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

März/April 2017

SWITCH

I. Cyberkriminelle nehmen Mac-User stärker ins Visier

«Für keine Seele gibt es heut´ noch Sicherheit – es ist der Fluch der Zeit.» Schon 1993 verwies Rainhard Fendrich darauf, dass lange Zeit als sicher geltende Regionen inzwischen ebenso bedroht seien wie einst Jericho oder Troja. Nun bedroht ein Trojaner Rechner unter Mac OS, deren Besitzer sich bisher vor Malware-Angriffen in vermeintlicher Sicherheit gefühlt hatten. Die Security-Firma Sixgill hat in einem russischen Cybercrime-Message-Board ein Angebot entdeckt, das für den gezielten Einsatz gegen Mac-User entwickelt wurde: Das Proton genannte trojanische Remote Administration Tool ist offenbar in der Lage, Tastatureingaben zu überwachen, Screenshots zu ziehen, Dateien hochzuladen und Kommandozeilen-Befehle als Root auszuführen. Damit Apples integrierte Schutzfunktion Gatekeeper keinen Alarm schlägt, kann Proton mit einem Sicherheitszertifikat ausgestattet werden. Im Gesamtpaket für 45.000.- Euro ist neben der Lizenz für unlimitiert viele Installationen auch eine Art «Pull-Marketing» enthalten: Um Mac-User zur Installation zu motivieren, wird die Malware als Fernwartung- und Überwachungstool oder alternativ als Home-Banking Software angepriesen. Einzellizenzen sind ebenfalls erhältlich. Sie kosten gegenwärtig 2 Bitcoins, cirka 2.500.- Schweizer Franken.

Von einer weiteren überaus bösartigen Crypto-Ransomware-Kampagne gegen Apple-User berichtet welivesecurity.com. Die Cyberkriminellen hinter dem in Swift geschriebenen Verschlüsselungs- und Erpressungstrojaner verlangen zwar Lösegeld, können aber keinen Schlüssel anbieten, um die in Geiselhaft genommenen Daten wieder zu befreien: Totalverlust der Daten auf dem Mac auch bei Zahlung von 0,25 Bitcoins für angebliche Entschlüsselung in 24 h und 0,45 Bitcoin für sofortige Datenwiederherstellung. Der Erpresser schleicht sich – getarnt als Patcher zum Cracken von Adobe- und Microsoft-Programmen – via Download von verschiedenen Torrent-Seiten auf die Macs (Details unter dem 2. Link unten).

Davon, dass Cyberkriminelle Mac-User als neue Zielgruppe entdeckt zu haben scheinen, berichtet auch Bill Brenner im nakedsecurity-Blog: Derweil sind einige Böse schon einen Schritt weiter und entwickeln ihre Malware als Hybridversion, die Rechner sowohl unter Windows als auch solche unter Mac OS kompromittiert. Sie tarnt sich als Word-Dokument und bittet die User, Makros zu aktivieren, die dann den befallenen Rechner mit den Servern der Cyberkriminellen verbindet, ohne dass derzeit klar ist, was diese dann mit dem befallenen Rechner vorhaben.

Im Gegensatz zu diesen nebulösen Intentionen haben sich vor kurzem Vermutungen bestätigt, dass die CIA Apples Ethernet/Thunderbolt-Adapter gehackt hat und sich damit Zugriff auf jedes Mac OS-Gerät verschaffen kann, um dort Malware zu installieren, die selbst mit einem komplett neu aufgesetzten Betriebssystem nicht mehr zu entfernen ist. Waren die Ende März auf wikileaks veröffentlichten Dokumente zunächst noch als fragwürdig eingestuft worden, so berichtet Spiegel Online, dass inzwischen sowohl CIA als auch FBI davon ausgehen, dass sie echt seien. Der Fluch der Zeit macht offenbar auch vor Macs nicht Halt.

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Proton-Signierter-Mac-Trojaner-wird-fuer-45-000-Euro-gehandelt-3655096.html
https://www.welivesecurity.com/deutsch/2017/02/23/neue-crypto-ransomware-mac-os
http://www.silicon.de/41641273/eset-warnt-mac-nutzer-vor-neuer-ransomware
https://nakedsecurity.sophos.com/2017/03/21/your-mac-is-not-malware-proof-a-look-at-the-threats-and-defenses
https://threatpost.com/malware-that-targets-both-microsoft-apple-operating-systems-found/124531
http://www.spiegel.de/netzwelt/netzpolitik/wikileaks-enthuellung-vault-7-so-soll-die-cia-auf-apple-geraete-zugreifen-a-1140065.html

