Bild: Troy Hunt, CC-BY-4.0

Der Hacker-Hunter

Troy Hunt und der riesige Passwort-Fund „Collection #1 bis #5“

2,2 Milliarden Passwörter zu Onlinekonten sind im Netz aufgetaucht. Woher kommen die Daten und wer muss jetzt mit Angriffen auf seine digitale Identität rechnen? Der australische Sicherheitsforscher Troy Hunt hat Antworten darauf.

Von Fabian A. Scherschel

Nach dem Hackerangriff auf Adobe, der im Herbst 2013 bekannt wurde und mehr als 150 Millionen Onlinekunden des Softwareherstellers betraf, kam der australische Sicherheitsforscher Troy Hunt auf die Idee, einen Webdienst einzurichten, über die Betroffene herausfinden können, ob ihre Daten von so einem Hackerangriff betroffen sind. Heute ist Hunt der Hüter der Datenlecks schlechthin und wacht über Mailadressen und Passwörter von über sechs Milliarden Onlinekonten. Die Daten stammen aus über 250 verschiedenen Hackerangriffen.

Anfang Januar sorgte Hunt für weltweites Aufsehen, als er eine Sammlung an gehackten Onlinekonten mit über einer Milliarde Kombinationen aus Anmeldenamen und Passwörtern ausfindig machte und publikumswirksam in den Datenfundus seiner Webseite integrierte. Kurz nach der „Collection #1“ tauchten weitere Sammlungen „Collection #2 bis #5“ auf. Die fast 700 GByte großen Dateien umfassen Sammlungen von 2,2 Milliarden Onlinekonten, darunter Mailadressen und Passwörter – im Klartext oder als Hash-Werte.

Der Australier ist oft einer der ersten nichtkriminellen Hacker, der aus Angriffen auf Server stammende Daten zu Gesicht bekommt. Da er seit gut fünf Jahren solchen Passwortsammlungen hinterherrecherchiert, hat er mittlerweile gute Verbindungen in die dunkleren Seiten des Internets, wo entsprechende Daten gehandelt werden.

Mit seiner Website Have I Been Pwned (HIBP) betreibt Troy Hunt den weltweit führenden Dienst zur Überprüfung von Onlinekonten in Hinsicht auf Datenlecks. Die Regierungen von Australien, dem Vereinigten Königreich und Spanien nutzen den Service, um Mailadressen ihrer offiziellen Domains auf Sicherheitsvorfälle zu überprüfen. Hinzu kommen Millionen von Einzelnutzern, die sich per Mail von dem Dienst informieren lassen, wenn Hunt ihre Adresse in einem Datenleck ausfindig macht. Alleine nach seiner Analyse der „Collection #1“ musste Hunt nach eigenen Angaben knapp 768.000 E-Mails an die Abonnenten seines Warndienstes verschicken.

Mehrere Onlinedienste wie das Multiplayer-Spiel EVE Online und der australische Handelsriese Kogan betteten HIBP direkt in ihren Anmeldeprozess ein. Auch der Passwortmanager 1Password nutzt das API von Hunts Dienst, um Nutzer vor kompromittierten Passwörtern zu warnen.

Der Australier scheint seine Sammlung an Zugangsdaten gewissenhaft und transparent zu verwalten. Versuche, ihn unter Vorwänden dazu zu verleiten, die Passwörter zu bestimmten Mailkonten oder gar Teile seines Datenfundus herauszugeben, lehnt er konsequent ab.

Einen ähnlichen Service bietet in Deutschland das in Potsdam ansässige Hasso-Plattner-Institut (HPI) an. Nachdem Hunt mit der Collection #1 vorgelegt hatte, war man dort dem Australier sogar bei der Prüfung der Collection #2 bis #5 einige Tage voraus.

Die Collections #1 bis #5

Da wir die kurz vor Redaktionsschluss aufgetauchten fast 700 GByte an Daten nur stichprobenartig einsehen konnten, wissen wir noch nicht, woher die riesigen Sammlungen stammen. Die Informationen, die Hunt preisgibt, deuten darauf hin, dass ein oder mehrere Hacker die Sammlungen aus Datensätzen verschiedener Hacks zusammengetragen haben, darunter altbekannte, aber auch neue. Eine Verzeichnisauflistung erlaubt ein paar Rückschlüsse auf mögliche Quellen. Offenbar wurde der Datenschatz zusammengetragen, um sogenanntes Credential Stuffing im großen Stil zu ermöglichen.

Bei manchen Angriffen versucht der Hacker gezielt in ein Onlinekonto des Opfers einzudringen. Oft kennt er den Anmeldenamen (meist eine Mailadresse) seines Ziels und versucht, das dazugehörige Passwort zu erraten – notfalls per Brute-Force-Methode, bei der Wörterbücher sowie weitere Zeichenkombinationen durchprobiert werden. Beim Credential Stuffing ist es dem Angreifer jedoch relativ egal, welches Konto er knackt. Er will nur irgendeinen Zugang zum System erlangen – je mehr desto besser. Später kann er diese Zugänge dann meistbietend verkaufen. Dazu bedient er sich Listen mit Mailadressen und zugehörigen Passwörtern, die er bei einem anderen Webdienst abgegriffen oder im Darknet erworben hat. Mit diesen füttert er dann automatisch die Anmeldemasken der Zielwebseite, bis er Zugang erhält.

