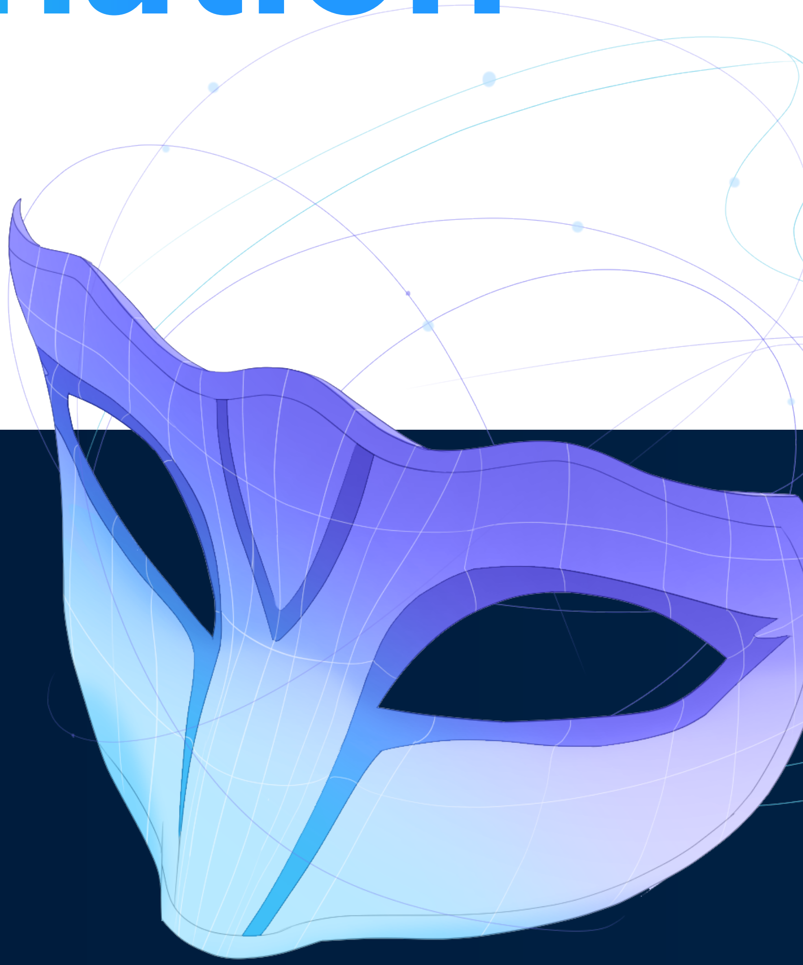
bfore.ai

Definitive Guide To

Online Brand Impersonation



Try it now - sales@bfore.ai

Introduction

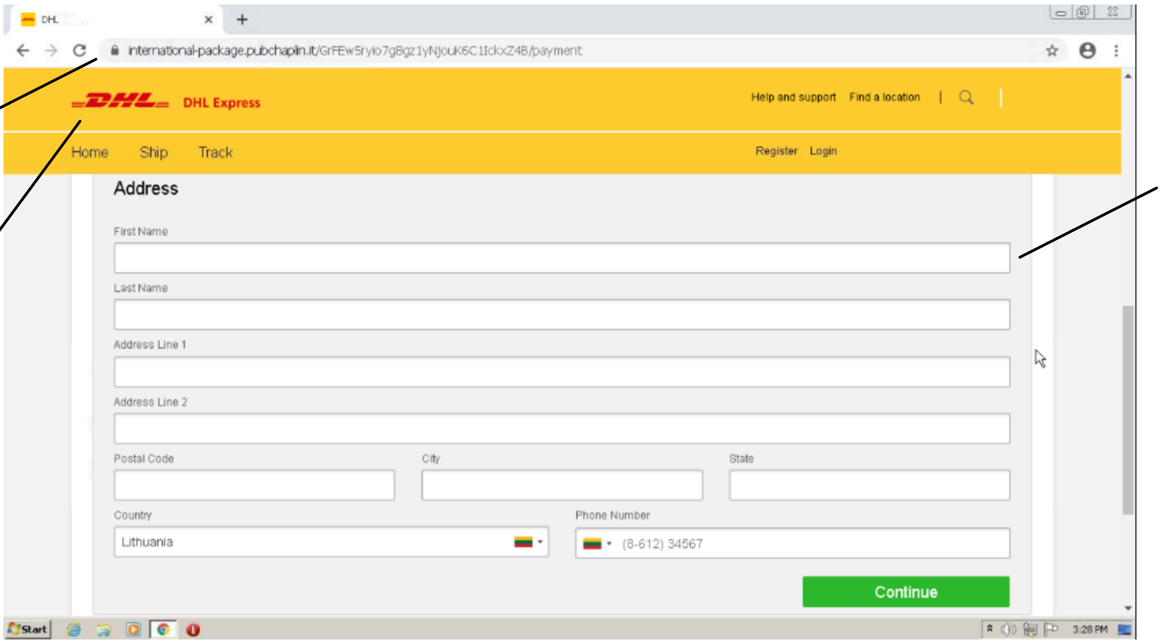
In business today, reputation is everything. Visitors build trust in a brand and have expectations for levels of reliability and security for anything associated with it. Attackers are cleverly conducting impersonation attacks to undermine carefully constructed confidence by posing as legitimate sites to deliver misinformation, install malware, and conduct fraudulent sales.

Attackers use fraudulent domain names to hijack legitimate traffic, tricking users into accessing their information. Fraudulent domain names appear close to the actual domain name, confusing users. According to a study by Proofpoint, nearly 96% of businesses have identical DNS names but different top-level domains such as .net instead of .com. With over 30000 malicious domains detected every day, controlling domain names and blocking fraudulent usage is crucial for organizations to avoid damaging sales and reputation. Many of these domains do not post any web content and remain dormant for several months before the threat actor launches an attack which can result in a data breach ultimately costing an average of 4.35 million USD.

This ebook covers the core concepts of impersonation attack concepts, tactics, and what organizations can do to stop attacks before they can damage their organization.

