



Link: <https://www.channelpartner.de/a/android-malware-erpresst-smartphone-nutzer,3042526>

**Android-Trojaner verlangt Lösegeld**

## **Android-Malware erpresst Smartphone-Nutzer**

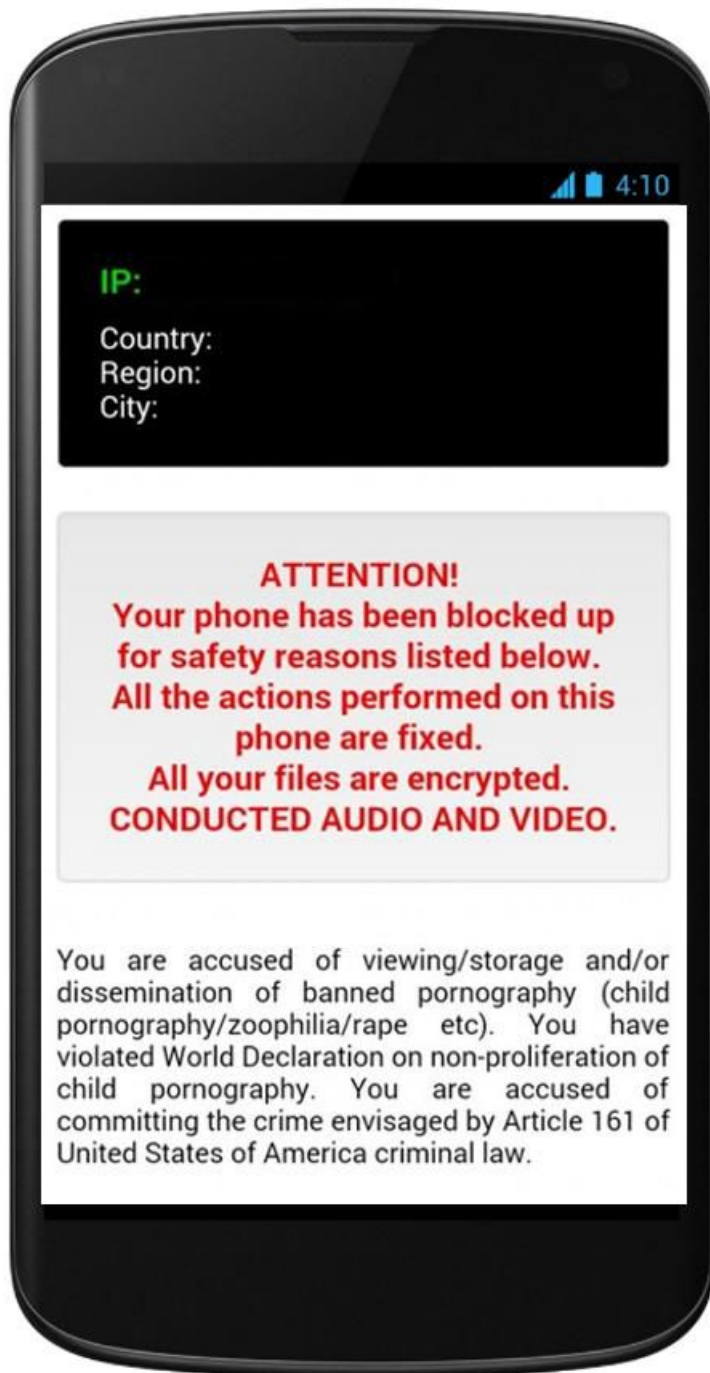
Datum: 06.06.2014  
Autor(en): Moritz Jäger

**Eine Malware verschlüsselt gespeicherte Daten auf Android-Smartphones und verlangt Lösegeld. Anstecken kann man sich unter anderem auf manipulierten Erotik-Webseiten.**

Ransomware ist im PC- und Windows-Umfeld eine Kriminellen eine beliebte Art um Geld zu erpressen: Die Schadsoftware verschlüsselt den Zugang zum Computer oder wichtigen Dokumenten (etwa Word-Dateien) und verlangt vom Nutzer ein Lösegeld. Nur wenn er zahlt, so die Meldung, die erscheint, erhält er den Schlüssel, um den Zugriff auf seine Daten zu erhalten. Nun haben diese Schädlinge scheinbar den Sprung auf das mobile Betriebssystem Android geschafft.

