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

März 2015

SWITCH

I. Wenn der Fisch den Angler beisst – Lenovo, Komodia und der SuperFish

Der Wurm muss dem Fisch und nicht dem Angler schmecken. Dieser Leitsatz aus dem analogen Werbezeitalter meint, dass sich Werbung an die Umworbenen und nicht an die Entscheider im werbenden Unternehmen richten soll. Mit SuperFish hat die «Digital Badvertising»-Entwicklung einen neuen, Besorgnis erregenden Höhepunkt erreicht. Denn jetzt beisst der Fisch den Angler, respektive die Nutzer von Laptops, auf denen der chinesische Hardwareriese Lenovo die von SuperFish und dessen Zulieferer Komodia stammende Bloatware vorinstalliert hat. Damit bringen die Laptops neben den üblichen Crapware-Ärgernissen gleich zwei gravierende Sicherheitsprobleme mit. Problem Nummer 1: SuperFish installiert ein eigenes Root-Zertifkat, um Werbung auch auf verschlüsselten Webseiten einblenden und von Usern als gesichert wahrgenommene Verbindungen bespitzeln zu können. Alleine dafür hätten SuperFish, Komodia und Lenovo den Titel für die unverschämteste (zivile) IT-Sicherheitsmanipulation des Jahres verdient, wenn es denn eine solche Auszeichnung gäbe. Aber es kommt noch schlimmer, weil SuperFish – Problem Nummer 2 – die Sicherheitsarchitektur von

Windows so manipuliert, dass Cyberkriminellen Tür und Tor für Man-in-the-Middle-Angriffe geöffnet wird. Bekannt wurde dies, nachdem Chris Palmer, ein für Google arbeitender Sicherheitsingenieur auf seinem neu gekauften Lenovo-Laptop einen Man-in-the-Middle-Hack seiner Bank of America-Verbindung erleben musste und dies in der IT-Security-Community publik machte. In einer ersten Stellungnahme reagierte Lenovo schon beinahe zynisch: «...we pre-installed a piece of third-party software, Superfish, on some of our consumer notebooks. The goal was to improve the shopping experience using their visual discovery techniques.» Auch SuperFish-CEO Adi Pinhas wies alle Schuld von sich und machte für die Sicherheitsprobleme die von Komodia zugekaufte SSL-Unterbrechungs-Komponente verantwortlich, die auf deren Website als «Advanced SSL-Hijacker» beworben wurde.

Ironie des Ganzen: Dieser fortschrittliche Datenräuber ist u.a. auch in der Anti-Adware-Software «Lavasoft» sowie dem gratis verteilten Kinderschutz-Programm «KeepMyFamiliySecure» installiert, so dass das CERT/CC eine Warnung vor diesen und cirka einem Dutzend ähnlicher Softwarepakete veröffentlicht hat. Damit sind nicht nur Lenovo-Laptops, sondern alle Rechner gefährdet, auf dem eines der aufgelisteten Programme installiert wurde.

Zwischenzeitlich haben zwar alle Beteiligten Besserung gelobt – nicht zuletzt, weil sich vor allem Lenovo von Sammelklagen bedroht sieht. So will Lenovo SuperFish nicht mehr installieren und stellt ein automatisches De-Installationstool bereit. SuperFish will den Komodia-Hijacker entfernen und Komodia will ein Update mit weniger Sicherheitsrisiken zur Verfügung stellen. Dennoch wird dringend empfohlen, Lenovo-Laptops aus den betroffenen Baureihen sowie alle Rechner, mit den betroffenen Programmen zu testen und gegebenenfalls die Malware und das Zertifikat zu entfernen (siehe die untenstehenden Links auf filippo.io).

Nachzulesen unter:

http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl

http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections

http://blog.erratasec.com/2015/02/some-notes-on-superfish.html

http://www.kb.cert.org/vuls/id/529496

http://www.heise.de/security/meldung/Gefaehrliche-Adware-Mehr-als-ein-Dutzend-Anwendungen-verbreiten-Superfish-Zertifikat-2557619.html

http://www.nzz.ch/mehr/digital/lenovo-superfish-visual-discovery-sammeklage-1.18488867

