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

Mai 2016

SWITCH

I. Schneller als Odysseus: E-Banking-Trojaner Gozi attackiert die Schweiz via Newsportal

Bekanntlich belagerte das antike griechische Heer Troja zehn Jahre lang, bevor Odysseus die Idee hatte, ein riesiges hölzernes Pferd zu erbauen, sich mit einer militärischen Eliteeinheit darin zu verstecken und die belagerten Einwohner Trojas im guten Glauben zu lassen, etwas Wertvolles zu erbeuten, wenn sie das Pferd in ihre Stadt zögen – was dann ja allen Warnungen des weisen Priesters Laokoon und der Königstochter Kassandra zum Trotz geschah und zur Zerstörung der Stadt führte. Knapp 3.000 Jahre später brauchte Gozi, ein virtuelles Trojanisches Pferd, für sein zerstörerisches Werk gerade mal 20 Minuten – besser: 20min.ch. Denn das grösste Schweizer Newsportal wurde Anfang April von Cyberkriminellen gleich zweimal als Verteilstation für Schadsoftware genutzt, um flächendeckend auf Schweizer Rechnern gespeicherte Bank- und Login-Daten zu erbeuten. Damit hat das sogenannte Malvertising, also die Verbreitung von Schadsoftware (Malware) via Werbung (Advertising) in der Schweiz eine bisher noch nicht beobachtete Dimension erreicht.

Zuvor hatten wir bereits im Dezember Security Report über die eskalierende Auseinandersetzung um AdBlocker berichtet. Zudem hatten wir in einem Blog-Artikel im Februar 2016 nicht nur die allgemeine Malvertising-Situation beschrieben, sondern auch explizit darauf hingewiesen, dass vor allem Newsseiten dazu missbraucht werden, E-Banking-Trojaner zu verteilen (wobei am Rande vermerkt sei, dass die allgemein übliche Verkürzung des Begriffs «Trojanisches Pferd» zu «Trojaner» zu einer eigentlich völlig falschen Bezeichnung geführt hat. Schliesslich waren die Trojaner, also die Einwohner Trojas, die Angegriffenen und nicht die Angreifer).

Keine zwei Monate später sah sich dann das Bundesamt für Informatik und Telekommunikation gezwungen, 20min.ch vorübergehend zu sperren, um «das Risiko eines erfolgreichen Malware-Angriffs zu vermindern», weil das grösste Newsportal der Schweiz den E-Banking-Trojaner Gozi ISFB verbreitete. Die Rechner der 20min.ch-Besucher (Mobile-App-User waren nach Angaben des Unternehmens nicht betroffen) wurden per Drive-by-Download, also bereits beim einfachen Aufruf der Seite ohne weiteres Zutun der User, infiziert. Eine verseuchte Flash-Datei direkt im System von 20min.ch startete im Hintergrund ein manipuliertes Java-Script, das versuchte, Malware auf die Rechner der Besucher zu laden und dort auszuführen.

Noch während SWITCH-Sicherheitsexperten Interviews und Ratschläge zum Umgang mit Gozi gaben, wurde 20min.ch erneut Ziel eines Angriffs. «Bedep», ein Trojaner, der Hintertüren in Rechner installiert, damit diese von Hackern als Teil eines Botnets ferngesteuert werden können, wurde offenbar über ein kompromittiertes Werbenetzwerk auf die 20min.ch-Website gebracht.

Angesichts des Doppelschlags gegen 20min.ch wirkt es schon beinahe zynisch-paradox, dass das Portal ein Woche vor der ersten Angriffswelle die Leser aufgefordert hatte, Adblocker abzuschalten. Im Falle 20min.ch und aus der Perspektive der Finanzierung eines Gratismediums ist das verständlich. Wenn aber ein bekannter Technikverlag, der sich bis anhin sehr um Cyber-Security verdient gemacht hat, dazu auffordert, hinterlässt das doch ein gerüttelt Mass an Ratlosigkeit: Seit Neuestem bittet nämlich auch der Heise-Verlag Besucher von heise.de darum, installierte AdBlocker zu deaktivieren. Es bleibt nur zu hoffen, dass sich Heise zum 20. Geburtstag seiner News-Site damit nicht ein

Danaergeschenk gemacht und sich selbst als nächstes Angriffsziel für Gozi & Co. empfohlen hat.

