SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy

Februar 2016

SWITCH

I. ICSI Haystack sucht Nadeln im androiden Heuhaufen – und Betatester für Feldstudie

Bereits mehrfach hatten wir an dieser Stelle über immer wieder aufklaffende Sicherheitslücken in Android-Betriebssystem-Versionen und -Apps berichtet. Nun hat sich eines der führenden Forschungszentren für Informatik, das an der Universtity of California in Berkeley domizilierte International Computer Science Institute ICSI, der Problematik angenommen. Ein sechsköpfiges Forscherteam hat mit Haystack eine App entwickelt, die Android-Device-Besitzern helfen soll, herauszufinden, welche Apps undichte Stellen aufweisen und persönliche Informationen preisgeben, wohin diese fliessen, welche Protokolle sie verwenden und welche Datensammler hinter diesen Apps stehen. Die Betaversion von Haystack steht auf Google Play zum Download bereit. Nach Auswertung der Daten der ersten 200 Betatester haben die Forscher erste Ergebnisse in ihrem Blog publiziert. Danach fanden Sie 423 Apps, die persönliche und/oder sicherheitsrelevante Informationen wie IMEI-Code, IMSI-Nummer, Seriennummer oder MAC-Adresse des Android-Smartphones oder -Tablets verrieten.

Zur App-Diagnose muss Haystack ziemlich tief in die Kommunikation auf dem Device eingreifen und u.a. ein eigenes Root-Zertifikat installieren. Warum das so ist, wo der Nutzen liegt und wie das funktioniert, erklären die Stecknadel-im-Heuhaufen-Sucher auf ihrer Microsite haystack.mobi. Schliesslich hoffen sie darauf, dass Haystack von möglichst vielen Usern genutzt wird, um ein umfassendes, vor allem aber valides und repräsentatives Bild über die Sicherheitslage im Android-Ökosystem zu bekommen.

Nachzulesen unter:

https://haystack.mobi
https://haystack.mobi/wordpress/index.php/2015/12/11/haystack-preliminary-results

II. Comeback mit Blackout: Makro-Trojaner sind wieder da – und offenbar für den weihnachtlichen Stromausfall in der Westukraine verantwortlich

Eigentlich galten Makro-Trojaner, also Malware, die sich in Form von Makros in Micosoft-Office-Dokumenten versteckt, um bei Ausführung schwere Infektionen auf dem betroffenen Rechner zu verursachen, als nahezu ausgerottet. Entscheidend dazu beigetragen hat sicher Microsofts Entscheidung, Makros in Office-Software werksseitig zu deaktivieren. Umso mehr überraschte der Softwareriese aus Redmond zum Jahreswechsel mit der Warnung, dass Cyberkriminelle via Mail wieder verstärkt Makro-Trojaner verbreiten. Dazu verschicken sie täuschend echt aussehende, fingierte und zur Zahlung bereits überfällige Rechnungen einer gefakten Bestellung in einem real existierenden Online-Shop. Darin fordern sie den Empfänger auf, endlich die als Office-Dokument angehängte Rechnung zu bezahlen und drohen mit Konsequenzen. Öffnet der besorgte Mailempfänger dieses Dokument z. B. in der Annahme, jemand habe unbefugt in seinem Namen bestellt, wird er aufgefordert, Makros zu aktivieren. Tut er das, startet unbemerkt der Schadcode-Download und der Rechner wird als Teil eines Bot-Netzes durch die Cyberkriminellen fernsteuerbar. Info-Stealer wie Dridex, Banking-Trojaner wie Zbot oder Ransomware wie Cryptowall finden so den Weg auf die Rechner unbescholtener User – allesamt sehr ernsthafte Infektionen mit weitreichenden Folgen.