What is impersonation?

Impersonation attacks play off of a business's reputation and trust to trick victims. Attackers create imposter sites that mimic legitimate content to create an illusion that their content is legitimate. They trick users with phishing emails, social media links, and domain spoofing to catch unwary visitors. Once visitors make it to the site, they may be subjected to malicious code to install ransomware and rootkits, misinformation about the brand, or fake commerce to steal payment card information. The impersonation creates confusion between the real brand and the fake sites, leading visitors to associate malicious activity with the original brand.



Fake Domain

Known Brand

Asks for Details

international-package.pubchaplin.it/GrFEw5rylo7gBgz1yNJouK6C1IckxZ4B/payment

Address

First Name

Last Name

Address Line 1

Address Line 2

Postal Code	City	State

Country: Lithuania

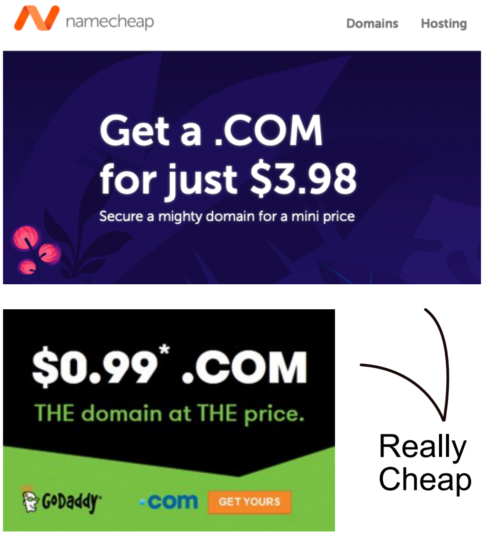
Phone Number: (8-612) 34567

Impersonation attacks are growing in number

Brand impersonation attacks are so effective that their usage has risen 171% from 2019 to 2021. One of the biggest vectors for accomplishing impersonation attacks is domain names. Using variations on an established domain name makes it appear that the link is legitimately associated with the business without raising suspicion for potential victims.

