ChannelPartner
VON IDG

ChannelPartner
VON IDG

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

Android-Trojaner verlangt Lösegeld

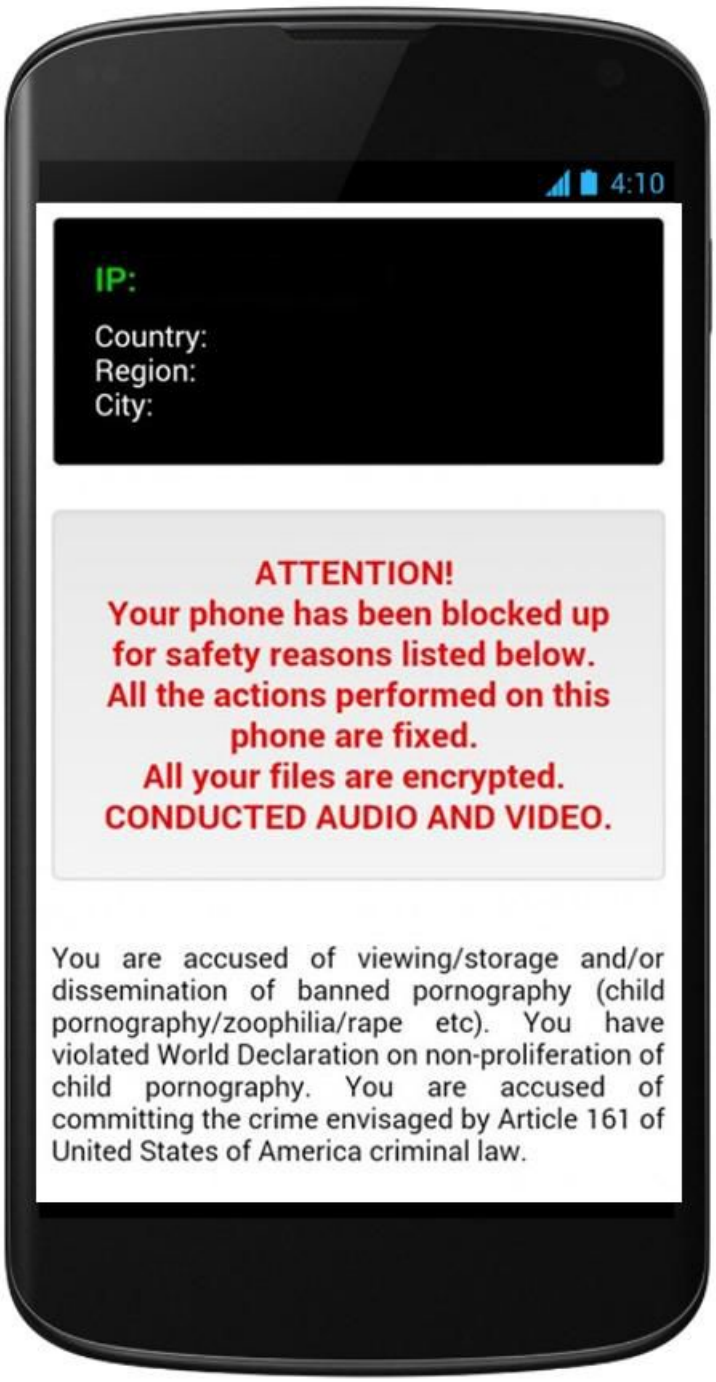
Android-Malware erpresst Smartphone-Nutzer

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**[1] namens **Koler**[2] 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 unbekannten 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)