So hat jüngst Eugene Bryksin vom Computer Emergency Response Team der Ukraine (CERT-UA) bestätigt, dass der Blackout, der am 23. Dezember 2015 die Stromversorgung einer knappen dreiviertel Million Menschen in der Westukraine lahmgelegt hatte, via Makro-Trojaner, der in einem Word-Dokument versteckt war, verursacht worden war. Der Guardian berichtet zudem, dass mit der gleichen Malware ein Cyberangriff auf eines der grössten ukrainischen Medienhäuser ausgeführt worden sei und der ukrainische Geheimdienst beide Angriffe mit einer Hackergruppe in Verbindung bringe, die von der russischen Regierung zumindest unterstützt würde. Als Urheber des BlackEnergy genannten Trojaners nennen Forscher bei Symantec eine Hackergruppe namens «Sandworm», die sie für weitere Angriffe auf ukrainische Organisationen, aber auch auf die NATO, verschiedene westeuropäische Staaten und Energiefirmen verantwortlich machen. Ausserdem verdichten sich die Hinweise, dass physische Infrastrukturen, wie z. B. die Energie- oder Wasserversorgung, zunehmend ins Visier von Cyberkriminellen geraten. So warnte etwa der ehemalige NSA-Chef Michael Hayden oder der ehemalige Nationale Sicherheitsberater Richard Clarke davor, dass so genannte «Smart Bombs» auch in den USA wichtige physische Infrastrukturen beschädigen könnten und ein Angriff wie der auf das ukrainische Stromnetz auch in den USA möglich sei. Beide müssten es tatsächlich wissen. Denn schliesslich sind auch die USA in dieser Art Cyberwar aktiv und haben mit Stuxnet einen eigenen Malware-Wurm von der Angel gelassen, um die Zentrifugen der iranischen Urananreicherungsanlage Natanz so zu manipulieren, dass diese massenhaft ausfielen.

Grossflächige, lang anhaltende Blackouts ganzer Versorgungsgebiete haben jedoch eine nochmals andere Qualität, wie sie nüchtern im Projektbericht «Gefährdung und Verletzbarkeit moderner Gesellschaften» des Büros für Technikfolgenabschätzung beim Deutschen Bundestag und fiktional in Marc Elsbergs Thriller «Blackout – morgen ist es zu spät» beschrieben ist. Mit der technischen Seite des hochkomplexen Themas setzt sich der Vortrag von Mathias Dalheimer auf der 32C3 auseinander (Video dazu siehe Links).

Nachzulesen unter:

http://www.heise.de/security/meldung/Wieder-in-Mode-Trojaner-in-Office-Macros-2512377.html
https://blogs.technet.microsoft.com/mmpc/2014/12/30/before-you-enable-those-macros
https://blogs.technet.microsoft.com/mmpc/2015/04/27/social-engineering-tricks-open-the-door-to-macro-malware-attacks-how-can-we-close-it
http://www.heise.de/security/artikel/Analysiert-Das-Comeback-der-Makro-Malware-2573181.html
http://www.zeit.de/digital/internet/2016-01/stromausfall-hacker-ukraine-blackenergy
http://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company
http://www.golem.de/news/ex-nsa-chef-warnt-vor-blackout-der-himmel-verdunkelt-sich-1601-118511.html
http://www.tab-beim-bundestag.de/de/untersuchungen/u137.html
https://media.ccc.de/v/32c3-7323-wie_man_einen_blackout_verursacht#video&t=10

III. Is it really smart? Viele Smart Home-Lösungen offerieren Sicherheitslücken in der Grösse von Garagentoren

Glaubt man den Hochglanzprospekten für smarte Haushalts- und Unterhaltungselektronik-Geräte oder Smart Home-Automation, dann wird schon morgen der Smart TV dem Smart Fridge mitteilen, dass dieser anlässlich des für Samstagabend terminierten Fussball-WM-Finalspiels besser Bier und Tiefkühlpizza be- und kühlstellen solle. Zugleich bekommt die smarte Heizungssteuerung die Anweisung, die Temperatur um 3 Grad herunterzuregeln, weil viele Leute zu erwarten seien. Und für den Fall der Fälle hat der Hausbesitzer schon heute die Möglichkeit, Temperatur, Beleuchtung, Zutrittsberechtigungen, Abschattung oder Lichteinlass via Smartphone ferngesteuert zu regeln und das smarte Zuhause dank Überwachungskameras immer im Blick zu haben, auch wenn er oder sie weit weg davon sein sollte.