Why do attackers misuse web domains?

Domain misuse is easy for attackers to commit as it only takes a small amount of time and cash to register a fake domain. They use similar domain names to legitimate domains such as “www.youbusinessname.com” instead of “www.yourbusinessname.com” where the only difference is missing an ‘r’ in “business.” Attacks like this prey on the user’s inability to perfectly differentiate misspellings and slight differences at a glance.



Really Cheap

A trap awaiting for its vicitim

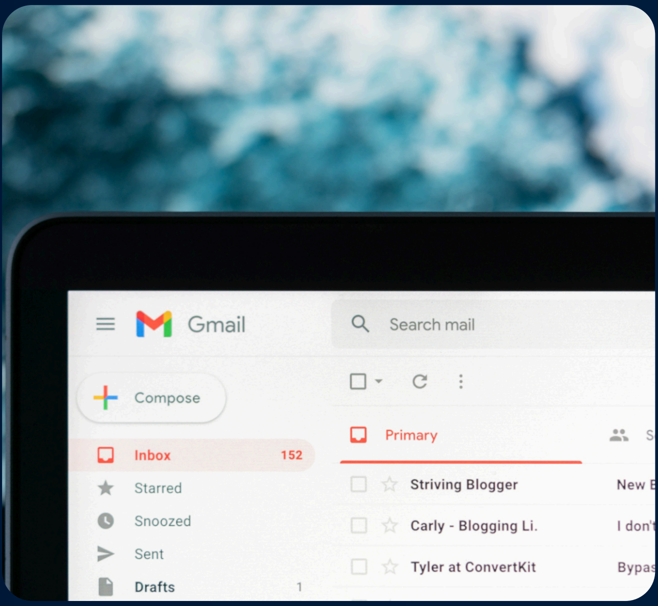
Malicious domains are dangerous artifacts affecting not only who mistyped the domain but those following links on websites, emails, or social media. Similar domain names draw users away from legitimate sites and direct them to locations controlled by attackers. The actual scope of the abuse is far broader as attackers misuse domains to damage a company’s reputation, deliver malware, conduct phishing attacks, or commit fraud.

There is no control over newly registered domains

Malicious URLs have become a mainstay of phishing attacks to lure victims to spoofed websites, appearing 3-4x more than malicious attachments. The most common cause of a data breach revolves around stolen or compromised credentials, with phishing attacks coming in second. In terms of website spoofing, the goal is generally to get users to sign in to what they think is their personal account allowing attackers to record their personal information and use it on the legitimate website and/or sell the stolen credentials on the dark web.

Companies at risk

Employees are a prime target for attackers looking to conduct more significant attacks against the organization. The same psychology that makes it difficult for consumers to notice a fraudulent domain applies just as readily to company employees.



Suppliers can be a backdoor

Phishing emails that originate from similar domains to the corporate domain or vendors and partners don’t always flag as a trick to employees. Instead, they appear to be legitimate, and information or requests contained in the email are assumed to be valid. This attack is so effective that 94% of organizations have observed fraudulent domains used in emails for an attack.

Account Takeover

Impersonation is one of the primary paths to a successfull account take over attack. Stopping impersonation attacks before they become active is the best way to protect your employees and assets.

A silly mistake can cost thousands

In ATO type attacks, perpetuators with stolen credentials can masquerade as actual users, accessing the same resources as the user could. Executed programs can install ransomware that creates direct revenue for attackers or launch a rootkit on the endpoint, allowing attackers a tunnel into the internal network. With a rootkit, attackers can stage more complex and persistent attacks that can compromise large quantities of data over time with little risk of being caught.

