Cyber attack could threaten major banks, credit card companies - CW 15

Information provided by CNN.com:

Some of the nation's biggest banks are at risk of a massive cyber attack next year that could potentially siphon funds from unsuspecting customers, according to a leading digital security firm.

The fraud campaign, known as Project Blitzkrieg, is a credible threat, the Internet security firm McAfee Labs concluded in a new report.

The malware has been lying dormant in U.S. financial systems and is scheduled to go active by the spring of 2013, McAfee researchers concluded.

The project «appears to be moving forward as planned,» the report states.

People familiar with the study said some 30 financial institutions are targets of the campaign.

CNNMoney: Not a single bank is malware-free

They include Fidelity, E*Trade, Charles Schwab, PayPal, Citibank, Wachovia, Wells Fargo, Capital One, Navy Federal Credit Union and others.

Information about the intended cyber attack was discovered in September by the Internet security firm RSA during the course of monitoring a web chat room that the company says was run by a Russian hacker known as vorVzakone.

According to the report, the Russian was believed to be using the chat room to recruit fellow hackers to steal assets from bank accounts as part of a criminal enterprise.

At the time, there were doubts about the credibility of the threat, with some experts suggesting it was part of a Russian law enforcement sting.

«Our researchers have been poring into this and what they have found, they actually found somewhere between 300 to 500 devices in the U.S. that have actually been infected with the particular malware that this individual is talking about,» said Pat Calhoun, a senior vice president at McAfee.

«That, combined with some additional research we're doing, has led us to believe this is true. This is actually a real operation that this individual is planning to launch sometime before spring 2013.»

The McAfee report states, «The targets are U.S. banks, with the victims dispersed across various U.S. cities, according to the telemetry data. Thus this group will likely remain focused on U.S. banks and making fraudulent transactions.»

Calhoun said that McAfee has access to the malware and, through reverse engineering, has learned much about its capability and targets.

«We see the IP addresses and names of banks and so on or references to URLs.»

Calhoun said the behavior of the Trojan suggests it is a variant of a previous known strain called Gozi. RSA labeled this latest version, Gozi Prinimalka.

Cyber attack could threaten major banks, credit card companies - CW 15

But it's a tedious task dissecting the malware, and the company is still trying to figure out how it would create fraudulent bank transactions, Calhoun said.

Based on their analysis, the McAfee researchers believe the plan is to attack a small group of bank customers.

«This strategy is necessary if the attackers hope to succeed in transferring several million dollars over the course of the project,» the report states. «A limited number of infections reduces the malware's footprint and makes it hard for network defenses to detect its activities.»

But Calhoun said the fact the malware has been detected allows for a defense to be mounted.

«Since we know about it, we will be able to protect against it,» Calhoun said. «We're working very closely with law enforcement and a lot of the potential targets to make sure they understand this and know how to behave or how to protect themselves against it.»

Wells Fargo, the only financial institution to respond to questions about preparations it might be taking to thwart the potential attack, said it was watching for the threat.

«Security is core to our mission and safeguarding our customers' information is at the foundation of all we do,» Wells Fargo said in a statement. «We constantly monitor the environment, assess potential threats, and take action as warranted.»

The Department of Homeland Security, which takes the lead for the government on cyber security issues, had no comment on the McAfee report or Project Blitzkrieg.