SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

November / Dezember 2017

SWITCH

I. Dresscode für Apps im Google Play Store: Bösartig

«Mobile first» – die Strategie, neue Angebote primär für die Nutzung auf Mobilgeräten und erst in zweiter Linie für Desktops zu entwickeln, scheint auch in der Cyberkriminalität immer stärkeren Anklang zu finden. Als Spielplatz der Bösen machte kürzlich wieder einmal der Google Play Store Schlagzeilen in Security-Kreisen. Seit April 2016 sind dort hunderte als reguläre Spiele, Video- oder Phone Utilitiy Apps getarnte Apps aufgetaucht, die Malware transportieren, die als «Dresscode» bezeichnet wird. Dresscode wird dazu genutzt, in Netzwerke einzudringen und dort Daten zu stehlen, das Device ungefragt in einem Botnetz zur Verbreitung weiterer Malware, SPAM oder DDoS-Attacken zu verwenden oder über Router in Heimnetzwerke einzudringen, um dort weitere Geräte zu befallen oder Smart Devices im Internet der Dinge zu manipulieren.

Jüngstes Beispiel: «Update WhatsApp». Diese Fake-Version von WhatsApp war für normale User im Store nicht vom Original zu unterscheiden. Logo, Look und Feel glichen dem Original aufs Haar. Um nicht entlarvt zu werden, hängten die Entwickler an die Adresse der WhatsApp Entwickler-ID einfach den Unicode %C2%Ao an, der

im Play Store nicht zu sehen war. Unsichtbar blieb auch die Fake App auf den Geräten der Nutzer, weil dort ein sogenanntes Blank Icon installiert wurde. Auch wenn die App offenbar «nur» dazu verwendet wurde, ihren Entwicklern Einnahmen aus Werbung zu verschaffen, könnte sie auch dazu genutzt werden, Malware auf die Geräte zu bringen.

Dies zeigt zum einen, welche Mühe Google als Store-Betreiber hat, die Sicherheit der angebotenen Apps zu prüfen, geschweige denn zu gewährleisten – bei derzeit 3,3 Millionen Apps im Google Play Store sicher auch eine monumentale Aufgabe. Deshalb gelingt es Cyberkriminellen immer wieder, dort bösartige Apps zu lancieren, die Malware einschleppen oder – neuster Trend – zum Schürfen von Kryptogeld (coin mining) verwendet werden.

Wie raffiniert dabei z.B. die Entwickler von Mobile Banking Trojanern vorgehen, zeigt der unten verlinkte Artikel auf «welivesecurity.com», der die mehrstufige Architektur und Verschlüsselung solcher Malware Apps erklärt. Ganz im Gegensatz dazu steht die Schlamperei des API-Entwicklers Twilio. Dessen Programmierschnittstelle (REST-API) lässt die Zugangsdaten für Apps völlig ungeschützt und öffnet Angreifern ein Einfallstor, um sämtliche Inhalte auslesen zu können. Sicherheitsforscher von Appthority hatten die Lücke im Twilio-API entdeckt und herausgefunden, dass mehr als 680 Apps sowohl für iOS (56%) als auch für Android (44%) betroffen sind.

Bleibt die Frage, was Nutzer tun können, um sich vor solchen bösartigen Apps zu schützen oder sie im Ernstfall wieder los zu werden. Für diesen Ernstfall empfiehlt welivesecurity.com ein dreistufiges Vorgehen:

1) Adminrechte für die heimlich installierte Nutzlast (z.B. Trojaner) ausschalten
   Zu **Einstellungen** > (**Allgemein**) > **Sicherheit** > **Geräteadministratoren** navigieren und nach den Einträgen *Adobe Flash Player*, *Adobe Update* oder *Android Update* suchen.
2) Die Nutzlast deinstallieren
   Zu **Einstellungen** > (**Allgemein**) > **Anwendungsmanager/Apps** navigieren und nach der entsprechenden App (*Adobe Flash Player*, *Adobe Update* oder *Android Update*) suchen
3) Die aus dem Store bezogene App deinstallieren
   Gleiche Navigation wie unter Punkt 2, aber andere Apps. Daher nach diesen Namen suchen: MEX Tools, Clear Android, Cleaner for Android, World News,

WORLD NEWS, World News PRO, Игровые Автоматы Слоты Онлайн or Слоты Онлайн Клуб Игровые Автоматы.

