Überwachungs-Apps im Handy aufspüren und beseitigen

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion–hide“>zurück zum Artikel</p><figure class=„printversionlogo“><svg preserveaspectratio=„xMinYMin“ xmlns=„http://www.w3.org/2000/svg“ viewbox=„0 0 2000 718“ width=„200“ height=„72“><path d=„M440.61,0H603L517.23,350H435.51l48.18-196.5H403L440.61,0ZM625.18,0,539.59,348.21,530.46,385c-14.23,64.76-21,102.25-21,125.7C509.5,618.13,589,705.26,715.68,704H860.33l47.1-191.65H768.65s-18.3-.21-28.68-4.76c-10.95-4.81-17-9.44-23.9-19.2-5.83-8.24-8-14.07-9.64-24-2.17-13,4-33.49,4-33.49l20-81.32H908.11L950.5,177.1H772.92L816.46,0ZM330.49,177C143.78,176.73,0,357.94,0,510c0,107.4,78.64,196.75,205.68,193.89H403.19l47.13-191.66H247.93C206.2,512,193.51,470,193.51,444.51c0-44.7,50.19-94.93,98.51-95.05H412.59L455,177ZM1069,198.18h-28.78L1013.7,296.9h28.78l12.6-47c4.45-16.78,10.27-24.29,18.65-24.29,5.93,0,8.66,4.42,7.45,11.48-.38,2.21-.82,3.76-2,8.39l-13.88,51.46h28.78l12.6-47c2-7.73,3.73-12.59,5.45-15.46,3.39-5.52,8.32-8.83,13.55-8.83,6.1,0,8.8,4.63,7.39,12.81-.34,2-1.41,6.18-2.48,10.38l-13,48.15h28.6l14.13-51.9c2.58-9.94,4.28-16.79,5-21,3-17.45-4.67-28.72-19.67-28.72-11.16,0-20.15,4.64-31.87,17-2.9-12.59-8.24-17-19.76-17-11.16,0-19,4.2-29.58,15.91Zm206,0h-28.78l-1.93,11.26c-6.87-10.82-12.06-14.14-22.87-14.14-23.72,0-45.36,24.52-51.08,57.87-4.85,28.27,4.74,46.6,24.45,46.6,10.64,0,18.4-3.53,28.86-13.69l-3.95,10.82h28.78ZM1223.13,224c9.59,0,14,7.73,11.79,20.76-2.57,15-12.35,26.28-22.64,26.28-9.59,0-14.33-8-12.18-20.54C1202.71,235.28,1212.66,224,1223.13,224Zm155.43-25.84H1350L1347,212.31c-5.9-12.37-12.42-17-23.59-17-23,0-43.18,23-48.75,55.44-2.57,15-1.55,27.39,3,35.56a25.93,25.93,0,0,0,23,13.47c9.07,0,15.22-3.31,25.3-13.25l-4.19,15.24c-4.26,15.68-10.67,22.53-21.66,22.53-8.37,0-12.77-4.86-12.34-13.48h-27.38c-1.08,15.46.21,23.19,5.11,30.26,5.79,8,15.22,11.93,29.35,11.93,19.54,0,32.84-6.4,42.59-20.54,6-8.39,11-21.2,16.77-42.85ZM1325.65,224c9.59,0,14,8,11.71,21.21-2.61,15.24-11.23,25.84-21.18,25.84-9.42,0-14.22-8.61-11.95-21.87C1306.74,234.62,1315.7,224,1325.65,224ZM1482,198.18h-28.78l-1.93,11.26c-6.87-10.82-12.06-14.14-22.87-14.14-23.72,0-45.36,24.52-51.08,57.87-4.85,28.27,4.74,46.6,24.45,46.6,10.64,0,18.4-3.53,28.86-13.69l-3.95,10.82h28.78ZM1430.13,224c9.59,0,14,7.73,11.79,20.76-2.57,15-12.35,26.28-22.64,26