$150,000

Is the cost of a succesful phishing attack

$170,000

Is the cost of a succesful data breach

$330,000

Is the cost of a succesful security incident

Trust no one

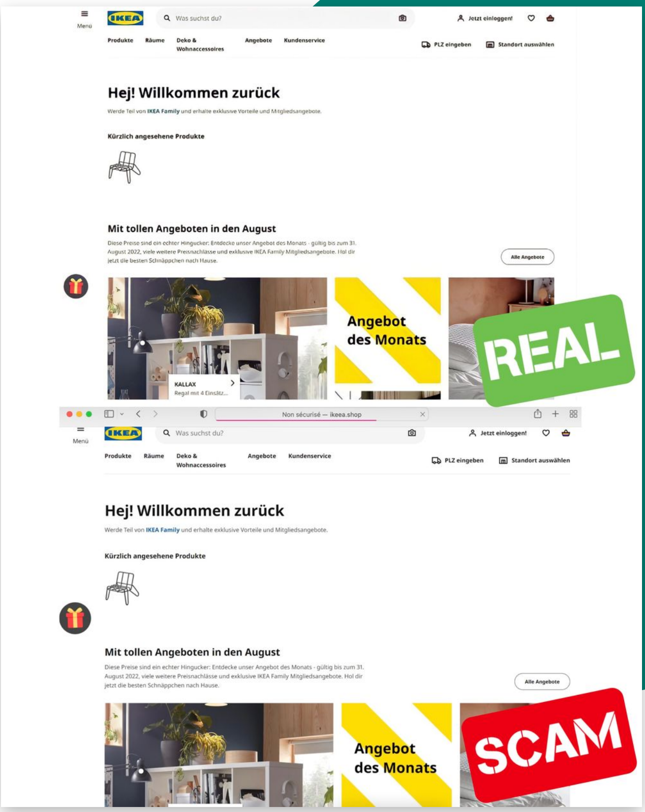
Attacks may be as simple as asking users to fill out a form to update their password, such as the Twilio breach in August 2022 where employees were asked to update their login passwords via a malicious domain that recreated their IT service management page from Okta, their sign on provider. In this breach at least one employee fell for the scam which allowed the threat actor to access sensitive customer information and company data.

Protect customers & stakeholders

Another target of many fraudulent domain attacks is the consumer. Consumers browsing a fraudulent domain are often presented with a site that is an apparent duplicate of the domain they expected, adding to the challenge of differentiating the fraud. Any information given is interpreted as being from the actual organization, and the storefronts provided appear every bit as functional as the original.

Brand reputation can be hit hard

Tricked users purchase products on the site that will never be delivered and willingly hand over their credit card information to attackers, such as in the scam targeting IKEA, detected by Bfore.Ai in August 2022. In this scam threat actors created a website under the domain ikeea[.]shop and duplicated the original site (ikea.com) making it near impossible to differentiate between the real and the fake. Once a purchase is made on the malicious site, users are disappointed when their purchases never arrive and infuriated when their cards are used illegally.



Hej! Willkommen zurück

Werde Teil von IKEA Family und erhalte exklusive Vorteile und Mitgliedsangebote.

Kürzlich angesehene Produkte

Mit tollen Angeboten in den August

Diese Preise sind ein echter Hingucker: Entdecke unser Angebot des Monats - gültig bis zum 31. August 2022, viele weitere Preisnachlässe und exklusive IKEA Family Mitgliedsangebote. Hol dir jetzt die besten Schnäppchen nach Hause.

Hej! Willkommen zurück

Werde Teil von IKEA Family und erhalte exklusive Vorteile und Mitgliedsangebote.