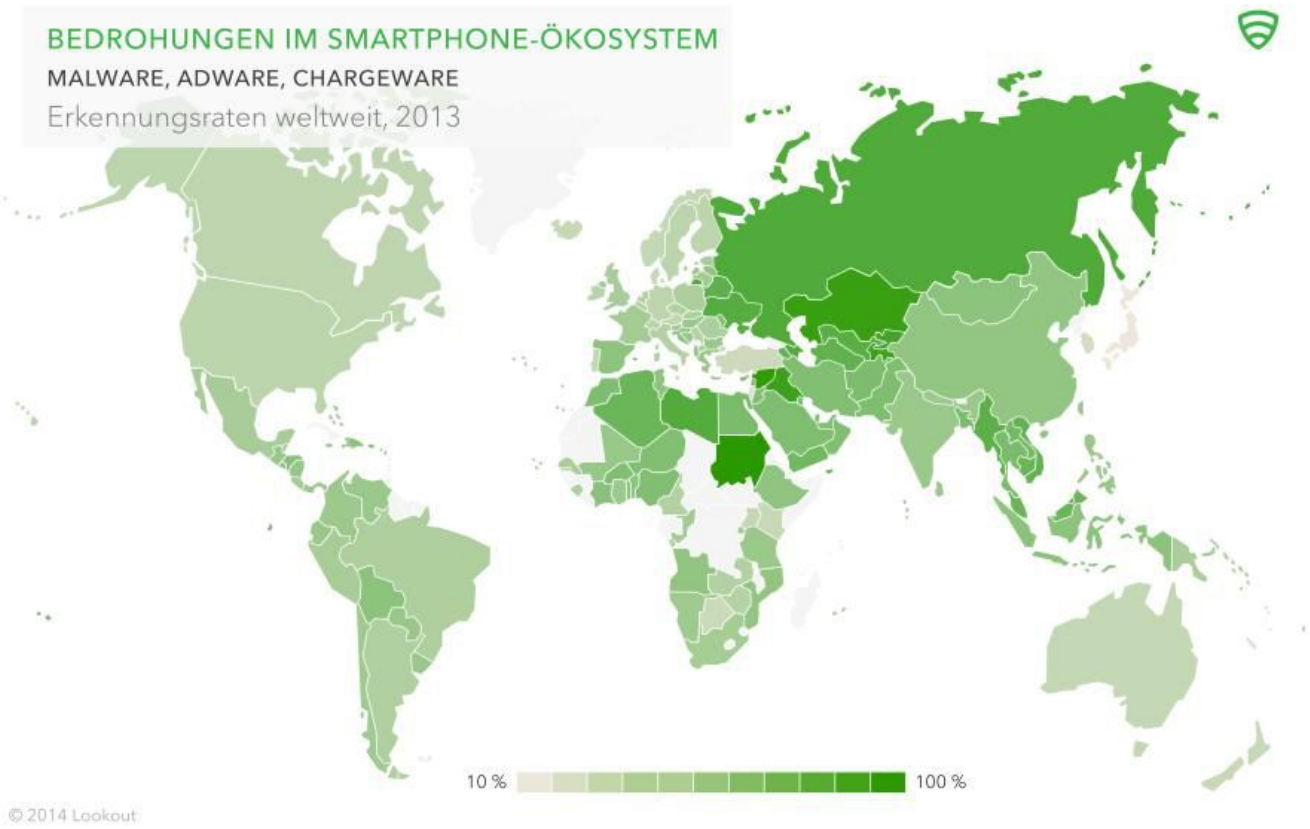
[Hinweis auf Bildergalerie: **Lookout Mobile Threat Report -**] gal1

Links im Artikel:

[1] **http://www.f-secure.com/weblog/archives/00002704.html**
[2] **http://www.f-secure.com/v-descs/trojan_android_koler.shtml**

Bildergalerien im Artikel:

