



INTERVIEW TRANSCRIPT

Navigating the New Internet Attack Surface

Bolster's Shashi Prakash on Responding to the New Volume and Velocity





SHASHI PRAKASH

Prakash 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.

It's the largest attack surface in history, and adversaries are taking advantage by launching attacks at an unprecedented volume and velocity. **Shashi Prakash** of Bolster discusses how to monitor and manage this new and shifting range.

Prakash, the CTO and chief scientist at Bolster, defines the new attack surface and how it has evolved. In an interview with Information Security Media Group, he discusses:

- The volume and velocity of attacks;
- Nuances by industry;
- Emerging threats to prepare to face in 2022.

The Internet Attack Surface

TOM FIELD: The internet attack surface can mean different things to different organizations. How do you define it by what you see today, and how has it evolved in this past year?

SHASHI PRAKASH: By internet attack surface, we mean this broad spectrum of all external online threats that might be targeting your brand or your organization. All businesses are moving to online these days, and most of it has been driven by the pandemic. As a result of that, our presence has gone into a bigger, broader spectrum. Now we don't just have a website; we also have a presence on social media or other platforms that we use for our day-to-day business. Internet attack surface means covering all of these different external sources that you have daily interaction with that may be used to target your organization.

Top Attack Types

FIELD: What are some of the predominant types of attacks you see today, and why are they so successful?

PRAKASH: There are many attack surfaces that people can target you through, and one of the primary ones these days is email. Email is not a new attack vector, but right now we're seeing vendor email compromise, where bad actors are creating fraudulent domains, or types of sporting domains, to target not just your organization, but also your vendors and the partners you interact with. These attacks are incredibly easy to do because bad actors can create sporting domains across thousands of different top-level domains and just start targeting your organization through phishing campaigns. Even though your internal structure or security posture is robust, the external posture may not be as robust. So your vendors may still be compromised by someone pretending to be you or your organization.

There are also a lot of social media-based attacks. Everybody has a social media presence on Twitter, Facebook and a lot of these other popular platforms, and bad actors are doing executive impersonation or brand impersonation or impersonating goods that your organization may be selling online and selling fraudulent, counterfeit goods.

Attack Types Based on Industry

FIELD: How do attacks vary by industry? For instance, I would think in financial services there are a lot of account takeover attempts because adversaries are trying to get to the money. In healthcare, perhaps they're trying to get to personally identifiable information. What industrial differences do you see?

PRAKASH: For consumer-facing brands selling, for example, merchandise or luxury goods online, bad actors are creating websites to sell fraudulent goods. There are toolkits available to create fraudulent websites pretty easily, and they can be deployed in a matter of minutes. It's a direct revenue hit for these large, consumer-facing organizations. In non-consumer-facing verticals, bad actors are using account takeover for large e-commerce platforms and banking and financial organizations. And email-based attacks target the vendors and partners of organizations.

Volume and Velocity of Attacks

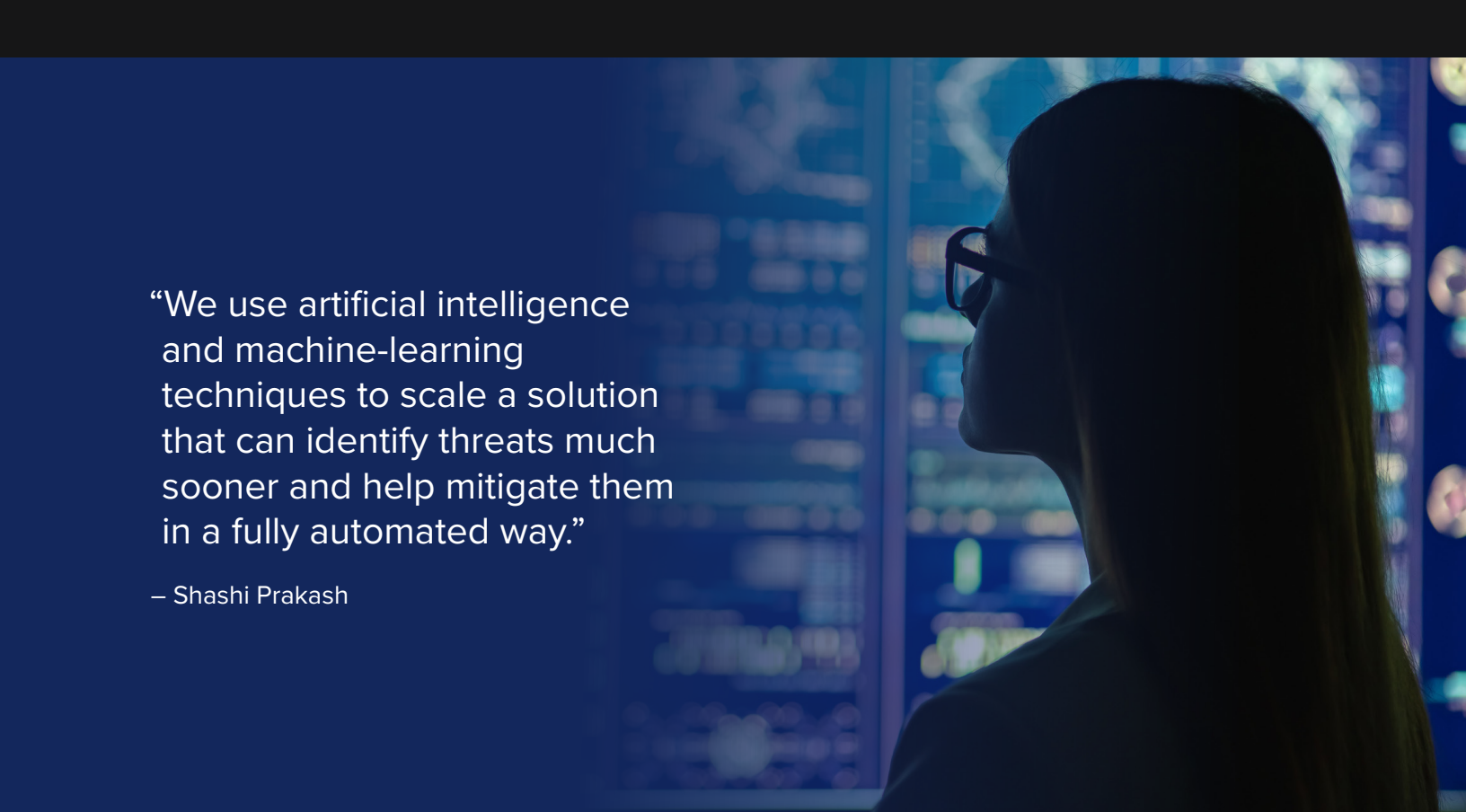
FIELD: Given everything we've seen this year, from SolarWinds to Colonial Pipeline to Kaseya, the average consumer knows that we've got a heavy volume and velocity of attacks. What do security leaders in particular need to know about the speed and the scale of the attacks that you're seeing?