Kürzlich angesehene Produkte

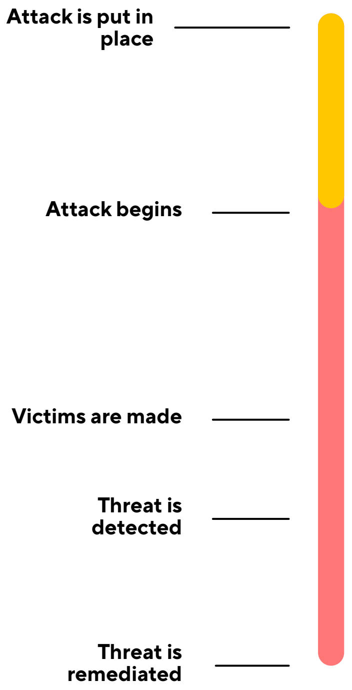
Mit tollen Angeboten in den August

Diese Preise sind ein echter Hingucker: Entdecke unser Angebot des Monats - gültig bis zum 31. August 2022, viele weitere Preisnachlässe und exklusive IKEA Family Mitgliedsangebote. Hol dir jetzt die besten Schnäppchen nach Hause.

Even though the owner of the existing domain does not host fake domains, consumers still feel that the existence of such a site is a sign of weakness in the organization's security. Any misinformation delivered, or mistreatment suffered by the customer is directly blamed not on the fraudster but on the proper domain owner. Companies unaware of the fake domains will continue to suffer the ill effects of their existence until they are aware of the domain and take appropriate action to remove it.

How online impersonation attacks are carried out?

Online impersonation attacks are more than just creating and loading a spoof website with misleading or malicious content. Effective use of impersonation attacks requires driving others to the content. This is accomplished by embedding links in social media, email, SMS, and other common communication channels. Users are enticed to click on these links either through messaging that creates a sense of urgency or by making the link appear to be a standard part of a workflow such as invoicing.



The attacker wants individuals seeing the links to believe it is a legitimate website, not a fake one, so the exact style and layout will often be copied. When visitors enter the site, the consistent theme will help to reassure them that nothing is amiss, helping build confidence and hopefully encouraging the visitor to stay.

94% of organizations have observed fraudulent domains used in emails for an attack

Defending from Online Impersonation

Organizations are not without recourse for protecting themselves against fraudulent domains. Creating content to populate fraudulent sites and seeding out fake links does not happen instantly. Companies that watch registrations for similar domains and swiftly issue takedown orders allow companies to stop attacks before they have time to ramp up.

Train your team

Building awareness of impersonation attacks with employees and staff is a component of protecting your organization. Team members aware of these attacks and their potential impact serve as additional layers of detection, helping identify and alert when they are seen. In addition to supporting the organization's identification efforts, awareness helps them not become attack targets, preventing them from going to spoofed sites where they could become victims of phishing or malware.

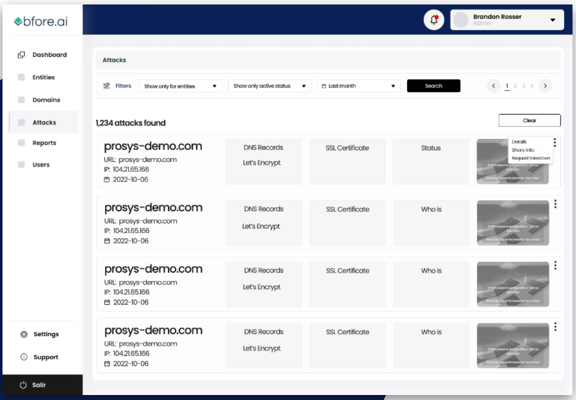
Humans can *still* be deceived

While awareness is an important layer, it is not a sufficient substitute for an automated solution to proactively detect and defend against impersonation. As individuals are not perfect identifiers, it only takes one misstep in detection for an employee to fall victim to such sites, leading to data disclosures or malware infections. Technology solutions defending the organization are far more accurate and consistently apply the layer of protection throughout the organization, improving its overall effectiveness.

