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

Januar / Februar 2017

SWITCH

I. The Guardian mit WhatsApp-Story im Postfaktischen?

Seit 1821 steht die britische Tageszeitung «The Guardian» für unabhängigen, verlässlichen, liberalen Journalismus für progressive, intellektuelle Leserinnen und Leser. Viermal wurde die in London beheimatete Zeitung bei den British Press Awards als «National Newspaper of the Year» ausgezeichnet. Ihr Online-Ableger «theguardian.com» galt bislang als seriöse Quelle gerade auch für Nachrichten zum Themen IT-Security und Privacy. Und nun das: In einer Exklusivstory behauptete theguardian.com am 13. Januar 2017, dass eine Backdoor in der bislang als abhörsicher geltenden Ende-zu-Ende-Verschlüsselung von WhatsApp Geheimdiensten die Möglichkeit eröffne, Nachrichten abzufangen. The Guardian bezog sich dabei neben anderen Verschlüsselungs- und Sicherheitsexperten auf den Krypto- und Security-Forscher Tobias Boelter von der University of California in Berkeley, der gemäss seiner Darstellung auf dem eigenen Blog «tobi.rocks» die Schwachstelle bereits im April 2016 entdeckt und Facebook gemeldet hatte. Dass die Schwachstelle nicht gefixt wurde und WhatsApp gemäss Boelters Blogeintrag vom 13. Januar 2017, die Schwachstelle nicht als Bug, sondern als Feature für selten auftretende

Übertragungsprobleme deklarierte, legte nicht nur für Boelter, sondern auch für andere im Guardian-Beitrag zitierte Forscher den Schluss nahe, WhatsApp lasse die Lücke bewusst als Backdoor für Geheimdienste offen.

«There is no WhatsApp ‚Backdoor'», konterte noch am Tag der Guardian-Veröffentlichung Moxie Marlinspike, Kryptoexperte und Co-Autor des von WhatsApp eingesetzten Verschlüsselungsprotokolls «Signal» auf der Website «whispersystems.org». Seitdem schlagen die Wellen hoch. Auf dem Blog «technosociology.com» bezichtigte Zeynep Tufekci, Tech-Autorin und Asocciate Professor an der University of North Carolina den Guardian der unverantwortlichen Berichterstattung. Denn die deutliche Mehrheit der Verschlüsselungs- und Sicherheitsexperten stimme darin überein, dass die gefundene Lücke keine Backdoor sei, sondern ein Sicherheitsfeature, dass den täglichen Gebrauch von WhatsApp so erleichtere, dass dafür eine vernachlässigbare Gefährdung in Kauf genommen werden könne. Zur Untermauerung liefert Tufekci gleich noch die Unterschriften von deutlich mehr als 50 Experten im Anhang ihres Beitrags. Auch andere Veröffentlichungen auf Security-Blogs und Websites von «nakedsecurity» bis «techcrunch.com» griffen Tufekcis Kritik und die Forderung verschiedener Forscher an den Guardian auf, den fraglichen Artikel zurückzuziehen. Dieser hat dahingehend reagiert, dass die Bezeichnung «Backdoor» in der Artikelüberschrift durch «Vulnerability» ersetzt wurde. Denn eine solche besteht bei WhatsApp weiterhin, argumentiert Mohit Kumar, Gründer und CEO von The Hacker News. Und er verweist darauf, dass bis heute weder Sicherheitsexperten noch WhatsApp oder Facebook abgestritten haben, dass im Fall des Falles staatliche Stellen WhatsApp-Nachrichten mitlesen können.

Und da kommt «Zitis» ins Spiel, die neue Dienstleistungszentrale für deutsche Strafverfolgungsbehörden und Geheimdienste. Zitis steht für "Zentrale Stelle für Informationstechnik im Sicherheitsbereich" und soll vor allem verschlüsselte Online-Kommunikation von WhatsApp und anderen Messengerdiensten entschlüsseln und behördenlesbar machen. Bis 2022 sollen dazu mit den Steuergeldern der überwachten Bürger in München 400 Stellen besetzt werden. Dass dort schon heute zahlreiche Unternehmen domiziliert sind, die sich auf die Bereitstellung von Staatstrojanern und andere Überwachungssoftware

konzentrieren, dürfte bei der Standortwahl als Plus für die Rekrutierung von Fachkräften gewertet worden sein.