Erkauft wird dieser Komfort und das vermeintliche Sicherheitsgefühl mit riesigen Sicherheitslücken in vielen der aktuell angebotenen und installierten Smart Home Lösungen. Das führt zur völlig paradoxen Situation, dass viele Smart Home-Lösungen, die die eigenen vier Wände sicherer machen sollen, virtuell versierten Einbrechern Türen und Tore öffnet. Hauptproblem: Weil alle Geräte im Internet of Things permanent online sind, sind sie von Hackern und spezialisierten Suchmaschinen, wie z. B. SHODAN leicht zu finden.

Leicht zu hacken sind die meisten dieser Geräte ebenfalls – und das ist nun wirklich ein echtes vermeidbares Ärgernis – weil ihre Hersteller an entsprechender Verschlüsselung sparen, und wenn sie denn eine vorsehen, die Geräte mit Passwörtern wie «000», «12345» oder «abc» ausliefern, die von ihren neuen Besitzern nicht geändert werden. So haben Sicherheitsexperten herausgefunden, dass Samsungs

sprachgesteuerte Smart-TVs Daten zur Stimmerkennung und Textinformationen unverschlüsselt durchs Netz schicken – ein gefundenes Einfallstor für Hacker ins gesamte WLAN, in dem der TV eingebunden ist. Noch drastischer sieht die Sicherheitslage bei Überwachungskameras aus: Preisdruck und mangelndes Sicherheitsbewusstein oder –Knowhow führen dazu, dass die meisten dieser Kameras ohne jeden Passwortschutz ausgeliefert werden und das, was sie sehen, unverschlüsselt übers Netz senden – Bilder von schlafenden Babies ebenso wie den Blick ins Wohnzimmer oder auf den PC-Monitor im Home Office.

Völlig aberwitzig wird die Situation aber dann, wenn ZigBee-Funknetze in der für Smart Homes entwickelten Version «Home Automation 2.1» eingesetzt werden, um damit Fenster, Türen und Tore zu steuern. Sicherheitsforscher haben darin nämlich einen eklatanten Konstruktionsfehler entdeckt. Zwar kommunizieren Geräte im ZigBee Home Automation 2.1 Netzwerk grundsätzlich verschlüsselt, doch verlangt das ZigBee-Konsortium, dass alle Geräte ein und dasselbe Schlüsselpaar kennen und akzeptieren müssen. Dieses Schlüsselpaar ist aber öffentlich bekannt! Hackern wird es damit leicht gemacht, die Steuerung zu übernehmen und so umzuprogrammieren, dass die vorgesehene Kontroll-App diese Manipulation weder bemerkt, geschweige denn melden würde. Damit können Einbrecher Türen, Tore und Fenster nach Belieben öffnen und haben quasi einen virtuellen Schlüssel unter der Fussmatte.

Nachzulesen unter:

http://www.sueddeutsche.de/digital/ueberwachung-wenn-die-webcam-zum-spion-im-wohnzimmer-wird-1.2833317
http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html
http://resources.infosecinstitute.com/how-hackers-violate-privacy-and-security-of-the-smart-home
http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies
http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html
http://futurezone.at/digital-life/unsicheres-smart-home-nutzer-koennen-nichts-tun/147.484.799
http://www.heise.de/security/meldung/Deepsec-ZigBee-macht-Smart-Home-zum-offenen-Haus-3010287.html

