Look Beyond Typosquatting

PreCrime™ Brand for Impersonation

When people think of brand impersonation, typosquatting is often the first thing that comes to mind. While detecting typosquats is critical, relying solely on typosquatting tools to identify impersonation is risky. It's like diagnosing cancer online versus getting a thorough exam from a doctor. Our PreCrime™ technology goes far beyond simple string and typosquat matching to bring clarity to your brand protection efforts.

PreCrime™ Technology: A Step Ahead of Cyber Criminals

PreCrime technology is a cybersecurity game-changer, leveraging predictive AI to stop attacks before they happen. Unlike traditional detection and response methods, which rely on blacklists and signature-based security models, PreCrime predicts, disrupts and takes down malicious infrastructure - often before it even contains content.

BforeAI's predictive approach enables organizations to block out cyber criminals before they find a way in. Our technology uses behavioral analytics to help our customers shift from a reactive stance to a preemptive cyber defense model, preventing threats before they escalate into full-scale cyberattacks.

Why BforeAI Doesn't Flag Benign Typosquats as Threats

Not all typosquatted domains are malicious. Many are:

- **Parked domains**
- **Used for internal testing**
- **Registered for defensive purposes**

Flagging **every typo variation** would generate excessive noise with little value. Instead, we **analyze real-world harm**, focusing on:

- **DNS structure**
- **Registrant details**
- **How the domain interacts with the broader internet**

How PreCrime™ Technology Goes Beyond Typosquatting

Ransomware Attacks Predicted Months in Advance

Our system has predicted ransomware campaigns months before execution by identifying domain clusters with behavioral fingerprints linked to past ransomware operators.

A threat actor set up domains mimicking internal IT services. While no phishing was live, our metadata analysis flagged them due to similarities with past ransomware C2 setups.

Predicting Subdomain Registration Services Abuse

Many phishing kits and malware C2 panels use shared subdomain providers to evade scrutiny.

Something traditional typosquatting tools would completely miss.

We uncovered a large-scale phishing operation abusing a free subdomain service. Attackers rotated subdomains to bypass blacklists, but our models flagged them based on:

- **Registration velocity**
- **Shared SSL certificates**
- **Historical abuse patterns**

Tracking Redirector Domains and Mapping Infrastructure

Many phishing and malware operations don't rely on brand misspellings. Instead, they use intermediary redirectors that pass traffic dynamically to malicious sites.

We identified a network of redirector domains that never hosted phishing content directly but funneled traffic to impersonation sites based on:

- **Geographic targeting**
- **User-agent filtering**

***By monitoring their behavior, we took action before the final-stage phishing went live.**

A Prediction-Driven Future

Typosquatting detection is just one small piece of the cybersecurity puzzle. PreCrime's preemptive approach focuses on deep behavioral analysis, monitoring:

- Domain ecosystems
- Registration patterns
- Network activity

By understanding and detecting anomalous behavior, we predict and preempt cyber threats before they strike. Unlike traditional methods that rely on predefined signatures, our behavioral analytics model identifies even the most sophisticated and novel threats—long before they become active attacks.