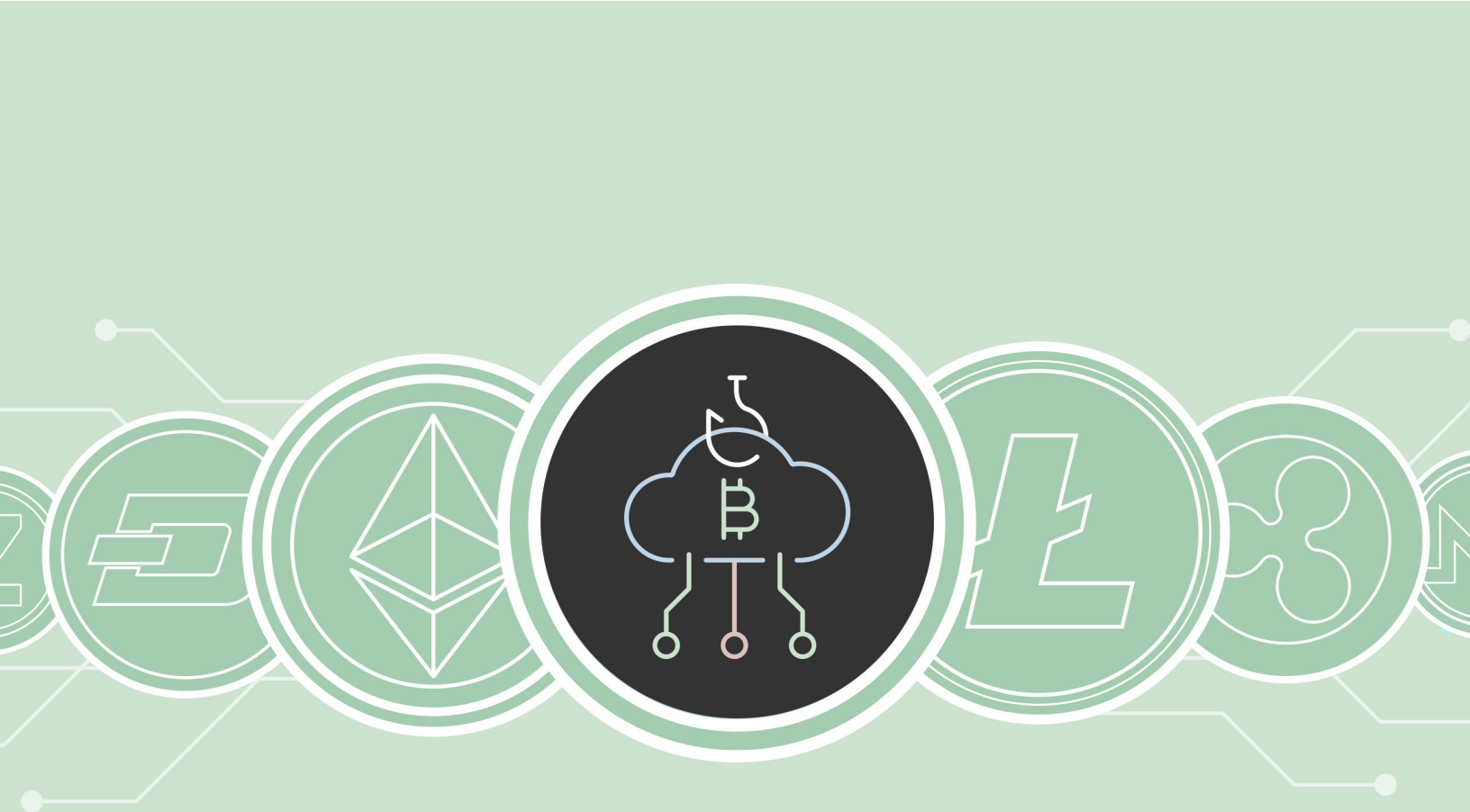
BOLSTER

iSMG INFORMATION SECURITY MEDIA GROUP

Protect the Brand: Online Fraud and Cryptocurrency Scams

Bolster's Jeff Baher Shares New Research, Tactics for Defending Brands From Scammers



BOLSTER

Phishing, online fraud, cryptocurrency scams – they are coming at lightning speed, threatening enterprises and their brands. And just as fraudsters rely on automation to deliver these attacks, defenders can use automated tools to protect their brands. **Jeff Baher** of Bolster tells how.

