



AV-TEST

Sicherheitslage Android

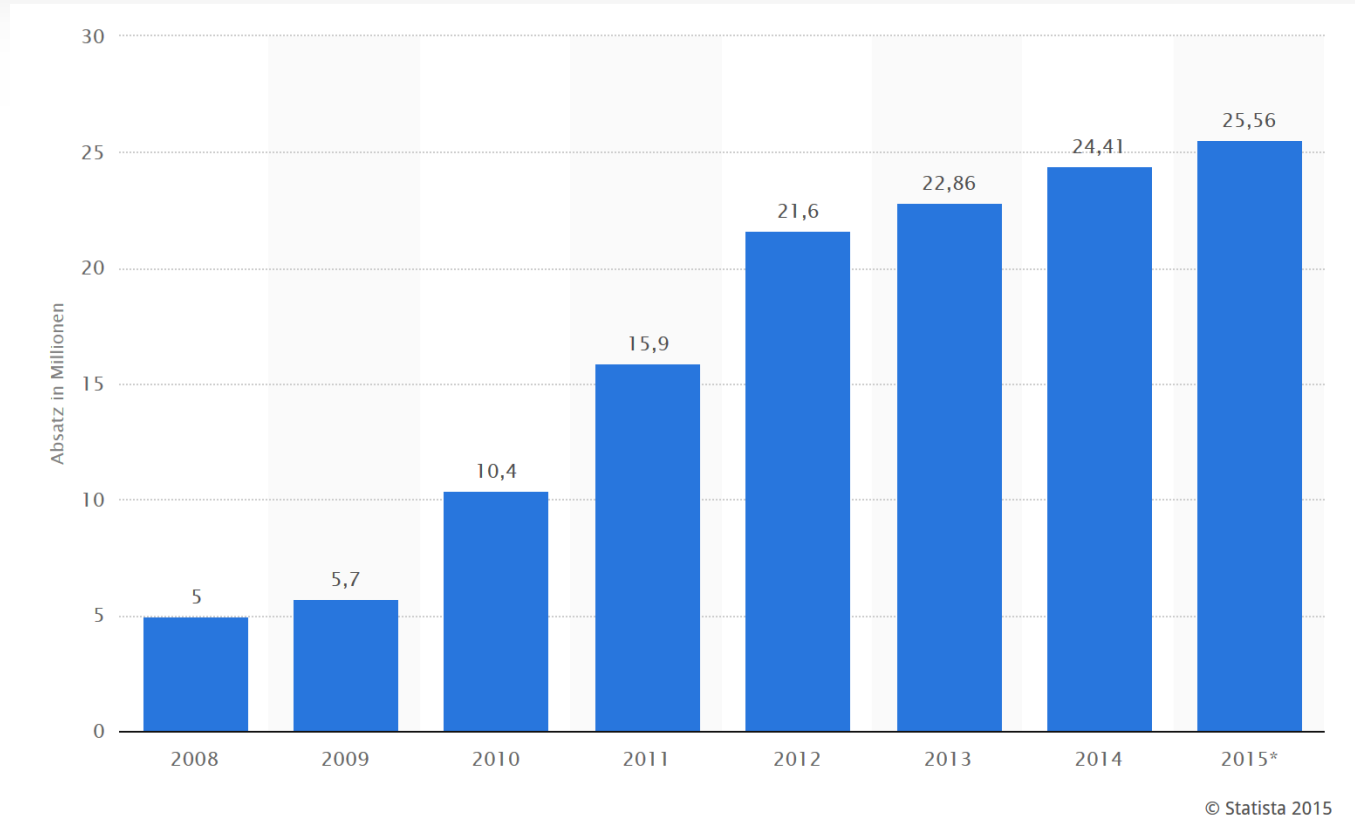
SICHERHEITSLAGE ANDROID

- MEHR ALS 30 IT-SPEZIALISTEN
- MEHR ALS 15 JAHRE EXPERTISE IM BEREICH ANTIVIREN-FORSCHUNG
- UNTERNEHMENSGRÜNDUNG 2004
- **EINE DER GRÖßTEN VIREN-DATENBANK DER WELT**
- **400 CLIENT- UND SERVERSYSTEME**
- **1.000 TERABYTE TESTDATEN**
- **MEHR ALS 5.000 EINZEL- UND VERGLEICHSTESTS PRO JAHR**
- ANALYSE, TESTING, DEVELOPMENT, CONSULTING & SERVICES FÜR AV-HERSTELLER, FACHMAGAZINE, BEHÖRDEN & UNTERNEHMEN