.28-9.59,0-14.33-8-12.18-20.54C1409.71,235.28,1419.66,224,1430.13,224Zm132.14,44.84h-37.67l59.73-70.68H1502l-8.47,28h34l-60.26,70.68h86.51Zm61.49-70.68H1595l-26.52,98.72h28.78Zm-.22-58.75c-9.59,0-19.1,9.72-21.11,21.42-2.09,12.15,3.92,21.87,13.52,21.87,9.42,0,18.58-9.72,20.67-21.87C1638.66,148.92,1632.79,139.43,1623.54,139.43Zm46.62,58.75h-28.78l-26.52,98.72h28.78l12-44.61c3-11.27,5.07-16.35,8-20.32s7.55-6.4,11.74-6.4c6.8,0,9.52,5.52,7.78,15.68-.57,3.31-1.2,6-2.78,12.15l-11.82,43.51h28.78l14.95-55.66c1.43-5.3,2.88-11.7,3.6-15.9,3.3-19.22-3.57-30-19.45-30-10.63,0-18.26,3.76-30.94,15.68Zm136.15,28h19.54l7.6-28h-19.54l4.57-17.45c3.23-11.7,7.37-16.57,14-16.57,3.49,0,5.88,1.33,8.76,4.86l8.31-31.14c-6.23-3.31-11.06-4.63-17.35-4.63a34.72,34.72,0,0,0,0-18.39,5.52c-10.59,6.85-17.54,17.89-22.35,35.79l-6.32,23.63h-12l-7.6,28h12l-18.92,70.68h28.61Zm120.69-28h-28.78l-13.88,51.46c-3.64,14.14-8.81,19.88-17.53,19.88-7.67,0-11.28-4.42-10-12.15.23-1.32,1.44-6.4,3.13-12.14l12.6-47H1843.8l-13.33,49.25c-1.21,5.08-2.44,10.16-3,13.69-4.21,24.51,7.5,38.65,32.26,38.65,14.3,0,27.06-4.2,35.36-11.93,7.5-7.07,12.58-17.45,18-37.54Zm-45.59-54.56c-7.5,0-14.72,7.51-16.34,17s3,17,10.69,17c7.32,0,14.54-7.51,16.13-16.79C1893.52,151.35,1888.91,143.62,1881.41,143.62Zm34,0c-7.5,0-14.89,7.51-16.48,16.79-1.63,9.49,3.15,17.22,10.83,17.22,7,0,14.41-7.73,15.92-16.57C1927.32,151.58,1922.57,143.62,1915.42,143.62Zm55.32,54.56H1942l-26.52,

98.72h28.78l11.21-42c2.82-10.38,4.59-14.58,7.4-18.77a18.91,18.91,0,0,1,15.91-8.39c5.06,0,8.32,1.32,12.33,4.42L2000,198.4c-2.41-.22-4.32-.22-5.54-.22-11,0-17.62,3.09-28.29,13.47ZM1063.15,410.7a37.59,37.59,0,0,0,0-22.38-6.85c-24.94,0-47.05,23.19-52.55,55.22-5,28.93,7.08,49.25,28.88,49.25,6.45,0,10.66-1.11,21.31-5.3l8.27-30.92c-7.05,5.52-11.23,7.51-16.64,7.51-9.77,0-14.65-8.17-12.41-21.21,2.57-15,12.28-25.84,22.92-25.84,6.1,0,10,2.43,14.35,8.83Zm53.76-6.85c-27.74,0-51.19,21.87-56.46,52.57-5.3,30.92,9.94,51.9,37.5,51.9,15.52,0,27.46-5.52,38.26-17.67a73.31,73.31,0,0,0,17.09-35.56C1158.68,423.73,1144.65,403.85,1116.91,403.85Zm-4.4,28.72c9.59,0,14,7.73,11.79,20.76-2.57,15-12.35,26.28-22.82,26.28-9.6,0-14.34-8-12.18-20.54C1091.92,443.83,1101.87,432.56,1112.52,432.56Zm94.89-25.84h-28.78l-26.52,98.73h28.78l12.6-47c4.44-16.78,10.27-24.29,18.64-24.29,5.93,0,8.66,4.42,7.45,11.48-.38,2.21-.82,3.76-2,8.39l-13.88