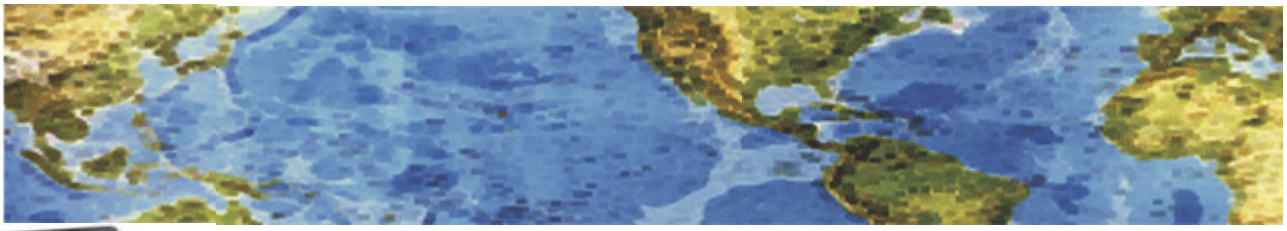
HALL ASSOCIATES



Risk-Based Decision Making Commentary
3 July 2013 Newsletter

Cybercriminals Improve Android Malware Stealth Routines with OBAD

We have been seeing apps that exploit vulnerabilities in Android, with most of them attempting to gain higher privileges on user devices. In recent days, a stronger and far more advanced Android malware named ANDROIDOS_OBAD has come into play. ANDROIDOS_OBAD is found to be **equipped with ability to avoid being uninstalled** from devices and triggers more malicious code.

This new malware family has overall stealth and anti-reverse methods for both normal users and security researchers. When installed, it asks for root privileges and activates the device administrator. Because of ANDROIDOS_OBAD's gaining root privilege, the malware takes complete control of the device and may allow an attacker to utilize this fully. If the user does not activate as instructed, the malware displays frequent pop-up messages when the device restarts. Additionally, if users press the back button, pop-ups appear once again. If the home button is pressed, the pop-ups appear any time later. Here, users will finally have the chance to uninstall it, but if device administrator is activated, the malware will instead run fully in stealth mode.

Still, you can carefully distinguish the malicious app from the mixed Android system apps under Apps Management. However, you won't be able to uninstall it because it's a device admin app. The "anti-uninstall" tricks also work on Android's vulnerability by hiding itself from Device Administrator management view. This malware is capable of the following behavior:

- **Hiding the launcher, and run as a background service with the highest priority.**
- **Automatically try to open Wi-Fi connections and connect to a remote server.**
- **Collect user's contacts, call log, SMS inbox and installed apps.**
- **Download, install and uninstall apps (with root privileges, this can be done silently).**
- **Distributing malware to other phones via Bluetooth.**

ANDROIDOS_OBAD shares similar features with that of its predecessor ANDROIDOS_JIFAKE. The latter is a fake app installer that tricks user into installing and executing them, after which it will silently register as a service connecting to remote servers as it waits for commands. The remote server can then **trigger sending premium text messages** and do the same "anti-uninstall" tricks.

The anti-uninstall trick is exploited through Android's Device Administration feature. If one app is installed and enabled as the device admin application, it will be entrusted with more power to constrain user's device, including enforcing security policy, lock or wipe user's device. Under this level, an app cannot be easily uninstalled, which contributes much for the anti-uninstall tricks.

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/?goback=.gde_1765567_member_249721248

Two Middle TN Mapco stores at risk in data breach

More details have emerged about a data security breach that Brentwood-based convenience store operator Mapco Express Inc. disclosed a month ago. The accounts of consumers who used their debit or credit cards at any of the company's 373 locations from March 19 through March 25 might have been affected, according to an updated FAQ on Mapco's website..
Also, card transactions at two specific Middle Tennessee locations – 1301 Dickerson Road in Goodlettsville and 6624 Charlotte Pike in Nashville – on April 14 and 15 and at certain, undisclosed stores on April 20-21 also might be at risk.

That's because malware installed on Mapco's payment card processing system might have been active at those times and locations, the company said. Those are the first details that have been released since Mapco disclosed the breach on May 6. At the time, the company identified only the dates but gave no details about potentially affected locations. A spokesman said Friday that the company had no comment, citing an ongoing investigation. The company previously said that private security experts and the FBI also were looking into the breach. The hackers who installed the malware targeted systems that transmit certain card information needed for transaction approval, potentially stealing information that could be used to initiate fraudulent purchases, the chain previously said. The malware since has been disabled.
http://blogs.tennessean.com/business/2013/06/10/two-middle-tn-mapco-stores-at-risk-in-data-breach/

The Various Ways That Criminals Can Monetize Hacked PCs

The following graphic was designed to explain simply and visually to the sort of computer user who can't begin to fathom why criminals/hackers would want to hack into his/her/their PC. "I don't bank online, I don't store sensitive information on my machine! I only use it to check email. What could hackers possibly want with this hunk of junk?," http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/