Nachzulesen unter:

http://www.heise.de/newsticker/meldung/Schweizer-News-Site-verbreitet-Schadcode-Behoerden-und-Firmen-reagieren-3165287.html
http://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2015-12_de.pdf
https://securityblog.switch.ch/2016/02/10/attack-of-the-killer-ads
http://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident
http://www.inside-it.ch/articles/43486
http://www.tagesanzeiger.ch/digital/computer/ebankingtrojaner-gozi-das-raten-experten/story/13376685
http://www.watson.ch/!661270267
http://www.nzz.ch/digital/kampf-gegen-werbeblocker-klick-und-weg-ld.9431
http://www.heise.de/Adblocker-auf-heise-online-1164703.html

II. Heartbreak remote – Chipimplantate und die Sicherheit implantierter codegesteuerter medizinischer Geräte

«We are the Borg … We will add your biological and technological distinctiveness to our own. Your culture will adapt to service us. Resistance is futile.» Wurde die Erweiterung menschlicher Wesen durch Implantation von Geräten und Maschinen im Starg Trekg Film «First Contact» noch als Horrorszenario dargestellt, dem man sich trotz der Drohung, dass Widerstand vergeblich sei, entgegenstellen müsse, scheint das Thema «Augmented Humanity» bei vielen Menschen inzwischen auf Gegenliebe zu stossen. So schlossen in einer repräsentativen europaweiten Studie im Auftrag des Securityg Anbieters Kapersky lediglich 29% der Befragten kategorisch aus, sich ein Chipimplantat unter die Haut pflanzen zu lassen. Lediglich in Deutschland und in der Schweiz liegt der Anteil derer, die sich einem solchen Biohacking kategorisch verweigern, bei 49% oder höher. Per Near Field Communication (NFC) kontrollierte Chipimplantate zu Identifikationsg , Steuerungsg (Türöffner, Futterrationierung) oder medizinischen Zwecken sind bei Katzen, Hunden und anderen Hausg und Nutztieren ja bereits weit verbreitet. Dennoch zeigten sich die Autoren der Studie überrascht davon, wieviel Menschen dem Gedanken positiv gegenüberstehen, einen körpereigenen Minicomputer zu tragen, obwohl weder rechtliche, noch technische oder gar sicherheitstechnische Fragen geklärt sind. Dass Chipimplantate ausgelesen und mit Malware kompromittiert werden können, hat Kaspersky zusammen mit der schwedischen

Pro-Biohacking-Gruppe BioNyfiken in einem Feldversuch nachgewiesen. Auf diesem Weg könnten etwa Terroristen mit einer vom Chip gestohlenen Identität Zugang zu Flugzeugen erlangen – die Fluggesellschaft SAS bietet seit neuestem den bioimplantatgesteuerten Check-in an. Auch ist es denkbar, Herzschrittmacher oder Insulinpumpen zu manipulieren oder gar abzuschalten. Die kommunizieren zwar nicht via NFC, sondern über WLAN, dennoch stimmen u. a. die beeindruckenden Vorträge der Sicherheitsforscherin Marie Moe, die ohne ihren mit zwei WLAN-Schnittstellen ausgestatteten Herzschrittmacher nicht lebensfähig wäre, überaus nachdenklich.

Überhaupt scheint das Thema «Security» in der ICT-gestützten Medizin auch körperextern eher rudimentär behandelt zu werden. So warnte Ende März das Industriesteuerungs-CERT der US-Regierung vor dem automatischen Medikamenten-Verteilsystem Pyxis SupplyStation der Firma Carefusion. Sicherheitsexperten hatten zuvor 1418 (in Worten: eintausend-vierhundertachtzehn!) Sicherheitslücken gefunden, von denen 715 als hochprioritär, kritisch oder gar sehr kritisch eingestuft wurden. Viele davon seien einfach und teilweise auch per Fernzugriff auszunutzen.

Vielleicht sind digitale Bodyenhancer, die einem helfen, gesund zu bleiben und Spitalbesuche zu vermeiden, dann doch die bessere Lösung …