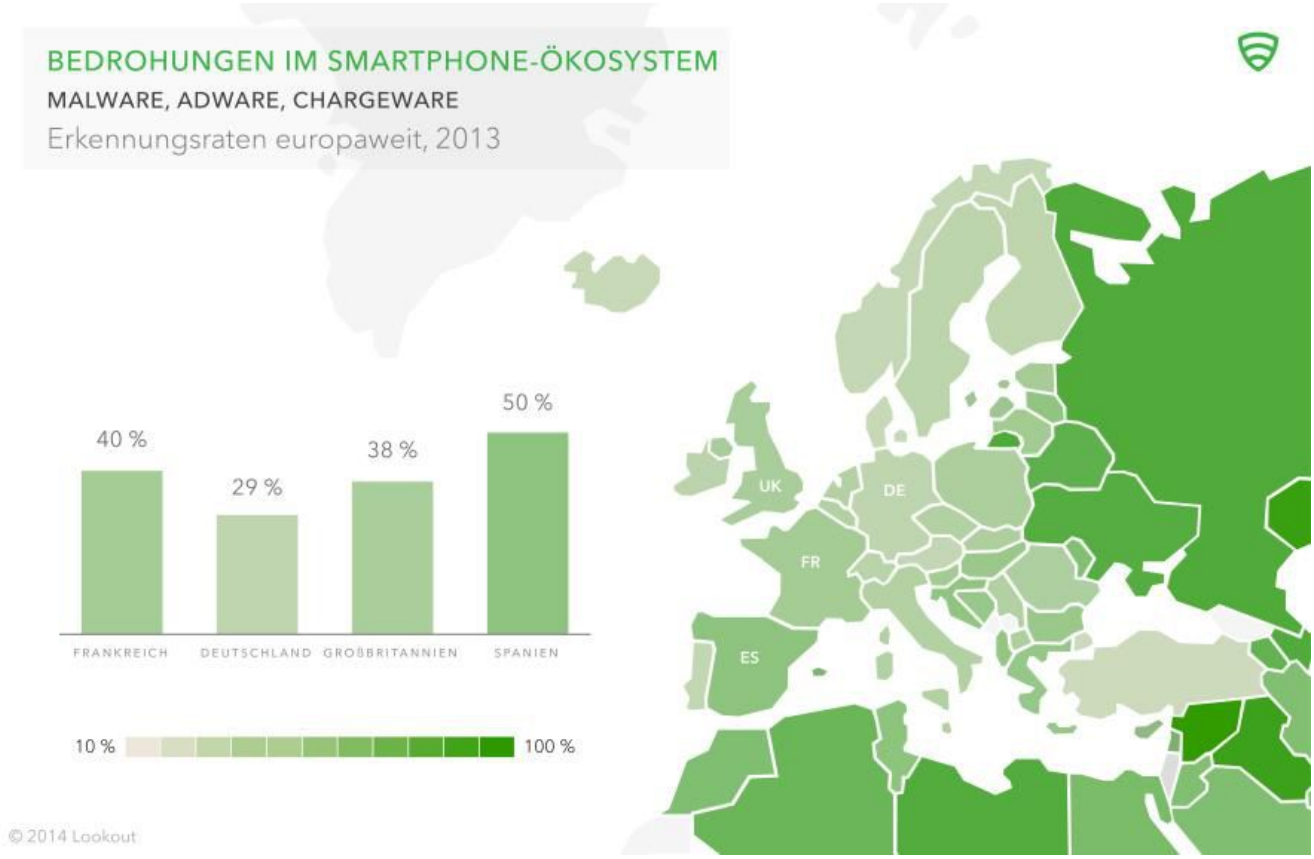
gal1 **Lookout Mobile Threat Report -**



Lookout Security Report 2014

Die weltweiten Erkennungsraten von Lookout.

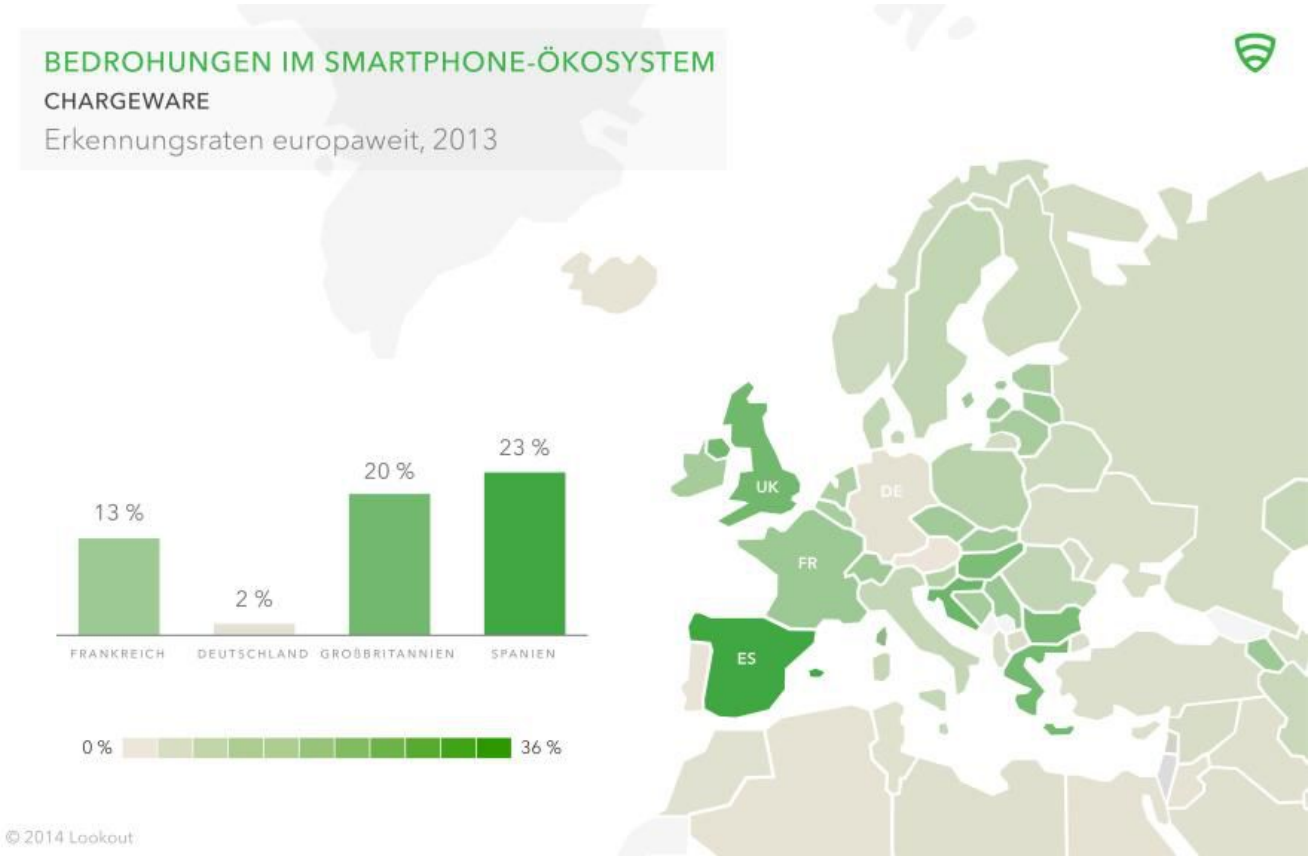
Foto: Lookout



Lookout Security Report 2014

Die Malware-Erkennungsraten in der EU.