Das zumindest meldet der Sicherheitsanbieter F-Secure in seinem Blog. Eine angebliche **Police Ransomware**<sup>1</sup> namens **Koler**<sup>2</sup> zeigt an, dass der Nutzer unerlaubtes, meist pornografisches Material auf dem Smartphone gespeichert hat. Gegen die Zahlung einer Summe X wird ein angebliches Verfahren eingestellt.

Der Trojaner in Aktion: Das Android-Smartphone ist nicht mehr sinnvoll nutzbar.  
Foto: F-Secure



Diese Version infiziert Smartphones, wenn der Nutzer zuvor manipulierte Webseiten vom Smartphone aus besucht. Die Seite meldet, dass ein bestimmter Videoplayer installiert werden müsse, dazu muss der Nutzer die Installation aus unbekanntem Quellen erlauben. Statt der Abspielsoftware wird allerdings der Trojaner namens "Koler" installiert, der anschließend das Gerät sperrt. Ist keine Anti-Viren-Software auf dem Smartphone eingerichtet (mit der die Installation direkt geblockt wird), gibt es zwei Wege, den Trojaner wieder zu entfernen:

Koler blockt die Zurück-Taste von Android, erlaubt aber die Nutzung der Home-Taste. Laut F-Secure hat der Nutzer nur ein paar Sekunden Zeit, um in die Einstellungen zu wechseln und dort die Malware zu deinstallieren oder das Gerät auf Werkseinstellungen zurückzusetzen. Alternativ kann man in den Recovery-Modus booten und das Gerät dort zurücksetzen. Die Tastenkombination unterscheidet sich teilweise von Gerät zu Gerät, meist muss man aber während dem Startvorgang die Leiser-Taste gedrückt halten. (cvi)

[Hinweis auf Bildergalerie: **Lookout Mobile Threat Report -** ] <sup>gal1</sup>

## Links im Artikel:

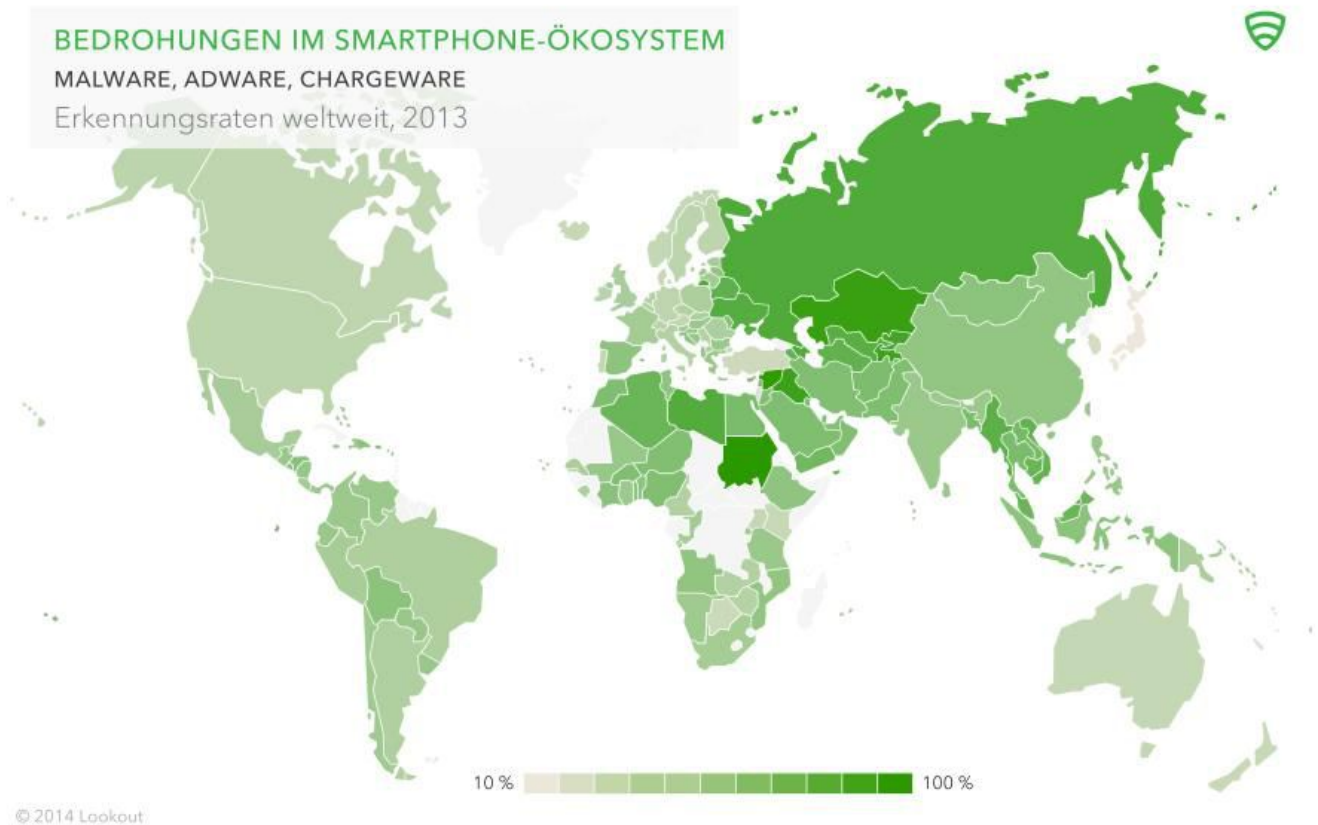
<sup>1</sup> <http://www.f-secure.com/weblog/archives/00002704.html>

