Brand Impersonation: It's an InfoSec Problem

Bolster's Shashi Prakash on How to Lead Response to This Growing Fraud Trend

BOLSTER

ISMG
INFORMATION SECURITY
MEDIA GROUP

BOLSTER

Shashi Prakash

Brand impersonation – it isn't just a marketing or reputational issue. It's an InfoSec problem, says **Shashi Prakash** of Bolster. He describes the growing issue and why security is best positioned to lead detection and response.

In this video interview with Tom Field of Information Security Media Group, Prakash discusses:

- The prevalence of brand impersonation;
- Why it's an InfoSec problem;
- The impersonation takedown process.

Prakash is the CTO and co-founder of Bolster. He has extensive experience working at the intersection of cybersecurity and AI. Prior to Bolster, he was a security researcher at Cisco, where he developed machine-learning algorithms to catch billions of spam messages.

Growth of Brand Impersonation

TOM FIELD: Your company seeks out and takes down sites that make illicit use of company brands and logos. How prevalent is this problem, and what costs does it exact from the companies that are fleeced?

SHASHI PRAKASH: Every company that has an online presence today has this problem in one form or another. It's a massive issue that's been going on for the last few years. In 2019, there were more than 4 million scam sites, and companies lost about $400 billion. In 2020, we expect to have about 5 million sites, with almost 14,000 sites discovered each day. The financial damage because of this will also be more than last year. It's a growing problem, and it needs to be tackled right away.

"Brand infringement and impersonation are a new attack vector, in addition to the traditional attack vectors we've seen for any organization."

It's an InfoSec Problem

FIELD: It's easy to see that it's a brand issue and a marketing issue, but why is it an InfoSec issue?

PRAKASH: InfoSec today sits at the center of it all. InfoSec works with various departments in an organization, including finance, customer support, IT, fraud and risk. And InfoSec now is more and more responsible for not just internal attacks, but also attacks that are threatening to the brand from the outside. An external attack passes on to become an internal threat because the same actors who are compromising a brand's reputation externally can change their attack tactics and get into the internal network and do other kinds of damage.

That's why this is an InfoSec problem. Brand infringement and impersonation are a new attack vector, in addition to the traditional attack vectors we've seen for any organization.

How InfoSec Can Respond

FIELD: Why is security in the best position in the organization to respond to these violations?

PRAKASH: An arsenal of tools and techniques are available to InfoSec teams, and these tools and techniques can be used to fight some of these external threats. That's why we think security is in the best position to fight these attacks. For example, if someone is using a company's logo and doing some kind of impersonation or selling counterfeit goods, those attacks can be stopped by internal tools and methods. If security organizations get in on this problem in the early stages of the attacks, they can quickly solve them.