"The volume of phishing and scam activity just continues unabated," says Baher, head of product marketing at Bolster. "The volume is just eye-popping."

In an interview with Tom Field of Information Security Media Group, Baher discusses:

- Bolster's new State of Phishing and Online Fraud Report;
- Takeaways from Bolster's Cryptocurrency Scam Report;
- How enterprises can use automation to respond to fraudsters in real time.

Baher is head of product marketing at Bolster Inc., an industry leader in AI-driven brand protection and fraud prevention. He has deep experience in digital infrastructure, cybersecurity, product marketing and go-to-market strategy and has held leadership positions at Fortune 500, midsize and startup technology companies, including Cisco for 10 years and Dell EMC for eight years.

Phishing and Scams Have Increased

TOM FIELD: Let's discuss the State of Phishing and Online Fraud Report that Bolster released recently. What were some of the key findings that got your attention?

JEFF BAHER: Our system scans millions of URLs on a daily basis, which gives us an interesting snapshot of what occurred through 2020. The volume of phishing and scam activity just continues unabated. From 2019 to 2020, we detected about a 75% increase in the number of phishing scam links. There were almost 7 million scam sites last year. From the first quarter to the fourth quarter, there was a 185% increase. The volume is just eye-popping. The fraud manifests itself in different industry verticals and for different brands.


Jeff Baher

Fraudsters Are Opportunistic

FIELD: What did you learn about the emerging threat landscape in some of the scams that you referenced?

BAHER: Scammers leaned in heavily to things that rank high on the fear gauge. Wherever there is an opportunity, fraudsters are on top of it and quickly set up fake sites. In the beginning of the year, there was a significant number of suspicious domains and scam activity around the initial COVID-19 threat. Then, when there were PPE opportunities, scams immediately emerged around that. As we moved closer toward vaccine development, we started to see specific attacks on some of the leading pharmaceutical manufacturers. The "work from home" shift resulted in immediate attacks on login sites and in people trying to steal credentials or gain access into video conference sessions.

Automation Is Needed

FIELD: What do the volume and persistence of scams point to in the future? What's the outlook beyond 2021?

BAHER: We see greater sophistication combined with greater speed with which scams can occur. The problem is quickly outstripping the capabilities of traditional mechanisms, which were largely manual and based on people checking for things that looked suspicious or were malicious. With the rate at which scams are occurring today, the job can't be done manually. We need to meet that scale with something that is machine scale.

"Wherever there is an opportunity, fraudsters are on top of it and quickly set up fake sites."

Fraudsters Target Cryptocurrency

FIELD: Bolster also just released a Cryptocurrency Scam Report. What are the biggest takeaways?

BAHER: Wherever there is interest and hype, you immediately see, within hours, fake sites. There's a novelty and a sense of urgency to cryptocurrency. It has become a mainstream investment instrument, and fraudsters are quick to scam unassuming investors. And now, with non-fungible tokens, it's a distributed infrastructure. It's not like traditional banking or credit cards where there's a number you can call if something isn't going right. You can be defrauded because it is inherently a decentralized system.

There is a direct correlation between the hype that you see around a specific currency, such as Bitcoin or Dogecoin, and suspicious domains and scamming. As the currency prices increase, so does the number of suspicious domains – fake sites that are looking to capitalize on the name of Bitcoin or leveraging personalities or brands that were attached to giveaways or scams related to Bitcoin. Earlier this year, some particular pump-and-dump hype cycle was occurring with Dogecoin, and it had a significant spike within a 24-hour period. Now we're seeing this again. It has continued through this year.

Know You're a Target

FIELD: It's overwhelming. How do enterprises need to think about protecting themselves from these growing scams?

BAHER: Enterprises that are directly in the line of sight – those that are running foundations in cryptocurrency; playing specifically in cryptocurrency; playing in SaaS-based applications like Zoom and others, where they know they're now much more front and center in terms of that which is being consumed; and places where people are now starting to transact more and more – need to recognize that they're increasingly targets of scams that could happen at significant scale and very quickly. If a scam happens, they need to know how to deal with it.

