2017/21 Lifestyle

https://jungle.world/artikel/2017/21/orange-new-hack

Wie Hacker versuchten, Netflix und andere Unternehmen zu erpressen

Orange Is the New Hack

Von **Elke Wittich**

Mit Hilfe sogenannter Ransomware verlangen Hacker Lösegeld für von ihnen erbeutete Daten. Auch die Erpressungssoftware »Wannacry« funktioniert so. Betroffen sind verschiedene Firmen.

Millionenverluste und dazu noch schlechte Chancen, dringend benötigte neue Abonnenten zu bekommen: Netflix stehe vor großen Problemen, da waren sich eine Menge Kommentatoren sicher, unmittelbar nachdem bekannt geworden war, dass die neue Staffel der Serie »Orange Is the New Black« gehackt wurde. Die Serie ist schließlich weltweit ein Hit und bisher hatten die neuen Folgen regelmäßig für Zigtausend neue Kundinnen und Kunden des Streamingdienstes gesorgt. Die bei der Postproduktionsfirma Larson gestohlenen Folgen wurden nach und nach tatsächlich bei Pirate Bay veröffentlicht, allerdings nur zehn der insgesamt 13 Folgen, weil das Unternehmen mit der Bearbeitung der gesamten Staffel noch nicht fertig war.

> The Dark Overlord versuchte, Netflix zu erpressen. Ohne Erfolg, der Sender erklärte, bereits im Februar, das FBI eingeschaltet zu haben.

Als verantwortlich für das vorzeitige Erscheinen der neuen Folgen gilt die Hackergruppe The Dark Overlord (TDO), ein Name, der zum ersten Mal im Sommer vergangenen Jahres bekannt wurde. Vor acht Monaten berichtete der Computersicherheitsexperte Graham Clueley auf hotforsecurity.bitdefender.com, dass TDO »eine neue Ära der Online-Erpressung eingeläutet« habe. Im Gegensatz zu sogenannter Ransomware wie »Wannacry«, mit der Computer und Datenbanken verschlüsselt und gegen Zahlung wieder entschlüsselt werden, oder DDoS-Attacken, die erst dann enden, wenn die Betroffenen zahlen, stellt TDO die betroffenen Unternehmen oder Institutionen vor die Wahl: Entweder bezahlen sie die geforderte Summe in Bitcoins oder die Daten werden veröffentlicht und sorgen für einen unabsehbar großen Imageschaden.

Zum ersten Mal hatte TDO im Juni 2016 mit dem Diebstahl von rund 600 000 Patientenakten und neun Millionen Datensätzen von Krankenversicherten in den USA von sich reden gemacht. Damals rätselten Experten noch, was die Hacker mit den erbeuteten Informationen überhaupt anfangen könnten. Manche gingen davon aus, dass es sich um Identitätsdiebstähle handeln könnte, die zum Beispiel für Versicherungs- oder Kreditbetrug nutzbar wären. Eine andere Vermutung war, dass die Daten für Bestellungen von Luxuswaren im Versandhandel genutzt

werden könnten. Gleichzeitig wunderte man sich über den hohen Preis, zu dem die Hacker-Beute im Darknet angeboten wurde, 750 Bitcoins, damals fast 450 000 Dollar, verlangte TDO.

Kurz darauf wurde allerdings klar, dass die Daten nur zum Schein offeriert wurden. Das eigentliche Ziel von TDO war eine auf Dauer angelegte Erpressung der betroffenen Unternehmen, denen angedroht wurde, ihre Namen und die persönlichen Daten ihrer Kunden zu veröffentlichen. Eine Stellungnahme der Hacker machte klar, dass dies noch lange nicht das Ende ihrer Aktivitäten sein würde: »Das nächste Mal, wenn euer Gegner euch eine Möglichkeit anbietet, das Ganze zu vertuschen und gegen eine kleine Gebühr das Leak zu verhindern, nehmt dieses Angebot an. Es wird noch viel mehr folgen.« Für die betroffenen Unternehmen war eine schwierige Situation entstanden, denn sie hatten nur die Wahl, Ärger mit ihren Kunden zu riskieren oder zu zahlen und sich damit als künftiges Opfer zu qualifizieren.

Hatte es zunächst noch so ausgesehen, dass TDO sich auf Datendiebstahl im Gesundheitsbereich spezialisiert hatte, wurde im späteren Verlauf des Sommers 2016 klar, dass auch andere Unternehmen sich nicht vor den Erpressern sicher fühlen konnten. WestPark Capital, einer Investmentbank aus Los Angeles, wurden etwa interne Dokumente gestohlen – und online veröffentlicht, nachdem sie das »attraktive Geschäftsangebot« zurückgewiesen hatte. Es folgten weitere Unternehmen aus ganz unterschiedlichen Branchen, der Datendiebstahl bei Pre-Con Products wurde von TDO politisch begründet: Die Firma sei »eine interessante Wahl« gewesen, weil sie an »interessanten Projekten im Zusammenhang mit der US Navy« arbeite. Dazu gehöre eine Website für Luftüberwachungsradar. Warum das für die Hacker so interessant war, ist unklar. Das Unternehmen scheint allerdings auf die Erpressung nicht eingegangen zu sein, denn Ende 2016 wurden die erbeuteten Daten ebenso wie die anderer Firmen veröffentlicht.