SICHERHEITSLAGE ANDROID

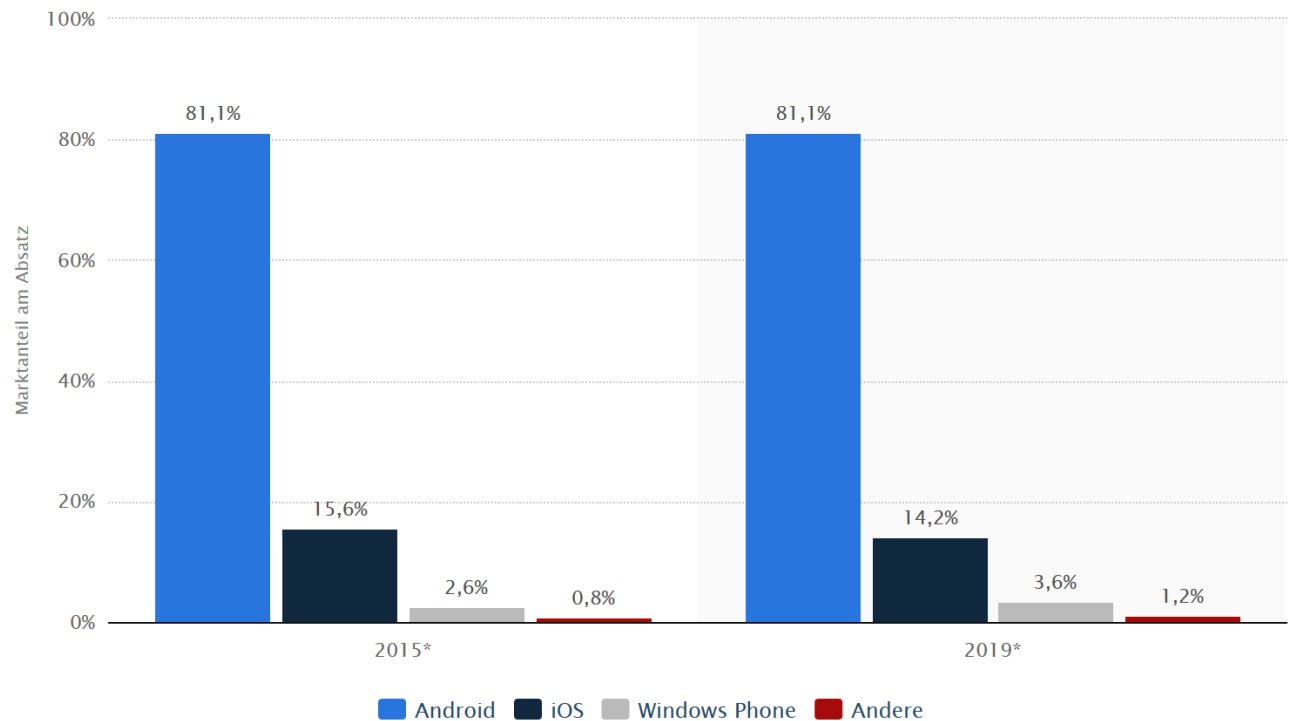
Über 25 Millionen
neue Smartphones
pro Jahr in
Deutschland



