Trends In Mobile Malware

by Steve Brown

In the popular 1997 action flick Face/Off, an FBI agent trying to avenge the death of his son undergoes face-transplant surgery and dons the identity and physical appearance of a ruthless terrorist in order to bring him down. His best laid plans, however, go horribly awry when the criminal mastermind undergoes a similar surgery and begins impersonating the agent. The result is an action-packed battle of wits and brawn, good vs. evil, driving home the message that not everything can be taken at face value.

This strikes a chord when it comes to the growing problem of mobile malware targeting banking applications. Unsurprisingly, banking Trojans--malicious computer programs that misrepresent themselves to appear useful, routine or interesting so a user installs them--have become a widespread threat to mobile customers. They now account for more than 95% of mobile malware, according to cybersecurity firm Kaspersky Lab.

Today's smartphones are more like personal computers than purebred phones, yet they are not typically protected by firewalls and other security measures that are more standard on PCs. As smartphone use continues to proliferate, there's evidence to suggest that cybercriminals are becoming more ambitious about targeting and infiltrating them.

To fight back, some banks are starting to offer information on their websites about mobile malware as well as tips on how to avoid problems. A recent test by Kaspersky underscores why additional education is necessary. The research showed that many users don't follow basic security rules when they make online payments or log into an online banking system. Indeed, 50% of the people polled said they do not check if they are using the authentic website of their bank or payment system. They also don't pay attention to the HTTPS prefix to ensure they have an encrypted connection. Some of those polled have even visited a website with a misspelled address--a blatant indicator that something's amiss.

Clearly it's an ongoing battle and based on the proliferation of attacks, more customer education and sophistication detection tools are needed. At a minimum, banks need to ensure they are employing app-scanning security solutions that allow them to identify security vulnerabilities and fix security holes.

This year is also the big year for biometrics authentication, so get ready for that too. It is becoming an increasingly important tool for fraud avoidance and the biggest banks are launching or have launched biometric offerings. Some banks are also responding by providing customers with more fraud alerts and taking swift action when suspicious activity is detected.

Banks need to be aware of the latest threats, so you can create necessary patches and make customers aware. There's a lot of malware out there and the threats often mutate so ongoing vigilance is critical.

Mobile researchers from FireEye, for instance, recently identified a series of Android Trojan apps, dubbed SlemBunk. These are designed to imitate the legitimate apps of 31 banks worldwide and two popular mobile payment service provider apps. These malicious apps masquerade as common, popular applications and stay incognito after running for the first time. They have the ability to phish for and harvest authentication credentials when specified banking and other similar apps are launched and eventually drain bank accounts.

There are numerous other examples as well. In 2015, two families of mobile banking Trojans appeared in Kaspersky's rankings of the top 10 financial malware families. Malware from the Faketoken family for instance, work in connection with computer Trojans, while those in the Marcher family steal payment details from Android devices.

The problem isn't going away any time soon because the bad players know there is money in apps, online banking and ultimately sitting in bank accounts that can be siphoned off. This year we're certain that new threats will pop up and existing ones will mutate, so be prepared and vigilant as you prepare for combat in the ongoing face-off against the bad guys.

BANK NEWS

M&A Activity

1) The Huntington National Bank ($71B, OH) will acquire FirstMerit Bank ($25.5B, OH) for about $3.4B in cash and stock or roughly 1.6x tangible book. 2) Three-bank holding company Chemical Financial ($9.2B, MI) will acquire Talmer Bank and Trust ($6.6B, MI) for about $1.1B in cash and stock. 3) Opus Bank ($6.6B, CA) will acquire alternative asset custodian Pensco Trust for $104mm in cash and stock. Pensco has nearly $11B in custodial assets from 45,000 customers and delivers about $1B of low cost core deposits to Opus.

Hike Timing

The latest CNBC Fed Survey of Wall Street economists finds: 88% expect the next Fed move to be a rate increase; 80% say the Dec rate hike was "the right move"; 56% feel recent market volatility will delay future rate hikes; and most expect the next rate increase to be in May now.

Millennial Analysis

Facebook did some analysis of information on its platform related to millennials and reports: 86% are saving money each month; 68% do not feel like they are understood by their bank; 57% would prefer to pay with cash vs. credit; 53% do not have someone they trust to give them financial advice; 50% are open to changing banks, credit card companies or brokerage accounts; 49% bank using their smartphone; 36% bank using a branch; 9% bank using a computer; and a mere 8% trust institutions for guidance.

Bank Equity

Analysts say bank stocks are trading poorly because investor concerns are running high around energy exposures, weak top line revenue growth and concerns the Fed may not raise rates as rapidly as expected. These factors and others add downward pressure to bank equities and could derail M&A deals in the works due to weakness in buyer stock prices.