,51.46h28.78l12.6-47c2-7.73,3.73-12.58,5.44-15.46,3.39-5.52,8.32-8.83,13.55-8.83,6.1,0,8.8,4.64,7.39,12.81-.34,2-1.41,6.18-2.48,10.38l-13,48.15h28.6l14.13-51.9c2.58-9.94,4.28-16.79,5-21,3-17.45-4.68-28.72-19.67-28.72-11.17,0-20.16,4.64-31.87,17-2.9-12.59-8.25-17-19.76-17-11.17,0-19,4.2-29.59,15.91Zm150.38,0H1329L1287.91,560h28.78l19-71.34c5.33,13.7,13,19.66,24.71,19.66,22.33,0,41.05-22.75,46.92-57,5-29.15-4.25-47.49-24-47.49-10.11,0-17.77,4-29.82,15.24Zm8.13,25.84c9.59,0,14,7.73,11.79,20.76-2.57,15-12.35,26.28-22.64,26.28-9.6,0-14.34-8-12.18-20.54C1345.5,443.83,1355.46,432.56,1365.92,432.56Zm149.52-25.84h-28.78l-13.88,51.46c-3.85,14.36-8.81,19.88-17.71,19.88-7.67,0-10.93-4.42-9.49-12.81.34-2,1.52-6.85,2.67-11.48l12.77-47h-28.78L1418.91,456c-1.22,5.08-2.44,10.15-3,13.69-4.2,24.52,7.51,38.65,32.27,38.65,14.3,0,27.06-4.2,35.19-11.93,7.67-7.07,12.58-17.45,18.12-37.54Zm44.7,28.05h15.35l7.6-28.05h-15.35l8.38-31.58h-28.61L1539,406.72h-12.21l-7.6,28.05h12.39l-19.1,70.68h28.78Zm101.1,28.72c.85-4,1.63-7.51,1.9-9.06,5.41-31.58-6.32-50.58-31.27-50.58-14.13,0-26.59,5.52-36.64,16.34-9.42,10.16-16.49,25-19.06,40-5.15,30,6.92,48.14,32.21,48.14,13.43,0,25.21-4.64,34.4-13.47,5.7-5.74,9.43-11.27,14.64-22.31H1626c-2.22,6.85-6.45,10.16-12.73,10.16a11.45,11.45,0,0,1-9.94-5.08c-1.56-3.1-1.65-6.63-.37-14.14Zm-52.82-20.54c3.48-10.16,9.24-15.24,17.09-15.24,7.67,0,11.3,5.3,10.12,15.24Zm106.31-36.22H1686l-26.52,98.73h28.78l11.21-42c2.82-10.38,4.59-14.58,7.4-18.78a18.91,18.91,0,0,1,15.91-8.39c5.06,0,8.32,1.32,12.33,4.42l8.93-33.79c-2.41-.23-4.32-.23-5.54-.23-11,0-17.62,3.09-28.29,13.47Zm-715,237.73h15.35l7.6-28.05h-15.35l8.38-31.58H987.13l-8.55,31.58H966.37l-7.6,28.05h12.39l-19.09,70.68h28.78Zm99.95,28.72c.85-4,1.64-7.51,1.9-9.06,5.41-31.58-6.32-50.58-31.27-50.58-14.13,0-26.59,5.52-36.64,16.34-9.41,10.16-16.48,25-19.06,40-5.15,30,6.92,48.14,32.21,48.14,13.44,0,25.21-4.63,34.4-13.47,5.7-5.74,9.43-11.27,14.64-22.31h-31.4c-2.22,6.84-6.45,10.16-12.73,10.16a11.45,11.45,0,0,1-9.94-5.08c-1.56-3.1-1.65-6.63-.37-14.14Zm-52.82-20.54c3.49-10.16,9.24-15.24,17.09-15.24,7.67,0,11.3,5.3,10.12,15.24Zm137.93-32.25a37.59,37.59,0,0,0,0-22.37-6.85c-24.94,0-47.06,23.19-52.55,55.22-5,28.93,7.08,49.25,28.88,49.25,6.45,0,10.66-1.1,21.31-5.3l8.27-30.92c-7.05,5.52-11.23,7.51-16.64,7.51-9.77,0-14.65-8.18-12.41-21.21,2.57-15,12.28-25.84,22