<sup>2</sup> [http://www.f-secure.com/v-descs/trojan\\_android\\_koler.shtml](http://www.f-secure.com/v-descs/trojan_android_koler.shtml)

---

## Bildergalerien im Artikel:

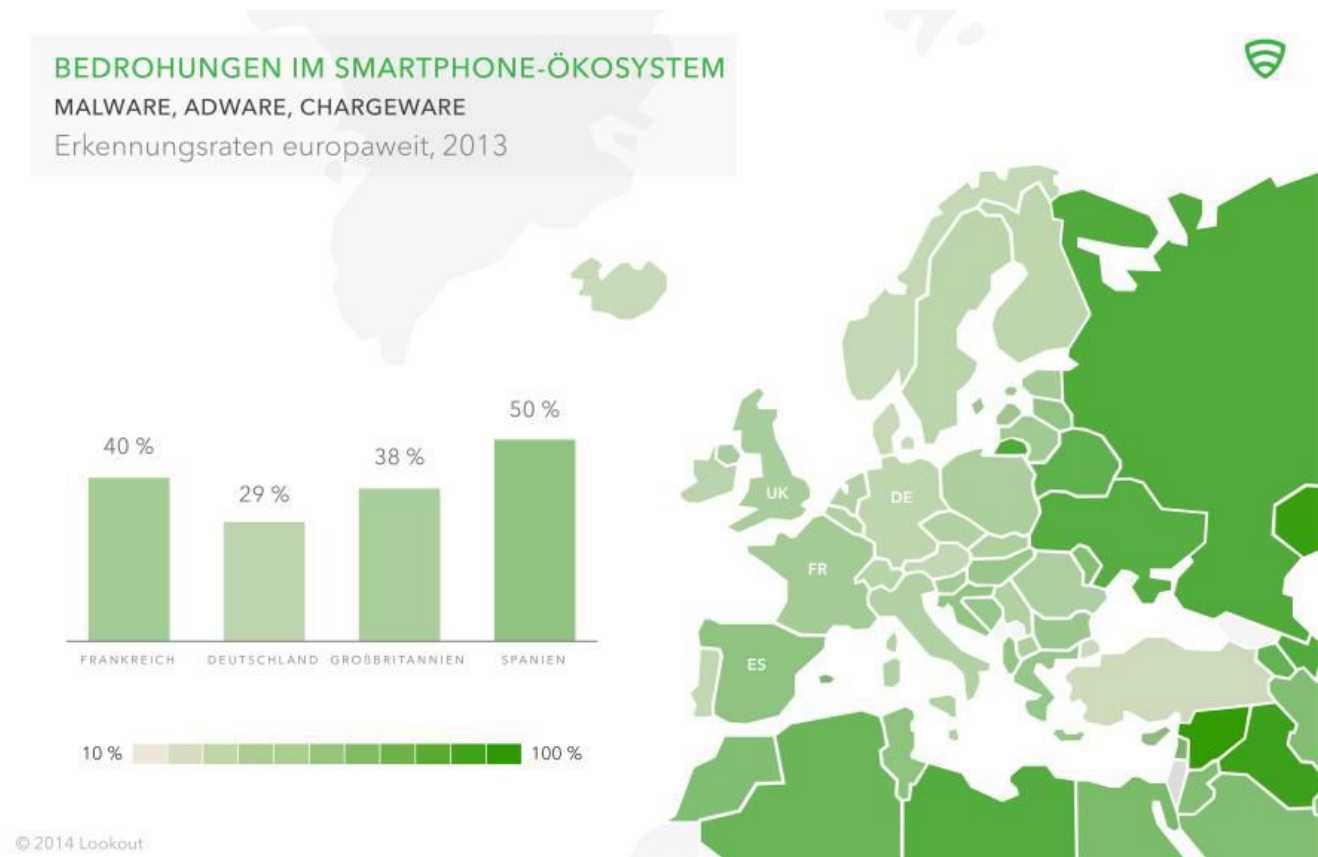
gal1 **Lookout Mobile Threat Report -**



### Lookout Security Report 2014

Die weltweiten Erkennungsraten von Lookout.

Foto: Lookout



### Lookout Security Report 2014

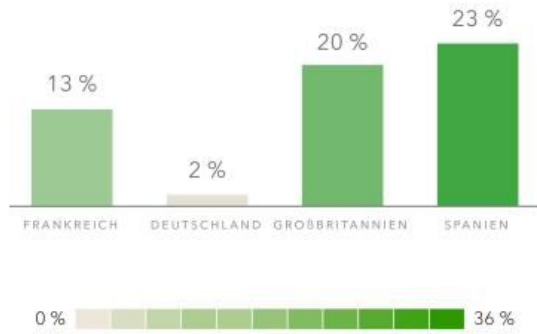
Die Malware-Erkennungsraten in der EU.

Foto: Lookout

## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### CHARGEWARE

Erkennungsraten europaweit, 2013



© 2014 Lookout