Besser ist es natürlich, bösartige Apps gar nicht erst aus den Stores herunterzuladen. Da aber offenbar weder Google noch Apple trotz anderslautender Selbstdarstellung nicht in der Lage sind, ausreichenden Schutz vor Malware Apps zu bieten, bleibt Nutzern vor dem Download oft nur die Möglichkeit, sich über das Kontrollieren der Ratings und das Studieren der Kommentare über eine App schlau zu machen. Fatalerweise hilft aber auch das nicht immer: Die Fake-WhatsApp App hatte ein 4-Sterne-Rating und mehr als 6.000 Kommentare.

Nachzulesen unter:

http://www.zdnet.com/article/fake-whatsapp-app-fooled-million-android-users-on-google-play-did-you-fall-for-it
https://uk.norton.com/internetsecurity-emerging-threats-hundreds-of-android-apps-containing-dresscode-malware-hiding-in-google-play-store.html
https://www.heise.de/security/meldung/Eavesdropper-Entwickler-Schludrigkeit-gefaehrdet-hunderte-Apps-3887665.html
https://www.welivesecurity.com/deutsch/2017/11/15/mehrstufige-malware-im-google-play-store-aufgetaucht

II. Quad9 – bietet die datenschutzfreundliche Alternative zum Google-DNS Surfen?

Dass Google mehr über uns weiss als wir selbst, ist ein weitverbreiteter Aphorismus des Internetzeitalters mit wahrem Kern. Denn praktisch alles, was wir im Netz tun, generiert erst einmal eine Anfrage nach den IP-Adressen einer Domain. Bevor wir eine Website aufrufen, eine Mail verschicken oder ein Programm laden, wird im Domain Name System (DNS) die Herausgabe der benötigten IP-Adresse angefordert. Weil das DNS wissen muss, wohin diese Daten geschickt werden sollen, wird die eigene IP-Adresse preisgegeben. Diese Kombinationen aus Absenderdaten und Anfrageinhalten liefern den Stoff, aus dem Marketing- und Profiling-Träume gemacht werden. Folglich sind sie also heiss begehrte (und teuer bezahlte) Güter. Mit seinem Public-DNS-Netz hat sich Google in den vergangenen Jahren einen immer grösseren Anteil an diesem Kuchen gesichert. Mit der Nutzung von Google-DNS können Internetprovider viel Geld für den Aufbau eigener Infrastruktur sparen. Im Gegenzug

bezahlen die Nutzer mit der Preisgabe ihrer Daten an Google – das Geschäftsmodell folgt also dem bekannten Google-Business as usual.

Nun gibt es zum Google-DNS eine Alternative, die mit mehreren Sicherheitsfeatures und dank TLS-Verschlüsselung das Abgreifen der Daten durch Dritte verhindern soll: Quad9. Im Namen spiegelt sich die Adresse 9.9.9.9, die die Gründerorganisationen IBM, PCH (Packet Clearing House) und GCA (Global Cyber Alliance) gegen Googles 8.8.8.8 in Stellung gebracht haben. Mit derzeit 100 Servern will Quad9 eine datenschutzfreundliche Alternative bieten, bei deren Nutzung laut Angabe der Betreiber keinerlei persönliche Daten gesammelt oder Daten zum Clickverhalten vermarktet werden. Finanziert wird der Dienst durch Spenden und Beiträge der öffentlichen Hand.