SICHERHEITSLAGE ANDROID

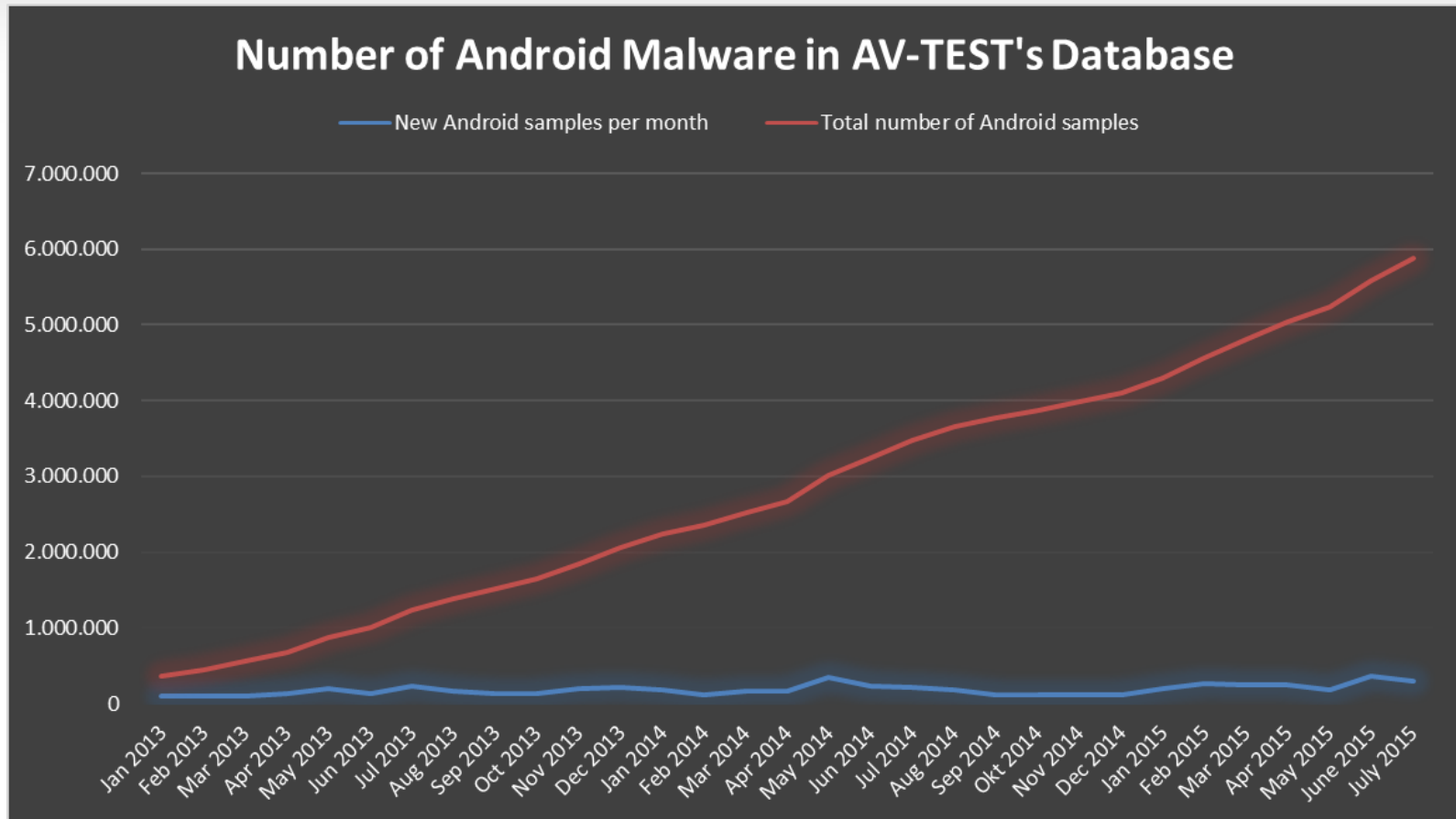
80% aller Smartphones in Deutschland sind Android-Geräte.

Und das wird wahrscheinlich auch so bleiben.

