m.networkworld.com

24/10/2012 00:05

Android Trojan attacks SMS smartphone bank security

Security company Trusteer is warning about an Android Trojan that is being distributed by criminals to beat the SMS smartphone authentication systems employed by European banks to verify money transfers.

Man-in-the middle (MitM) attacks on 2FA technology via mobiles started around a year ago based on the simple observation that the apparent strength of SMS verification is also its weakness if hackers are able to compromise the handset itself.

BACKGROUND: Banks warned of sophisticated new online scam

The SMS one-time passcode or transaction PIN looks like a way of shutting out online bank fraudsters who have gained access to a user's online account so criminals have devoted time to working out how to intercept that code.

Trusteer has now seen the first mobile attacks based on the recent 'Tatanga' Trojan, as well as new configurations of the infamous SpyEye Trojan it has named 'SPITMO' (SpyEye in the mobile).

Users infected by the Windows Trojan are asked for their mobile numbers before being directed to a website that installs what is claimed to be a mobile security application. Once they have entered an 'activation code' - actually just a way for the attackers to know the mobile is live - the attackers are free to capture any traffic sent to that device.

The mechanics of the attack vary by country and that is perhaps the biggest feature of this attack - it targets a range of major European online banks, particularly those in Spain and Germany.

«Once fraudsters have infected a victim's web and mobile endpoints, very few security mechanisms can prevent fraud from occurring,» said Trusteer CTO, Amit Klein, whose company offers in-browser tools that specialise in blocking such attacks.Where are the attacks based? Perhaps China or the US, both countries from which the fake websites were registered but nobody can be sure.

«This discovery confirms that Man-in-the-Mobile attacks are focusing primarily on Android devices. Multiple studies show that Android devices account for more than 60 percent of smartphone market in the targeted countries,» he said.

«Android popularity and the relative ease of developing and distributing Android applications are probably the reasons why Cybercriminals have singled out this particular platform for mobile malware attacks. «

The attack is really about finding a way around the two-factor authentication systems that are starting to become common on many online banking systems, including those accessed via mobiles. Given the relative simplicity of the social engineering involved this now looks like a serious avenue of attack.

«With nearly 60 percent of the market and a reputation for weak app security, it's no surprise that Android has become the preferred target for financial malware,» emphasised Klein.

X

Install this web app on your phone: tap + and then **Add to Home Screen**.