### Lookout Security Report 2014

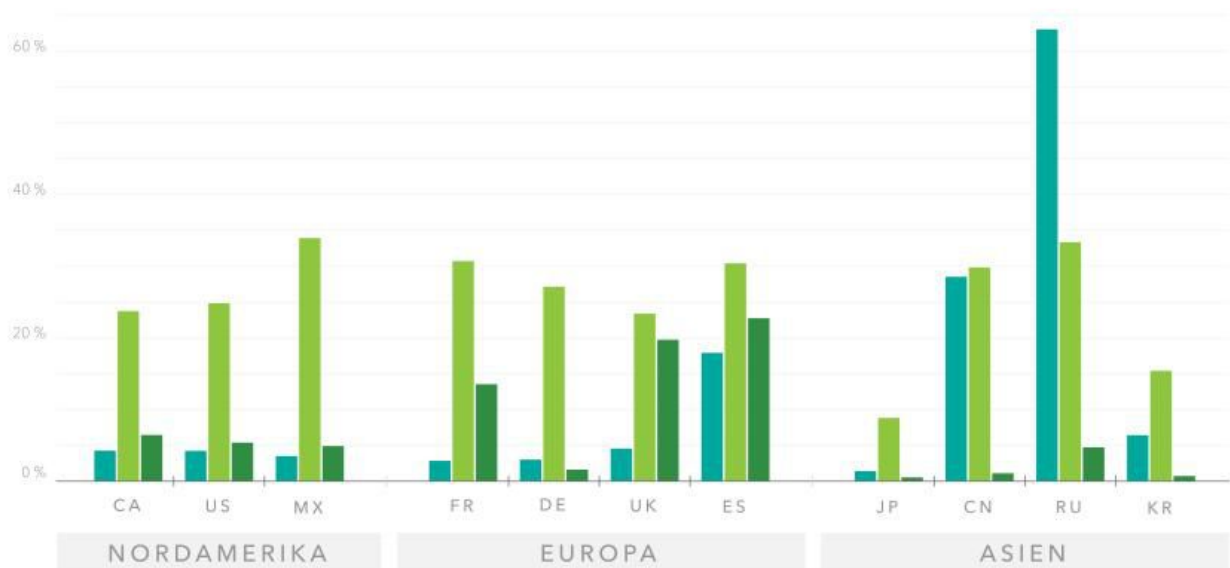
Chargeware-Verteilung in Europa - Deutschland ist angenehm sicher.

Foto: Lookout

## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### MALWARE, ADWARE, CHARGEWARE

Erkennungsraten weltweit, 2013



© 2014 Lookout

### Lookout Security Report 2014

Malware weltweit auf einem Blick.

Foto: Lookout

## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### MALWARE

Erkennungsraten weltweit, 2013



© 2014 Lookout

### Lookout Security Report 2014

Mobile Malware beschränkt sich - mit Ausnahme von Spanien - auf Russland und Asien.