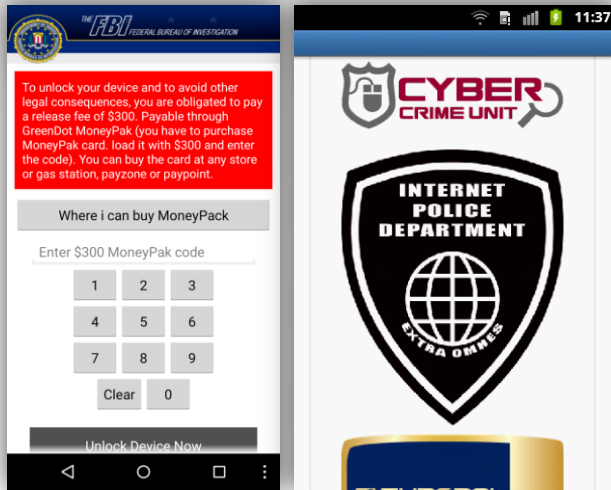


© Statista 2015

SICHERHEITSLAGE ANDROID



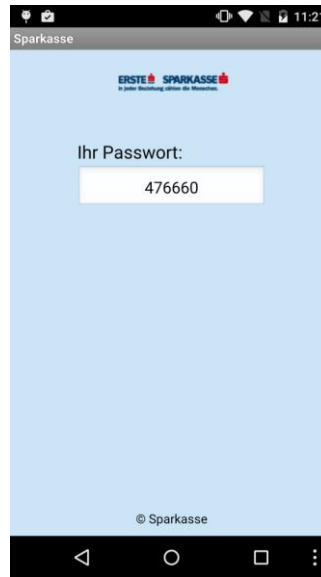
SICHERHEITSLAGE ANDROID



Ransomware

Rootkits

Adware



Banking Trojaner



Bitcoin Miner / Botnetze

Backdoors

Spyware

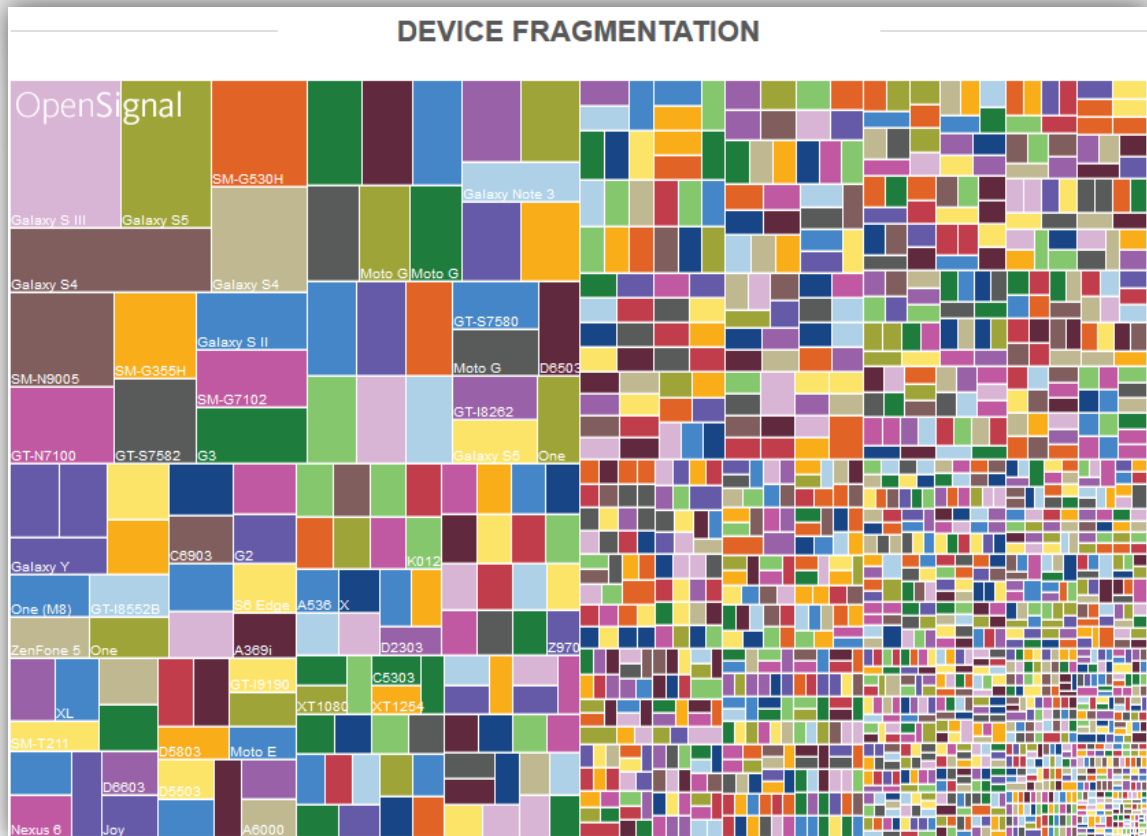
SICHERHEITSLAGE ANDROID

Jeder Hersteller produziert dutzende Modelle

Für jedes Modell müssen Sicherheitsupdates entwickelt und getestet werden

Mobilfunkprovider müssen die Updates an Kunden verteilen

Nur die Top-Geräte erhalten Update-Support!



Quelle: <http://opensignal.com/reports/2015/08/android-fragmentation/>

SICHERHEITSLAGE ANDROID

android
open source project

Change 162630 - Merged Reply...

Prevent reading past the end of the buffer in 3GPP

Metadata processed within the parse3GPPMetaData function may not be NUL terminated and thus calling setCString may read out of bounds. Ensure proper NUL termination, but take care not to interfere with other special cases (ie, albm).

Bug: 20923261
Change-Id: Ie93b3038b534b4c4460571a68f4d734cff7ad324

Owner [Jon Larimer](#)
Reviewers [Jon Larimer](#) [Nick Kravovich](#)
[Joshua J. Drake](#)
Project [platform/frameworks/av](#)
Branch [master](#)
Topic
Updated 4 weeks ago

Code-Review +2 [Nick Kravovich](#)
Verified +1 [Jon Larimer](#)

Related Changes (12)

- Fix several ineffective integer overflow checks
- Detect allocation failures and bail gracefully
- Fix integer overflow during MP4 atom processing
- Fix integer underflow in ESDS processing
- MPEG4Extractor: still more NULL dereference fixes
- Fix null-pointer-dereferences accessing the SampleTable
- Fix multiple division-by-zero conditions in MPEG4 parsing
- Prevent integer overflow when processing covr MPEG4 atoms
- Fix integer overflow when handling MPEG4 tx3g atom
- Prevent integer underflow if size is below 6
- Fix integer underflow in covr MPEG4 processing
- ▶ Prevent reading past the end of the buffer in 3GPP