Nachzulesen unter:

https://www.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages
https://tobi.rocks/2017/01/whatsapp-vulnerability-bug-or-backdoor
https://whispersystems.org/blog/there-is-no-whatsapp-backdoor
http://technosociology.org/?page_id=1687
https://nakedsecurity.sophos.com/2017/01/16/whatsapp-backdoor-turns-out-to-be-known-design-feature
https://threatpost.com/why-whatsapps-backdoor-isnt-a-backdoor/123113
http://www.golem.de/news/sicherheitsbehoerde-zitis-soll-von-muenchen-aus-whatsapp-knacken-1701-125722.html

II. Fruitfly-Spionagesoftware lebt auf Macs lang

Fruitfly heisst eine Spionagesoftware, die zwar erst kürzlich bei Versuchen entdeckt wurde, Macs in biomedizinischen Forschungseinrichtungen auszuspionieren, sich aber auffallend alter Funktionen bedient, die noch aus der Zeit vor OS X Yosemite stammen. Das jedenfalls veröffentlichte Thomas Reed, Sicherheitsforscher bei Malwarebytes in seinem Firmenblogeintrag vom 18. Januar 2017. Reed hatte herausgefunden, dass die von Apple auf den Namen Fruitfly getaufte Malware versucht, Screenshots anzufertigen, auf integrierte oder angeschlossene Webcams zuzugreifen und die erbeuteten Daten an Server der Angreifer zu schicken. Einmal im Apfel eingenistet soll die Fruchtfliege auch Funktionen zur Fernsteuerung der befallenen Macs beherrschen. Dabei ist nicht sicher, wie die Fliege in den Apfel kommt, will sagen Fruitfly die Macs infiziert. Fest steht aber, dass die Spionage-Software auch Linux-Shellbefehle umfasst – möglicherweise könnte die Malware damit auch Linux-Varianten ausbilden, die jedoch noch nicht gesichtet wurden. Apple hat inzwischen ein Sicherheitsupdate veröffentlicht, um Rechner gegen Fruitfly-Attacken abzusichern.

Nachzulesen unter:

https://blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code
https://www.heise.de/security/meldung/Fruitfly-Apple-Update-soll-Spionage-Software-blockieren-3603628.html
http://www.macnotes.de/2017/01/22/fruitfly-apple-vertreibt-update-gegen-spionage-malware
http://thehackernews.com/2017/01/mac-os-malware.html
http://www.giga.de/downloads/macos-sierra/news/fruitfly-macos-malware-blieb-anscheinend-jahrelang-unentdeckt

III. Gute Malware: Das FBI in der Absurditätsfalle

Alle Strafverfolgungsbehörden dieser Welt verteidigen den Einsatz staatlicher Malware mit dem Argument, dass damit neben Terroristen, Drogenhändlern und allgemeinen Gewaltverbrechern auch Kinderschänder von ihrem verwerflichen Tun abgehalten werden oder im Fall des Falles dafür zumindest zur Rechenschaft gezogen werden können. Zu welcher grotesken Situation diese Argumentation führen kann, zeigt ein aktueller Fall aus den USA. Dort wurde ein mit FBI-Malware entlarvter Ring mutmasslicher Pädokrimineller wieder auf freien Fuss gesetzt, weil das FBI der Aufforderung des Gerichts nicht nachkommen wollte, den Quellcode für die Malware offen zu legen. Diese wurde vom FBI eingesetzt, um die IP-Adressen mutmasslicher Pädophiler zu ermitteln, die über das Tor-Netzwerk auf der Plattform «Playpen» Darstellungen missbrauchter Kinder getauscht und gehandelt hatten, bis die Plattform vom FBI geschlossen wurde. In der Folge wurden 135 Personen angeklagt. Einige unterzeichneten nach der Enttarnung Schuldeingeständnisse, andere setzten sich mit ihrer Klage, dass die Beweismittel rechtswidrig erlangt worden seien, durch. Zumindest in einem Fall forderte das Gericht das FBI auf, den Quellcode offen zu legen. Im Dilemma zwischen der Möglichkeit zur Verurteilung eines mutmasslichen Täters oder der weiteren Benutzung der Malware entschied sich das FBI dafür, den Quellcode zu schützen und auf eine weitere Verfolgung des enttarnten mutmasslichen Pädokriminellen zu verzichten.

