9-CNBC-How the cybercrime

How the cybercrime industry fueled Target breach: McAfee

Published Mon, Mar 10 20142:13 PM EDT

Updated Mon, Mar 10 20146:29 PM EDT

VIDEO2:3902:39

McAfee CTO: Target attack was defendable *[Disappointment]*

The cyberattacks that led to the massive data breach at Target last year marked the “coming-of-age” for a black-market service industry that caters to malicious hackers and identity thieves, computer security company McAfee Labs said in a quarterly report Monday.

That industry allowed the thieves to not only buy custom-made malware for the theft, but also to quickly sell credit card numbers from 40 million shoppers affected by the breach. The thieves sold the numbers through online back-channels that security experts call the “dark web,” the company said.

“Retailers in general took this as a wake-up call,” said Mike Fey, chief technology officer at McAfee, on ” Squawk on the Street .” “They saw an essentially off-the-shelf … piece of malware modified for a unique environment, which was Target. A lot of retailers assumed that if they don’t have a standard point-of-sale system, they were somehow safe. And I think Target showed them that’s not the case.” *[Disappointment]*

Zmeel Photography | E+ | Getty Images

McAfee Labs released its quarterly report on cybersecurity threats on Monday. The company focused its attention on the dark web malware industry that fueled the point-of-sale attacks on Target and other retailers late last year. The high-profile cyberattacks were unsophisticated

technologies that identity thieves bought off the shelf from the cybercrime "service" community, which customized the software specifically for the attack, McAfee said.

(Read more: Cybersecurity stock valuations on the rise)

McAfee researchers discovered that the Target thieves offered credit card information for sale in batches between 1 million and 4 million numbers, the cybersecurity company said. What's more, Fey said Target could have defended against the point-of-sale attacks if it had a cost-effective method of deploying existing security technology *[Disappointment]*.

"You take a look at the Target attack," Fey said. "That was defendable by technology that has been around. It didn't require a new silver bullet" *[Disappointment]*

Last week, Target's chief information officer resigned as the retailer seeks to overhaul its security protections.

VIDEO3:1903:19

Key deadline for Target

Charles Koppelman, the former CEO of Martha Stewart Living Omnimedia and former chairman of Steve Madden, said the massive data breach at Target appears to remain limited to the retailer. Other large retailers have enlisted help from tech companies to better protect consumers, he said

"Once the Target issue happened, other retailers are looking into their systems," Koppelman said. "The big technology companies are going to benefit from this. They're all going to be ahead of the curve. This is a Target-centric issue."

[Disappointment]

(Read more: Avoiding Target stores? You're not the only one)

Companies should look to shore up their own defenses rather than finding a third-party to house their data *[Disappointment]*, he added. Having a single,

industrywide data storage center won't allay concerns about individual retailers storing consumer's credit card numbers themselves *[Disappointment]*, for example, Koppelman said. That will just provide a bigger target for sophisticated identity thieves, he added.

"Every time you look at taking your data and giving it to someone else to handle, you're opening up another Pandora's box *[Disappointment]*," Koppelman said. "At the end of the day if there's going to be one massive data storage place, we're going to have difficulties with them of course *[Disappointment]*."

In addition to the cybercrime service community, McAfee identified the following threats as ones to watch this year:

Mobile malware: McAfee recovered nearly triple the number of mobile malware samples last year compared with the end of 2012, collecting 2.47 million new samples in 2013â€"about 744,000 just in the last quarter.

Ransom-ware: The use of attacks against computers and companies to hold them for pricey ransoms has increased significantly in the past year. McAfee doubled its collection of ransom-ware samples in the fourth quarter of 2013 compared with the final quarter of 2012. The use of such malicious software drew headlines last week when social networking website Meetup.com became locked in a battle with cybercriminals who demanded $300 to lift an ongoing digital siege on the company's website.

Suspicious URLs: Be vigilant for sketchy looking links. McAfee recorded a 70 percent increase in suspect URLs throughout 2013.

McAfee also called into the question the way Web service providers authenticate trusted third parties. More and more malware now comes "signed" by certificate authorities, a model that brands third-party information providers as safe and trusted. That means Web users can no longer rely on certificates as a badge of security on third-party links or software.

(Read more: The next thing you'll pay for online: Your privacy)

McAfee has seen a threefold increase in the number of “malicious signed binaries”â€”or malware signed by ceritificate authoritiesâ€”in the past year, its report said.

â€”By CNBC’s Jeff Morganteen. Follow him on Twitter at @jmorganteen and get the latest stories from “Squawk on the Street.” Reuters contributed to this report.