Foto: Lookout

## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### ADWARE

Erkennungsraten weltweit, 2013



© 2014 Lookout

### Lookout Security Report 2014

Adware ist weltweit aktiv.

Foto: Lookout

## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### CHARGEWARE

Erkennungsraten weltweit, 2013



© 2014 Lookout

### Lookout Security Report 2014

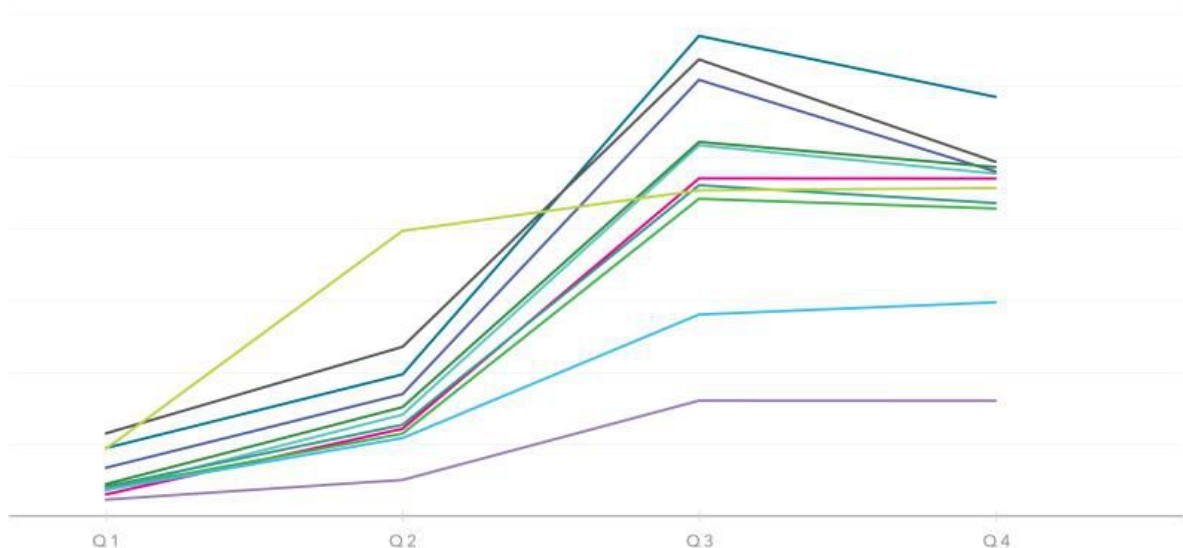
Die Chargeware-Verteilung weltweit.

Foto: Lookout

## ADWARE

### QUARTALSWEISE, NACH LAND

Erkennungsraten 2013



© 2014 Lookout

### Lookout Security Report 2014

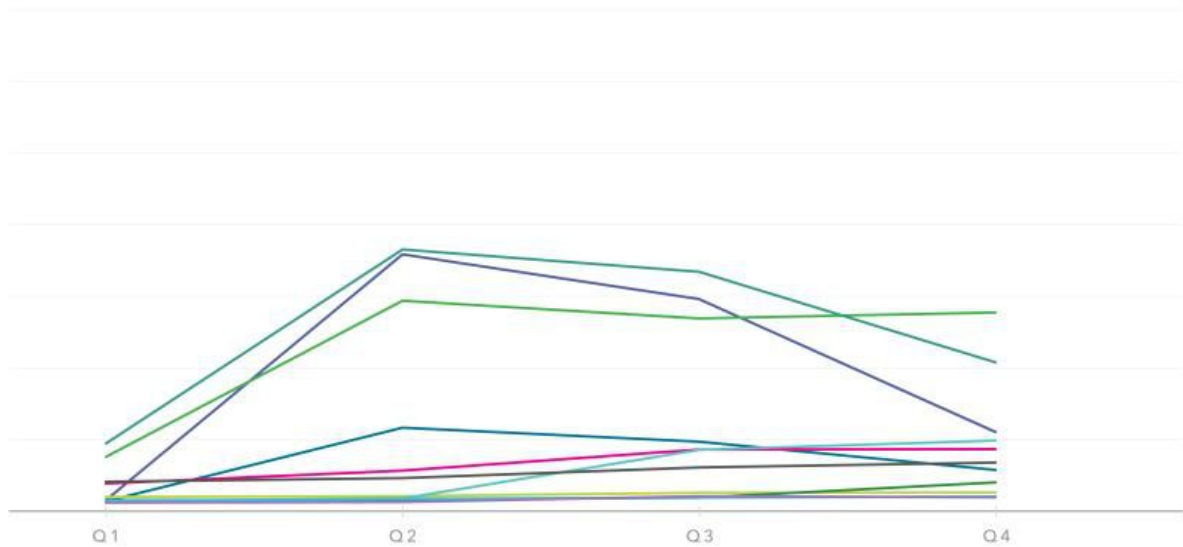
Adware: Starker Anstieg, langsamer Rückgang.