Automate to win

Chasing down squatters is not a task that is accomplished once, and you can return to business as usual. Squatters will repeatedly return with new spoofed sites and faked domains, attempting to lure in the unsuspecting. Managing this challenge requires continuous monitoring to detect when they return and eliminate them as expeditiously as possible.

Monitoring sounds like a straightforward process, as all domain registrations are essentially public, so watching for similar domain names to appear on the list should be trivial. However, in reality, the number of permutations that attackers can make to an existing domain is quite significant when factoring in the combinations of substitutions, omissions, and transpositions of letters that attackers could use to mimic a single domain.



1,234 attacks found

prosys-demo.com
URL: prosys-demo.com
IP: 104.21.65.166
2022-10-06
DNS Records
Let's Encrypt
SSL Certificate
Status

prosys-demo.com
URL: prosys-demo.com
IP: 104.21.65.166
2022-10-06
DNS Records
Let's Encrypt
SSL Certificate
Who is

prosys-demo.com
URL: prosys-demo.com
IP: 104.21.65.166
2022-10-06
DNS Records
Let's Encrypt
SSL Certificate
Who is

prosys-demo.com
URL: prosys-demo.com
IP: 104.21.65.166
2022-10-06
DNS Records
Let's Encrypt
SSL Certificate
Who is

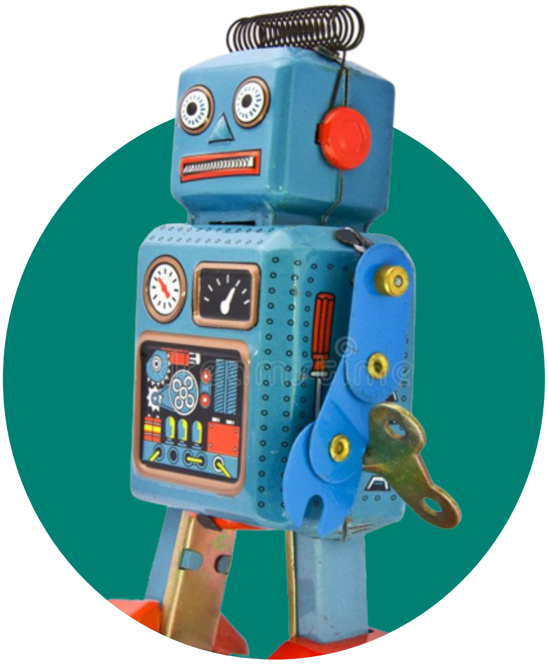
Solutions exists

Tools like Bfore.Ai designed to automate the preemptive identification of malicious vectors helps get the job done.

With over 5 million new domains registered per month (more than 180,000 per day) and considering the number of possible permutations of similar domain names, manual efforts to monitor new registrations are time-consuming and not exceedingly effective. ... Bfore.Ai detects over 120,000 malicious domains per month...

Build your toolbox

Automation is essential to protect against new threats. A single malicious actor could register hundreds of domains to impersonate your brand. If you don't actively monitor your domain names, you'll never know. Effective brand protection relies on automation to keep track of all potential attacks



Web Domain Monitoring

Continuous monitoring of malicious domain DNS changes and new registrations is ineffective with manual processes. With the volume of daily domain changes worldwide, new registrations are easily missed. Massive workforce investment is required to identify potential threats and analyze their content for verification.

Automation is crucial to avoid threats correlated to your domain and those of suppliers. With automation, the tedious identification and analysis are handed off to machines that excel at such tasks rather than humans, who become bored and have other jobs to manage. Reducing this load allows staff to validate identified threats more effectively and leverage takedown capabilities integrated with the service, streamlining the entire process.

Social Media Monitoring

Social media is used not just by the organization alone but also executives whose messaging is considered an alternate voice of the company. Taking over social media accounts or masquerading as legitimate accounts gives attackers a receptive channel to deliver malicious messaging, such as toxic URLs or misinformation.

