You don't need a fast car to rob a bank any more, just malware

July 30 2014, by Bill Buchanan

Swag bags and getaway cards are so 20th century. Credit: Andrey_Popov

The number of physical robberies on banks has fallen dramatically in recent years, but the amount of money banks are losing through electronic methods has rocketed. In 2013 for example, the annual fraud indicator estimated the annual cost of fraud in the UK was £52bn what it was five years before. So it's easy to put up CCTV cameras, bulletproof glass and alarm bells, but in an electronic world there are infinite ways to commit fraud.

In fact there are so many targets in a electronic world that criminals can focus their efforts on the customer, the bank or the merchant. With virtually no footprint at all, criminal gangs can install malware within any part of the e-commerce infrastructure and either steal user credentials or modify transactions. It may be tempting to see this as a victimless crime, but large-scale fraud can have serious implications on the global financial market, not to mention user trust.

Individuals have been finding ways around electronic security for decades. Well known examples include John Draper (aka Captain Crunch), who in the 1970s used a whistle tuned to 2.6kHz that was given away in cereal packs to fool the pitch-controlled security system on the US telephone network, allowing him to make long-distance calls free of charge. Then there was Vladmir Levin, from Russia, who siphoned off millions from Citibank customers in the early 1990s by finding a way around their dial-up wire transfer service.

These days, any script kiddie can create their own targeted attack on the finance system. You don't need extensive programming skills or even a deep knowledge of how the e-commerce infrastructure works. A key target is the end user, since they tend to be the weakest link in the chain.

Holy Boleto!

The latest reminder came with the recent attacks on Boleto Bancário, the Brazilian inter-bank payment system, which were announced earlier this month. Known colloquially as Boleto, a vast amount of low-dollar transactions were hijacked by the latest malware, most probably set up by Brazilian organised crime gangs. With the theft amounting to nearly $4bn (£2.4bn), it could be the largest fraud in history.

Boleto is the second-most-popular payment method in Brazil after credit cards and has around 18% of all purchases. It is typically used to pay

phone and shopping bills. One reason it is popular is that many Brazilians don't have a credit card, and even when they do have one, they are often not trusted.

The fraud worked very simply. It tricked customers to install a piece of malware on their system and then waited until they visited their bank's website. It spread using what is called spear phishing, which is the most common method these days, where users are sent emails with links on them. When the user clicks on them, they will run a program on their computer, and install the malware.

The malware used what is called a man-in-the-browser attack, where the malware sits in the browser, including Google Chrome, Mozilla Firefox and Microsoft Internet Explorer. It is known commonly as a Eupuds, which is classified as an information-stealing Trojan that stays alive by writing itself on to a user's hard drive and modifying the relevant Windows registry key so that it starts every time the computer is booted up. As well as infecting browsers using Windows operating systems, it can also steal information through the likes of Windows Live/Hotmail and Facebook.

In the case of Boleto, it worked by detecting the traffic between the browser and server by searching for specific relevant strings linked to bank sites. It then recorded all the information that had to be submitted about the recipient of the Boleto transaction. It then submitted the transfer for payment and modified it by substituting an attacker's account for the recipient's one. As many as 200,000 IP addresses were infected and 83,000 user email credentials were stolen in a move that had been going on for two years.

Of the statistics received, all the infected machines were running Microsoft Windows as their operating system. The majority were running Microsoft Windows 7 (78.3%), with Microsoft Windows XP

second-most popular (17.2%). Of the browsers detected, the most popular was Internet Explorer (48.7%), followed by Chrome (34%) and Firefox (17.3%); and the most popular email domain used to steal user credentials was hotmail.com (94%). The reason that the impact was so great is that Boleto is only used in Brazil, thus malware detection software has not targeted it since it is a limited market.

All the same, the threat should have been detected more quickly. The first signs of the ZIP file containing the malware appeared in 2010. Cisco Systems was highlighting the distribution of the spam emails in 2012 and more warnings highlighted the threat last year.

Wake up and smell the malware

These attacks should serve as a wake-up call for the finance industry and governments around the world. What is most worrying about this type of fraud is that it could compromise the whole of the finance industry. It could even bring down major finance companies and even nation states with a single large-scale event.

As long as there's one person who will to click on a link in an email, there will be the potential for fraud. This is why the focus is moving towards end-users. So what's the solution? Users need to watch what they click, and also protect their systems by installing the latest upgrades from the likes of Microsoft and having up-to-date virus software. Until customers and major organisations find a way of getting fully across these threats, these are dangerous times to bank.

Provided by The Conversation