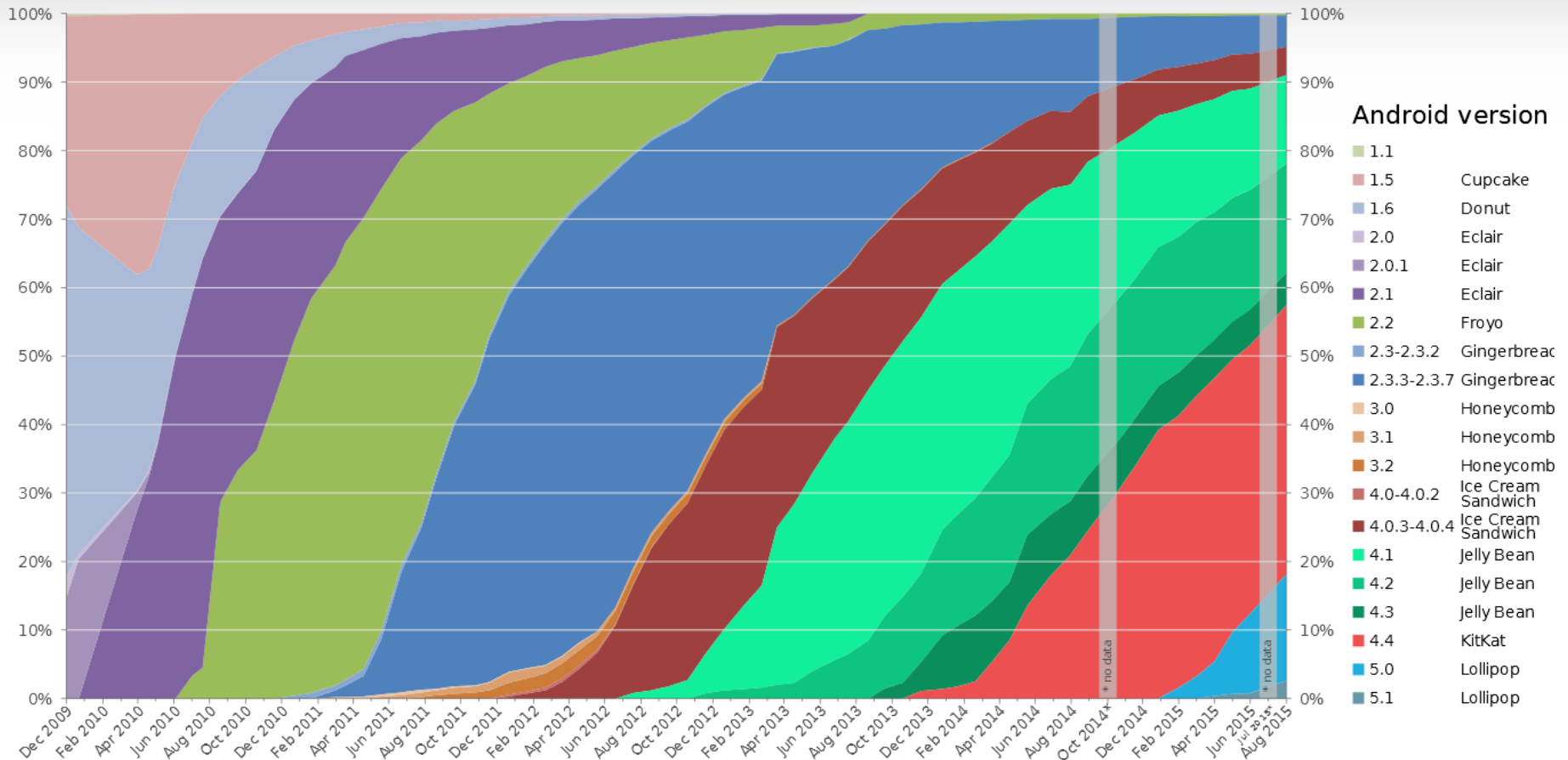
Author [Joshua J. Drake <android-open-source@qoop.org>](#) May 5, 2015 12:33 AM
Committer [Jon Larimer <jlarimer@google.com>](#) Jul 31, 2015 9:04 PM
Commit [1760fbf496acfb0f808baea5461e02158b6faa5](#) (gitiles)
Parent(s) [8fddd03a20d6e4c0a339d68387933135a08873da](#) (gitiles)
Change-Id [Ie93b3038b534b4c4460571a68f4d734cff7ad324](#)