Leadership is at stake

Monitoring the company brand and executive profiles must be managed 24/7, as any lapse can rapidly lead to trouble. Optimal solutions have automation to monitor continuously, efficiently detecting problems before attackers can exploit them. Built-in takedown capabilities are vital for an effective solution, rapidly resolving the issue once detected.

Threats on social media continues to rise with a 47 percent increase from Q1 to Q2 2022

Remediating an attack

Just because the registration process has minimal validation for new domains does not mean there are no rules regarding appropriate registrations. Domain names that infringe upon existing business names, trademarks, or exist for fraud can be removed through a takedown process. Identifying and requesting a takedown falls to the existing domain holder, making the case to authorized registrars for domain removal.

Build your evidence

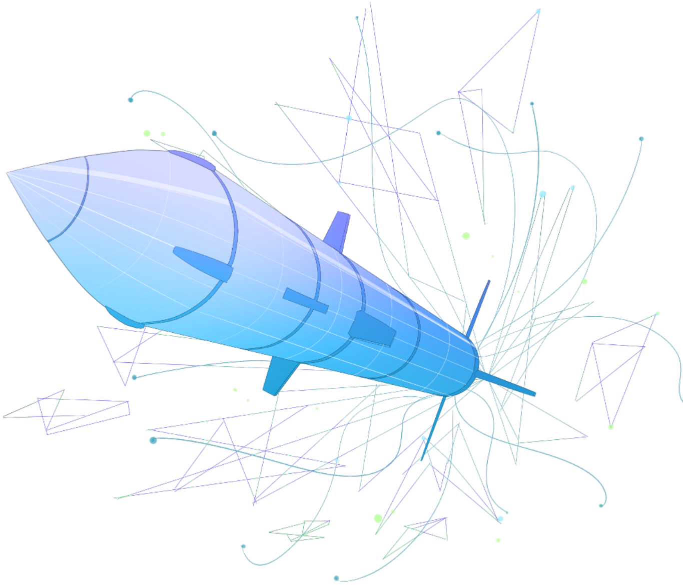
Companies must outline why they believe a domain was registered in bad faith. Finding a similar domain does not ensure it is sufficient grounds for an immediate takedown. Numerous businesses have identical names and use them as part of their registration.

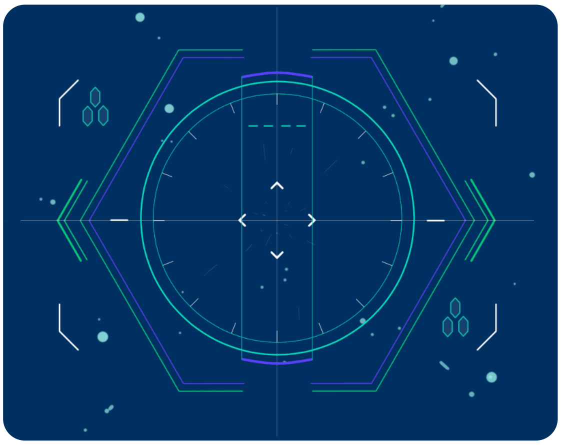
Domain look a like may not be everything

This was seen in the case of Nissan motors vs. Uzi Nissan which persisted for years and required a court to decide ownership of the domain.

How to takedown an attack?

The takedown process usually is full of manual steps to manage. Contacting the abuse team at the domain registrar, gathering evidence about why the domain is acting maliciously, and continual follow-up, working with the registrar until the domain is removed. This process is repeated for every suspect domain permutation, creating a set of communication threads. Managing this process without automation requires significant time and labor investment across your organization.