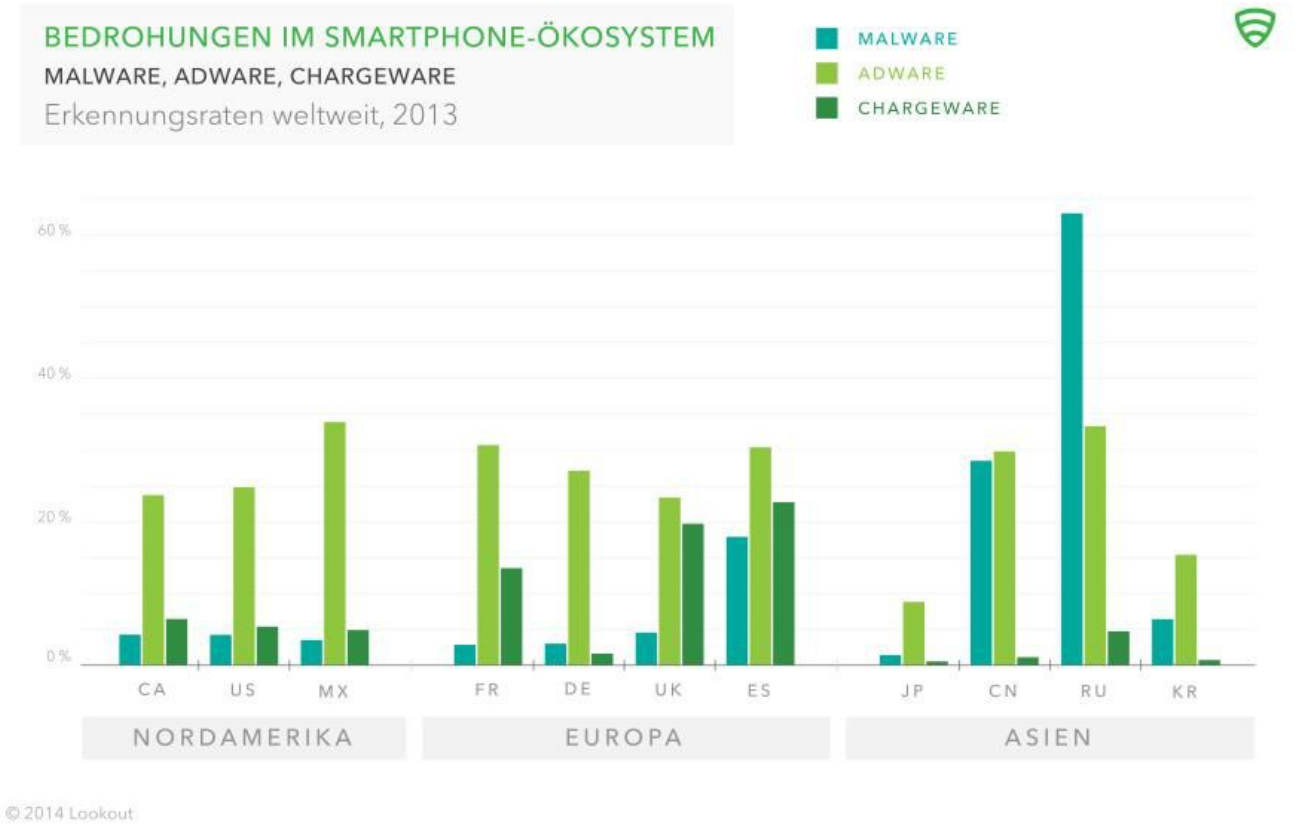
Foto: Lookout



Lookout Security Report 2014

Chargeware-Verteilung in Europa - Deuschland ist angenehm sicher.

