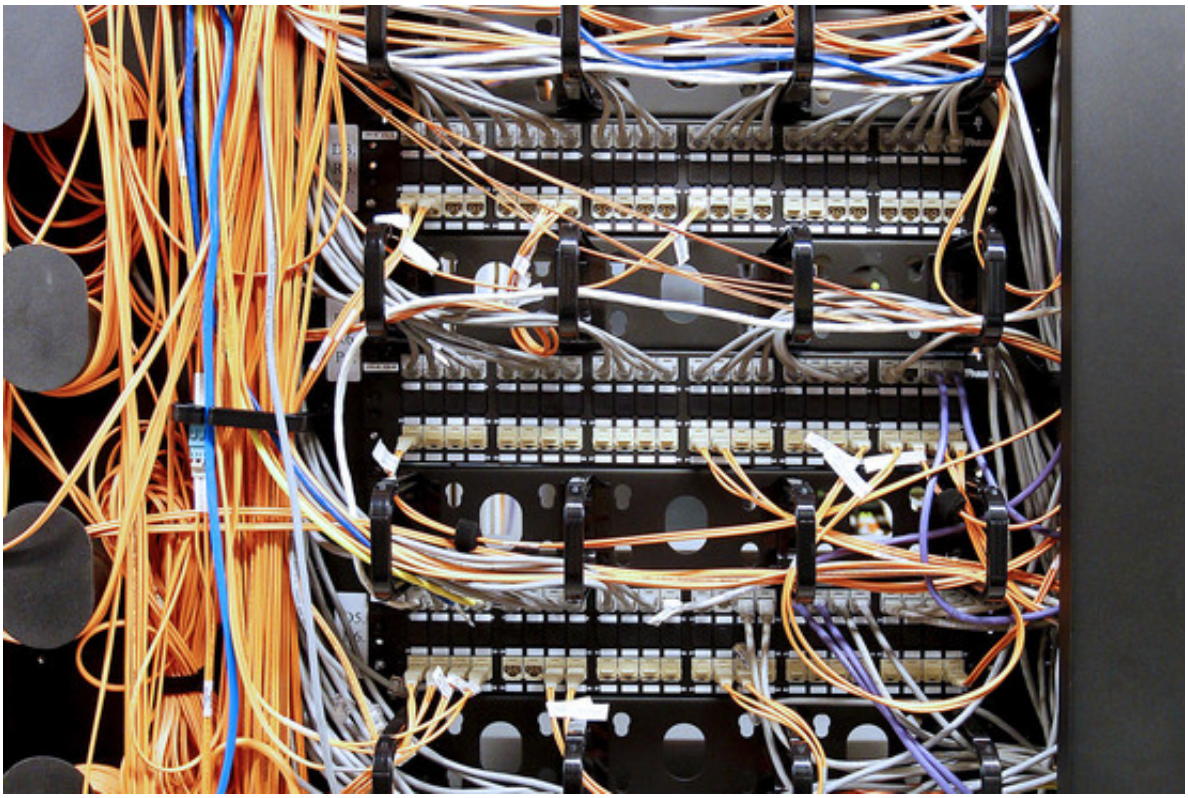
BUSINESS

Card-Theft Software Grew in Internet's Dark Alleys

Version of Malware Used Against Target Was for Sale for $2,000 a Year Ago

By CHARLES LEVINSON and DANNY YADRON

Jan. 21, 2014 8:12 p.m. ET



Network cables run to server racks at the headquarters of Symantec Corp. in Mountain View, Calif. *Bloomberg*

The malicious software that infected Target Corp. popped up in January 2013 with a price tag of $2,000 and spent nearly a year evolving in the Internet's black markets before an unknown attacker slipped it into the retailer's computer systems.

That life cycle, pieced together by security firms that track down and identify dangerous software, shows the new nature of the threat faced by American retailers hoping to defend themselves from attacks like that at Target, which compromised 40 million credit and debit cards over the holidays.

Security experts say computer intrusion has evolved from one of solitary hackers or groups of hackers into an industry where rogue programmers are developing tools they can sell on an increasingly formal online marketplace. The buyers, often tied to organized crime, are in turn

bringing greater sophistication and ambition to their efforts.

The targets, increasingly, are American retailers, which continue to rely on magnetic-stripe credit-card technology, which is less secure than the chip-based cards that have been used for years in Europe. Luxury retailer Neiman Marcus Group also suffered a data breach over the holidays. On Tuesday, sporting-goods maker Easton-Bell Sports Inc. said it too was attacked, with data from around 6,000 online shoppers stolen during December.

The new trend "is to move directly against these massive storage databases for credit cards," said Dmitri Alperovitch, chief technology officer of security firm Crowdstrike Inc., and an expert in Russian-speaking cybercriminals. In the past, Russian-speaking hackers tended to focus on fraud through email scams or other unsophisticated attacks, he said.