II. Malware ab Werk für Android

Zugegeben: Ganz korrekt ist die Überschrift nicht. Denn die Schadsoftware, die Sicherheitsforscher auf 36 Mobilgeräten unter Android entdeckt haben, war wohl nicht werkseitig vorinstalliert worden, wohl aber auf dem Weg vom Hersteller zu einem nicht näher bezeichneten Telekommunikationsunternehmen und einem multinationalen Technologieunternehmen. Betroffen sind Android-Smartphones und Tablets nahezu aller Hersteller, von Asus über Lenovo, LG und Oppo bis Samsung, Xaomi und ZTE. Wie die bösartigen Programme auf die Geräte gelangten, ist derzeit noch völlig unklar. Was sie auf den Geräten tun, dafür umso mehr. Der Blog checkpoint.com berichtet, dass die Malware die Geräte ausspioniert und ein Ad-Network installiert, dass auf betrügerische Weise Werbeeinnahmen generiert. Eine Ransomware-Funktion zur Datenverschlüsselung und Lösegelderpressung sei ebenfalls installiert worden. Die Malware ist nicht im ROM der Geräte installiert worden, wohl aber mit Systemrechten, so dass sie nur durch einen kompletten Reset auf die Werkseinstellungen entfernt werden kann.

Bereits im Februar haben wir im SWITCH Security-Blog auf eine weitere Bedrohung für verschiedene Android-Geräte verschiedener chinesischer Hersteller hingewiesen, die anstelle von Googles Original-Updatesystem die Software «FOTA» (für Firmware Over the Air) der in Shanghai domizilierten Firma Adups einsetzen. Als System-APK hat FOTA unbegrenzten Zugang zu allen Daten auf den Geräten und macht davon auch reichlich Gebrauch, um Daten über Nutzung, Kontakte, Kontakthistorie einschliesslich kontaktierter Adressen und ausgetauschter Inhalte sowie der eindeutigen Identifizierungscodes IMSI und IMEI an Server unbekannter Dritter zu schicken. Ein «Leistungsausweis» der keineswegs aktiv getarnten Firmware findet sich im unten zitierten Artikel von Kryptowire. Er zeigt ebenso wie unser Blogartikel, dass Privatsphäre und Sicherheit eine von allen Seiten bedrohte Existenz führen. Und es wird deutlich, dass es keine einfachen Lösungen zur Behebung der genannten Probleme gibt.

Nachzulesen unter:

http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users
http://www.kryptowire.com/adups_security_analysis.html

III. Casinokasse leer? Netzsperre her! Für 320 Millionen Franken bricht die Schweiz mit dem Tabu der Netzneutralität

Die Schweiz bricht mit einem Tabu und führt nach heftiger aber kurzer Debatte Netzsperren für ausländische Onlinecasino-Seiten ein. Gleichzeitig schuf der Nationalrat mit dem Ende Februar verabschiedeten neuen Geldspielgesetz die Grundlage dafür, dass einheimische Casinobetreiber eine Konzession für Onlinespiele erwerben können – und führt damit das Argument zumindest teilweise ad absurdum, dass man die Netzsperre zum Schutz der Spieler einführen wolle.

Laut Bundesrätin Simonetta Sommaruga hat diese Netzsperre mit Zensur nichts zu tun, weil sich Zensur auf Medien beziehe und nicht auf Wirtschaftstätigkeiten. Die Gegner der Sperre sehen diese als unverhältnismässig an und befürchten vor allem den Anfang vom Ende der Freiheit des Internets. Denn auf die Netzsperre für Casinoseiten könnten andere folgen. Darüberhinaus bringen Netzsperren mehr Probleme als Lösungen, sie sind auf einfachen Wegen zu umgehen und weitaus ineffektiver als die Löschung krimineller Inhalte und die Bestrafung ihrer Urheber. Im Fall der Casino-Netzsperre geht es wohl einfach um Geld, wenn auch um viel: Im Jahr 2015 flossen aus den Spieleinsätzen der Schweizer Casinos 47 Mio. Franken in die Kassen der Standortkantone und weitere 273 Mio. Franken in die der AHV. Doch diese Einnahmen sind bedroht, denn immer mehr Spieler weichen auf Onlinecasinos, ausländische Spielhallen und nicht-konzessionierte inländische Spielclubs aus, weshalb die Schweizer Casinos klagen, Spieleinsätze im Bereich mehrerer Hundert Millionen Franken zu verlieren.

