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

Juli / August 2017

SWITCH

I. Family Business: Petya und seine Abkömmlinge rollen als neue Ransomware-Welle um den halben Globus

Keine zwei Monate nach der globalen Attacke des Erpressungstrojaners WannaCry und seiner Abkömmlinge rollt eine zweite Ransomware-Welle um den halben Globus. Sicherheitsforscher gingen zunächst davon aus, dass es sich um einen weiteren Abkömmling des erstmals 2016 aktiven Cryptolockers Petya handelte. Dessen vier Varianten – insbesondere unterscheidbar an der Farbe der Totenköpfe auf den befallenen Monitoren – und die mit ihnen verwandten Ransomware-Abkömmlinge Goldeneye und Mischa befielen vor allem 2016 via E-Mail-verschickter gefakter pdf-Dateien einige Rechner und verschlüsselten deren Festplattenverzeichnis und/oder Dateien auf den kompromittierten Geräten (eine detaillierte Zusammenfassung findet sich u.a. auf wikipedia). Die als Urheber vermutete Hackergruppe Janus Cybercrime veröffentlichte am 5. Juli einen als echt bestätigten Masterschlüssel, mit der Daten und Festplatten, die von Petya, Mischa oder Goldeneye befallen waren, wieder zugänglich sind.

Kurz nach dem Ausbruch des vermeintlichen neuen Petya-Ablegers Ende Juni verwiesen aber mehrere Sicherheitsforscher darauf, dass der nunmehr NotPetya

getaufte neue Schädling eine völlig neue Qualität aufwies, die mit den Erpressungstrojanern der Petya-Familie nur wenige «Gemeinsamkeiten» hatte. NotPetya ist offenbar nicht auf Geld aus, sondern auf die völlige Zerstörung der Daten auf den kompromittierten Geräten, ist also kein Erpressungstrojaner, sondern ein so genannter «Wiper». Nach tieferer Analyse der Schäden muss davon ausgegangen werden, dass die Autoren der Ransomware die Daten nicht wiederherstellen können, auch wenn Lösegeld gezahlt werden würde. Die meisten Experten vermuten daher hinter NotPetya eher politische Motive anstelle von Geldgier. Auch kommt NotPetya nicht via Phishingmail oder E-Mail-Anhang auf die Rechner, sondern war in Softwareupdates einer in der Ukraine von zahlreichen Steuerzahlern genutzten Software eingeschleust. Allerdings wollen einige Forscher auch nicht ausschliessen, dass die NotPetya-Urheber schlichtweg geschlampt haben.

Nachzulesen unter:

https://de.wikipedia.org/wiki/Petya
https://www.heise.de/security/meldung/Rueckkehr-von-Petya-Kryptotrojaner-legt-weltweit-Firmen-und-Behoerden-lahm-3757047.html
https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware
https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
https://www.heise.de/security/meldung/Alles-was-wir-bisher-ueber-den-Petya-NotPetya-Ausbruch-wissen-3757607.html?artikelseite=3
https://www.heise.de/security/meldung/Master-Schluessel-der-Erpressungstrojaner-GoldenEye-Mischa-und-Petya-veroeffentlicht-3767637.html
https://www.heise.de/security/meldung/Petya-NotPetya-Kein-Erpressungstrojaner-sondern-ein-Wiper-3759293.htm
https://www.netzwelt.de/news/160887-keylogger-hp-notebook-hersteller-veroeffentlicht-statement.html

