

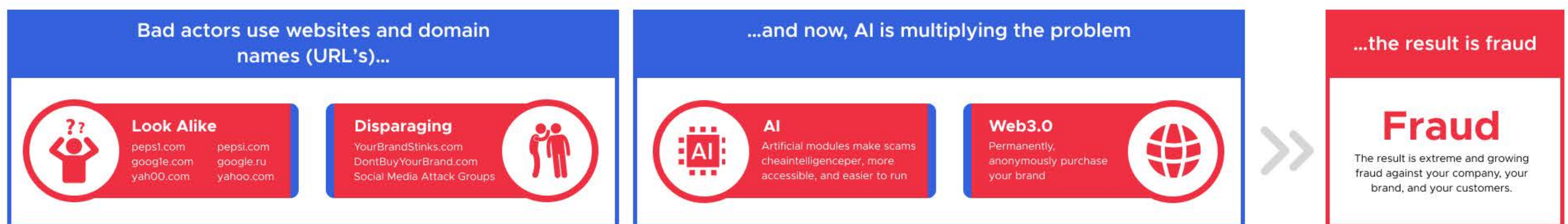


# AI-Powered Digital Brand Protection

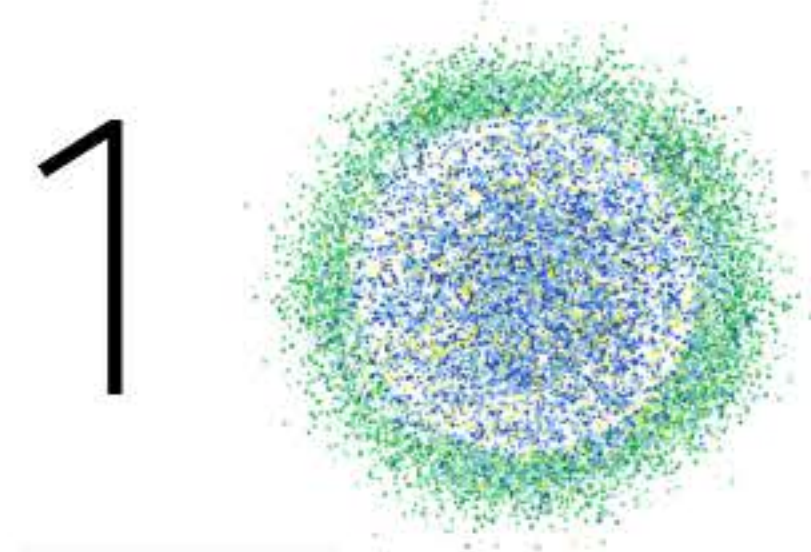
Find and shut down phishing attacks and fake websites *before* they begin

DomainSkate is a leading innovator of digital brand protection. Our predictive threat intelligence platform uses generative AI to find the domains and digital assets that will most likely be used by threat actors in phishing attacks, fake websites, and other online fraud. Once detected, our experienced team quickly works with our clients and channel partners to shut down the offending material, and continue to track the scammer to ensure they do not attempt to re-launch the fraudulent activity

Online Fraud Can Take Many Forms.  
Common Types We **Monitor** And **Enforce** Include:

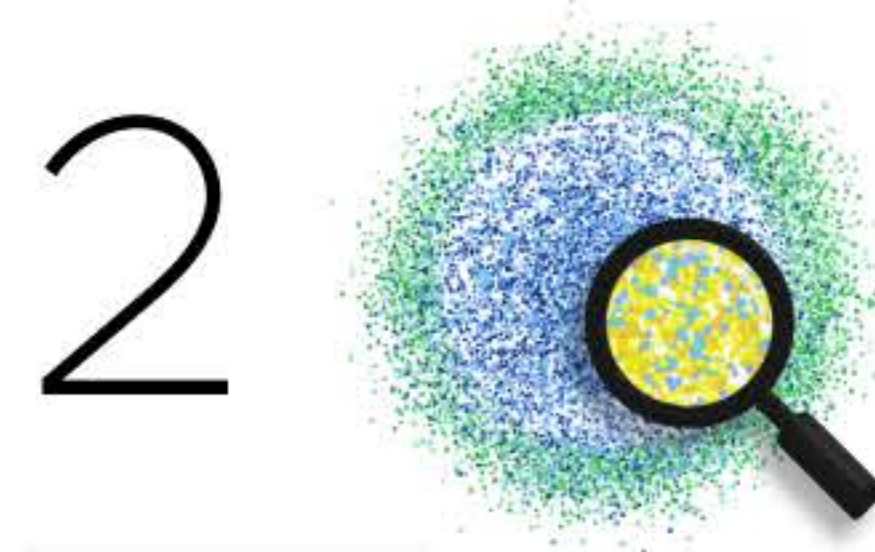


How our team of **DomainSkate** experts and our AI-driven platform protect your digital assets:



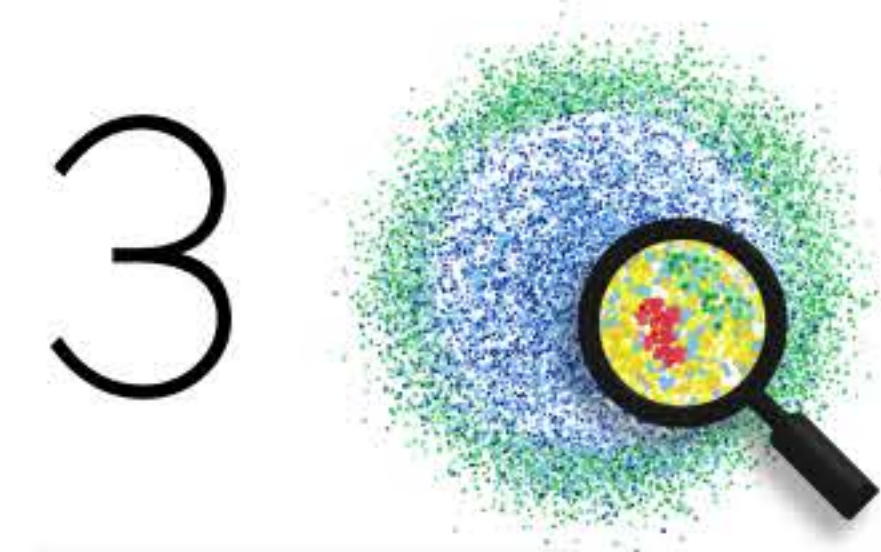
**Find**

Search 390M Domains against databases totaling over 500M



**Watch**

Monitor for changes every day and alert you for urgent issues



**Enforce**

Respond quickly with flagging, takedowns, or forced acquisitions

## Use Cases:

A web marketplace got spoofed, the scammers collected money but delivered nothing.

A lawyer files a trademark application, then needs to help their client protect the mark online.

An bank website is spoofed. Customers enter their password, and hacker empties customer's account.

A web developer builds a website, but needs to help their clients to avoid the new site from getting spoofed.

A scammer spoofs a non-profit or politician site, and collects donations fraudulently.



# We Use AI To Hunt for Scammers

We find online attacks against your brand like phishing, fake websites, and look-alike domains, before the scammer costs you money.

DomainSkate trains our generative AI platform to look for patterns that scammers leave behind. When we shut down a fake website or an email phishing attack, our database is used to find all historical details of that event so our AI can 'learn' what to look for in a future attack. When we see that pattern based on countries of origin, DNS records, IP Addresses, MX records (enables email), registrars, hosting companies, or redirects, our system gets increasingly better at finding these scams *before* they begin.

## Patterns We Find.

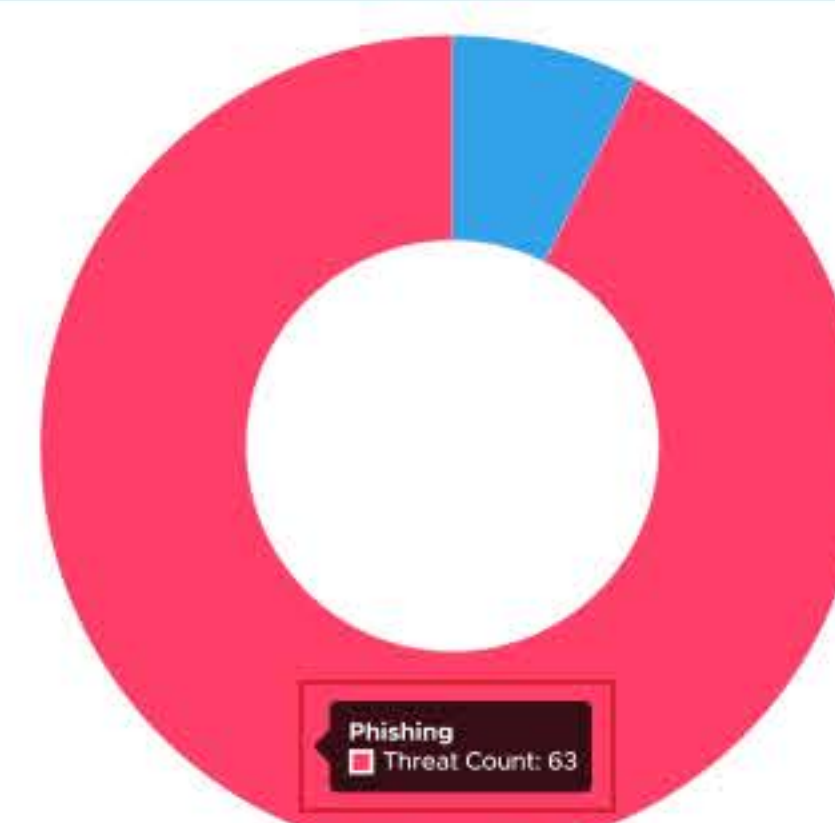


### Countries

Number of domains similar to yours in a 'heat map' by country - darker shades have more domain registrations.