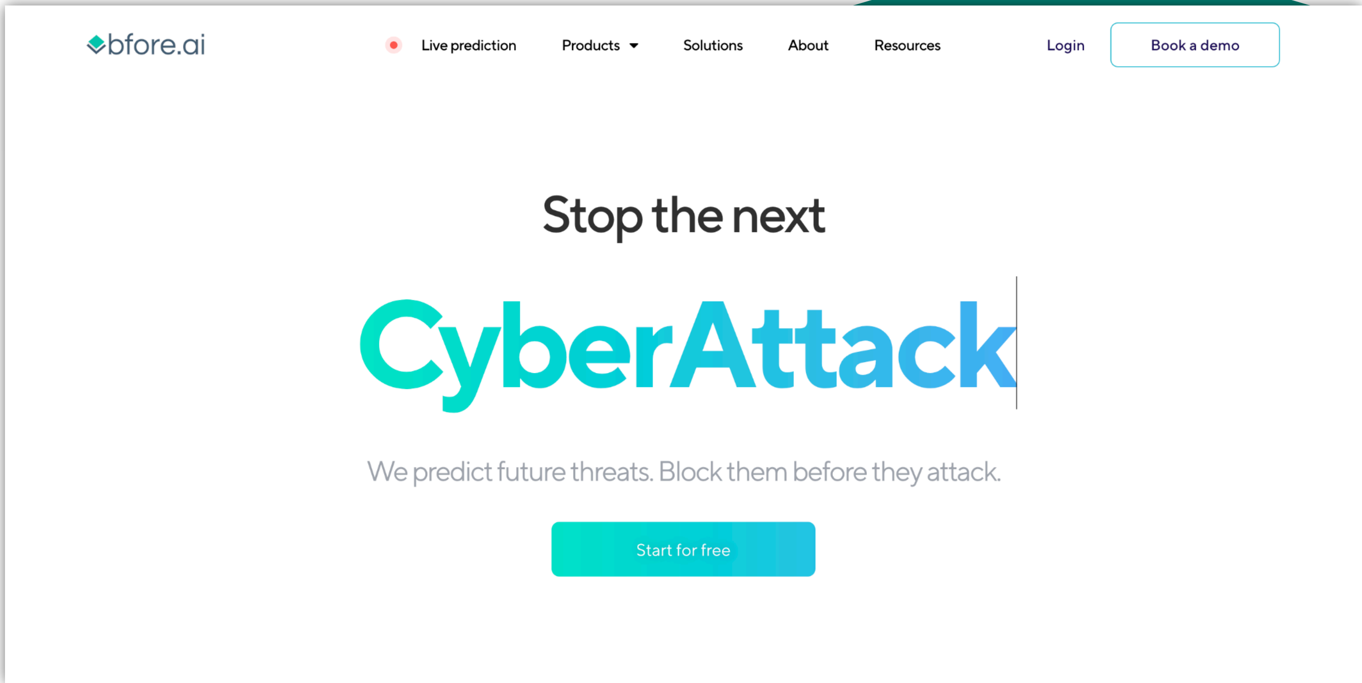
Do it faster

In order to do this faster, safer and to achieve a successful takedown, working with an authorized security partner is crucial. Security takedown experts will know how to gather evidence and push domain registrars to achieve takedowns, sometimes in even less than 10 minutes.

Once a takedown occurs, the public registrar eliminates the record of the fraudulent domain. Even if users click on links containing the name, the DNS servers will not be able to resolve it to an IP address, effectively stopping its use of it as an attack vector.

Go predictive, stop chasing

Stopping fraudulent domain usage quickly after registration is vital for eliminating an attack before it damages an organization. Doing this requires continuous monitoring of all new and existing domains for the existence of fraudulent activity. Bfore.ai empowers organizations with automated monitoring and assessments of registered domains. Bfore.ai has a comprehensive set of solutions to defend your organization against fraudulent activity, deploying countermeasures to limit the impact and managing the takedown process.



Stop the next

CyberAttack

We predict future threats. Block them before they attack.

Learn more how prediction can help

Book a Demo

Visit Website

bfore.ai