Zur Sicherung der Privatsphäre und zum Schutz vor Cyberkriminalität können die Anfragen über TLS verschlüsselt und auf den kurzen Wegen des DNS-Anycast-Netzes von PCH beantwortet werden, um mögliche Angriffszeiten zu verringern. Allerdings muss dazu erwähnt werden, dass «DNS over TLS» (RFC7858) heutzutage die Installation eines Stub-Resolvers «stuby» voraussetzt oder lokal ein «Unbound DNS Resolver mit DNS Forwarding» implementiert werden muss. Die Validierung von DNSSEC-signierten Domains verhindert Phishing und kann staatliche DNS-Blockaden sichtbar machen. Zudem ermöglicht Quad9 in punkto Sicherheit auch KMUs und privaten Nutzern, was bisher eher grossen Unternehmen vorbehalten war: das Filtern von DNS-Verkehr zum Schutz vor Cyberattacken. Dazu sind neben dem DNS-Filter des Sicherheitsdienstes IBM X-Force die Security Alerts und Listen von achtzehn weiteren Filteranbietern in Quad9 integriert.

Für den einen oder anderen mag das alles zu gut klingen, um wahr zu sein. So weist der IT-Security und -Privacyexperte Mike Kuketz in seinem Blog darauf hin, dass mit IBM einer der grossen Player im Big Data Geschäft massgeblich an Quad9 beteiligt ist und hinter der CGA Sicherheitsbehörden wie die New Yorker und die Londoner Polizei stehen, die Quad9 mitfinanzieren.

Der Vollständigkeit halber sei an dieser Stelle noch erwähnt, dass die sicherste Massnahme bezüglich Privacy und Datenschutz der Betrieb eines eigenen DNS Resolvers ist. Lokale Resolver haben auch den Vorteil, dass sie neben besseren Antwortzeiten meistens bessere Resultate von CDN (Content Delivery Network) liefern.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Quad9-Datenschutzfreundliche-Alternative-zum-Google-DNS-3890741.html
https://quad9.net/#/about
https://www.kuketz-blog.de/quad9-datenschutzfreundliche-alternative-zum-google-dns

III. Taxi ins Darknet – Kunden- und Fahrerdaten jetzt Uber-all?

Der Schweizer Internet-Pionier Jörg Eugster hat in seinen Vorträgen und seinem Buch «Übermorgen – eine Zeitreise in die Zukunft» für Unternehmen und Branchen, die der digitalen Disruption nicht standhalten konnten, den Begriff «weggeubert worden» geprägt. Nun müssen dem Begriff eine, eventuell gar zwei neue Bedeutungen zugesprochen werden. Denn Ende November wurde bekannt, dass bei einem Hackerangriff auf den Fahrdienstvermittler die Daten von 50 Millionen Passagieren und 7 Millionen Fahrern gestohlen wurden, eben: – weggeubert. Peinlicherweise musste Uber nicht nur den Datendiebstahl selbst eingestehen, sondern auch die Tatsache, dass dieser bereits im Oktober 2016 stattgefunden hatte und man sich gegen eine Zahlung von 100.000 Dollar von den Hackern die Zusicherung erkauft hatte, die Daten zu vernichten. Offenbar wollte das seit längerem von verschiedenen Skandalen geplagte Unternehmen den Börsenkurs und anstehende Geschäfte mit wichtigen Investoren vertuschen – eben: wegubern. Darauf deutet jedenfalls das Informationsverhalten des Taxibüros hin, das zuerst den potenziellen Investor Softbank unterrichtete, bevor man nach dreiwöchiger Pause an die Öffentlichkeit ging. Daraufhin leitete die Staatsanwaltschaft von New York sowie Datenschutzbeauftragte mehrerer Länder Ermittlungen gegen Uber ein. Zumal die Uberzahlung an die Datendiebe entweder nicht die zugesagte Vernichtung der Daten nach sich gezogen oder Trittbrettfahrer auf den Plan gerufen hat. So berichtet der Online-Nachrichtendienst «thedailybeast.com», dass sich die Meldungen über gefakte Mails mit dem Absender noreply@uberapp.com häuften, in denen sich Uber für den Hack entschuldigt und Fahrgäste auffordert, Ihr Passwort zu ändern. In ihrer Dreistigkeit gingen die Mailversender sogar so weit, den «Sicherheitsratschlag» zu geben, die Passwörter aller anderen Online-Accounts ebenfalls zu ändern, «um weiteren Schaden zu vermeiden.»