Nachzulesen unter:

http://www.kaspersky.com/de/about/news/allgemeine/2016/Chip_unter_der_Haut_29_Prozent_sagen_Nein
http://www.computerworld.ch/news/politik-gesellschaft/artikel/chip-implantate-werden-wir-alle-zu-cyborgs-nur-29-prozent-sagen-nein-69966
https://www.wa.de/hamm/cyborg-osttuennen-hamm-reckmann-chip-implantiert-testet-bio-hacking-6263352.html
http://www.bionyfiken.se/nfc-implantproject
http://www.oe24.at/digital/Herzschrittmacher-im-Visier-von-Hackern/225607394
https://www.youtube.com/watch?v=wAg-KJQ9ACA
http://www.heise.de/newsticker/meldung/Los-Hacker-brecht-mir-das-Herz-Sicherheit-von-vernetzter-Medizintechnik-auf-dem-Pruefstand-3145186.html
http://www.wired.com/2016/03/go-ahead-hackers-break-heart
http://www.heise.de/security/meldung/Automatisierte-Medikamenten-Verteiler-mit-ueber-1400-Sicherheitsluecken-3159439.html

III. One Point Three Million Dollar Phone – Im iPhone-Streit mit Apple hat das FBI viel Geld auf den Tisch gelegt, um das Telefon hacken zu lassen

Und noch ein Filmzitat zu Beginn eines Security-Themas: «Wie war ich, Boss?» – «Du warst gut!» Es stammt aus Clint Eastwoods Oscar-prämiertem Film «Million Dollar Baby». Deutlich mehr scheint das FBI ausgegeben zu haben, um im Fight mit Apple um das Entsperren des iPhone 5c des San Bernadino-Attentäters einen technischen K.O. zu erzwingen. Die Summe von mehr als 1,3 Millionen US-Dollar errechneten Journalisten aus den Angaben von FBI-Direktor James Coney auf einem Sicherheitsforum in London gemacht hatte, nachdem am 29. März bekannt geworden war, dass es von der US-Bundespolizei beauftragten professionellen Hackern gelungen war, das iPhone zu entsperren.

Während Regierungsbehörden Ende März verlauten liessen, dass für sie der wochenlange Streit damit ad acta gelegt sei, deuten aktuelle Entwicklungen darauf hin, dass sich diese Aussage wohl ausschliesslich auf den San-Bernardino-Fall bezogen hatte und Apples Befürchtungen, dass damit ein Präzedenzfall geschaffen werden sollte, real werden. Der iPhone-Konzern aus Cupertino hatte offiziell wie folgt Stellung genommen: «Apple glaubt fest daran, dass die Menschen in den USA und in der ganzen Welt ein Recht auf Datenschutz, Sicherheit und Privatsphäre haben. Das Eine für das Andere zu opfern, setzt Menschen nur noch größerer Gefahr aus.» Kurz darauf legte das US-Justizministerium klar: «Sicherzustellen, dass Strafverfolger Zugriff auf (…) entscheidende digitale Informationen bekommen, bleibt eine Priorität der Regierung, sei es durch die Kooperation mit den betreffenden Beteiligten oder durch die Gerichte, wenn die Kooperation nicht zustande kommt.» Apples Antwort ließ nicht lange auf sich warten: «Wir werden die Sicherheit unserer Produkte weiter verbessern, da die Bedrohungen und Angriffe auf unsere Daten regelmäßiger und ausgefeilter werden.»

Wie zum Beweis meldete heise.de bereits zwei Tage nach der «ad-acta»-Bekundung, dass das FBI seine Entsperrmethode auch anderen staatlichen Ermittlern, Staatsanwälten und Behörden anbietet. Am 2. April, also wiederum zwei Tage später, zitierte die Nachrichtenagentur Reuters einen landesweit verschickten Brief des FBI, in dem dieses seinen Partnern anbietet, Mobilgeräte

nicht nur von nachweislichen Verbrechern, sondern auch von Verdächtigen zu entsperren, soweit dies mit Gesetz und Politik vereinbar sei.

Während sich Apple nach wie vor weigert, die eigenen Telefone zu hacken, zeigt sich das Unternehmen bei der Beantwortung von Anfragen der Sicherheitsbehörden nach Offenlegung persönlicher Daten kooperativer, zumindest solange diese Anfragen mit einem gültigen Durchsuchungsbeschluss belegt und von Apples Juristen geprüft und gutgeheissen worden seien. So berichtete die deutsche Tagesschau am 19. April 2016, dass Apple im 2. Halbjahr 2015 ca. 31.000 Anfragen für mehr als 167.000 Geräte erhalten hatte. Die meisten davon stammten aus – Deutschland! Allerdings ging es mehrheitlich um die Herausgabe von Name und Adresse der Besitzer gestohlener oder verlorener Geräte. Die Zahl der Anfragen zu Nutzerkonten oder gar Daten, die auf den Geräten lagerten, sei deutlich niedriger. Zudem beteuert Apple: «Wir geben nur Daten heraus, wenn wir uns vergewissert haben, dass die Anfrage angemessen ist, und wir geben nur das Allernötigste heraus.» Mittlerweile hat auch der bei Jugendlichen führende Kurznachrichtendienst WhatsApp angekündigt, per sofort alle Nachrichten mit einer Ende-zu-Ende-Verschlüsselung für Dritte unlesbar zu machen. Nach dem Update sei es WhatsApp auch nicht mehr möglich, Daten an Sicherheitsbehörden weiterzugeben.