Android ist Open Source

Änderungen am Code (Bug Fixes) sind öffentlich nachvollziehbar

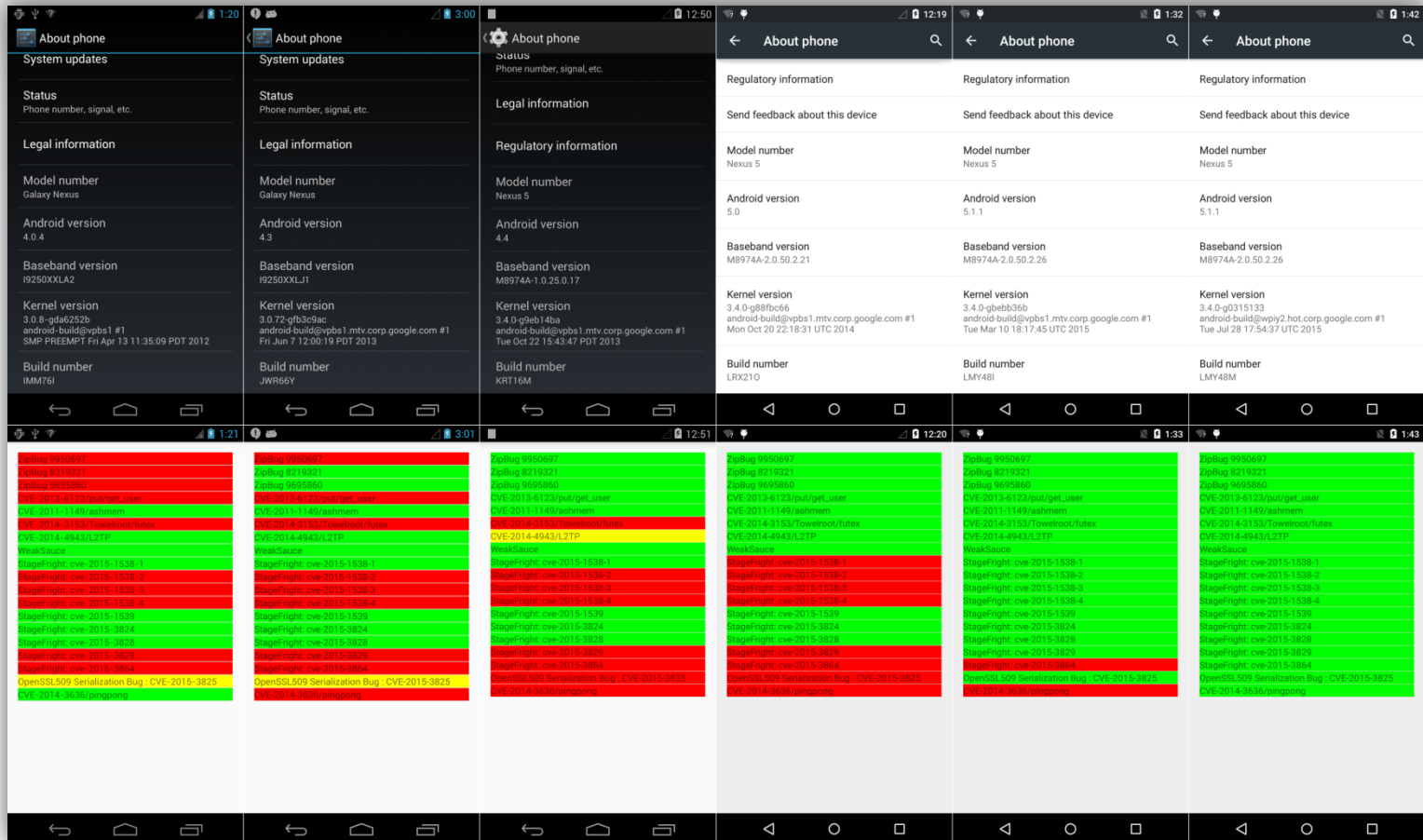
Exploits für geschlossene Sicherheitslücken können rückwirkend entwickelt werden

SICHERHEITSLAGE ANDROID



Quelle: https://en.wikipedia.org/wiki/Android_version_history

SICHERHEITSLAGE ANDROID



Android Vulnerability Test Suite: <https://github.com/nowsecure/android-vts>



Eine Sicherheitslücke in der Multimedia-Bibliothek von Android erlaubt Zugriff auf Mikrofon, Kamera, Bluetooth und Internet

Über Webseiten, Nachrichten und Werbeanzeigen kann die Lücke ausgenutzt werden

Angreifer können per MMS Malware auf einem Zielgerät installieren, ohne dass der Nutzer es merkt

Angreifer können manipulierte Werbung schalten, um eine große Menge an Endgeräten mit Schadsoftware zu infizieren







Quelle: <https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/>




Experts Found a Unicorn in the Heart of Android

By Z Team

Monday, Jul 27 2015 at 13:02

 Share 10.4K  Tweet 4543  Like 165  G+ 84  Share 182  Email 233

 Share 31K

The Latest on Stagefright: CVE-2015-1538 Exploit is Now Available for Testing Purposes