II. Lösegeld zahlen, um nichts zu sehen: «Extortionware» entblösst ihre Opfer und ist auf dem Vormarsch

Auch im Cyberspace gibt es nichts, was es nicht gibt. Auf der einen Seiten fordern Erpressungstrojaner wie WannaCry, Petya & Co. von den Usern befallener Geräte Lösegeld, damit diese ihre Daten wieder sehen können. Andererseits drohen neuerdings die Autoren von «LeakerLocker» damit, alle Daten auf kompromittierten Android-Smartphones und -Tablets zu vervielfältigen und an alle im Gerät gefundenen Kontakte zu senden, falls die Nutzer die geforderten 50 US-Dollar Lösegeld in Bitcoins nicht bezahlen. Die Ransomware mit dem «innovativen Geschäftsmodell» droht, Browserverlauf, Fotos, E-Mails und Facebooknachrichten offenzulegen. Dass sie dies nur in Ansätzen kann, haben ihre Entdecker, Sicherheitsforscher von McAfee, im unten verlinkten Factsheet nachgewiesen. Zudem hat Google die beiden Apps, unter deren Deckmantel sich die Ransomware auf die Devices geschlichen hatte (Booster & Cleaner Pro sowie Wallpapers Blur HD), inzwischen aus dem Play Store entfernt.

Dennoch sehen auch andere Security-Experten die Entwicklung mit Sorge und befürchten, dass «LeakerLocker» angesichts des enormen Potenzials für «Entblössungs-Ransomware» erst der schüchterne Anfang für weitere Angriffsszenarien sein könnte.

Nachzulesen unter:

https://futurezone.at/digital-life/ransomware-droht-browserverlauf-an-alle-kontakte-zu-senden/274.616.209
https://securingtomorrow.mcafee.com/mcafee-labs/leakerlocker-mobile-ransomware-acts-without-encryption
https://www.infosecurity-magazine.com/news/leakerlocker-extortionware
https://www.hackread.com/leakerlocker-android-ransomware-pay-or-data-leak
http://www.independent.co.uk/life-style/gadgets-and-tech/news/leakerlocker-malware-leaked-photos-ransom-pictures-internet-history-messages-privacy-security-send-a7838836.html

III. Metadaten positiv genutzt – Cisco kann Malware-Traffic auch in verschlüsseltem Netzwerk-Verkehr erkennen

Im letzten SWITCHcert Report hatten wir dargestellt, wie Metadaten dazu genutzt werden, Internet-Nutzer zu deanonymisieren, um ihre Profile zu Werbezwecken einzusetzen bzw. zu verkaufen. Dass Metadaten auch positiven Zwecken dienen können, haben nun die drei Cisco-Mitarbeiter Blake Anderson, Subharthi Paul und David McGrew in einer Forschungsarbeit gezeigt. Diese weist einen möglichen Weg auf, Malware auch dann zu erkennen, wenn sie sich hinter Verschlüsselungsprotokollen versteckt, wie z.B. hinter TLS (dem Nachfolger des bekannten SSL-Protokolls für sichere Datenübertragung im Internet).

Anderson und seinen Mitautoren ist es gelungen, ein Machine-Learning-System so zu trainieren, dass es den Netzverkehr, den Malware verursacht, mit einer Verlässlichkeit von über 99 Prozent von legitimen Datenflüssen unterscheiden konnte – und zwar ohne die TLS-Verschlüsselung aufzubrechen. Statt dessen fokussierte das System hauptsächlich auf die Metadaten, die auch bei verschlüsseltem Verkehr anfallen, so unter anderem auf Netflow-Daten (Ports, Bytes In/Out, Dauer usw.), typische Paketlängen (Sequence of Packet Lengths and Times, SPLT), die Byte-Verteilung und vor allem unverschlüsselte TLS-Header-Daten.

Auch wenn die Forscher in ihrer Arbeit (zum Nachlesen: 1. Quellenlink unten) gleich selbst ein Beispiel dafür liefern, dass sich diese Erkennung umgehen lässt, bleibt doch die Erkenntnis, dass es zum datenschutzrechtlich wie auch sicherheitstechnisch bedenklichem Aufbrechen von Verschlüsselungsprotokollen Alternativen geben könnte, die es allemal wert wären, näher erforscht zu werden.