#### INSIGHT:

In this example, 37 look-alike domains were originated in Germany. If the client does not have a base of operation in Germany, then this would be an area that we would focus on to determine if there is a threat to the business.

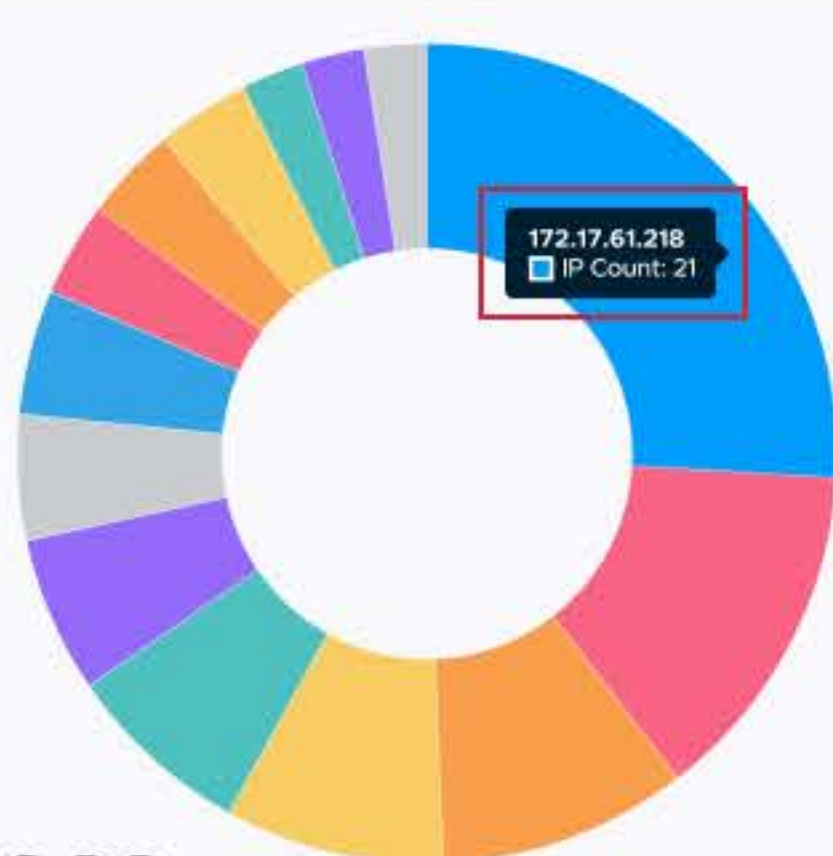


### Existing Threats

Domains that have previously been reported to contain malware, or used in a phishing email campaign.

#### INSIGHT:

Domains that are reported to a fraud prevention site are often abandoned by the scammer. We look for patterns to shut down new domains that share characteristics of previously reported domains.