Nachzulesen unter:

http://www.tagesanzeiger.ch/schweiz/standard/die-schweiz-bricht-tabu-und-sperrt-websites/story/12456995
https://www.srf.ch/news/schweiz/session/parlament-will-unbewilligte-online-gluecksspiele-sperren
https://www.nzz.ch/schweiz/geldspielgesetz-nationalrat-will-netzsperren-fuer-online-geldspiele-ld.148619
https://netzpolitik.org/2017/schweiz-fuehrt-netzsperren-fuer-gluecksspielangebote-ein
http://www.luzernerzeitung.ch/nachrichten/schweiz/Netzsperren-sind-unverhaeltnismaessig;art9641,976775
https://www.srf.ch/news/schweiz/session/netzsperren-bringen-statt-loesungen-nur-probleme
http://www.luzernerzeitung.ch/nachrichten/schweiz/Schweizer-Spielcasinos-darben;art9641,941488
https://de.wikipedia.org/wiki/Zensur_im_Internet

IV. Wie Spielzeug im Internet der Dinge kleine und grosse Kinder ausspioniert

Bereits im Mai 2015 wiesen wir im SWITCH Security Report darauf hin, dass Smart Toys, wie Hello Barbie, Kinderzimmer ausspionieren und die Gespräche, die Kinder mit ihnen führen, aufzeichnen und an den Hersteller senden. Im November des gleichen Jahres warnte der Guardian davor, dass Hello Barbie ein leichtes Angriffsziel für Hacker sei, über das sie nicht nur die Kinder ausspionieren, sondern sich auch Zugriff zum gesamten WLAN verschaffen könnten.

Hatte Oren Jacob, CEO des Systemherstellers ToyTalk 2011 noch verkündet: «No user data, no Barbie content, and no major security nor privacy protections has been compromised to our knowledge.», so sind nun 2,2 Millionen Sprachdateien offen ins Netz gestellt worden, die von Teddybären der Marke CloudPets mit einem System von Spiral Toys aufgezeichnet und gespeichert worden waren. Bereits im Februar hatte die deutsche Bundesnetzagentur die smarte Puppe «My Friend Cayla» verboten. Weil die Agentur in der Kombination aus Mikrofon mit Spracherkennung, Vernetzung bei mangelhafter Sicherheit, bedenklichen Datenschutzklauseln und Informations-übertragung an ein Drittunternehmen in den USA Indizien dafür sah, dass Cayla eher als unzulässiges Spionagegerät einzustufen sei, denn als harmloses Spielzeug, wurden alle Eltern aufgefordert, die Puppe zu zerstören.

Sicherheitslücken und ungewollte Datentransfers sind aber nicht nur bei Spielzeug im Kinderzimmer zu finden. Besonders pikant wird das ganze, wenn es sich um Erwachsenen-Spielzeug handelt. Im März diesen Jahres wurde der Fall der smarten Sexspielzeuge des kanadischen Herstellers «We-Vibe» bekannt. Dieser hatte «zu Marktforschungszwecken und ohne Möglichkeit einer personenbezogenen Auswertung» (Aussage des Unternehmens) Daten zu Nutzungszeit und -dauer sowie zum ausgewählten Vibrationsmodus seiner smartphonegesteuerten Sex Toys gesammelt – ohne vorher die Einwilligung der Userinnen und User einzuholen. Angeblich muss We-Vibe nun insgesamt bis zu vier Millionen an Schadensersatzsummen zahlen.

Und wenn dies alles nicht eigentlich schon reichen würde: Kurz vor Redaktionsschluss dieses Reports macht die Nachricht über «Siime Eye» die Runde, einem smarten Vibrator mit eingebauter Kamera, die man auch von der anderen Strassenseite aus ausspionieren kann. Das Gerät ist nicht nur mit einem Webinterface,

sondern auch mit voreingestellten Zugangsdaten für WLAN und Webzugang (Nutzer: admin, Passwort: blank) ausgestattet.

Nachzulesen unter:

http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-05_de.pdf
https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children
https://www.heise.de/security/meldung/Cloudpets-2-2-Millionen-Sprachdateien-von-Kinderspielzeug-offen-im-Netz-3637923.html
http://www.computerbild.de/artikel/cb-News-Sicherheit-CloudPets-Sicherheit-17471813.html
http://derstandard.at/2000052783832/Behoerde-Eltern-muessen-Puppe-My-Friend-Cayla-zerstoeren
http://www.primelife.co/lovely-wearable-fuer-sex
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-08.pdf
http://www.newsweek.com/sex-toys-connected-internet-risk-being-hacked-437366
https://www.nzz.ch/datenschutz-sex-toy-hersteller-spionierte-kunden-aus-ld.151135
https://www.heise.de/security/meldung/Svakom-Siime-Eye-Vernetzter-Kamera-Vibrator-ist-ein-Sicherheitsalptraum-3674827.html

Neu im SWITCH-CERT Security Blog

Adups — The Spy in your Pocket

A „Firmware Over The Air“ Updater that phones home:

https://securityblog.switch.ch/2017/02/28/adups-the-spy-in-your-pocket/

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.