.92-25.84,6.1,0,10,2.43,14.36,8.83Zm60.73-66.26h-28.78l-43.3,161h28.78l12.56-46.82c2.42-9.06,4-13,6.16-16.57,3.14-5.08,8-7.95,13-7.95,7.15,0,9.63,4.86,7.78,15.68-.65,3.76-1.31,6.63-4,16.12l-10.61,39.54H1256l13.52-50.36c1.55-6,3.32-13.25,3.89-16.56,3.83-22.31-2.95-34.68-19.34-34.68-9.25,0-16.4,3.1-27.65,11.71ZM1328,616.4h-28.78l-26.52,98.73h28.78l12-44.61c3-11.27,5.07-16.34,8-20.32s7.55-6.4,11.74-6.4c6.8,0,9.52,5.52,7.78,15.68-.57,3.31-1.2,6-2.78,12.15l-11.82,43.51h28.79l14.95-55.66c1.43-5.3,2.88-11.7,3.6-15.9,3.3-19.22-3.57-30-19.44-30-10.64,0-18.26,3.76-30.95,15.68Zm100.48,0h-28.78l-26.52,98.73H1402Zm-.22-58.75c-9.59,0-19.1,9.72-21.11,21.43-2.08,12.15,3.92,21.86,13.52,21.86,9.42,0,18.59-9.71,20.67-21.86C1443.42,567.15,1437.54,557.66,1428.3,557.66Zm63.76-3.53h-28.78l-43.3,161h28.78l12.48-46.38a270.82,270.82,0,0,0,0-13.55,29.82,29.82,0,0,0-8.67-16.56h35.06l-27.25-53.67L1533,616.4h-36.28l-31,35.34Z“/></svg></figure><h2 class=„printversionuntertitel“/> Haben Sie den Verdacht, dass Ihr Smartphone von einer Spionage-

Software infiziert wurde? Unsere Tipps helfen Ihnen, Überwachungs-Apps zu erkennen und zu entfernen. Befürchten Sie, dass Ihr Smartphone infiziert ist? Wir helfen Ihnen, etwaige Schädlinge aufzuspüren und zu beseitigen. Zunächst einmal sollten Sie prüfen, ob Ihr Handy gerootet ist, denn einem gerooteten Gerät können Sie nicht mehr vertrauen – auch dann nicht, wenn Sie den Root aus gutem Grund irgendwann selbst durchgeführt haben. Auf gerooteten Geräten können Angreifer ein Spionage-Tool so gut verstecken, dass Sie es mit einfachen Handgriffen nicht entdecken. <h3 class=„subheading“ id=„nav_root_entdecken_1“>Root entdecken</h3> Durchsuchen Sie Ihr Gerät unter „Einstellungen/Apps“ deshalb nach Tools, die klassischerweise zum Rooten verwendet werden. Dazu zählen unter anderem SuperSu, BusyBox oder KingRoot. Außerdem überprüfen Sie mit der App RootChecker direkt, ob Ihr Handy gerootet ist. Bei gerooteten Geräten haben Sie zwei Möglichkeiten: Entweder, Sie setzen Ihr Smartphone wieder auf die Werkseinstellung zurück, oder Sie reparieren das gerootete System, was jedoch mit einem hohen Aufwand verbunden ist. Dabei sollten Sie jemanden hinzuziehen, der mit gerooteten Systemen Erfahrung hat. Einen Einblick in mögliche Vorgehensweisen gibt der c't-Artikel Android-Trojaner seziert [1].