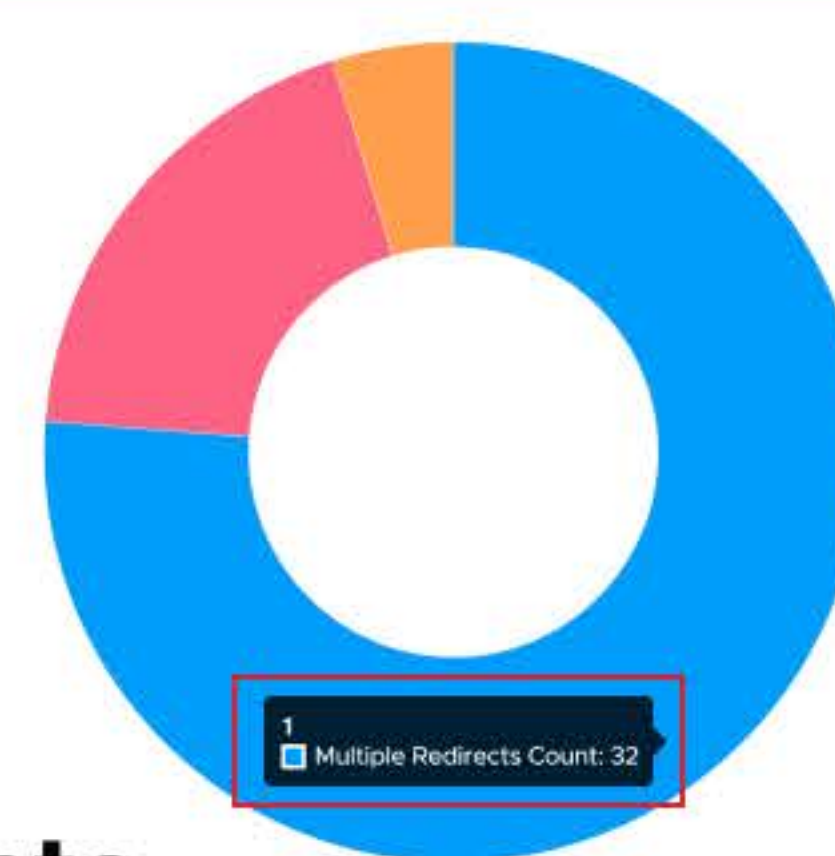


### IP Address

Number of domains similar to your brand which use the same Domain Registrar.

#### INSIGHT:

In this chart, 21 of look-alike domains share the same IP, which could be an indicator of threat activity, especially if that IP address had been used in any previous attack. These are attributes that our AI-powered platform analyses daily.



### Redirects

Number of times a domain similar to your brand is automatically redirected to another site (often invisible to user).

#### INSIGHT:

Scammers use redirects to hide their suspicious websites. If we find domains that look like your brand, but have multiple redirects to another site, then our system automatically flags that domain as a potential threat.



## About Us

Complete domain management, including monitoring, threat detection and removal services for both Web2 and Web3 top-level domains.

### We Prevent Online Attacks.

By scanning every internet domain every day, we can find everything that can be used to attack your brand. That's because our proprietary database of over 750M domains is compared to the entire internet daily, and we can alert you as soon as any attack begins so we can shut it down before any money is stolen from your customers, or any damage is done to your brand name.

### What Could You Save?

Loss per Phishing Attack  
**\$4.6 M**

#### Don't let a phishing attack cost you serious money.

There are multiple potential phishing attack domains already registered that could be used to attack your brand today. Stop the next attack by finding these domains, & shutting them down with DomainSkate. With DomainSkate's Fraud Preventer service, we will shut down up to 150 per year for you. According to the 2023 IBM / Ponemon study, one successful phishing attack cost an enterprise **\$4.6 Million**.

Register 500 Domains  
**\$10,000**  
per year

#### You could try to register hundreds of these domains, but shouldn't.

The price range to register a domain is generally an average of \$20 per year. We estimate that it would cost over \$10,000 per year to register 500 different versions of your brand name to protect your brand. But even if you could register all of those domains, the scammers would simply find more 'look-alike' and 'typosquatting' domains to attack your brand. Monitor, don't register, with DomainSkate.

### About Us

DomainSkate's AI-powered platform protects your customers and your brand from fake websites, phishing attacks, counterfeit products, social media hacks, and more. Get daily, weekly, or monthly insights that help take down malicious website before an attack begins. Our unique tools address both the current Internet, and the new blockchain-based Internet (Web3).

### Trusted By Worldwide Brands.

Customers trust DomainSkate to protect their brands from fraudulent web activity. Household names rely on DomainSkate to monitor hundreds of millions of domains worldwide, every day, find and mitigate threats to your brand, your revenue, and your consumer's funds.

NEU  
DOMAINS  
Digital Strategy & Brand Protection

HENRY SCHEIN®

Bitrefill

12TH  
TRIBE

CONFIDENTIAL  
BRANDS

BOAG PLLC  
INTELLECTUAL PROPERTY LAW

### For More Information

For more details on this report contact us for a free demo:

David W. Schropfer, EVP, Operations  
DomainSkate LLC, 175 Varick Street New York, NY 10014  
dws@domainskate.com  
calendly.com/dws1/30m

### DOMAINSKATE AT A GLANCE



Founded in 2015



Headquartered in New York City

## Internet

- 390M Domains Scanned Daily
- Proprietary Database of 400M+ Domains
- Integrated with 20+ Security Monitors
- Proprietary Internet Crawlers
- Proprietary Algorithm
- Artificial Intelligence Scanning
- Manual Screening from our Security Experts

## Web3 (Blockchain)

- Immediate Holds
- Purchase Recommendations
- Expedited Acquisitions

## Our Clients

Multi National Customers Worldwide

- Top 100 IP Law Firms
- Top 5 Financial Services Company
- Top 5 Hotel Chain
- Top 5 Insurance Company
- Top 5 Pharmaceutical Company
- Top 5 Medical Equip. Manufacturer
- Top 5 Self-Defense Manufacturer

## Counterfeits

- Contact Amazon, Alibaba and Ebay for fraudulent or unauthorized use of your products
- Contact Social Media channels
- Takedown recommendations
- Expedited removal

[www.domainskate.com](http://www.domainskate.com)

[protectme@domainskate.com](mailto:protectme@domainskate.com)