Startup fights fraud as hackers breach networks

November 6 2017, by Rex Crum, The Mercury News

With every new hack of computer networks comes questions about how it happened and what kind of security can prevent the next one.

Yet the recent hacking of consumer credit reporting agency Equifax's network has raised the question of not only what can be done to stop such attacks, but also what hacking victims can do after the fact.

The Equifax hack exposed Social Security numbers, credit card accounts and other personal information of as many as 143 million people. For individuals, fewer things are more personal than identity, and people want to know that when they shop or do anything else online, their personal data will be secure.

That's where software startup Sift Science comes in. The company offers products designed to attack potential areas of online fraud for industries and businesses. Its goal is to catch fraudulent activities before they affect those businesses' operations and, eventually, their customers.

"Breaches happen. They are a fact of life and are going to be of larger and of greater magnitude," said Jason Tan, chief executive of the 6-year-old company. "As more information is stored in the cloud, finding an intelligent approach to figuring out what to do after a hack attack occurs is critical."

With so much havoc being wreaked with each new hack, San Francisco-based Sift Science has found a place in the market for its approach to post-attack network security.

The company, with 122 employees, was launched out of the Y Combinator incubator program. Insight Venture Partners, Spark Capital and Salesforce CEO Marc Benioff are among its investors. Sift Science won't disclose its value, but said it has taken in $53.6 million in venture investments.

After the attack on Equifax, the consumer credit reporting agency acknowledged the hack in early September, but also admitted that it knew of the flaw in its system two months before hackers got in and took millions of Americans' personal data.

"If you look at the Equifax situation, that was a case of there being some kind of delay between the breach and the consequences," Tan said. "That allowed for plenty of time for the stolen information to make its way to the dark web, where it could be sold to bidders who then would use it to get access to people's personal accounts. The name of the game is turning data into something more valuable."

But Tan and Sift Science work to mitigate the effect of a hack after it takes place.

"There is all this information flying around - Social Security numbers, passwords, credit card numbers - the question is: 'How do you prevent them (hackers) from abusing this information once they have it?' We build what is, in effect, a big brain that analyzes a person's activity in real time, and identifies if it looks like someone is going to do something malicious."

Sift Science uses machine-learning technology, in which a computer network is set up to learn new tasks and capabilities without having to be repeatedly programmed to do so.

For example, say your spouse often shops on typical e-commerce websites like Amazon, eBay or Zulily. There would probably be nothing untoward to pick up on that kind of activity.

But, then the Sift Science software sees that your spouse is logging in from a computer in Taiwan. A program runs to calculate the possibility that the transaction is legitimate, and whether accounts have been compromised.

"We're going to try to look at that, see if this address matches, say, others that are similar or look suspicious, and use that data to put together a case to keep you from getting harmed," Tan said.

Sift Science, while smaller on the security front compared to the likes of Symantec, Palo Alto Networks, McAfee or Fortinet, is no small fry when it comes to its client list. The company says more than 6,000 companies use Sift Science to fight fraud and improper hacking on their sites, including Twitter, Airbnb, Instacart and Zillow.

An example of how consumers can benefit from Sift Science's security services can be seen in its work with online dating site Zoosk. When it comes to online dating, people tend be more selective with their personal profiles and financial information. Zoosk memberships are free, but paid subscriptions are required to use the site's full set of services. The company wanted to find a way to reduce the number of users providing false profile information and cut down on fraudulent activity on the Zoosk site. It brought in Sift Science to set up a system that analyzes user data for signs of suspicious behavior, blocks users who meet certain types of negative criteria and improves the security of its legitimate members' accounts.

"We want to be able to help companies make decisions about who is trustworthy, and so that they don't have to inconvenience everyone," Tan said. "You don't want to all of a sudden put up 10 fences around your house. You want to be able to live your life with relative peace of mind and be more secure in your home."

For consumers, the best way to minimize becoming a hacking victim is to use as much common sense as you can.

"First off, don't panic. It doesn't do any good to live in fear," Tan said. "Second, before you open emails, think very carefully about the subject line and who it's from. Don't be so trusting just because something looks official. Finally, use strong passwords. The best ones are those that use two or three words together that would be hard for someone to guess, but easy for you to remember."

©2017 The Mercury News (San Jose, Calif.)
Distributed by Tribune Content Agency, LLC.

Citation: Startup fights fraud as hackers breach networks (2017, November 6) retrieved 19 April 2024 from https://phys.org/news/2017-11-startup-fraud-hackers-breach-networks.html