Bleibt die Frage, wie sinnvoll der Einsatz einer Software zur Überführung von Kriminellen ist, wenn diese nach ihrer Enttarnung und Ergreifung wieder auf freien Fuss gesetzt werden, weil sonst die Software nicht mehr eingesetzt werden kann. Diese Logik verstehen offenbar nur Behörden, die gemäss gizmodo.com behaupten, dass ihre Malware keine Malware sein könne, weil sie ja von den Guten zu einem guten Zweck eingesetzt werde.

Nachzulesen unter:

http://www.golem.de/news/um-eigene-malware-zu-schuetzen-fbi-laesst-paedokriminellen-laufen-1701-125496.html
https://arstechnica.com/tech-policy/2017/01/feds-may-let-playpen-child-porn-suspect-go-to-keep-concealing-their-source-code
http://www.zeit.de/digital/datenschutz/2017-01/strafverfolgung-fbi-geheimer-tor-exploit-dilemma
http://gizmodo.com/the-fbi-says-its-malware-isn-t-malware-because-the-fbi-1783537208

IV. Star Wars auf Twitter: Schlummerndes Twitter-Botnet mit über 350.000 Bots entdeckt

Stars Wars Fans wissen es längst: Das (böse) Imperium schlägt zurück – auch wenn es über lange Zeit den Anschein hat, als ob es zerschlagen wäre. Dass ein seit 2013 inaktives Twitter-Botnet von seinen Entdeckern den Namen «Star-Wars-Botnet» bekam, hat aber andere Gründe. Aber der Reihe nach: Anfang Januar 2017 veröffentlichten die beiden Wissenschaftler Juan Echeverria und Shi Zou am Department of Computer Science des University Colleges London auf arvix.org eine Forschungsarbeit, in der sie darstellen, wie sie ein riesiges, derzeit inaktives Netz von 356.957 Bots entdeckten, das im Kurznachrichtendienst Twitter sein Unwesen getrieben hatte und jederzeit reaktiviert werden könnte. Bei der Untersuchung englischsprachiger Tweets fiel beiden auf, dass 3.244 Nutzer auf hoher See oder an sehr unbewohnten Gegenden twitterten. Der Tatsache, dass diese Gruppe auffallend häufig Texte oder Textfragmente aus Star Wars zitierten, verdankt das Star-Wars-Botnet seinen Namen. Nachdem die Forscher weitere Gemeinsamkeiten entdeckt hatten, trainierten sie einen sogenannten Klassifizierer, der die Tweets von cirka 14 Millionen englischsprachigen Twitter-Usern untersuchte. Dabei identifizierte er die gut 350.000 Bots. Weiterführende Beobachtungen brachten Echevarria und Shi zum Schluss, dass diese ein riesiges Netz bilden mussten. Sie vermuteten, dass das Netz auch deshalb bislang unentdeckt blieb, weil alle Bots seit dem 14. Juli 2013 aufgehört hatten, Tweets zu posten. Vor dem Hintergrund, dass die riesige Armee virtueller Storm Troopers jederzeit wieder aktiviert werden könnte, orten die Forscher Nachholbedarf bei der Methodenentwicklung zur Detektion von Twitter-Botnetzen. Möge die Macht mit ihnen sein!

Nachzulesen unter:

https://www.heise.de/newsticker/meldung/Forscher-entdecken-riesiges-Twitter-Botnetz-Star-Wars-3604196.html
https://arxiv.org/pdf/1701.02405v1.pdf
https://www.engadget.com/2017/01/23/twitter-botnet-quotes-star-wars-from-the-middle-of-the-sea
http://gizmodo.com/massive-twitter-bot-army-exposed-by-its-obsession-with-1791464124
http://digitalchew.com/2017/01/22/star-wars-twitter-bots

Neu im SWITCH-CERT Security Blog

Background - Malware: Usage of .ch domain names for spamming malware Tofsee stopped
https://securityblog.switch.ch/2016/12/22/tofsee-ch-domain-names-stopped/

Background - Malware: A file that wasn't there
https://securityblog.switch.ch/2016/12/20/a-file-that-wasnt-there/

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