Verena Luekens Filmkritik zu Million-Dollar-Baby aus der Frankfurter Allgemeinen vom 24.03.2005 passt als Kommentar dazu wie die sprichwörtliche Faust aufs Auge: «Dieser Rahmen … ermöglicht ein Ende, das dunkel ist, aber vielleicht nicht ganz hoffnungslos.»

Nachzulesen unter:

http://www.dw.com/de/fbi-zahlt-13-millionen-dollar-für-iphone-entschlüsselung/a-19207258
http://www.computerworld.ch/news/it-branche/artikel/was-das-fbi-fuer-das-hacken-des-iphones-bezahlen-musste-70072/
http://www.zeit.de/digital/datenschutz/2016-03/apple-versus-fbi-iphone-geknackt-analyse
http://www.heise.de/newsticker/meldung/Entsperrhack-FBI-will-weitere-iPhones-und-iPods-knacken-3159476.html
http://www.reuters.com/article/us-apple-encryption-letter-idUSKCN0WZ055
http://www.tagesschau.de/wirtschaft/apple-daten-sicherheit-101.html
http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/mehr-sicherheit-whatsapp-will-alle-daten-verschluesseln-14162785.html
http://www.faz.net/aktuell/feuilleton/kino/video-filmkritiken/kino-ein-klassiker-clint-eastwoods-million-dollar-baby-1105370.html

IV. Sieht nicht nur hässlich aus, sondern ist es auch: «Jigsaw» verbreitet wieder Horror – diesmal in digitaler Version

Der 2004 ins Kino gekommene amerikanische Psycho-Horrorfilm «Saw» war einer der erfolgreichsten seines Genres überhaupt. Darin setzt der «Jigsaw Killer» oder kurz «Jigsaw» genannte Protagonist Menschen, die in seinen Augen ihr Leben als Selbstverständlichkeit erachten, zynisch-grausamen Tests aus, damit diese seinen wahren Wert schätzen lernen. Der Doppelmotivation aus «Reich werden» und «Menschen den wahren Wert elementarer Dinge ihres Lebens lehren» sind nun auch Cybererpresser gefolgt. Via Malvertising oder kompromittierter «Adult-Sites» verbreiten sie einen wirklich bösartigen Erpressungstrojaner, der nicht nur Dateien verschlüsselt, sondern jede Stunde in zeitabhängig steigender Anzahl Dateien löscht, bis die Besitzer befallener Rechner das geforderte Lösegeld von 0,4 Bitcoins (ca. 160 Franken) bezahlen. Ist das Lösegeld binnen 72 Stunden nicht bezahlt, löscht Jigsaw alle Dateien auf dem befallenen Rechner – und es erscheint auch noch die Fratze der Horror-Puppe Billy aus dem eingangs zitierten Film. Zwar findet sich unter dem unten angegebenen heise.de-Link ein Entschlüsselungstool für Jigsaw, doch ist diese Ransomware nur ein Beispiel dafür, dass immer mehr und immer aggressivere Krypto-Trojaner in Umlauf sind. Den besten Schutz vor den Folgen von Erpresser-Trojanern bietet nach wie vor eine durchdachte, systematisch angelegte Backup-Strategie, bei der am besten mehrere Backups auf entkoppelten Speichermedien angelegt werden.

Nachzulesen unter:

http://www.heise.de/security/meldung/Nur-72-Stunden-Erpressungs-Trojaner-Jigsaw-droht-Dateien-zu-loeschen-3172217.html
http://blog.trendmicro.de/neue-crypto-ransomware-jigsaw-spielt-fiese-spiele
http://www.n-tv.de/technik/Jigsaw-zerstoert-stuendlich-mehr-Dateien-article17515046.html
https://www.basicthinking.de/blog/2016/04/20/krypto-trojaner
http://www.nzz.ch/digital/trojaner-toolkit-spyeye-urteil-gegen-hacker-ld.15545
https://id-ransomware.malwarehunterteam.com
https://objective-see.com/products/ransomwhere.html

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