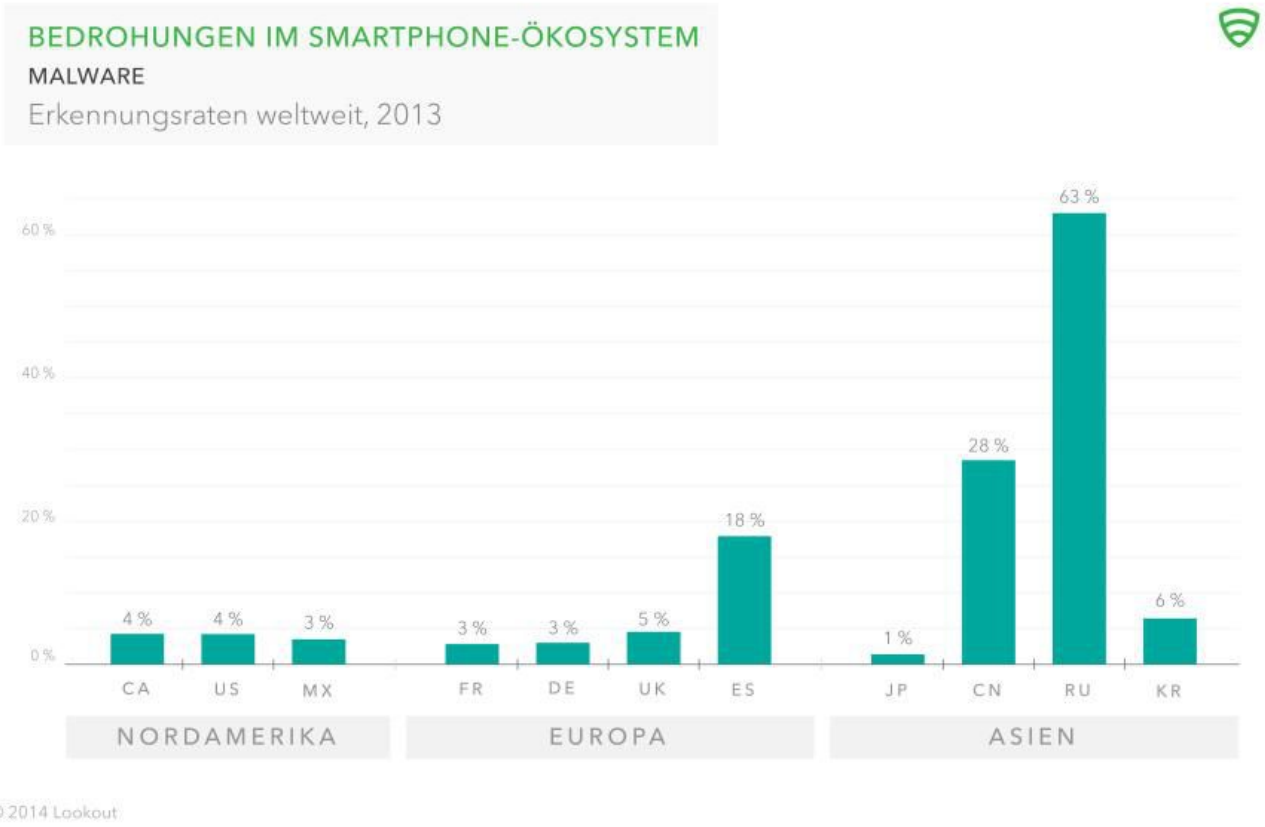
Foto: Lookout



Lookout Security Report 2014

Malware weltweit auf einem Blick.