Darauf, dass solche Schäden in Zukunft zunehmen werden, verweist auch Professor Hannes Lubich von der Fachhochschule Nordwestschweiz in einem Interview mit bazonline.ch. Lubich, der zuvor u.a. am Aufbau und am Betrieb des SWITCH-CERT-Sicherheitszentrums beteiligt war, befürchtet, dass die Zahl bekannter Datendiebstähle in Zukunft aus zwei Gründen steigen wird: Zum einen versprächen sie den Hackern guten Gewinn bei geringem Risiko. Zum zweiten werde die neue europäische Datenschutzrichtlinie den Druck auf gehackte Unternehmen, Institutionen und Personen erhöhen, Angriffe und Datendiebstähle sofort zu melden, anstatt sie wegzuubern.

Nachzulesen unter:

https://www.nzz.ch/wirtschaft/cyber-attacke-auf-uber-daten-von-57-millionen-kunden-erbeutet-ld.1331053
https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach
https://www.heise.de/newsticker/meldung/Datenklau-Uber-informierte-erst-potenziellen-Investor-Nutzer-blieben-im-Dunkeln-3901025.html
https://www.thedailybeast.com/hackers-are-using-ubers-57-million-account-data-breach-to-steal-passwords
https://bazonline.ch/digital/mobil/Die-Zahl-der-DatenDiebstaehle-wird-ansteigen/story/27945022

IV. Der Feind in meinem Ohr: Wenn Kopfhörer zu Abhörwanzen werden

Nicht folgsame Kinder sehen sich ab und zu mit der Aufforderung konfrontiert: «Sperr´ Deine Ohren auf!» SPEAK(a)R, ein neuer Typus von Spyware, gibt diese Aufforderung an Computer und macht daran angeschlossene (Passiv-) Kopfhörer oder Lautsprecher zu Mikrofonen. Vier Sicherheitsforscher vom Cyber Security Research Center der Ben-Gurion University präsentierten SPEAK(a)R beim Usenix Workshop on Offensive Technologies (Woot ´17) Mitte August in Vancouver. In ihrem nachstehend zitierten Paper schildern sie detailliert, dass es handelsübliche Audio-Chips erlauben, die Aufgabenverteilung der Anschlüsse per Software zu verändern. Hat sich also ein Hacker Zugang zum Rechner verschafft, kann er durch einfaches Umdefinieren der Anschlussbuchse angeschlossene Kopfhörer oder Lautsprecher zu Mikrofonen machen und die Sprachsignale in einem Umkreis von bis zu neun Metern aufzeichnen. Und zwar unbemerkt vom Nutzer, weil SPEAK(a)R dann bei regulärer Nutzung das Signal kurzfristig wieder umdreht, um eine normale Audio-Wiedergabe zu ermöglichen.

Allerdings funktioniert das virtuelle Ohren-Aufsperren nur bei den Kleinen, will sagen: bei unverstärkten Audio-Devices, die über Kabel mit dem Computer verbunden sind. Aktiv-Lautsprecher und –Kopfhörer, bei denen das Computerausgangssignal zunächst durch einen Verstärker läuft oder Bluetooth-Devices lassen sich nicht zur Ohrwanze umfunktionieren. Verstärker wie auch das Bluetooth-Protokoll lassen das Tonsignal nämlich nur in einer Richtung durch den Äther.

Nachzulesen (und nachzuhören) unter:

http://derstandard.at/2000063472070/Forscher-Kopfhoerer-koennen-zu-Wanze-umfunktioniert-werden
https://www.usenix.org/system/files/conference/woot17/woot17-paper-guri.pdf
https://www.youtube.com/watch?v=ez3o8aIZCDM
https://m.heise.de/security/meldung/Malware-kann-Kopfhoerer-zur-Abhoerwanze-machen-3818074.html

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