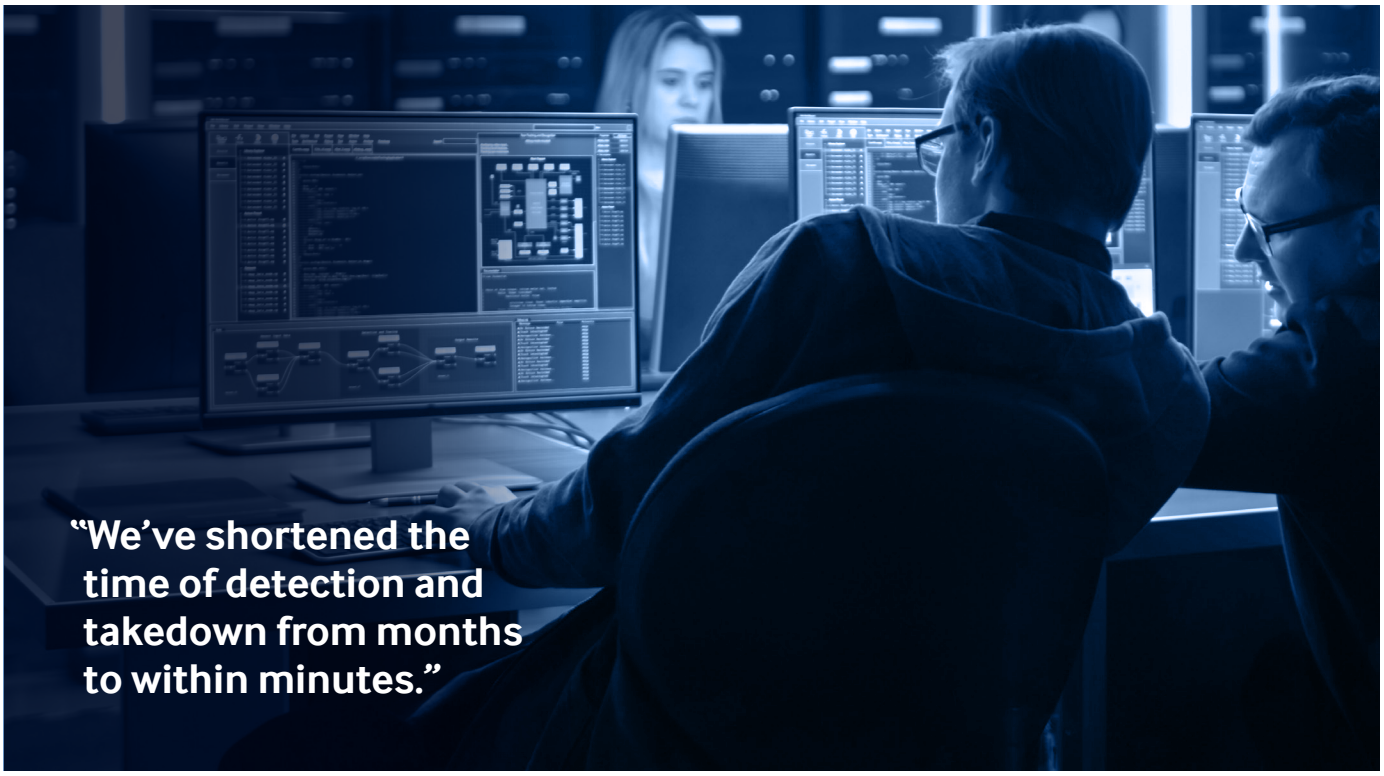
Automated Solutions

FIELD: What automated solutions lead to faster detection and response of these issues?

PRAKASH: Automation is the key to fighting this problem. If we don't fight this problem of scale with scale, then it's a losing battle. It's a very labor-intensive task if you have to go out and find these sites and analyze and detect these violations manually. That's what we're trying to change with automation. We've built a technology from ground up that can look at a website just like you and I would, as humans would look at it, and identify different kinds of counterfeiting, phishing or other kinds of impersonation targeted toward a brand.

The tricky part is: There are legitimate cases where a brand's logos or trademarks could be used. For example, if someone is writing a news article or if a vendor or partner of the brand that's allowed to use their trademarks and logos is using them. So, a traditional, simplistic method of detecting these incidents would not work. You need to understand the intent of the site. We've built deep learning models, or AI models, to look at a site from the visual aspect and the natural language content aspect and really understand the intent of the site. That's why we are able to do this automatically at scale and with high accuracy.

That's one part of it, and the second part is the takedown. How do you conduct automated takedowns at scale if there are millions of sites coming up? The detection part needs to be extremely accurate to not cause any false positives or errors. Then, the takedown part can be automated. We've automated both of these aspects of fighting counterfeiting and fraud. It's much faster and can scale really well to solve this problem.



Bolster's Approach

FIELD: Talk to me about the takedown process and some of Bolster's most successful efforts.

PRAKASH: We've shortened the time of detection and takedown from months to within minutes. We can detect and take down sites in about three minutes in certain cases where we have an API integration. That's what we've really automated. We protect some of the world's largest, most beloved and most well-known brands, including Dropbox, LinkedIn, Zoom, Fitbit and Booking.com.

During the pandemic, Zoom saw an explosive growth in its user base, as everybody who was working from home had to start using online collaboration tools and Zoom was the most prevalent. Bad actors or criminals try to create counterfeit websites targeting Zoom. When we started working with Zoom, in the first 24 hours, we found about 1,500 sites, and we took 99% of them down. To highlight the scale of the problem, these sites were across 28 different hosting providers spread across seven different countries. That gives you an idea of how we're fighting this at scale and helping some of the large brands solve the problem of online counterfeiting in a really fast way.

2021 Fraud Trends and Responses

FIELD: 2021 is here. What fraud trends concern you the most in the area of impersonation, and how are you going to help your customers respond?

PRAKASH: One of the clear trends is the availability of automated tools that bad actors can use to create fraudulent sites. For example, phishing kits are available for $20 or $25. A bad actor can use one to deploy counterfeit or fraudulent sites or phishing sites at scale. Hundreds of these sites can be registered and set up within minutes. In order to fight this problem of scale, solutions need to be automated, as well. Just as you cannot bring a knife to a gunfight and hope to win, an approach that's not scalable is not going to work.

The trend of sophistication and automation around creating these fraudulent sites has increased over the last few years, and we are trying to fight it with automation. InfoSec teams in a company should work with other teams, including fraud, risk and IT, to solve this problem, along with an automated solution like ours. That's what we think should happen in 2021. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io