



## **Na, herzlichen Glückwunsch: Mobile Malware wird 10 Jahre alt**

***Im Juni 2004 fing alles an: Sophos erzählt die Geschichte der mobilen Schadsoftware und stellt Tipps und Tools für die Sicherheit zur Verfügung***

**Wiesbaden, 4. Juni 2014** – Kurz nach der Jahrtausendwende war die Ära des gewöhnlichen Mobiltelefons beendet. Wer konnte, telefonierte, mailte, spielte und navigierte mit einem Smartphone. Die kleinen Begleiter waren ebenso intelligent wie vielseitig, und so ließ die erste Schadsoftware für Smartphones nicht lange auf sich warten.

Im Juni 2004 läutete Cabir, alias Caribe, das Zeitalter der Mobile Malware ein und attackierte Mobiltelefone mit Symbian Betriebssystem via Bluetooth-Schnittstelle. Die Lösung damals: Bluetooth abschalten oder unsichtbar stellen – so schön einfach war Malware-Schutz im Jahr 2004.

### **Erpressung, Bespitzelung und Rick Astley: Malware ist immer wieder anders**

2005 wurde es das erste Mal gemein: Drever verschaffte sich als erste Malware Zutritt zu Smartphones, indem sie sich als Antivirus-App des russischen Herstellers Dr. Web ausgab. Damit hatte zu dem Zeitpunkt niemand gerechnet.

Das im Jahr 2007 entwickelte FlexSpy existiert bis heute und noch immer wirbt der Hersteller damit, dass betrügerische Liebhaber oder faule Mitarbeiter ganz einfach bespitzelt werden können.

2009 erschien die bisher erste und einzige iOS-Malware, die sich auf jailbreakten iPhones verbreitete. Auf ihnen erschien ein Wallpaper des 80er-Jahre-Stars Rick Astley. Sophos gelang es, den Entwickler bis nach Wollongong, New South Wales (Australien) zurückzuverfolgen. Die Ermittlungsbehörden nahmen sich der Sache jedoch nicht an und erhoben keine Anklage. Der junge Mann blieb seiner Profession treu und ist bis heute ein iPhone-App-Entwickler.

### **Nummernklau und Lösegeld**

Im Jahr 2010 wurde die Malware deutlich frecher. Auf der BlackHat-Konferenz identifizierten Malware-Forscher zahllose Wallpaper-Apps, die auf den Smartphones ihr Unwesen trieben und sich nicht im mindesten an ihre originäre Bestimmung hielten. Path und Hipster stahlen die Kontaktlisten, Flashlight verkaufte den Aufenthaltsort an Werbungtreibende und Snapchat sah die Genehmigung zur Nutzung der Telefonnummer als Einladung, gleich alle Nummern aus dem Telefonbuch an sich zu nehmen.

Seit 2011 sorgt Schadsoftware wie DroidDream, KongFu oder MasterKey für Beschäftigung in kriminellen- und Sicherheitskreisen. Häufig über Spiele aus dem GooglePlay Store eingeschleust, stören, stehlen und betrügen sie auf verschiedene Art und Weise. Das Market Security Tool dämmte diese Welle ein, Vorsicht ist aber immer geboten. Die aktuellsten

Schadsoftwarearten sind noch perfider: Koler, verriegelt das Endgerät und verlangt ein Lösegeld in Höhe von 300 US-Dollar. DownAPK ist eine Windows-basierte Malware, die gefälschte Banking-Apps installiert und Zugangsdaten abgreift.

Im Laufe der Jahre wurden Viren und Trojaner für Symbian, WinCE und sogar für das als relativ sicher geltende iOS entwickelt. Absoluter Liebling der Angreifer ist heute jedoch mit weitem Abstand das Android-Betriebssystem, dem fast alle Angriffe auf Mobilgeräte gelten. Hier verzeichnen die SophosLabs rund 2.000 neue Malware-Samples – pro Tag.

Zum Jahrestag der Mobile Malware hat Sophos eine Historie zusammengestellt, die unter <http://nakedsecurity.sophos.com/2014/06/01/from-cabir-to-koler-10-years-of-mobile-malware/> zu finden ist.

### **Sicherheitstools für private wie geschäftlich genutzte Geräte**

Für den gesicherten Gebrauch von mobilen Geräten im Geschäftsalltag hat Sophos einen Zehn-Punkte-Katalog zusammengestellt: <http://www.sophos.com/de-de/security-news-trends/security-trends/mobile-malware-prevention.aspx>. Mithilfe des neuen Sophos Mobile Control 4.0 können Unternehmen durch AV und Web-Filter nicht nur Sicherheit für alle im Unternehmen befindlichen Mobilgeräte (inklusive BYOD) erzielen, sondern zusätzlich alle Dateien verschlüsseln und damit für Angreifer unbrauchbar machen.

Auch private Anwender bleiben vor den Gefahren der Mobile Malware nicht verschont und tappen oftmals aufgrund der verstärkten Nutzung von Spielen und Social Media in die Falle der Angreifer. Ihnen stellt Sophos ein kostenloses Sicherheits-Tool für Android zur Verfügung, das unter <http://www.sophos.com/de-de/products/free-tools.aspx> zum Download bereit steht.

Bildmaterial:

[Anatomie eines gehackten Smartphones \(Infografik\)](#)  
[Zeitleiste Mobile Malware](#)

### **Über Sophos**

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter [www.sophos.de](http://www.sophos.de).

### **Pressekontakt:**

Sophos  
Jörg Schindler, PR Manager CEEMEA  
[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619  
Thilo Christ, +49-8081-954617  
Christiane Capps, +49-174-3335550  
Ulrike Masztalerz, +49-40-484434  
[sophos@tc-communications.de](mailto:sophos@tc-communications.de)