IV. Wenn Mad Men zu Bad Boys werden – Malvertising (Malicious Advertising) erschwert zunehmend das Malware Monitoring

Werbung wurde schon in jenen 1960er Jahren kontrovers diskutiert, in denen die erfolgreiche TV-Serie Mad Men spielt und das Leben und Arbeiten in der Werbeszene von New Yorks Madison Avenue portraitiert. Doch auch dem Ober-Ehrgeizling Don Draper wäre es nicht im Traum eingefallen, dass 50 Jahre später der Dreh- und Angelpunkt der Werbewelt nicht mehr im Big Apple liegt, sondern eher im kalifonischen Mountain View, wo Google jüngst bekannt gegeben hat, dass man alleine im Jahr 2015 ca. 780 Millionen (!) Online-Anzeigen blockiert habe, weil sie gegen die Regeln der Werbeschaltungen beim Suchmaschinen-Giganten verstossen hätten. Neben Verletzungen von Anstand, Menschenwürde, Gewalt- oder Sexismusverboten sind vor allem die Zunahme von betrügerischen oder solchen Anzeigen besorgniserregend, die Malware transportieren.

Die Kompromittierung eines Servers im komplexen Ökosystem der Werbeindustrie ist für Bad Boys aus verschiedenen Gründen besonders attraktiv. Zum einen filtern gerade die in Real-Time-Bidding-Prozesse eingebundenen Rechner die User nach lokaler Präsenz und Konsumpräferenzen. Zum anderen ist die in der E-Werbewelt gern und häufig eingesetzte Software OpenX/Revive Adserver für ihre unzureichenden Sicherheitsvorkehrungen bekannt. Weil sich damit Angriffswellen gezielt und auf wenige Tage konzentriert starten lassen, wird auch das Malware Monitoring erheblich erschwert. Nun wurde ein besonders dreister Fall publik, in dem die Hacker den Nutzern mit einer in böser Absicht angelegten Subdomain samt echtem Let´s Encrypt-SSL-Zertifikat eine vertrauenswürdige Sicherheit vorgaukelten, um deren Rechner mit einem bösartigen Online-Banking-Trojaner zu infizieren. Betroffen waren auch Branchengrößen wie DoubleClick oder Ebay.

Um Malvertising einzudämmen, bleiben vorderhand nur drei Wege:

1.) Ein Bewusstsein dafür schaffen, dass es Malvertising überhaupt gibt und was es anrichtet. SWITCH hat dazu u. a. eine Microsite zum Thema «Safer Internet» eingerichtet (https://www.switch.ch/de/saferinternet).

2.) Benutzer dazu motivieren, Endgeräte besser abzusichern, indem sie z. B. vertrauenswürdige AdBlocker installieren oder Flash und Java PlugIns abschalten, wie es die Website «Lifehacker.com» empfiehlt.

3.) Die Werber stärker in die Verantwortung nehmen, ihre Kunden (und die, die es werden wollen) intensiver zu prüfen als bisher. Dabei geht es auch darum, die zugelassene Werbung in der **Funktionalität einzuschränken**, also beispielsweise nur Bilder und Browser unterstützte Videoformate zuzulassen. Wenn das Vertrauen in die Sicherhet des Internets verloren geht, haben nicht nur die Benutzer als direkt betroffene Malvertising-Opfer den Schaden, sondern die gesamte Online-Werbeindustrie.

Nachzulesen unter:

https://googleblog.blogspot.ch/2016/01/better-ads-report.html
http://www.nzz.ch/digital/google-blockiert-780-millionen-anzeigen-ld.4394
http://www.heise.de/security/meldung/Erste-Malvertising-Kampagne-mit-Let-s-Encrypt-Zertifikat-3065115.html
http://www.golem.de/news/security-malware-angriff-aus-der-werbung-1509-116326.html
http://lifehacker.com/how-to-protect-yourself-from-malvertising-on-the-web-1745588094

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.