Nachzulesen unter:

https://arxiv.org/pdf/1607.01639.pdf
https://www.heise.de/security/artikel/Cisco-analysiert-verschluesselten-Traffic-um-Malware-zu-erkennen-3753229.htm
http://cloud-practice.de/hintergrund-cisco-analysiert-verschlusselten-traffic-um-malware-zu-erkennen

IV. Erfolgreicher Schlag gegen Waffen- und Drogenhandel im Darknet – Sicherheitsbehörden heben AlphaBay und Hansa aus

Ohne das Aufbrechen von Verschlüsselungen wäre wohl einer der spektakulärsten Ermittlungserfolge internationaler Sicherheitsbehörden im Darknet nicht möglich gewesen: Im Juli meldeten das FBI, Europol und die Staatsanwaltschaft Frankfurt, dass sie in eng koordinierter internationaler Zusammenarbeit u.a. mit kanadischen, französischen, thailändischen und litauischen Ermittlern mit AlphaBay und Hansa zwei Handelsplattformen für harte Drogen, Waffen, Falschgeld oder gefälschte Ausweispapiere, Malware und gehackte Daten für Kreditkarten und Internet-Konten stillgelegt und deren Betreiber verhaftet hätten. Mit mehr als 40.000 Händlern, 200.000 Kunden und Tagesumsätzen im hohen sechs-stelligen Bereich galt vor allem AlphaBay als bedeutendster Umschlagplatz für illegale Waren und Dienstleistungen im Darknet.

So positiv die Nachricht über die Zerschlagung von AlphaBay und Hansa auch ist, gibt es doch auch eine schmerzhafte Ambivalenz. Denn das Darknet bietet eben nicht nur Kriminellen, Terroristen, Cyber-Erpressern und anderen Bösen vermeintlich sicheres Terrain. Vielmehr ist es oft der einzige Rückzugsraum für Oppositionelle, Dissidenten, Journalisten oder Whistleblower in Diktaturen oder Schurkenstaaten. In der Netzdebatte zur Risikogesellschaft der deutschen Bundeszentrale für politische Bildung bezeichnet Christian Mihr, Geschäftsführer von Reporter ohne Grenzen, Orte digitaler Anonymität gar als essenziell für demokratische Gesellschaften. Unter anderem spiegeln sowohl Facebook als auch netzpolitik.org ihre Inhalte auf .onion-Seiten, um Menschen in repressiven Staaten den anonymisierten Zugang zu den dort verfügbaren Informationen zu verschaffen. In der gleichen Netzdebatte fordert der Direktor des Zentrums für Europäische und Internationale Strafrechtsstudien an der Universität Osnabrück mit Blick auf den Schutzleistung des Darknets für schlimmste Verbrechen und Verbrecher die Entschlüsselung des Darknets. Und offenbar werden Sicherheits- und Nachrichtendienste darin inzwischen immer besser. Das ist gut, wenn es darum geht, den Bösen das Handwerk zu legen, ist aber schlecht für die schutzbedürftigen Guten, die damit ihre letzten Rückzugsräume verlieren.

Nachzulesen unter:

https://www.nzz.ch/digital/aktuelle-themen/erfolg-im-bereich-cyber-crime-gegluckte-ermittlung-gegen-darknet-struktur-ld.1307107
http://www.sueddeutsche.de/digital/alpha-bay-ermittler-heben-groessten-illegalen-darknet-marktplatz-aus-1.3597381
http://www.chip.de/news/AlphaBay-Portal-Betreiber-haeufte-im-Darknet-gigantisches-Vermoegen-an_119390997.html
https://www.bpb.de/dialog/netzdebatte/239003/das-darknet-als-geschuetzter-raum-gegen-ueberwachung-und-selbstzensur
https://www.bpb.de/dialog/netzdebatte/242957/das-darknet-ein-paradies-fuer-kriminelle
https://motherboard.vice.com/de/article/d7yakj/bundesregierung-versucht-das-darknet-zu-erklaeren-und-zeigt-wie-kompliziert-das-alles-eigentlich-ist

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs 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.