http://support.lenovo.com/en/product_security/superfish_uninstall

https://filippo.io/Badfish

https://filippo.io/Badfish/removing.html

II. Gemalto-Gate – Der Geheimdiensthack geht an die Wurzeln der Sicherheit mobiler Kommunikation

Wenn SuperFish im zivilen Bereich einen Höhepunkt der Dreistigkeit markiert, dann haben die beiden Geheimdienste NSA und GCHQ mit dem Angriff auf den niederländischen «World leader in digital security» (eigene Werbeaussage) Gemalto behördlicherseits noch eins draufgesetzt. Mit ca. 2 Mrd. produzierten SIM-Karten pro Jahr gilt Gemalto als grösster Hersteller, der Kunden und Behörden rund um den Globus nicht nur mit den Telefonkarten, sondern auch mit Chips für Kreditkarten, Schliess-, Zugangs- und Bezahlsysteme, Pässe und andere ID-Karten beliefert. Seit Übernahme der Trüb AG aus dem Aargau ist Gemalto auch ein wichtiger Player im Schweizer Sicherheitsmarkt und Produzent des SwissPass für das elektronische Generalabo und Halbtax sowie der SuisseID. Die dem Investigativportal «The Intercept» aus den Snowden-Papieren zugespielten Präsentationsfolien des britischen Geheimdienstes legen nahe, dass GCHQ und NSA bei einem staatlich-digitalen Einbruchdiebstahl im Jahr 2010 in den Besitz der Schlüsselcodes für Gemalto SIM-Karten gelangt sind. Wie die deutsche Tagesschau herausfand, kommen diese SIM-Karten in etwa 50% aller deutschen Mobiltelefone zum Einsatz. In der Schweiz sind Handys aller drei Mobilnetzbetreiber mit den Karten ausgerüstet. Zudem werden in beiden Ländern SIM-Karten des deutschen Anbieters Giesecke & Devrient eingesetzt, der sich ebenfalls als Ziel der beiden Geheimdienste in den Snowden-Papieren aufgelistet findet. Dieser will allerdings keinen Angriff verzeichnet haben und verspricht, dass G&D-SIM-Karten nach wie vor sicher seien. Das tut inzwischen auch Gemalto, obwohl sich die Unternehmensleitung unmittelbar nach Bekanntwerden des Hacks noch bestürzt gezeigt und verkündet hatte, alles daranzusetzen, die Umstände und Folgen des Angriffs abzuklären. Nach ersten Abklärungen beteuerte das Unternehmen aber eine Woche später, dass Gemalto-

Karten sicher seien und man keine nennenswerten Schadensersatzforderungen erwarte.

Die könnten dem Unternehmen aber aus einer Panne entstehen, die ebenfalls auf das Jahr 2010, in dem Gemalto offenbar gehackt wurde, datiert. Damals funktionierten plötzlich 30 Millionen EC- und Kreditarten mit Gemalto-Chips nicht mehr und sind bis heute wenn überhaupt, dann nur eingeschränkt nutzbar. Gemalto hat die Verantwortung dafür inzwischen übernommen und versucht, den Schadensersatzforderungen der betroffenen Finanzinstitute mit Software-Updates entgegenzuwirken.

Auch die Geheimdienste sehen sich Forderungen nach Schadensersatz aus Politikerkreisen gegenüber. So forderte u.a. der österreichische Grünen-Abgeordnete Pilz seine Regierung zur Klage und zu Sanktionen gegenüber beiden Geheimdiensten auf, zumal das britische Geheimdiensttribunal «Investigatory Powers Tribunal (IPT)» Ende Januar zum Urteil gekommen war, dass die massenhafte Sammlung privater Daten gegen geltendes Europäisches Menschenrecht verstosse.

Nachzulesen unter:

https://firstlook.org/theintercept/2015/02/19/great-sim-heist

http://www.inside-it.ch/articles/39285

http://www.tagesschau.de/sim-karten-kryto-101.html

http://www.computerworld.ch/news/security/artikel/nsa-im-besitz-von-sim-karten-codes-schweiz-ev-betroffen-67361

http://www.computerworld.ch/news/it-branche/artikel/gemalto-unsere-sim-karten-sind-sicher-67373

http://motherboard.vice.com/read/worlds-largest-sim-card-maker-has-no-clue-whether-it-was-hacked-by-the-nsa

http://www.theregister.co.uk/2015/02/25/gemalto_everythings_fine_security_industry_hang_on_a_minute/

http://www.spiegel.de/wirtschaft/unternehmen/kartenpanne-franzoesische-firma-schuld-an-2010-fehler-a-670400.html

http://futurezone.at/netzpolitik/urteil-methoden-des-britischen-gchq-teils-illegal/112.357.248

III. Carbanak – Digitaler Bankraub im grossen Stil

Und noch eine unglaubliche Dreistigkeit höchst krimineller Art: Einem Bericht von Kaspersky zufolge soll die cyberkriminelle Vereinigung «Carbanak» seit 2013 zwischen 300 Millionen und einer Milliarde US-Dollar von mehr als 100

Finanzinstituten weltweit gestohlen haben, und die Angriffe sollen noch andauern. Der Mega-Coup zeugt von penibler, jahrelanger Vorbereitung und höchster krimineller Energie. Über gezielte Spear-Phishing-Attacken wurden Angestellten-Computer mit einer Backdoor infiziert und als Eingang ins interne Bankennetzwerk genutzt. Im nächsten Schritt wurden die Aktivitäten jener Mitarbeiter aufgezeichnet, die die Geldtransfersysteme betreuen. Dazu wurden auch die für die Videoüberwachung zuständigen Computer aufgespürt und übernommen. Ziel war es dabei, genügend Informationen zu sammeln, um die Handlungen der Bankangestellten imitieren zu können, um Geld zu überweisen oder bar auszuzahlen. Dazu nutzt Carbanak mehrere Wege, von der direkten Geldüberweisung oder Auszahlung via E-Payment-Systeme über die verdeckte Manipulation von Kundenkonten bis zur Anweisung an Geldautomaten zur Auszahlung zu einem Zeitpunkt, an denen dann ein Mittelsmann das Geld entnehmen kann. Weil nicht alle Mittelsmänner zur rechten Zeit kamen und die Geldautomaten dann vermeintlich unkontrolliert Geld in die Umgebung warfen, flog der Coup trotz aller Tarnung auf.