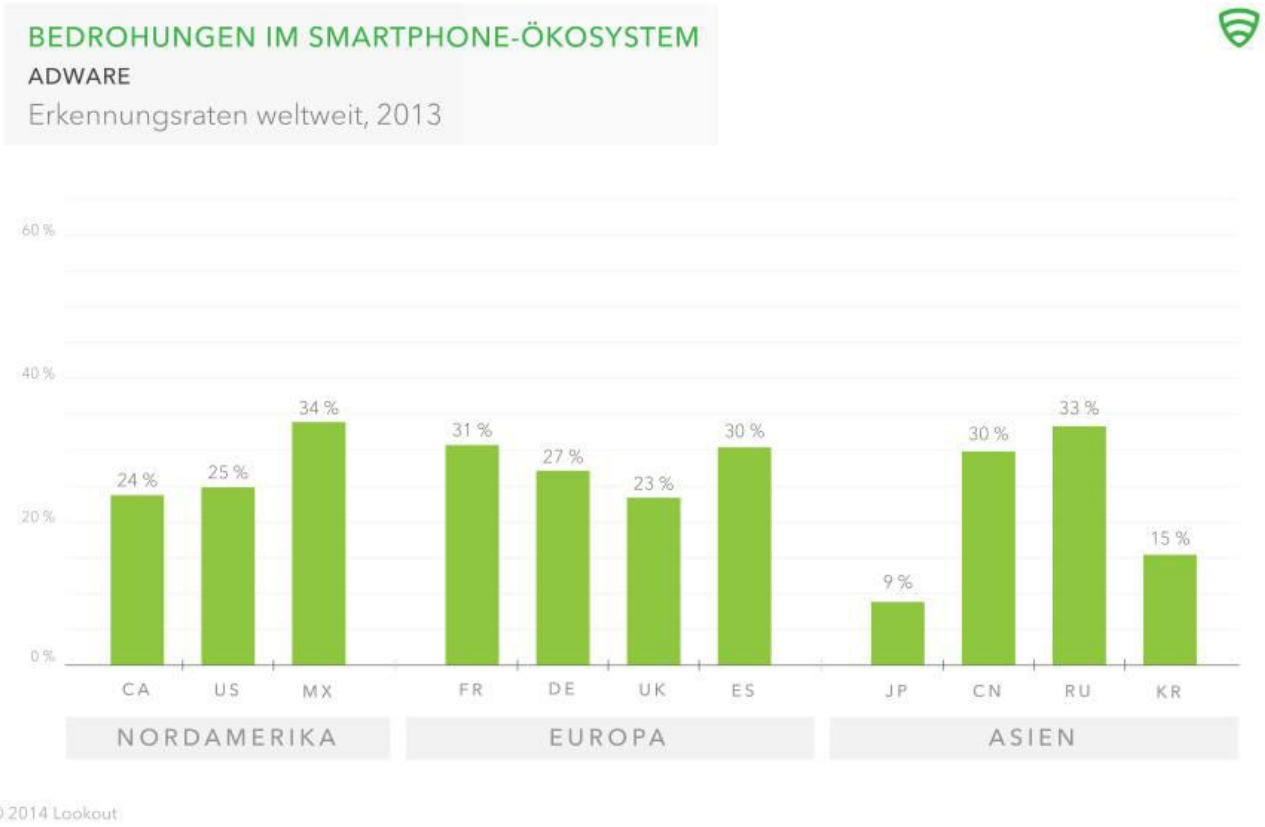
Foto: Lookout



Lookout Security Report 2014

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