Natürlich lässt sich nicht sagen, wie viele weitere Opfer von TDO es gibt, die sehr wohl Zigtausende Dollar in Bitcoins zahlten und es dadurch vermieden, in die Schlagzeilen zu geraten. Auf genau die scheint es TDO jedoch anzukommen, denn Ende des Jahres wandte sich die Gruppe, die durchaus nur die Tarnung für einen Einzeltäter sein kann, einem ganz neuen Geschäftsfeld zu: Erpressung mit der Drohung, neue Hollywood-Produktionen zu veröffentlichen. TDO hatte das auf Internetsicherheit spezialisierten Blog databreaches.net bereits am 26. Dezember darüber informiert, im Besitz Hunderter Gigabytes unveröffentlichter Hollywood-Produktionen zu sein. Unter den 37 von TDO aufgeführten Titeln befanden sich die 5. Staffel von »Orange Is the New Black« und die neue Netflix-Wissenschaftssserie »Billy Nye Saves the World«. Nachdem die Firma Larson kein Lösegeld hatte zahlen wollen, versuchte TDO, Netflix zu erpressen. Ohne Erfolg: Der Sender teilte bereits im Februar mit, das FBI eingeschaltet zu haben. Die Hacker reagierten pampig: »Wir wandten uns an Netflix und andere in einem Versuch, ein Arrangement zum gegenseitigen Nutzen zu finden, bei dem wir bezahlt werden und Netflix und seine Freunde nicht irgendwann aufwachen und das Ergebnis ihrer harten Arbeit überall im Internet verteilt vorfinden.« Alle Vorschläge seien jedoch unbeantwortet geblieben. »Wir waren sehr beleidigt über die Antworten unsere Zielobjekte (beziehungsweise über deren Ausbleiben)«, hieß es weiter.

Am 29. April meldete sich TDO erneut mit einem Pastebin-Posting: »Wir sind noch nicht ganz fertig«, es würden zehn Folgen der Netflix-Serie veröffentlicht. Die Sender ABC, Fox, National Geographic, IFC und »immer noch Netflix« müssten im Übrigen als Nächste mit der Veröffentlichung ihrer Produktionen rechnen. Ganz durchdacht scheinen die

Erpressungsversuche mit Filmen und Serien nicht zu sein, denn zu nennenswerter Empörung und größeren Imageschäden führt deren vorzeitige Veröffentlichung nicht. Außerdem hatte TDO im Falle von »Orange Is the New Black« Zeitungsberichten zufolge technisch miese Versionen der Folgen erwischt, so dass das Anschauen der illegal heruntergeladenen Staffel kein großes Vergnügen ist. Databreaches.net ist sich ziemlich sicher, dass die Hacker lieber das Geld gehabt hätten, als Menschen kostenlos deren Lieblingsserie zur Verfügung zu stellen.

Dass TDO immer wieder über verschlüsselte Chats mit databreaches.net kommuniziert, ist interessant, denn dort hatte man bereits im Dezember 2016 davor gewarnt, TDO versuche ganz gezielt, die Medien zu instrumentalisieren. Die Datendumps gehörten zur Selbstinszenierung, warnte unter anderem databreaches.net: »Sie benutzen die Medien, um sich als gefährliche Hacker darzustellen, die ihre Drohungen wahrmachen.« Zukünftigen Opfern solle damit demonstriert werden, was passiert, wenn sie nicht zahlen.

Aber wie sollten Medien mit den Datenveröffentlichungen umgehen? Während Graham Clueye bereits im November 2016 Gründe auflistete, warum man das Spiel von TDO nicht mehr mitspielen und deswegen auch keinesfalls die gehackten Informationen downloaden und darüber berichten sollte, sieht databreaches.net dies nicht als erfolgversprechende Strategie. Mediales Schweigen verhindere, dass die Öffentlichkeit, Politiker und Sicherheitsexperten auf die Hacks aufmerksam würden. Daher solle und werde man weiter berichten, allerdings das angebotene Material nicht anrühren. TDO macht derzeit weiter mit der Veröffentlichung von Akten, die bei Kliniken und Praxen in den USA gestohlen wurden. Der ganz große Beifall bleibt aber aus, was vielleicht auch daran liegt, dass die Securityblogs deutliche Worte fanden: »Möchtet ihr wirklich Leuten zujubeln, die private Patienteninformationen hacken und anschließend Kliniken erpressen, damit diese Daten nicht an die Öffentlichkeit gelangen? Sind das wirklich eure Helden?« Wahrscheinlich hätte es dieses Appells nicht einmal bedurft: Die Tweets, in denen TDO stolz seine Dumps vermeldet, wurden durchschnittlich von 25 Leuten geliked. Und der Ersatzaccount, den TDO schon vor einiger Zeit für den Fall eingerichtet hat, dass der eigentliche gesperrt wird, hat bislang nur einige Hundert Follower – die unter anderem damit unterhalten werden, dass dort Verse aus Shakespeare-Sonetten gepostet werden.