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

September 2014

SWITCH

I. Gehackt, gezwitschert und aufgeflogen: Interna über international eingesetzten Staatstrojaner auf Twitter veröffentlicht

Die weltweit tätige Gamma Group steht seit längerem in der Kritik, weil ihre als «Staatstrojaner» bezeichnete Spionagesoftware-Suite FinFisher und vor allem das Überwachungstool FinFisher FinSpy, an dessen Entwicklung die schweizerische Dreamlab Technologies AG massgeblich beteiligt war, auch in demokratiefernen und autokratischen Staaten zur Überwachung Oppositioneller eingesetzt wird. Nun ist ein Unternehmen der Gruppe, die FinFisher GmbH in München, offenbar gehackt worden: Seit Anfang August werden detaillierte Preislisten, Handbücher und Quellcodes einzelner Programme der Suite über den Twitter-Account «@GammaGroupPR» veröffentlicht. Zwar ist die Echtheit der Dokumente bis dato nicht offiziell bestätigt, doch behauptet das Netz-News-Portal NETZPOLITIK.ORG, diese verifiziert zu haben.

Als gesichert gilt indes, dass das deutsche Kriminalamt (BKA) FinFisher als «Übergangslösung» einsetzt. Die Arbeiten an einem sogenannten kleinen Bundestrojaner zur Quellen-Telekommunikationsüberwachung verzögern sich aufgrund von Auflagen des Bundesverfassungsgerichts aus dem Jahr 2008. Während im Rahmen der

Quellen-TKÜ nur einzelne VoIP-Kommunikationsvorgänge, wie z.B. etwa Skype-Telefonie oder Messenger-Dienste, belauscht werden, durchforstet der einsatzbereite «grosse» Bundestrojaner des BKA bei der Online-Durchsuchung alle Inhalte eines Zielrechners.

In der Schweiz verzichtet die Bundeskriminalpolizei gemäss eigenen Angaben nach massiver Expertenkritik an bis dahin erfolgten Einsätzen seit 2011 auf die Verwendung von Trojanern – zumindest bis zur grundlegenden Revision des BÜPF (Bundesgesetz betreffend die Überwachung von Post- und Fernmeldeverkehr). Mitte August hatte die Rechtskommission des Nationalrats die Beratung auf das nächste Quartal vertagt. Der Vorschlag kommt also frühestens in der Wintersession ins Ratsplenum.

Nachzulesen unter:

http://t3n.de/news/finfisher-staatstrojaner-gamma-international-561277

https://netzpolitik.org/2014/grosser-bundestrojaner-inzwischen-einsatzbereit-kleiner-bundestrojaner-wird-noch-eine-zeitlang-ausprobiert

http://www.tagesanzeiger.ch/schweiz/standard/Dein-Freund-und-Hacker/story/22064216

http://www.nzz.ch/schweiz/nationalratskommission-kritisch-gegenueber-buepf-1.18363983

II. Kein Anschluss unter dieser Nummer: Netzsperren in der Schweiz und Nachbarländern

Während das Oberlandesgericht Köln noch im Juni entschieden hatte, dass Internetprovider nicht dazu verpflichtet seien, Netzsperren für Angebote einzurichten, die Links auf widerrechtlich angebotene urheberrechtlich geschützte Inhalte enthalten, wurden in der letzten Augustwoche die vier grossen österreichischen Internetprovider A1, Tele2, Drei und UPC vom Verein für Antipiraterie (VAP) darauf verklagt, die Webseiten der zwei Torrent-Portale kinox.to und movie4k.to. zu sperren. Es wird erwartet, dass in Kürze der österreichische Musikverband IFPI nachlegen und Klage zur Sperrung der Portale thepiratebay.se, isohunt.to, 1337x.to und h33t.to einreichen wird. Da über diese Portale auch legale Inhalte gefunden werden können, dürfte sich jedoch die Abwägung zwischen der Verletzung von Urheberrechten einerseits und dem Recht auf Informationszugang andererseits bei diesen Webseiten weit schwieriger gestalten.

Die von den Klägern geforderte Kombination aus DNS- und IP-Blocking könnte ausserdem schnell zum «Overblocking» führen.

Dennoch empfiehlt auch die Schweizer Arbeitsgruppe zum Urheberrecht (AGUR12) in ihrem Ende 2013 veröffentlichten Schlussbericht Netzsperren zur Durchsetzung des Urheberrechts im schweizerischen Internet.

Mehr Netzsperren wird es künftig in Frankreich geben, wenn auch nicht zum Schutz des Urheberrechts, sondern zur Terrorabwehr. So sieht der Entwurf eines neuen Anti-Terrorismus-Gesetzes, das noch diesen Monat verabschiedet werden soll, vor, dass z.B. Seiten mit Bombenbauplänen und anderen terroristischen Inhalten gesperrt werden.