Foto: Lookout

## CHARGEWARE

QUARTALSWEISE, NACH LAND

Erkennungsraten 2013



© 2014 Lookout

### Lookout Security Report 2014

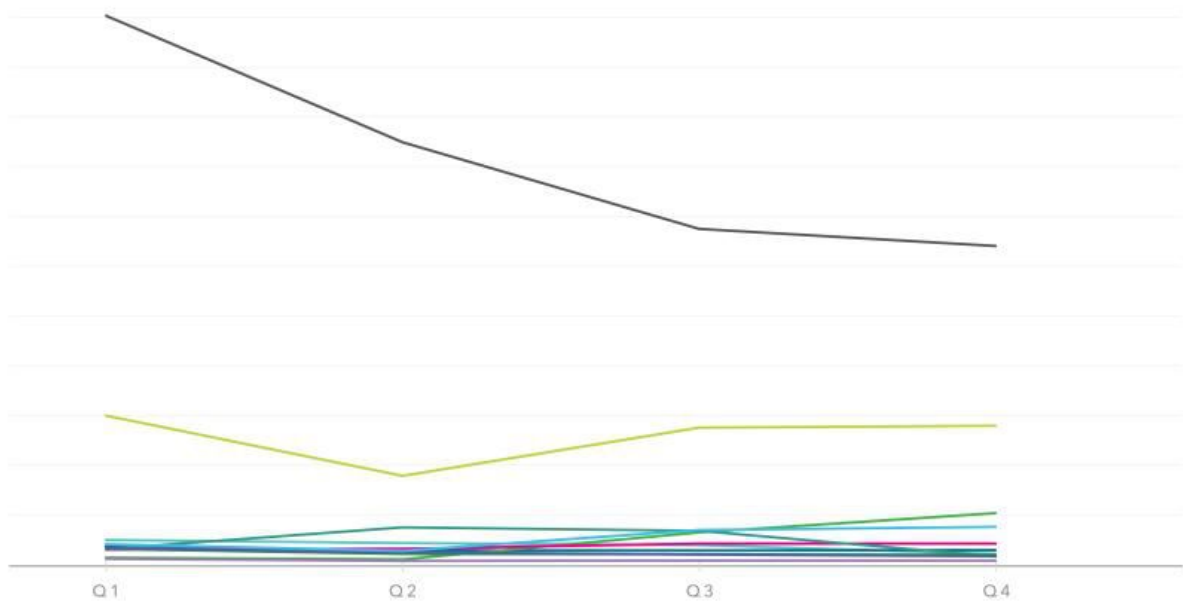
Chargeware stagniert vor allem in Spanien.

Foto: Lookout

## MALWARE

QUARTALSWEISE, NACH LAND

Erkennungsraten 2013



© 2014 Lookout

### Lookout Security Report 2014

Vor allem Russland leidet unter mobiler Malware.

Foto: Lookout



## BEDROHUNGEN IM SMARTPHONE-ÖKOSYSTEM

### RISIKO UND NUTZERVERHALTEN

Erkennungsraten weltweit, 2013



Wenn Sie einmal auf **Adware** gestoßen sind, ist die Wahrscheinlichkeit, ein zweites Mal eine App mit Adware herunterzuladen, zweimal so hoch.



Ein Trojaner auf dem Handy zu haben bedeutet eine siebenmal höhere Wahrscheinlichkeit, eine weitere App mit einem **Trojaner** herunterzuladen.



Ein Handy mit Chargeware verdoppelt Ihr Risiko, in einer weiteren App, die Sie herunterladen, auf einen **Trojaner** zu stoßen.



Ihr Risiko, einen **Trojaner** herunterzuladen, verdreifacht sich, wenn Sie bereits einen Root-Enabler heruntergeladen haben.

© 2014 Lookout

### Lookout Security Report 2014

Die wichtigsten Punkte zusammengefasst.

Foto: Lookout

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.