In the case of Zoom, Bolster took down almost 1,500 sites within the first 24 hours of the discovery process. It wasn't just that someone put up a fake login site; someone put in a lot of fake login sites across many hosting providers, across many different countries. It's not easy for an individual or a team to figure out all the places where fake sites exist and take them all down. That creates threats and risk for the business. Enterprises that are directly in the line of sight need to have plans in place to protect their brand and their customers. They need to have early warning mechanisms to anticipate these problems – for example, mechanisms can look for new registrations of domains that are variations of the company's domain or brand – look-alike domains or typosquatting sites. That's where scammers run a lot of these campaigns.

In enterprises that aren't directly in the line of sight, the employees and business are also at risk, because they are part of the broader industry. Employees get emails from investors or friends or share links up within the business. Sharing URLs about opportunities or links to different kinds of investments is seemingly benign, but the security team needs to scan those URLs and render verdicts on them to make sure the company is not receiving scams and then disseminating or amplifying them.

Individuals should continue to practice good, safe web browsing. If you have doubts about a link you want to click on, first do a scan. Bolster has a community-based platform called CheckPhish that is used by about 80% of the Fortune 500. People use it on a daily basis to scan URLs. It does real-time scanning and renders real-time verdicts. You can then report abuse or try to take down a site.

Protect Digital Touch Points

FIELD: Bolster is best known for brand and trademark protection. How is this threat landscape evolving beyond what you've told us so far?

BAHER: A big concern is digital touch points – the many ways in which your online brand touches a consumer. It can be through your website or advertising, search engines or social media sites. All of the different places where your brand can touch your consumer are areas where that consumer can get sidetracked, for example, by a fake site or a phishing campaign that starts an account takeover process. The number of digital touch points is constantly increasing so companies constantly need to get their arms around the different places their brand can be, where customers can interact with it.

A fake site can be used in different ways, such as to wreak havoc in the company's supply chain or for classic credential theft. The way it's used will trigger different areas within the enterprise. If it's brand interference, the legal team would typically get involved. But customer service wouldn't be involved until someone actually said that their account had been taken over, and the fraud department wouldn't get involved until there was actually some illicit fund taking place.

We have found that proliferation of the brand combined with the fragmentation of the company's response is what allows many of these attacks to occur and to persist. Enterprises need to know the different touch points and know that, if fraud occurs, it will hit the organization in a fragmented way. Our platform helps with that. It allows brand teams, security teams and fraud teams to have a common, single source of truth – a common pane of glass through which they can all see what's occurring so they can take collective action on it.

"The number of digital touch points is constantly increasing so companies constantly need to get their arms around the different places their brand can be, where customers can interact with it."

The Bolster Approach

FIELD: How is Bolster raising its game to help detect and take down fraudulent sites?

BAHER: Our platform scans 2 million to 3 million URLs a day. We've scanned well over 1 billion URLs to date. The platform provides real-time detection of phishing and scam sites in less than 100 milliseconds and triggers fully automated blocking and takedown processes to neutralize threats. The underlying engine is powered by a number of differing AI components, including natural language processing, computer vision, and deep learning models. This means we can do super-fast and accurate logo detection and render lightning-fast verdicts on credential theft.

Because of the volume of phishing sites, you immediately have to get your arms around what you're seeing and start prioritizing in terms of risk. Then comes the takedown. We have a fully automated process of blocking sites within the browser level and then taking the sites down. It works through APIs and integrations we have with hosting providers and registrars to take sites down and then continue to monitor the landscape so that the sites don't move to a different hosting provider and reemerge. Ongoing, continuous monitoring is important.

You have to match the scale with scale. It's important to understand the scope of the problem and then apply automation capabilities throughout the process, from detecting at scale to then alerting and taking down at scale. It's important to know that problems can emerge really quickly but that there are right-sized solutions if you have the ability to see quickly and render verdicts quickly. Then you can get ahead of scams and stay ahead of the volume of attacks we're seeing in this landscape. ■

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.

Contact

(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