Siehe:

http://futurezone.at/netzpolitik/netzsperren-klagen-bei-vier-providern-eingetroffen/82.780.541

http://www.heise.de/newsticker/meldung/OLG-Koeln-Provider-nicht-zu-Netzsperren-gegen-widerrechtliche-Angebote-verpflichtet-2292330.html

https://www.digitale-gesellschaft.ch/tag/netzsperren

https://netzpolitik.org/2014/neuer-anti-terrorismus-gesetzentwurf-in-frankreich-weitet-netzsperren-aus

III. Breaking Bad – Malvertising Ransomware: Zerolocker/Cryptolocker/Cryptowall/Synolocker

„Long gone are the days when you had to be browsing shady areas of the net to stumble across something malicious.“ So kommentiert der Sicherheitsexperte Graham Cluley in seinem Blog die aktuelle Entwicklung und Verbreitung von digitaler Erpressung via Malware. Oft reicht ein Klick auf ein Werbebanner, um sich bösartige Überraschungen mit Namen wie Zerolocker, Cryptolocker, Cryptowall oder Synolocker einzufangen. Diese verschlüsseln vordefinierte oder schlichtweg alle Dateien auf dem befallenen Rechner – bzw. im Falle des Synolockers auf Synology-Massenspeichern – und fordern den Benutzer auf, binnen weniger Tage die Daten mittels eines Schlüssels aus der digitalen Geiselhaft zu befreien. Dabei steigen die Preise für den Schlüssel mit fortlaufender Zahlungsfrist exponentiell an. Die Zahlung kann oft ausschliesslich in digitalen Währungen wie Bitcoins erfolgen und beginnt bei Summen von etwa 300 USD. Während bei einem Cryptowall-Befall nach Kauf des Schlüssels die Daten tatsächlich freigegeben werden, ist z.B. beim Zerolocker aufgrund eines Programmfehlers die Wiederherstellung der Daten nicht sichergestellt. Sicherheitsexperten und Strafver-

folger raten in jedem Fall von einer Zahlung ab und empfehlen im Schadensfall die Wiederherstellung via Backups oder wenn möglich das Nutzen von Services wie Decryptcryptolocker. Zur Prophylaxe werden aktuelle Sicherheitssoftware und sichere Backup-Systeme dringend empfohlen.

Mehr dazu:

http://www.zdnet.de/88202879/kaspersky-warnt-vor-neuer-erpresser-malware-zerolocker

http://grahamcluley.com/2014/08/yahoo-cryptowall

https://www.decryptcryptolocker.com/

http://community.spiceworks.com/how_to/show/85802-how-to-recover-files-from-cryptowall-ransomeware-infection

IV. Canvas oder Cookies – die Wahl zwischen Skylla und Charybdis

Wer seinem Browser das Speichern von Cookies untersagt, ist bekanntlich noch lange nicht davor gefeit, getrackt zu werden. Denn es gibt eine ganze Reihe anderer Techniken, um Browsern möglichst eindeutige Fingerabdrücke abzunehmen. Eine relativ neue Trackingtechnik ist das sogenannte Canvas-Fingerprinting. Ein Canvas ist ein Webseitenelement, mit dem es möglich ist, Grafiken mit Hilfe von JavaScript dynamisch zu erzeugen. Beim Fingerprinting können nun minimale Unterschiede jeder einzelnen Browser-Installation beim Erstellen von Canvas-Elementen als eindeutiger Zahlencode ermittelt werden. Dienste wie der Bookmarker AddThis, aber auch viele andere bekannte Webseiten, nutzen dieses Tracking bereits – in der Regel ohne die Besucher darüber zu informieren. Kaum zu überbieten ist die Dreistigkeit von AddThis, wenn der «Trackie» Usern zum Schutz vor seiner Technologie ein Opt-Out-Cookie anbietet, das aber nur funktioniert, wenn der Browser Cookies zulässt. Wirksameren Schutz versprechen dagegen das Deaktivieren von JavaScript – mit dem entsprechenden Verlust an Funktionalität - oder Tools wie NoScript.

Nachzulesen unter:

http://www.spiegel.de/netzwelt/web/canvas-fingerprinting-macht-internetnutzung-nachverfolgbar-a-982280.html

http://www.chip.de/news/Canvas-Fingerprinting-Adblock-Plus-stoppt-Tracking_71140183.html

https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

https://sites.google.com/a/chromium.org/dev/Home/chromium-security/client-identification-mechanisms

Zum Stöbern: spannende Präsentationen, Artikel und Videos

Konstantinos Karagiannis ist Security-Spezialist im Banken- und Finanzumfeld. In seinem Talk auf der letzten DeepSec-Konferenz behandelte er ein breites Themenspektrum, angefangen von den wahren Risiken der Username-Enumeration, über Sicherheitsprobleme im Hochfrequenzhandel bis hin zum Quantencomputer, der vielleicht noch in diesem Jahrzehnt alles verändern wird:

http://blog.deepsec.net/?p=1790

Bruce Schneier – neuerdings Chief Technology Officer von Co3 Systems – hat auf der BlackHat über die Herausforderungen bei der Incident Response berichtet. Ebenfalls interessant ist sein Interview im Securityadvisor Alliance-Podcast zum gleichen Thema:

https://www.youtube.com/watch?v=u54Radu2bFO&list=UUJ6q9le29ajGqKApbLqfBOg:

http://securityadvisoralliance.libsyn.com/11-security-advisor-alliance-ep11-ir-redux

Das National Institute of Standards and Technology (NIST) hat ein Draft mit dem Titel "Security of Automated Access Management Using Secure Shell," veröffentlicht. Dabei geht es um die Risiken eines schlechten oder nicht vorhandenen SSH-Key-Managements in Unternehmen:

http://www.bankinfosecurity.com/ssh-keys-managing-risks-a-7248

http://csrc.nist.gov/publications/drafts/nistir-7966/nistir_7966_draft.pdf

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