The malicious software that infected Target spent nearly a year evolving in the Internet's black markets before an unknown attacker slipped it into the retailer's computer systems. Charles Levinson reports. Photo: Getty Images.

An early version of the malicious computer code that many experts believe hackers used on Target's sales terminals was spotted in January 2013 by computer security firm Symantec Corp. and multiple security firms familiar with the retail hacks.

Symantec dubbed the malware Reedum. Other security firms that spotted it took to calling it Kaptoxa, a Russian slang word for potato. By February, a version of the software was being offered on hacker forums for around $2,000, advertised for stealing payment-card numbers, according to cybersecurity experts who were tracking the malware.

The Reedum malware worked like a Trojan horse by hiding its malicious nature and compromising systems from inside. According to iSight Partners Inc., once injected into retailers' computer systems, the software would seek out payment programs and monitor for the data on cards' magnetic stripes, which during the authorization process would be unencrypted and stored in the payment system's memory.

The data would be scraped and stashed on another compromised server—but only during the prime business hours of 10 a.m. and 5 p.m., allowing it to blend in with normal traffic. The hackers would later harvest that data from the retailer's server.

As the malware grew in popularity in the underground fraud community and spread during early 2013, cybersecurity firms learned what to look for and developed defenses. But the hackers adapted and modified the software, according to people tracking the software.

According to iSight, software for attacking point-of-sale systems is widely available under names like Dexter, vSkimmer and BlackPOS, of which the Target malware is a variant.

That commercialization could make it easier for attacks to take place.

Audio

Charles Levinson has more about how Target's data breach developed on The Wall Street Journal This Morning.

00:00 | 00:00

"It really could lower the barrier to entry," said Tiffany Jones, a senior vice president at iSight and its chief revenue officer. "It's going to drive cheaper prices, larger user bases and at the end of the day there's a growing demand."

It isn't clear how the hackers got Malware into Target's internal network. There is a good chance they lured an unsuspecting employee into clicking on an infected link through a bogus email disguised to look genuine, according to several security experts. The other likely scenario, according to experts, is that the attackers found a vulnerability in one of Target's public websites.

ISight, hired by the Secret Service and Department of Homeland Security to help with the investigation, said the bug had a "zero percent antivirus detection rate," meaning even updated security software couldn't tell it was harmful.

The hack involved several tools, iSight said. The Trojan horse scanned the point-of-sale system's memory for card data. Another logged when the stolen data was stashed inside Target's network. Yet another sent the stolen data to a computer outside the company. The coordination of those functions was complex and sophisticated, the firm said.

The breach began on Nov. 27, as shoppers prepared to swarm Target's nearly 1,800 U.S. stores to snag Black Friday weekend deals. It transmitted the first payload to a hijacked external computer on Dec. 2, and then repeated the process over the next two weeks, according to a report by the Israeli security firm Seculert, which analyzed the software.

A Target spokeswoman declined to comment on specific details of the attack, citing the investigation.

It wasn't long before fraudulent transactions involving the stolen card numbers started showing up.

In early December, an online hacking forum known as rescator.la began offering a massive batch of stolen credit cards for sale, according to online security expert and blogger Brian Krebs, who broke the news of the Target attack on his blog Dec. 18, a day before Target disclosed the breach.

The seller gave the fresh batch a nickname, according to Mr. Krebs: "Tortuga," Spanish for tortoise, and the name of a notorious pirate island referenced by Jack Sparrow in the movie "Pirates of the Caribbean." Tortuga is also a near anagram for Target.

The Secret Service, which is charged with protecting the country's financial infrastructure and payment systems as well as the president, started noticing a flood of new stolen cards entering the

market—a quarter-million to a half-million dropped at a time, way more than usual—and bought some of them, a person familiar with the matter said.

The Secret Service contacted Target about the fraudulent activity a few days before Dec. 15, people familiar with the matter said. At that point, Target's team began investigating and informing relevant executives, including CEO Gregg Steinhafel, one of the people said.

The Secret Service declined to comment.

On Dec. 15, Target determined it had indeed been breached, but four days passed before it disclosed the news. In an interview on CNBC, Mr. Steinhafel said the company had to first plug the hole in its systems and prepare to handle what could be millions of calls from customers. It shut down portals through which vendors and employees could access internal websites over the Internet.

The attackers did leave some clues. Embedded in the code found at Target was a string of text left in the malware's metadata, including the word "Rescator," the name of one of the online forums used to sell the cards, according to Messrs. Krebs and Alperovitch, as well as security firm McAfee, a unit of Intel Corp. That raises the possibility that the person or people running the forum where the cards are sold were also somehow involved in the attack, security experts say.The attack isn't likely to be the last.

—Paul Ziobro and Robin Sidel contributed to this article.

Write to Charles Levinson at charles.levinson@wsj.com and Danny Yadron at danny.yadron@wsj.com