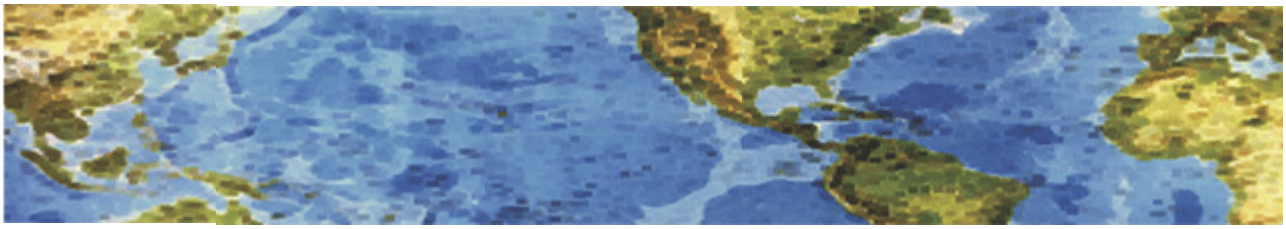
HALL ASSOCIATES



Risk-Based Decision Making Commentary
8 May 2013 Newsletter

Android Anti-Virus Software Easily Fooled

Anti-virus software made by 10 of the biggest Android security providers can be bamboozled by an embarrassingly easy malware disguise, according to a new report. Android phones are known for being more vulnerable to malware than their Apple peers, but they also come with lots of anti-virus options such as those provided by Symantec, AVG, Kaspersky Lab, Trend Micro, ESET, ESTSoft, Lookout, Zoner, Webroot and Dr. Web. Unfortunately, the Android anti-virus software made by all these companies is easily fooled by a simple trick, according to a report from researchers at Northwestern University and North Carolina State University.

Mobile anti-virus products don't provide real security value to users, given how easy they are to bypass. However, not installing a mobile anti-virus app is still a bad thing but users need to understand that an antivirus app will not protect at all times. Most anti-virus software works by checking potential malware against a list of known "signatures," or essential lines of code that can help identify a program's function. Scammers can evade these security measures by subtly tweaking their malware's code just enough to change its signature without affecting its function. This is called polymorphism.

Polymorphic malware has been a problem on desktop computers for years, and anti-virus companies have developed many solutions to combat it. In the past year, polymorphic malware has also begun cropping up on mobile devices. So researchers from Northwestern University's computer science department decided to see how well Android-specific anti-virus programs could handle polymorphic code. The researchers developed a program that could automatically take a malware's code and apply very basic polymorphic changes. They then ran these "disguised" types of malware through the Android anti-virus programs. In nearly all of the trials, the anti-virus programs failed to identify the disguised malware as a threat.

These findings are serious, but not surprising — mobile security is still a new field, and has far to go before it catches up to desktop. So users should be extremely careful about what they put on their Android phones/tablets. Be sure to at least encrypt your data and use the best antivirus/antimalware apps.

http://www.technewsdaily.com/17982-android-antivirus-serious-weakness.html?cmpid=525478

The full report is at this URL. http://list.cs.northwestern.edu/mobile/droidchameleon_nu_eecs_13_01.pdf

HALL ASSOCIATES

What security secrets might an attacker unearth about your business on Dropbox?

The recent "life hack" of journalist Mat Honan has demonstrated the degree to which many technology-savvy consumers **have tied together numerous online services, including Gmail, Twitter, Amazon, and Apple iCloud.** Due to rampant password reuse, however, attackers have been able to take passwords used on one site, and reuse them to log into a person's account on another site. In the case of Dropbox, that means that any corporate secrets stored there could be easily accessed. An example of such an exploit came to light this month, owing to a Dropbox employee having stored an unencrypted document on the service that contained Dropbox users' email addresses. An attacker logged into the Dropbox employee's account, using a password that the employee had reused on another--compromised--site, obtained a copy of the document, then used the email addresses to unleash a flood of spam at Dropbox users. Any business with employees using Dropbox should:

1. Monitor Dropbox use
2. Compare Cloud service security
3. Beware of lackluster Cloud security service practices
4. Treat Dropbox as a public repository
5. Make sure you can detect insider theft using Dropbox.

http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413

Malicious Flash Player Updates Hosted on Dropbox

Cybercriminals often disguise malware as updates for Flash Player. An interesting example has been analyzed recently by security experts from Zscaler. The attack starts with a number of websites that redirect their visitors to click-videox.com. Once victims land on this site, they're urged – in English or Turkish – to update their Adobe Flash Player in order to see a video. The interesting thing about this particular attack is that the malicious Flash Player update is actually stored in a Dropbox account. Once executed, the malicious files try to **disable the Windows UAC, the firewall, the antivirus and other security features**. Ultimately, a variant of the notorious Sality virus is dropped onto victims' PCs. While the malware itself is flagged by most antivirus solutions, the initial .exe files are detected only by a handful of products. The campaign appears to be highly successful. Zscaler found that the malicious **website was visited by over 1,400 users in a single day**.

http://news.softpedia.com/news/Malicious-Flash-Player-Updates-Hosted-on-Dropbox-351239.shtml

New Yahoo Accounts Have Dropbox

This is a notice I got yesterday about turning on Dropbox within my Yahoo account.

"Have you noticed yet? Your Yahoo! Mail now has Dropbox built in! Now you can attach stuff from Dropbox to emails you send (even if they're over 25 MB), or save the attachments you receive back to Dropbox. Happy emailing, The Dropbox Team"