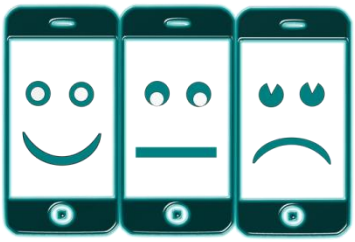
Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=new-threat-targets-older-androids

New Threat Targets Older Android Devices

Posted May 11, 2016



Smartphone users can be broken down into two camps: those who can't live without lining up to buy the latest and greatest model the day it hits the stores, and those who hold on to their tried-and-true phone until it suddenly dies one morning.

There's nothing wrong with sticking with "obsolete" hardware that still serves your purposes just fine.

But if your older Android phone (or tablet) is running an older version of the Android operating system (4.4/KitKat or earlier), you're the designated target of this month's new cyberthreat, dubbed **Dogspectus** by enterprise security firm Blue Coat.

Dogspectus combines elements of two types of malware we've already talked about: malvertising, passively spread through online ads, and ransomware, holding the victim's data hostage until a fee is extorted.

"They Never Saw It Coming"—A Drive-By Download

Unlike most malware, which requires action by the victim (such as clicking on a phony link), a Dogspectus infection occurs by simply **landing on a legitimate web page containing a corrupted ad** with an embedded *exploit kit*—malicious code which silently probes for a series of known vulnerabilities until it ultimately gains *root access*—essentially central control of the entire device.

“This is the first time, to my knowledge, an exploit kit has been able to successfully install malicious apps on a mobile device without any user interaction on the part of the victim,” wrote Blue Coat researcher Andrew Brandt after observing a Dogspectus attack on an Android test device. “During the attack, the device did not display the normal ‘application permissions’ dialog box that typically precedes installation of an Android application.”

“Hand Over the Gift Cards, and Nobody Gets Hurt!”

A Dogspectus-infected device **displays an ominous warning screen** from a bogus government security agency, “Cyber.Police,” **accusing the victim of “illegal” mobile browsing**—and **suggesting an appropriate “fine” be paid**. While most ransomware demands payoff in untraceable Bitcoin, Dogspectus prefers $200 in iTunes gift cards (two $100 or four $50 cards) via entering each card’s printed access code (Apple may be able to trace the users of the gift cards—unless they’re being resold on the black market).

The device’s “kidnapped” data files are not encrypted, as with traditional ransomware strains such as CryptoLocker. But **hijacked root access effectively locks the device**, preventing any function—apps, browser, messaging, or phone calls—other than delivering payment.

The victim is left with two choices: shop for gift cards (Dogspectus conveniently lists national retail outlets!) or reset the device to its out-of-the-box factory state—erasing all data files in the process. Apps, music, photos, videos all gone.

Short of upgrading to a newer Android device, your best defense against Dogspectus and future ad-based malware is to **install an ad blocker or regularly back up all your mobile data to another computer**. For more on defending against the latest emerging cyberthreats, contact us.