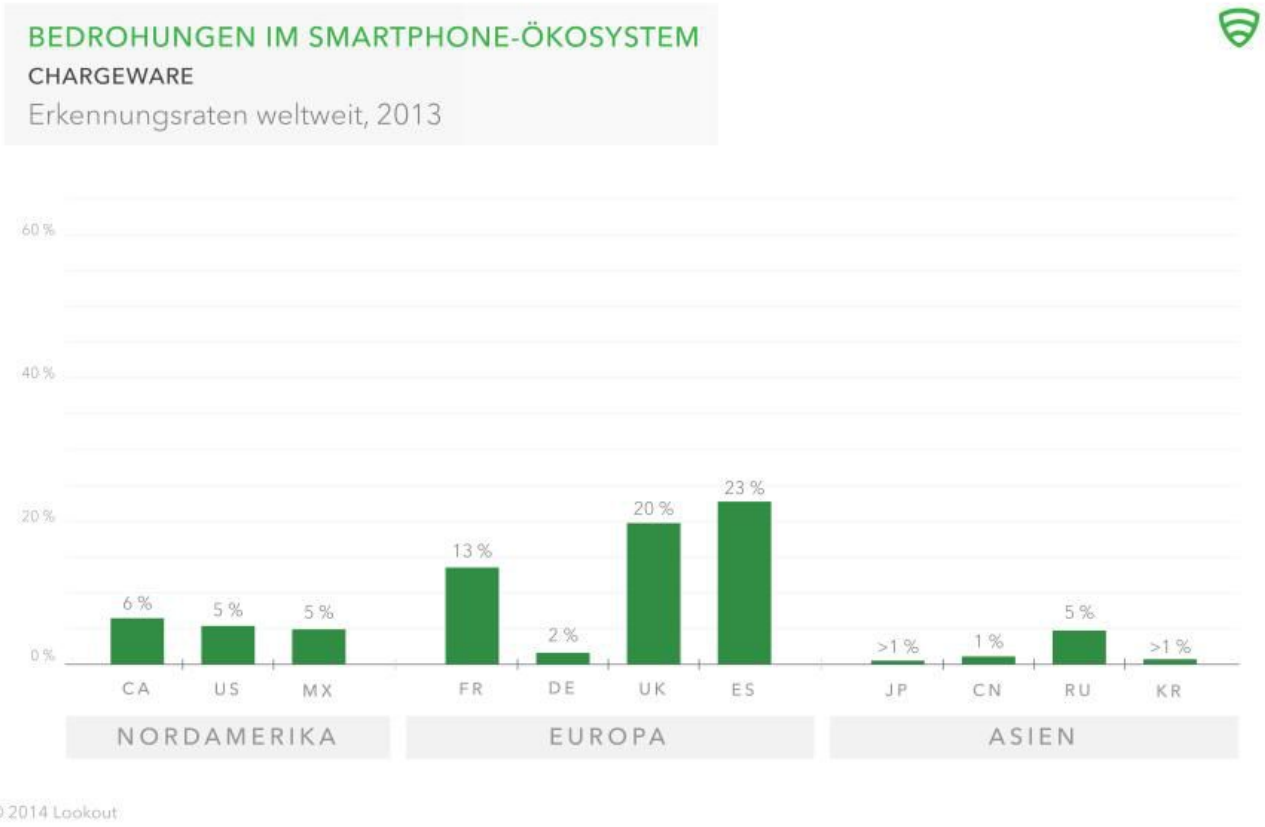
Foto: Lookout



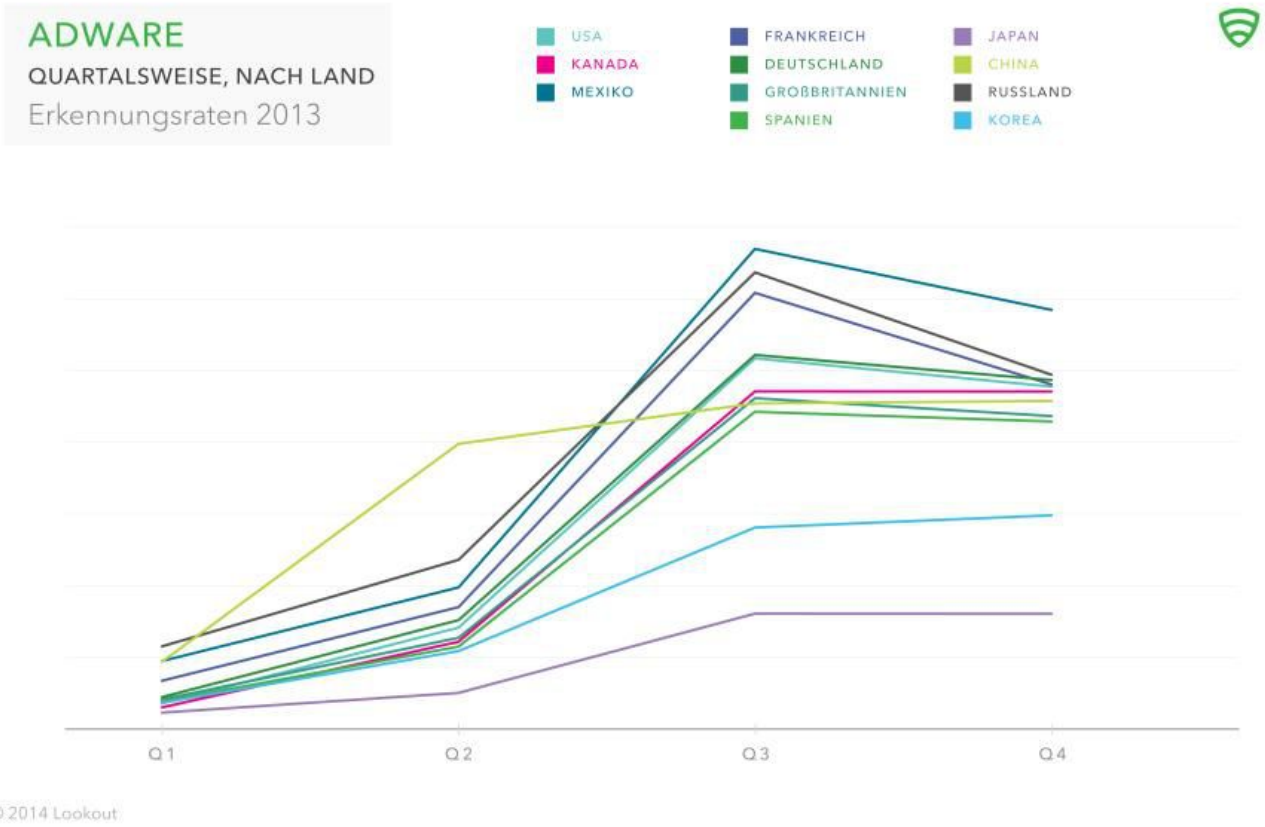
Lookout Security Report 2014

Adware ist weltweit aktiv.