Security-Experten zeigen sich nicht nur von der Dimension der Straftaten überrascht, sondern auch von der Tatsache, dass die Angriffe unabhängig von der eingesetzten Software stattfanden – und offenbar noch stattfinden.

Eine detaillierte Beschreibung findet sich im unten verlinkten PDF.

Nachzulesen unter:

http://newsroom.kaspersky.eu/de/texte/detail/article/der-grosse-bankraub-cybergang-carbanak-stiehlt-eine-milliarde-us-dollar-von-100-finanzinstitu

https://www.wired.de/collection/latest/carbanak-der-grosste-bankraub-aller-zeiten

http://futurezone.at/digital-life/massiver-cyberangriff-auf-banken-in-europa-und-usa/113.971.500

http://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts

https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

IV. Es gibt auch gute Nachrichten: Europol zerschlägt BotNet «Ramnit»

Seit 2010 hat das Botnetz «Ramnit» mehr als 3,2 Millionen Computer mit Malware infiziert, die sich die User als Drive-By-Downloads von bösartigen

Webseiten oder per E-Mail eingefangen hatten. Die Schadsoftware ermöglichte es den Ramnit-Betreibern, die Kontrolle über die infizierten Computer zu übernehmen, um Passwörter oder persönliche Daten zu stehlen, weitere Spam-Nachrichten zu verteilen oder illegale Angriffe auf andere Websites zu starten. In einer konzertierten Aktion, an der auch Microsoft, Symantec und AnubisNetworks beteiligt waren, gelang es nun dem European Cybercrime Centre (EC3) von Europol mit Polizeibehörden in Deutschland, Grossbritannien, Italien und den Niederlanden, das Botnetz zu zerschlagen. Vor dem Hintergrund der Grösse des Netzes appellieren die Behörden an alle User, ihre Rechner zu testen und ggfs. zu bereinigen. Dazu haben Microsoft und Symantec entsprechende Tools bereitgestellt (unten verlinkt). Der Erfolg der Europäer scheint das amerikanische FBI motiviert zu haben, auf den Kopf des BotNets «Zeus» und einen der Väter der Crypto-Locker-Methode (siehe Security-Report September 2014) eine Belohnung von drei Millionen US-Dollar auszusetzen. Dem Russen Jevgeni Michailowitsch Bogatschew werden die Infektion von über einer Million Computern und ein Schaden von 100 Millionen Dollar zur Last gelegt. Bogatschew kann damit den fragwürdigen Rekord für sich reklamieren, es auf die Liste der meistgesuchten Personen des FBI geschafft zu haben und das mit dem höchsten Kopfgeld, das jemals für einen Cyberkriminellen ausgelobt wurde.

Nachzulesen unter:

http://www.zdnet.de/88220112/europol-zerschlaegt-mithilfe-des-bka-botnet-ramnit

http://windows.microsoft.com/en-us/windows/detect-remove-ramnit-virus

http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

http://www.spiegel.de/netzwelt/web/zeus-botnet-fbi-setzt-drei-millionen-dollar-kopfgeld-aus-a-1020383.html

V. Wie man BMWs und Rolls Royce ferngesteuert öffnet

Unmittelbar nach Redaktionsschluss des letzten Security Reports mit dem Artikel zum Thema Automotive Security sorgte der ADAC für Schlagzeilen mit einem Test, in dem er nachwies, dass sich ca. 2,2 Millionen BMWs, Minis und – da wird´s besonders interessant – Rolls Royce, die zwischen März 2010 und Dezember 2014 gebaut wurden, relativ einfach unbefugt öffnen lassen, indem das dort installierte Connected-Drive-System via Smartphone gehackt wird. BMW hat die

Testergebnisse bestätigt und bietet neben einem entsprechenden Update auch eine Hotline an. Detaillierte Infos zu dem Hack finden Sie im Heise-Link unten.

Nachzulesen unter:

http://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html

http://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/bmw-luecke.aspx

http://www.computerworld.ch/news/security/artikel/bmws-lassen-sich-mit-dem-smartphone-oeffnen-67243

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Im Cisco-Securityblog gibt es einen guten Beitrag zum Angler Exploit Kit, dem aktuell «besten Exploit Kit auf dem Markt», inklusive einem Exkurs zu Domain Shadowing.

http://blogs.cisco.com/security/talos/angler-domain-shadowing

«11 ways to track your moves when using a web browser» ist ein aktueller Blogartikel vom SANS-Institut zum Thema User Tracking im Internet.

https://isc.sans.edu/forums/diary/11+Ways+To+Track+Your+Moves+When+Using+a+Web+Browser/19369/

Das spanische CERTSI hat eine sehr informative Studie zum Thema Android-Malware veröffentlicht.

https://www.incibe.es/CERT_en/publications/Studies/android_malware_situation_en

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