By zLabs

Wednesday, Sep 9 2015 at 08:05

 Share 910  Tweet 1850  Like 1.1k  G+ 73  Share 36  Email 91  Share 5818

Certifi-gate: Hundreds of Millions of Android Devices Could Be Pwned

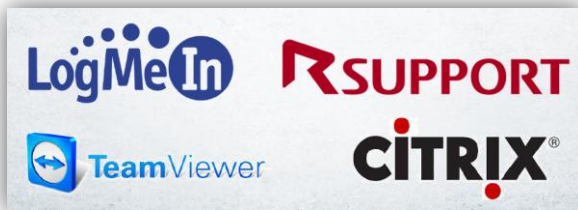
by Check Point Research Team posted 2015/08/06

Certifi-Gate ist ein Angriff auf Mobile Remote Support Tools

Gerätehersteller stellen Systemschnittstellen für solche Tools zur Verfügung

Die Tools werden unzureichend vom System authentifiziert

Malware kann die Schnittstellen nutzen und das Gerät fernsteuern



Certifi-gate Found in the Wild on Google Play

by Check Point Research Team posted 2015/08/25

Quelle: <https://www.blackhat.com/docs/us-15/materials/us-15-Bobrov-Certifi-Gate-Front-Door-Access-To-Pwning-Millions-Of-Androids.pdf>

Samsung Keyboard Security Risk Disclosed: Over 600M+ Devices Worldwide Impacted

**Eine vorinstallierte Tastatur sucht automatisch nach Updates
und benutzt eine ungesicherte Verbindung**

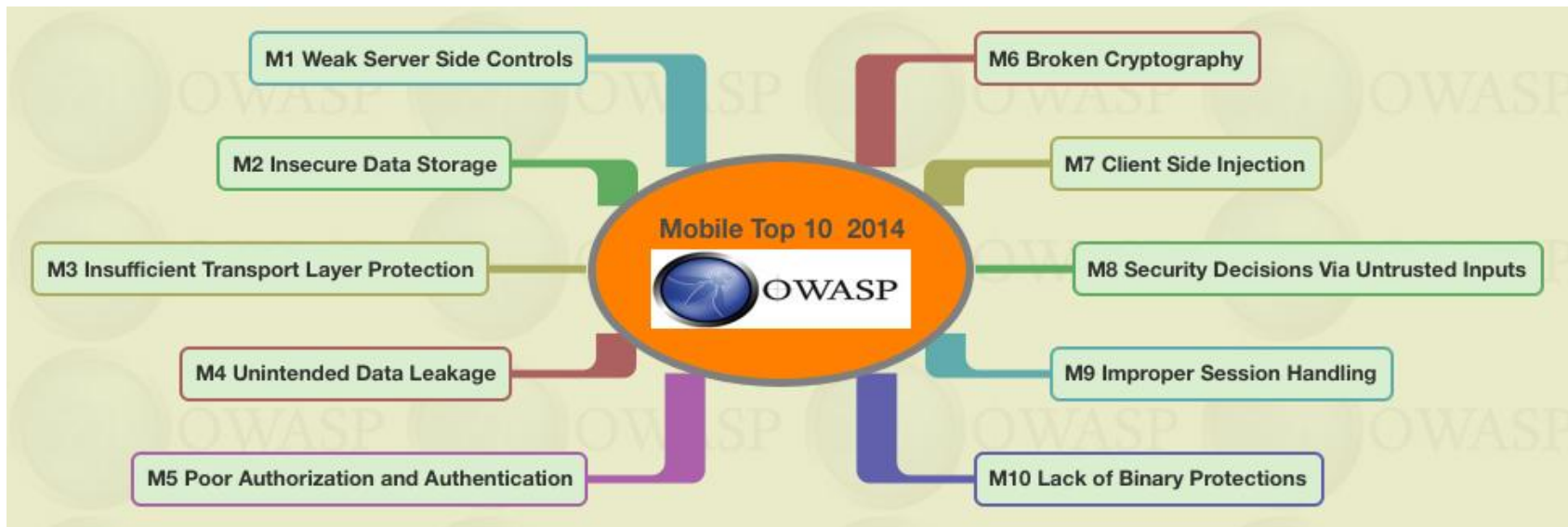
Die heruntergeladenen Updates werden unzureichend verifiziert

**Ein Angreifer kann infizierte Updates verbreiten und damit
Sensoren auslesen (GPS, Kamera, Mikrofon)
Malware installieren
und Daten auslesen oder manipulieren**

Quelle: <https://www.nowsecure.com/keyboard-vulnerability/>

**Neben den Sicherheitslücken im Betriebssystem
gibt es auch jede Menge Lücken in den eingesetzten Apps**

**Unsichere Apps betreffen auch andere Systeme
wie iOS, Windows Phone und BlackBerry**



Quelle: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

**Neben Schadsoftware hat Android ein
massives Problem mit Sicherheitslücken**

Die Verteilung von Sicherheitsupdates dauert zu lange

**Endbenutzer haben nur wenige Möglichkeiten,
sich mit Sicherheitsupdates zu schützen**

Unsichere Apps gibt es für alle Smartphone Plattformen

Welche Schutzmaßnahmen gibt es?