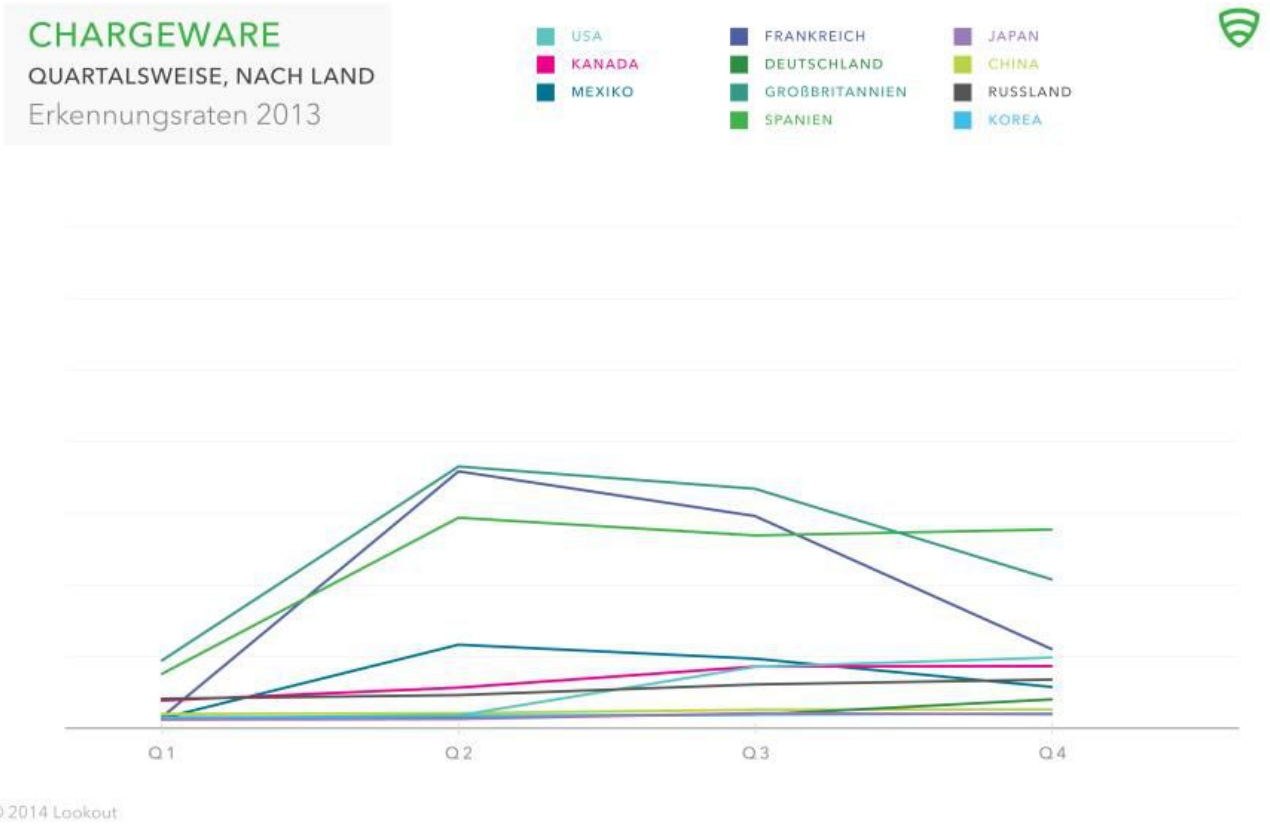
Foto: Lookout



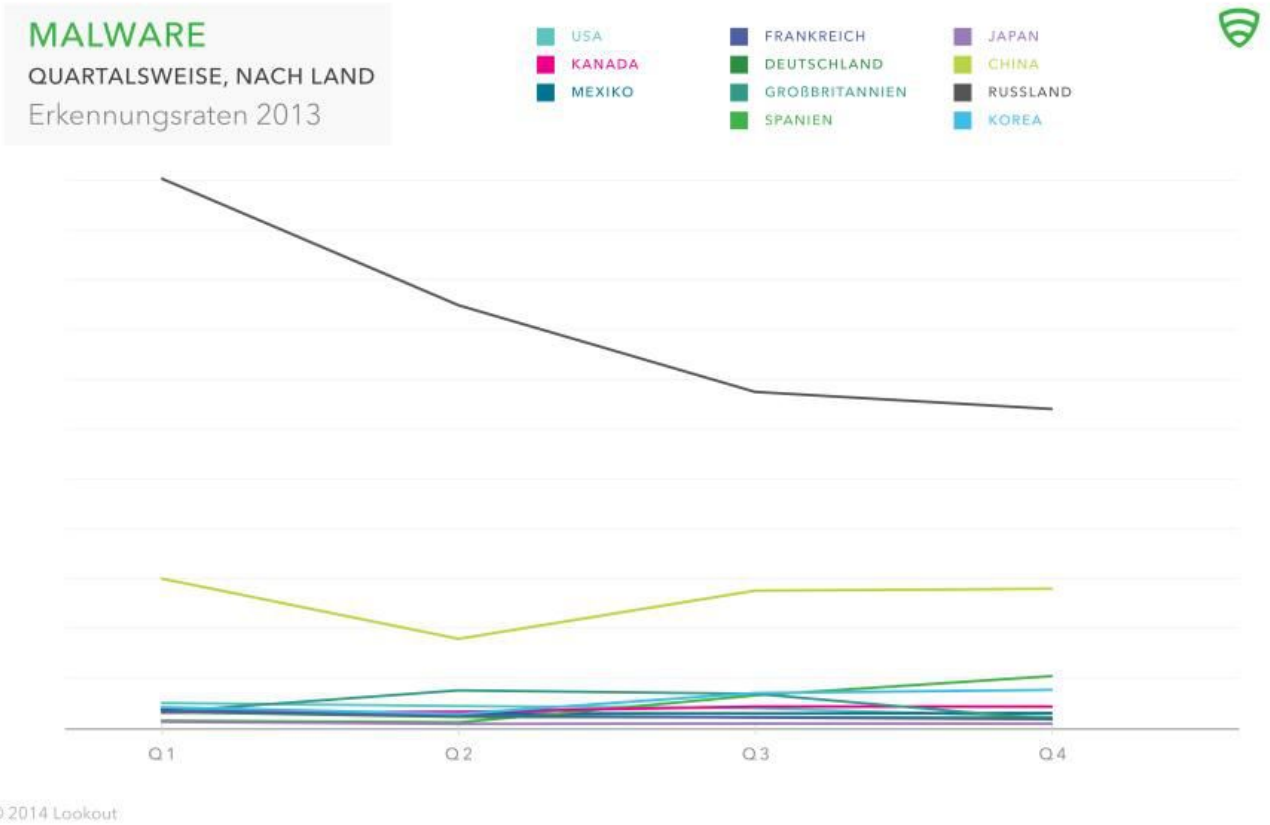
Lookout Security Report 2014
Die Chargeware-Verteilung weltweit.
Foto: Lookout



Lookout Security Report 2014
Adware: Starker Anstieg, langsamer Rückgang.
Foto: Lookout



Lookout Security Report 2014
Chargeware stagniert vor allem in Spanien.
Foto: Lookout



Lookout Security Report 2014
Vor allem Russland leidet unter mobiler Malware.
Foto: Lookout

Lookout Security Report 2014

Die wichtigsten Punkte zusammengefasst.

Foto: Lookout
