored manually.

One strategy to fight typosquatting is to preempt criminals by purchasing all possible domain variants. The average cost of annual registration is between $10 and $20 per domain. Using the low end ($10), purchasing every possible six-digit domain name costs $120,000. For a 10-character name, the price rises to $250,000.

However, typosquatters gobble up new domains as soon as they become available. The cost for their sites (when willing to sell) averages about $1,000 per name. Acquiring 100 from a typosquatter represents a minimum $100,000 annual investment — leaving thousands of other possible domains still available for cyber criminals.

The Scale Problem

- A 6-letter domain has 12,000+ variants
- 1,600 TLDs — 5x more than 10 years ago
- Typosquatters charge ~$1,000/ domain
- $10 x 12,000 = $120K just for 6-char names
- Manual monitoring is simply not feasible

Defensive Domain Registration Cost Estimates

Characters in URL	Possible Domains	Registration Cost
6	12,000	$120,000
7	15,000	$150,000
8	20,500	$205,000
9	22,000	$220,000
10	25,000	$250,000

In a ransomware scheme reported by Brian Krebs, typosquatters used .cm instead of .com to set up email and web servers targeting iTunes and AOL users — netting 12 million hits in three months in early 2018.

V. The Hands-On Approach: Site Takedowns

Corporations can try to identify and take down bogus sites, but hurdles arise. Legacy fraud detection tools are not designed to address this issue; they sorely lack the accuracy needed to detect fraudulent or phishing sites. The inaccuracy prohibits automatic reporting and takedown of typosquatted sites.

The challenges evolved gradually, so the tools to address them grew in an autonomous, hodgepodge fashion. One solution identifies a fraudulent site, but much more work is needed to determine where it is housed and take it down. Enterprises end up with a handful of solutions that each address only one segment of the problem.

Compounding the problem, current tools require extensive manual processing. These products rely on search support — they do not automatically scan, but provide search options that humans must input. Scanning via manual searches and legacy tools eats up time, manpower, and money. With TLD numbers swelling, staff becomes overwhelmed.

Manual Reviews Required

Each site requires human confirmation before a takedown can be requested, creating bottlenecks at scale.

Per-Takedown Pricing

Most services charge per takedown, making the economics prohibitive as attack volumes grow.

Evidence Gathering

Collecting screenshots and documentation is laborious; fraudulent sites come and go quickly.

Jurisdictional Barriers

Sites hosted abroad may fall under inconsistent copyright laws, adding legal complexity.

Even if a takedown is successful, criminals just create new pages on another server — and the corporation must repeat the entire process all over again.

VI. AI and Automation are the Solution

Technology advances created these problems, but they also offer a solution: automation at large scale. Corporations do not have the manpower to monitor and thwart malicious sites — but artificial intelligence and machine learning do. Yet not all AI systems are equal.

Bolster AI developed artificial intelligence that delivers human intelligence at machine scale. It combines deep learning, computer vision, and natural language processing to understand the intent of a page rather than static criteria. This algorithm is highly accurate and performs takedowns without human intervention.

The Bolster AI platform also considers whether an MX record has been established, a clear indicator a domain will be used for phishing campaigns. The platform identifies these sites as fraudulent and automatically submits takedown requests.

Bolster AI's algorithm recognizes minute differences between a legitimate Nike logo and a sophisticated illegitimate one. The result: a false positive rate of just 1 in 100,000 and a takedown rate of over 99% within 24 hours.

Bolster AI Technology Stack

Deep Learning

Accurate detection of brand hijacking via deep analysis of image and text content.

Computer Vision

Fast image recognition detects brand hijacking in milliseconds.

Natural Language Processing

Understands the intent of the website — not just keywords.

Threat Graph (10B Nodes)

Proprietary threat intel collected over years amplifies detection accuracy.

VII. Conclusion

Corporations are struggling to keep pace with the rapid rise in TLDs. With ICANN's expansion of Internet domain names has come a rise in criminals using typosquatting to tarnish brands large and small. All companies need to proactively search for bogus web sites and take them down before they and their customers suffer.

However, until now enterprises lacked both the financial and technical resources. The cost of purchasing bogus sites was prohibitive. The sheer volume of TLDs overwhelms security teams. Enterprises have not been able to move fast enough to identify and take down fraudulent sites before they cause damage.

The Bolster AI platform addresses these vexing issues. It offers corporations an effective, automated, proactive way to combat this rapidly growing problem. Industry leaders rely on it to protect their brand.

> *"How will your company ward off the bad guys who have your website in their crosshairs?"*
>
> *—Bolster AI Research Team*

CaptivateIQ

Customer Quote

"Even if you feel like you're a company that's not in a highly targeted space like financial industry, you still can be affected by attacks. Working with Bolster AI has been a great experience and it's especially important for us to help other out there."

—Senior Manager of Security @CaptivateIQ

Ready to protect your brand with Bolster AI?

Request a Demo

https://bolster.ai

BOLSTER AI

Making the Internet Safe for Everyone.

At **Bolster AI** our mission is to make the internet safe for everyone. That's why we created the first and only fully automated platform purpose-built to detect, monitor, and take down fraudsters on the Internet. We call it Automated Digital Risk Protection.

Our comprehensive platform offers the most efficient protection across web, social media, marketplace, app stores, and the dark web — helping the world's most recognizable brands combat fraudulent sites, phishing, and digital impersonation at scale.

Contact Bolster AI today:

2880 Lakeside Dr, Ste 150, Santa Clara, CA 95054

https://bolster.ai

Request a Demo