Mobile Security Apps

Mobile Device Management

Sicherheitsbewusstsein und Mitarbeiterschulung

Allgemeine Verhaltensweisen

Mobile Security Apps

Testergebnisse auf
www.av-test.de

Wichtige Funktionen:

- Anti-Virus
- Anti-Diebstahl
- Browserschutz



The screenshot shows the AVTEST website interface. At the top right, there are language selection icons for Deutsch, English, Français, and Español. The main navigation menu includes Institut, News, Tests, AWARD, Testverfahren, Statistiken, Publikationen, Presse, and Kontakt. Below the navigation, there are four large buttons representing different application categories: MOBILGERÄTE ANDROID, PRIVATANWENDER WINDOWS, PRIVATANWENDER MAC OS, and UNTERNEHMEN WINDOWS CLIENT. A link 'Einzelnen Hersteller betrachten' is visible below these buttons.

Die besten Antivirus Programme für Android

Getestete Betriebssysteme in Ihrer Auswahl: [Android](#)

Android		Marz 2015		
	Name		Schutzwirkung	Benutzbarkeit
■ Marz 2015	AhnLab V3 Mobile 2.1		●●●●●	●●●●●
■ Januar 2015	Mobile Security 2.0		●●●●●	●●●●●
■ November 2014	Security Manager 5.0		●●●●●	●●●●●
■ September 2014	AVL 2.3		●●●●●	●●●●●
■ Juli 2014	Mobile Security 4.0		●●●●●	●●●●●
■ Mai 2014	AVG AntiVirus Free 4.2		●●●●●	●●●●●
■ März 2014	Avira Free Android Security 3.9		●●●●●	●●●●●
■ Januar 2014	Baidu Mobile Security 5.5		●●●●●	●●●●●
■ November 2013	Bitdefender Mobile Security 2.36		●●●●●	●●●●●
■ September 2013	BullGuard Mobile Security 14.0		●●●●●	●●●●●
■ Juli 2013	Clean Master 5.9		●●●●●	●●●●●
■ Mai 2013				
■ März 2013				
■ Januar 2013				

ZUSAMMENFASSUNG & SICHERHEITSTIPPS



- DIE AV-TEST QUALITÄSSIEGEL „CERTIFIED“ UND „APPROVED“
- 1.270 VERGEBENE AV-TEST ZERTIFIKATE SEIT 2010
- AUSGEZEICHNET WERDEN DIE JAHRESBESTEN SCHUTZLÖSUNGEN FÜR DIE BEREICHE HEIMANWENDER, UNTERNEHMEN UND MOBILE SECURITY.
- DER AV-TEST INNOVATION AWARD FÜR INNOVATIVE IT-SCHUTZLÖSUNGEN

Mobile Device Management

Verwaltung aller Mobilgeräte im Unternehmen

Sicherheitsrichtlinien können Nutzerverhalten einschränken

Individuelle App Stores ermöglichen eine qualifizierte Vorauswahl

Unternehmensdaten werden von persönlichen Daten getrennt

Sicherheitsbewusstsein und Mitarbeiterschulung

Integrieren Sie IT-Sicherheit in betriebliche Unterweisungen

Zur Orientierung hilft der IT-Grundschutz-Katalog des BSI

www.bsi.bund.de

Allgemeine Verhaltensweisen

**Sperren Sie Ihre Geräte mit einem Lockscreen
mit PIN- oder Passwort-Eingabe**

Aktivieren Sie die Geräteverschlüsselung, sofern vorhanden

Benutzen Sie sichere und verschiedene Passwörter in allen Konten

**Nutzen Sie Ihr Smartphone zur 2-Faktor-Authentifizierung,
um Online-Konten zu schützen**

Allgemeine Verhaltensweisen

Installieren Sie regelmäßig verfügbare Sicherheitsupdates

Achten Sie auf verschlüsselte Datenverbindungen (SSL & VPN)

Erstellen Sie regelmäßig Backups Ihrer Daten

“Rooten” Sie Ihr Gerät nicht

Proben Sie den Ernstfall: Was muss ich tun, wenn ...?



Folgen Sie uns auf Twitter @avtestde



Finden Sie uns auf facebook.com/avtestorg

Aktuelle Test-Ergebnisse: www.av-test.de



**Vielen Dank für Ihre Aufmerksamkeit!
Haben Sie noch Fragen?**