 <h3 class=„subheading“ id=„nav_android_handys2“>Android-Handys schützen – Checkliste</h3> Wir gehen im Folgenden also davon aus, dass Ihr Android-Handy nicht gerootet ist. <figure class=„rteinlinebild akwa-inline-img akwa-inline-img col-lg-12 col-md-12 col-sm-12 col-xs-12 c2“><figcaption class=„rteinlinebild_source akwa-caption“>Diese Checkliste hilft Ihnen dabei, mögliche Spionage-Angriffe auf Ihrem Android-Smartphone zu entdecken.</figcaption></figure><h3 class=„subheading“ id=„nav_unbekann3“>Unbekannte Geräteadministratoren deaktivieren</h3> Geräteadministrator-Apps bekommen unter Android besonders viele Zugriffsrechte, deswegen sollten Sie diese Apps überprüften. In den Einstellungen unter „Sicherheit & Standort / Apps zur Geräteverwaltung“ (Achtung: in einige Smartphones heißen die Menüs für die Geräteadministratoren leicht abweichend) sehen Sie im Normalfall nur „Mein Gerät finden“ und „Google Pay“, möglicherweise auch das Mobile Device Management Ihrer Firma oder eine Mail-App. Sollten Sie hier jedoch andere Apps finden, könnte dies auf eine Infektion Ihres Gerätes hindeuten. Deaktivieren Sie in diesem Fall diese unbekannten Geräteadministratoren und deinstallieren Sie die dazugehörige App. Welche das ist, können Sie leider nicht immer eindeutig feststellen, denn eine App darf ihren Eintrag in der Geräteadministratoren-Liste beliebig benennen. <h3 class=„subheading“ id=„nav_das4“>Das Handy mit Play Protect scannen</h3> Sie sollten sich auch die Android-Sicherheits-Features genauer ansehen. Play Protect prüft alle Apps auf dem Smartphone und funktioniert auch unter älteren Android-Versionen. Sie finden Play Protect am Einfachsten in der App Play Store im Hamburger-Menü (die drei horizontalen Linien oben links). Die Option „Gerät auf Sicherheitsbedrohung prüfen“ muss aktiviert sein. Auch die „Erkennung schädlicher Apps verbessern“ sollte eingeschaltet sein. Hier sollten Sie unbedingt prüfen, wie lange der letzte Scan von Play Protect her ist: Ist er länger als ein paar Tage her, kann das auf einen Spionage-Angriff hindeuten. Führen Sie nun einen Scan aller Apps durch; hierbei muss der Internet-Zugang aktiviert sein. Play Protect erkennt beispielsweise die Spionage-Tools mSpy und FlexiSpy, die dann komplett deinstalliert werden

können. <figure class=„rteinlinebild akwa-inline-img akwa-inline-img col-lg-12 col-md-12 col-sm-12 col-xs-12 c3“><figcaption class=„rteinlinebild_source akwa-caption“>Androids eingebauter Virenscanner darf nicht deaktiviert sein (links), die letzte Überprüfung sollte nicht zu weit zurückliegen. Der Scanner erkennt nämlich durchaus gängige Spionage-Apps (rechts), auch wenn sie sich als „Update Service“ verstecken.</figcaption></figure><h3 class=„subheading“ id=„nav_spionage5“>Spionage-Software aus Fremdquellen aufspüren</h3> Angreifer müssen die Spionage-Tools im Allgemeinen manuell auf Ihrem Gerät installieren, denn Googles Virenscanner würde sie entdecken, weshalb die Apps im Play Store im Großen und Ganzen schädlingsfrei sind. Zur manuellen Installation muss der Angreifer zuerst die Sperre abschalten, die Ihr Gerät vor Apps aus Fremdquellen schützt. Diese Sperre finden Sie bei älteren Geräten in den Einstellungen unter „Sicherheit/Unbekannte Herkunft“. Bei neueren Smartphones gibt es keine zentrale Sperre mehr, sondern es ist einzelnen Apps wie FileManager, Dropbox oder Browsern erlaubt, aus Fremdquellen zu installieren. In den Einstellungen unter „Apps & Benachrichtigungen/Spezieller App-Zugriff/Unbekannt“ finden Sie eine Liste der Apps: Es sollte bei allen App „nicht zulässig“ stehen. Wenn Sie in der Liste eine App finden, bei der Fremdquellen zulässig sind, ist dies ein Indiz für einen Spionage-Angriff. In diesem Fall gucken Sie sich die Quelle der App genauer an. Neuere Android-Versionen zeigen dies in den Einstellungen unter „App-Benachrichtungen“ in der App-Detailansicht an. Die Quellen „Von Google Play Store geladene App“ oder „Von Galaxy Apps geladene App“ sind meist unbedenklich, eine „vom Paket-Installer geladene App“ ist dagegen sehr verdächtig. Diese App sollten Sie löschen. <h3 class=„subheading“ id=„nav_liste6“>Liste aller installierten Apps prüfen</h3> Wenn Sie ganz sichergehen wollen, dass Ihr Smartphone von keiner Spionage-Software befallen ist, sollten Sie alle installierten Apps kontrollieren. Öffnen Sie dazu in den Einstellungen unter „App-Berechtigungen“ die Liste aller Apps und prüfen Sie, welche Apps auf persönliche Daten zugreifen dürfen. Unter den App-Berechtigungen sollten neben Kontakte, SMS, Kamera und Standort keine Apps auftauchen, die Sie nicht selbst installiert haben. Unbekannte Apps sollten Sie deshalb deinstallieren. Notieren Sie zuvor stets den Paketnamen, um Ihre Arbeiten nachvollziehen zu können. Nach diesem Prinzip können Sie die Liste aller installierten Apps durchgehen, um verdächtige oder unbekannte Apps aufzuspüren. <h3 class=„subheading“ id=„nav_passwörter7“>Passwörter ändern</h3> Sollten Sie von einer Spionage-Software befallen sein, empfiehlt es sich, nach der Säuberung des Geräts auch die Passwörter aller Dienste zu ändern. Unter https://myaccount.google.com/device-activity [2] können Sie einsehen, welche Geräte Ihren Google-Account nutzen und wann zuletzt darauf zugegriffen wurde. Entfernen Sie verdächtige Geräte aus dieser Liste und ändern Sie Ihr Passwort. Gleiches gilt für andere Cloud-Dienste und Banking-Apps, die Sie nutzen. Besonders aufpassen müssen Sie bei Messenger-Diensten: Einige, darunter WhatsApp, Signal und Threema, können Sie auch über Ihren Browser nutzen. Auch wenn Sie selbst das nie genutzt haben, könnte ein Angreifer diese Option eingeschaltet haben. Dieser Browser-Zugriff kann auch nach Säuberung des Handys aktiv bleiben, weshalb Sie ihn explizit entfernen müssen. Sie finden ihn in den Apps unter Menüpunkten wie „WhatsApp

Web“ oder „Threema Web“ – löschen Sie auch hier die Zugriffe. Sofern Sie hier einen Zugriff sehen, ohne dass Sie selbst ihn eingerichtet haben, ist das ein ganz klarer Hinweis auf einen Angriff. <h3 class=„subheading“ id=„nav_auf8“>Auf Werkseinstellungen zurücksetzen</h3> Wenn nichts mehr hilft oder Sie noch Zweifel an der Sicherheit Ihres Smartphones haben, hilft nur noch das Zurücksetzen auf die Werkseinstellung. Zuvor sollten Sie Ihre persönlichen Daten (Fotos, Adressen und Termine etc.) sichern und die wichtigen Elemente Ihrer Konfiguration notieren. In den Einstellungen können Sie Ihr Handy unter „Systeme/Optionen zurücksetzen/Alle Daten löschen“ resetten, auf einigen Systemen finden Sie den Reset unter „Allgemeine Verwaltung/Zurücksetzen/Auf Werkeinstellungen zurücksetzen“ oder ähnlich genannt. Anschließend müssen Sie Ihr Handy neu einrichten. Wichtig: Installieren Sie es als neues Gerät ein und nicht etwas als Backup, ansonsten könnte es sein, dass Ihr Gerät aus dem Backup erneut infiziert wird. Und: Ändern Sie Ihre Passwörter erst nach dem Reset, damit ein möglicherweise installierter Keylogger nicht die neuen Passwörter erfährt. <h3 class=„subheading“ id=„nav_ios_geräte9“>iOS-Geräte schützen – Checkliste</h3> <figure class=„rteinlinebild akwa-inline-img akwa-inline-img col-lg-12 col-md-12 col-sm-12 col-xs-12 c4“><figcaption class=„rteinlinebild_source akwa-caption“>Diese Checkliste hilft Ihnen Spionage-Angriffe bei Geräten mit iOS zu enttarnen.