kindred

Security Newsletter

10 July 2017

Millions of Android Devices Using Broadcom Wi-Fi Chip Can Be Hacked Remotely

Google has released its latest monthly security update for Android devices, including a serious bug in some Broadcom Wi-Fi chipsets that affects millions of Android devices, as well as some iPhone models.

Dubbed BroadPwn, the critical remote code execution vulnerability resides in Broadcom's BCM43xx family of WiFi chipsets, which can be triggered remotely without user interaction, allows a remote attacker to execute malicious code on targeted Android devices with kernel privileges.

Read More

Fourth Largest Cryptocurrency Exchange Was Hacked. Users Lose Ethereum & Bitcoin

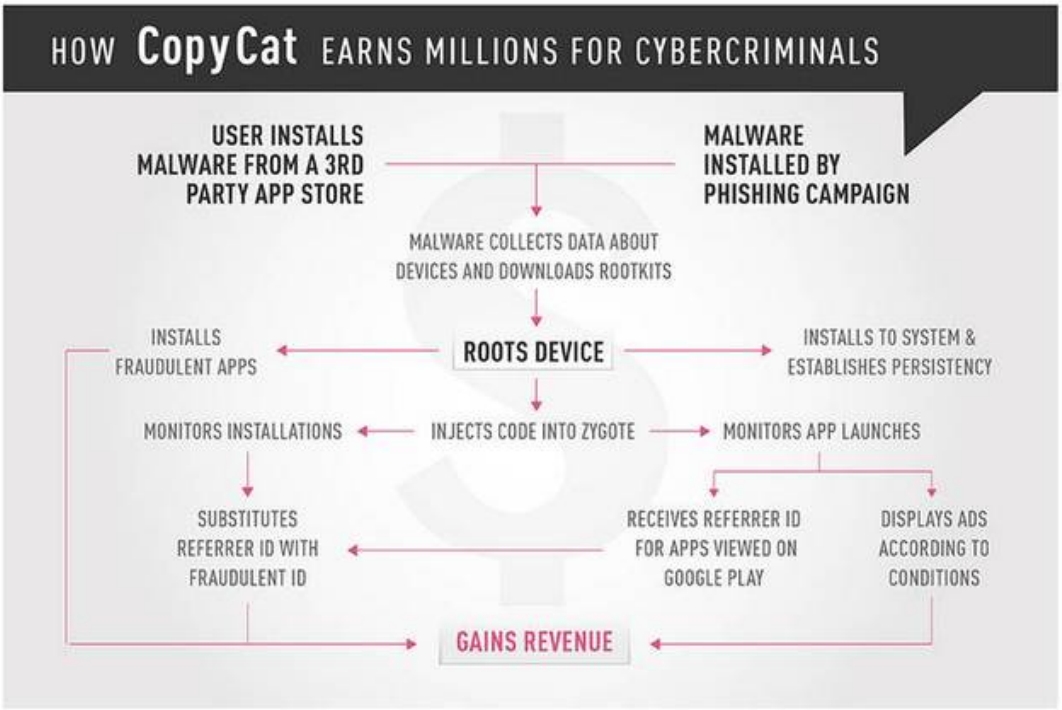
Bithumb, the world's fourth largest cryptocurrency exchange by volume, confirmed a security incident during which an unknown hacker was able to make off with an yet undetermined amount of funds.

Clues that something was wrong emerged on Thursday, when South Korean users, who make most of Bithumb's userbase, started complaining on a local social network about losing control over large funds stored in their Bithumb accounts.

A day later after these complaints, the company officially admitted the breach in a blog post on its website, albeit it did not provide any meaningful details.

Read More

CopyCat Android Rooting Malware Infected 14 Million Devices



A newly uncovered malware strain has already infected more than 14 Million Android devices around the world, earning its operators approximately $1.5 Million in fake ad revenues in just two months.

Dubbed CopyCat, the malware has capabilities to root infected devices, establish persistency, and inject malicious code into Zygote – a daemon responsible for launching apps on Android, providing the hackers full access to the devices.

Read More

Researchers Extract RSA-1024 Keys from Popular Crypto Library

A team of eight researchers from various universities has found a bug in the Libcrypto library that allows an attacker with local access to extract the RSA-1024 private key that was used to encrypt local data.

Their researcher paper was focused on GnuPG, an encryption software for Android, Linux, macOS, and Windows. More accurately, the researchers focused their work on Libgcrypt, GnuPG's module responsible for the actual GnuPG's encryption operations.

Researchers say they found that Libgcrypt used a method known as "sliding windows" to compute part of these mathematical equations behind data encryption. The problem, they say, was that "sliding windows" is a computation method known to leak data via side-channel attacks.

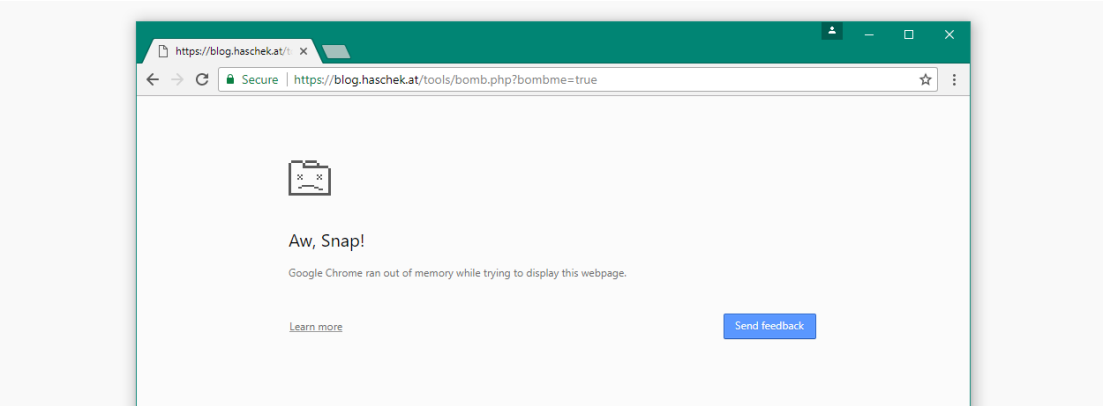
Read More

OWASP Mobile Security Testing Guide

OWASP has released a work-in-progress version of the OWASP Mobile Security Testing Guide. Since it's work-in-progress the content can change at any time.

Read More

ZIP Bombs Can Protect Websites From Getting Hacked



Webmasters can use so-called ZIP bombs to crash a hacker's vulnerability and port scanner and prevent him from gaining access to their website.

The term "ZIP bomb" refers to nested ZIP archives that when unzipped are decompressed to huge files that the victim's computer cannot process in its memory or cannot store on disk.

For example, a 4.5 petabyte file containing only zeroes can be easily compressed to 42 kilobytes because the ZIP compression system can handle repetitive data extremely well.

Read More

Attack on Critical Infrastructure Leverages Template Injection

Attackers are continually trying to find new ways to target users with malware sent via email. Talos has identified an email-based attack targeting the energy sector, including nuclear power, that puts a new spin on the classic word document attachment phish. Typically, malicious Word documents that are sent as attachments to phishing emails will themselves contain a script or macro that executes malicious code. In this case, there is no malicious code in the attachment itself. The attachment instead tries to download a template file over an SMB connection so that the user's credentials can be silently harvested. In addition, this template file could also potentially be used to download other malicious payloads to the victim's computer.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.