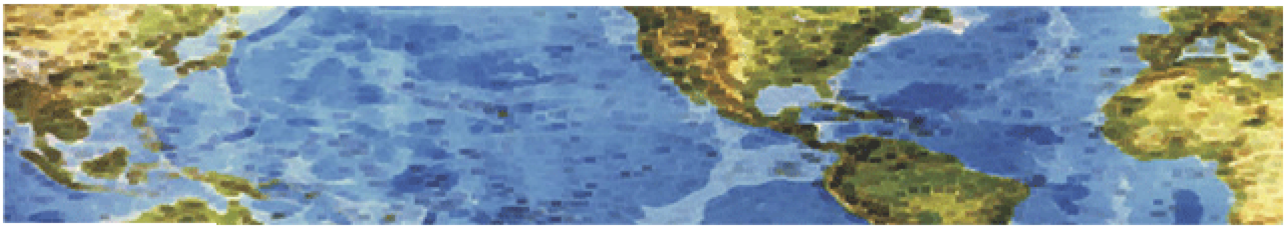
HALL ASSOCIATES



Risk-Based Decision Making Commentary

March 2013 Newsletter #1

Android App Licenses Sold in Malware Black Market

Verified Android developer licenses are being sold in an Internet black market for $100 each, giving buyers unfettered access to the official Google Play app store. So far, there's only been one buyer, but he's a maker of mobile banking Trojans. It may just be a matter of time before someone uses the verified licenses to sneak corrupted apps into the Google Play store.

If so, both legitimate and malicious apps could appear in Google Play under the same publisher's name, fooling app buyers into downloading or purchasing malware. Google charges only $25 for an Android developers' license, though the applicant must also have a Gmail account and a unique Web domain name. Successful applicants get digital signatures that verify the authenticity of their apps.   The $100-per-secondhand-license buyer has already made a fairly simple Android mobile banking Trojan called "Perkele," or "devil" in Finnish. Perkele is programmed to intercept two-step-authentication text codes texted to the victim's smartphone from his bank. Perkele works with existing PC banking Trojans that modify banking websites as the victim attempts to access their online bank account. The altered site prompts users to install a "security certificate" on their smartphones, which is actually Perkele.. Once installed, Perkele secretly waits for the user to log into their online bank account, then copies the two-step authentication code and sends it to the controller of the PC banking Trojan, who uses it to log into the victim's account.

Yet Perkele is hardly the biggest threat out there for Android users. Other banking Trojans, such as Zitmo or "ZeuS in the Mobile," are more dangerous because they manipulate both the PC and mobile connections between the victim and their bank at the same time. Android users can best protect themselves by paying attention to app-installation permissions and making sure new apps are scanned by Android anti-virus software or by Google's on-phone malware scanner (available only for Android 4.2 so far). Users should also check their Android security settings to make sure their smartphones or tablets cannot accept app installations from "unknown sources" outside Google Play. That won't stop corrupted Google Play apps, but it will stop lower-level stuff like Perkele. For the full article, go to http://www.technewsdaily.com/17214-android-license-black-market.html.

HALL ASSOCIATES

TECH SUPPORT SCAMS - SPAM - PHISHING - MONEY TRANSFER SCAMS - ONLINE DATING SCAMS - ONLINE PENNY AUCTIONS - IDENTITY THEFT - TAX RELATED IDENTITY THEFT - WORK AT HOME SCAMS - WEIGHT LOSS CLAIMS - LOTTERIES AND SWEEPSTAKES SCAMS - FAKE CHECK SCAMS - IMPOSTER SCAMS - MYSTERY SHOPPER SCAMS - BOGUS APARTMENT RENTALS - MIRACLE CURES - DEBT RELIEF SCAMS - PAY IN ADVANCE CREDIT OFFERS - INVESTMENT SCHEMES - THE "NIGERIAN" EMAIL SCAM

Scam artists use clever schemes to defraud. And they are getting better at it.

Tech Support Scam - Scam artists use clever schemes to defraud millions of people around the globe each year. Being on guard online can help you maximize the benefits of the internet and minimize your chance of being defrauded. Learn how to recognize common scams and what you can do to avoid them.

In a recent twist, scam artists are using the phone to try to break into your computer. They call, claiming to be computer techs associated with well-known companies like Microsoft. They say that they've detected viruses or other malware on your computer to trick you into giving them remote access or paying for software you don't need. They take advantage of your reasonable concerns about viruses and other threats. They know that computer users have heard time and again that it's important to install security software. But the purpose behind these schemes isn't to protect your computer; it's to make money.

Scammers have been peddling bogus security software for years. They set up fake websites, offer free "security" scans, and send alarming messages to try to convince you that your computer is infected. Then, they try to sell you software to fix the problem. At best, the software is worthless or available elsewhere for free. At worst, it could be malware - software designed to give criminals access to your computer and your personal information. The latest version of the scam begins with a phone call. Scammers can get your name and other basic information from public directories or social media. Once they have you on the phone, they often try to gain your trust by pretending to be associated with well-known companies or confusing you with a barrage of technical terms. They may ask you to go to your computer and perform a series of complex tasks. Sometimes, they target legitimate computer files and claim that they are viruses. Their tactics are designed to scare you into believing they can help fix your "problem."

Once they've gained your trust, they may ask you to give them remote access to your computer and then make changes to your settings that could leave your computer vulnerable, try to enroll you in a worthless computer maintenance or warranty program, ask for credit card information so they can bill you for phony services, trick you into installing malware that could steal sensitive data, like user names and passwords or direct you to websites and ask you to enter your credit card number and other personal information. **Regardless of the tactics they use, they have one purpose: to make money.**

If you get a call from someone who claims to be a tech support person, hang up and call the company yourself on a phone number you know to be genuine. A caller who creates a sense of urgency or uses high-pressure tactics is probably a scam artist. Keep these other tips in mind:

- Don't give control of your computer to a third party **who calls you out of the blue**.
- Do not rely on caller ID alone to authenticate a caller. Criminals spoof caller ID numbers. Many times, they are not even in the same country as you.
- Never provide your credit card or financial information to someone who calls and claims to be from tech support. If a caller pressures you to buy a computer security product or says there is a subscription fee associated with the call, hang up. If you're concerned about your computer, call your security software company/person directly and ask for help.
- **Never give your password on the phone. No legitimate organization calls you and asks for your password**.

For more information on all types of scams, go to http://www.onguardonline.gov/topics/avoid-scams