Credential Stuffing hat deswegen Erfolg, weil viele Webnutzer bei sehr vielen Onlinediensten ein und denselben Anmeldenamen verwenden; meistens eine Mailadresse. Und da viele Anwender auch ihre Passwörter bei mehreren Diensten wiederverwenden, kann man mit den Daten aus einem Servereinbruch wiederum bei anderen Servern einsteigen.

Herkunft der Daten

Credential-Stuffing-Listen wie die „Collections #1 bis #5“ werden in einschlägigen Untergrundforen oft als Abfallprodukt von Hackerangriffen weiterverkauft. Hat ein Hacker einen Dienst geknackt und dessen Passwortdatenbank mitgehen lassen, bedient er sich zuerst am Datensatz. Eventuell bricht er in einzelne Konten ein, die besonders viel wert sind oder klaut im großen Stil Zahlungsdaten. Wenn er mit den gesammelten Geheimnissen fertig ist, verkauft er sie weiter. So wandern solche Daten durch viele Hände, bis sie zuletzt in solchen Credential-Stuffing-Listen zur Resteverwertung landen. Verlangten Anbieter für die „Collection #1“ zunächst noch knapp 50 Dollar, so war das komplette 5er-Paket kurz vor Redaktionsschluss sogar kostenlos verfügbar.

Unsere eigenen Stichproben deuten darauf hin, dass die Daten teilweise aus älteren Datenlecks stammen. Mehrere Betreiber von Online-Diensten, die in der von Hunt veröffentlichten Verzeichnisstruktur auftauchen, bestätigten uns, dass sie in der Vergangenheit Opfer von Datenlecks wurden. Eine Quelle nannte uns sogar einen bisher unveröffentlichten Hackerangriff – allerdings nur unter der Bedingung, dass wir weder ihren Namen noch den des betroffenen Webdienst veröffentlichen. Demnach deutet alles darauf hin, dass die Daten authentisch sind und dass Hunt sie, wie angegeben, nach Hinweisen in einschlägigen Foren entdeckte.

Der Verzeichnisliste nach stammen die Daten aus allen Ecken der Welt. Wer auch immer sie zusammengesucht hat, scheint nicht besonders wählerisch gewesen zu sein und hatte es wohl nur auf eine möglichst große Gesamtzahl abgesehen. Es handelt sich hauptsächlich um kleinere Webseiten mit typischerweise zehntausenden bis hunderttausenden Accounts. Millionenlecks, wie sie Hunt sonst beschäftigen, sind nur vereinzelt dabei. Wie die Angriffe stattgefunden haben, mit denen die unbekannten Hacker die Daten erbeuteten, lässt sich nicht mehr nachvollziehen. Aller Wahrscheinlichkeit nach stammen sie aus unterschiedlichen Quellen.

Schutz vor Account-Klau

Wer wissen will, ob seine eigenen Onlinekonten in einem der Datensätze zu finden sind, die Hunt verwaltet, kann **HaveIBeenPwned.com** aufsuchen und dort seine Mailadressen prüfen. Zusätzlich sollte man auch den Identity Leak Checker des deutschen HPI unter **sec.hpi.uni-potsdam.de/ilc/** nutzen. Ist eine Adresse gelistet, sollte man zugehörige Account-Passwörter auf jeden Fall ändern – und zwar überall, wo man sie verwendet hat. Denn man muss davon ausgehen, dass die Adresse und das Passwort nun bei Hackern in Listen und Wörterbüchern für Brute-Force-Angriffe und Credential Stuffing zu finden ist. Das macht dazugehörige Onlinekonten zur leichten Beute von Kriminellen.

Beim australischen HIBP findet man auch den Dienst Pwned Passwords. Hier kann man ein Passwort eingeben und prüfen lassen, ob und wie oft es in Hunts Datenschatz vorkommt und damit höchstwahrscheinlich auch Kriminellen geläufig ist. Hunt gibt sich alle Mühe, das eingegebene Passwort zu schützen. Er überträgt es nicht im Klartext an seine Server, sondern prüft nur die ersten fünf Ziffern der Passwort-Hashes. Zurück kommt eine Liste mit Hashes aus der Datenbank, die lokal im Browser nach dem vollständigen Hash durchsucht wird.

Diese partielle Hash-Prüfung bietet bereits eine sehr hohe Sicherheit. Wem trotz allem aber selbst die Übermittlung von lediglich einem kleinen Teil der Hash-Werte unsicher vorkommt – egal wie gut der Ruf des Australiers ist –, kann die nötigen Hash-Dateien (11 GByte) auch über Hunts Webseite herunterladen und seine Passwörter offline testen. Hunts Dienst kann übrigens nicht prüfen, ob ein Passwort in einem bestimmten Datenleck vorkommt, sondern nur, ob irgendjemand es mal auf einer Seite verwendet hat, die gehackt wurde und deren Daten in Hunts Hände gelangten. *(hag@ct.de)* c't

Standorte gehackter Server

Ein Auszug der mutmaßlich gehackten Server: Bei den rot markierten Systemen können wir mit großer Sicherheit sagen, dass sie in den letzten Jahren Opfer eines Hackerangriffs wurden. Sie sind wahllos über den gesamten Globus verteilt.