PRAKASH: This is a problem of speed and scale. Bad actors have a lot of advantage because, for example, for a six-letter dot-com domain, you can create typosquatting variants of the order of 70,000 to 80,000 across different TLDs. With this kind of scale, anybody can spin up fraudulent websites targeting



“If we don’t find these attacks at scale and with high speed, the bad actors have already won. Security leaders need monitoring and visibility into these attacks.”

– Shashi Prakash



“We use artificial intelligence and machine-learning techniques to scale a solution that can identify threats much sooner and help mitigate them in a fully automated way.”

– Shashi Prakash

your organization within minutes and start targeting all of your employees, vendors and customers in a very short amount of time. And the longer these attacks are there on the internet, the larger the number of people who will get attacked. If we don't find these attacks at scale and with high speed, the bad actors have already won. Security leaders need monitoring and visibility into these attacks. They need to be aware of what's going on, what their internet attack surface looks like, and what different vectors they should be monitoring. And if they find something, they need to know how to go about mitigating it.

Emerging Threats in 2022

FIELD: As you look toward 2022, what emerging threats are you paying the most attention to today?

PRAKASH: All the different components of the internet attack surface – social media, websites – are platforms where people can share intellectual property and sensitive data. So there are different ways in which your organization can be targeted. In 2022, the complexity of this will grow. For example, someone can create a fraudulent website to sell counterfeit goods and advertise it on social media. Or they can put up a YouTube video talking about how you can win a cash reward. These kinds of scams will be perpetrated across multiple platforms and created in a very automated way. Even today, they're quite automated, but the scale of it will grow, with a lot of tools available for the bad actors to create them quickly. It will be critical for brands to have visibility into all the different kinds of threats that are out there targeting their organizations, and they'll need automated tools to help in this fight.

The Bolster Approach

FIELD: What is Bolster doing to help its customers monitor and manage the shifting, growing, exponential attack surface?

PRAKASH: We use artificial intelligence and machine-learning techniques to scale a solution that can identify threats much sooner and help mitigate them in a fully automated way. We have built a lot of capability around this to find different kinds of threats across the internet attack surface. For example, we can monitor all social media platforms or all third-party sharing sites, like Pastebin and GitHub, and tell you when someone is spinning up a fake Facebook page to sell something that infringes on your brand. Our tools do this automatically, and the number of avenues where they can be used is growing rapidly.

We also help you mitigate some of these attacks. If someone is weaponizing a domain to create a phishing attack, our solution can automatically figure out what's happening on the site, based on its content. Our solution includes global detection and natural language processing. Once you've identified these threats, we know how to mitigate them, with an automated piece that contacts the hosting provider and shuts them down automatically, within minutes sometimes. We can help in the entire life cycle of the threat, from before weaponization to weaponization and even after mitigation. ■

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 INFO SECURITY® Just for Credit Unions  GO INFO SECURITY®  HEALTHCARE INFO SECURITY®

 infoRisk
TODAY®

 CAREERS INFO SECURITY®

 Data Breach
Prevention, Response, Notification, TODAY

CyberEd.io


INFORMATION SECURITY
MEDIA GROUP