</figcaption></figure> iPhones lassen sich zwar deutlich schwieriger ausspionieren als Android-Geräte, doch sollte man bei Verdacht dennoch einem möglichen Spionage-Angriff nachgehen. Im ersten Schritt prüfen Sie dazu, ob Ihr iPhone per Jailbreak manipuliert wurde, denn ein Jailbreak setzt wichtige Sicherheitsmechanismen außer Kraft. Wenn Ihr iPhone die aktuelle iOS-Version nutzt, brauchen Sie keinen Angriff per Jailbreak befürchten – derzeit gibt es keinen öffentlich verfügbaren Jailbreak ab iOS 11.4. Welche iOS-Version gerade aktuell ist, dokumentiert Apple auf den Seiten zu Sicherheitsupdates. <figure class=„rteinlinebild akwa-inline-img rtepos_right col-lg-6 col-md-6 col-sm-6 col-xs-12 akwa-inline–right“><figcaption class=„rteinlinebild_source akwa-caption“>Apps wie die der Barclaycard verweigern den Dienst, wenn sie einen Jailbreak erkennen.</figcaption></figure> Nutzen Sie ein iPhone mit einer älteren iOS-Version, sollten Sie die typischen Anzeichen für einen Jailbreak überprüfen – beispielsweise mit den Apps Cydia, Electra und Pangu. Einige Anwendungen wie Online-Banking-Apps testen das Gerät beim Start und verweigern den Dienst im Falle eines Jailbreak. Ein weiteres Indiz für einen Angriff ist der Akkuverbrauch, denn eine dauerhaft aktive Spionage-App frisst Strom und auch Datenvolumen. Insgesamt sind iPhones relativ sicher vor Spionage-Überfällen per Jailbreak. Der zentrale Schlüssel zu den Daten ist hier nicht das Handy selbst, sondern der Apple-Account des Besitzers. Aus diesem Grund holt kommerzielle Spionage-Software sich die Daten aus der iCloud. <h3 class=„subheading“ id=„nav_bekannte10“>Bekannte Spyware erkennen</h3> Wenn Sie unsere Tipps beherzigen und die Checklisten zum Prüfen von Android- und iOS-Geräten durchgegangen sind, sollte Ihr Smartphone vor den meisten Spionage-Apps sicher sein. Zusätzliche Hinweise auf einen Spionageangriff mit bereits bekannter Spyware finden Sie die

folgende Tabelle. <section class=„rtetable-wrapper table-responsive akwa-inline-table“><table class=„rtetable table akwa-inline-tabletable“><tbody><tr><td class=„heise-table-subtitle c5“>Spyware</td> <td class=„heise-table-subtitle c5“>Hinweise auf eine Infektion</td> </tr><tr><td class=„heise-table-emph c5“>mSpy</td> <td class=„heise-table-emph c5“>Wählen von #000* öffnet das User-Interface von mSpy</td> </tr><tr><td class=„c5“>FlexiSpy</td> <td class=„c5“>FSXGAD_\<versionsnummer>.apk auf der SD-Karte; in /data/app/ liegt com.mobilefonex.mobilebackup-1.apk; http://djp.cc bleibt oft im Browserverlauf zurück; Wählen von *#900900900 öffnet das User-Interface von FlexiSpy</td> </tr><tr><td class=„heise-table-emph c5“>PhoneSheriff</td> <td class=„heise-table-emph c5“>hinterlässt alle abgefangenen Daten und EInstellungen unter /data/com.studio.sp2/</td> </tr><tr><td class=„c5“>MobileSpy</td> <td class=„c5“>Wählen von #123456789* öffnet das User-Interface von MobileSpy</td> </tr><tr><td class=„heise-table-emph c5“>OmniRAT</td> <td class=„heise-table-emph c5“>erzeugt Geräte-Administrator com.android.engine.Deamon</td> </tr></tbody></table></section> ()
 <hr/> URL dieses Artikels:
<small><code>http://www.heise.de/-4156760</code></small> Links in diesem Artikel:
<small><code>[1] https://heise.de/-4028629</code></small>
<small><code>[2] https://myaccount.google.com/device-activity</code></small>
<small><code>[3] mailto:jow@ct.de</code></small>
 Copyright © 2018 Heise Medien </html>