Gerhard Giese

Botnets – die unauffällige Bedrohung für Banken

Über 30 Milliarden böswillige Anmeldeversuche durch Botnets innerhalb von acht Monaten: Diese alarmierende Anzahl von Cyberattacken verzeichnete Akamai allein zwischen November 2017 und Juni 2018. Zudem registrierten die Sicherheitsexperten, dass sogenannte Credential-Stuffing-Angriffe in den vergangenen Monaten drastisch zugenommen haben. Denn zwischen Mai und Juni 2018 wurden laut dem „State of the Internet"-Sicherheitsbericht rund 8,3 Milliarden schädliche Logins pro Monat erkannt – das bedeutet eine Steigerung um 30 Prozent im Vergleich zu den Vormonaten.

Imageschäden durch Missbrauch gestohlener Daten

Besonders häufig sind Finanzdienstleister im Visier der Hacker und für sie stellen Credential-Stuffing-Angriffe eine große Bedrohung dar. Bei dieser Betrugsmethode setzen Hacker auf Anmeldeseiten von Banken und Versicherungen systematisch Botnets ein, um gestohlene Anmeldedaten aus einem bereits stattgefundenen Datenklau auf einen erfolgreichen Login zu testen. Sie machen es sich zunutze, dass die Mehrheit der erwachsenen Internetnutzer für verschiedene Konten und Services die gleichen Anmeldedaten verwenden.

Für ein Finanzunternehmen stellt eine solche Attacke eine ernsthafte Bedrohung dar. Denn laut dem Bericht „Die Kosten von Credential Stuffing", den das Beratungsunternehmen Ponemon Institute herausgegeben hat, können Unternehmen dadurch Beträge in Millionenhöhe verlieren. Neben finanziellen Einbußen drohen im Finanzwesen auch große Imageschäden, wenn das Unternehmen nicht mehr als vertrauenswürdig gilt, weil Kreditkarteninformationen oder andere sensible Daten abgegriffen wurden. Deshalb sollten Unternehmen frühzeitig selbst aktiv werden und zum Schutz ihrer Kundendaten in geeignete Sicherheitsmaßnahmen investieren, um gezielt Angriffe abzuwehren.

Die Bequemlichkeit der Internetnutzer macht es Hackern leicht, Anmeldedaten auszuspionieren: Anwender wählen häufig die gleiche Kombination aus Benutzername und Kennwort für verschiedene Onlinezugänge. Im Darknet werden seit geraumer Zeit unzählige Listen zum Kauf angeboten, in denen Millionen dieser Anmeldedaten gespeichert sind. Hacker können sie dort illegal erwerben. Mithilfe von Credential-Stuffing-Angriffen testen sie dann, ob die erbeuteten Logindaten auf anderen Websites funktionieren. Ist dies der Fall, kann der Datensatz teurer weiterverkauft werden. Grundsätzlich hat nicht jeder Credential-Stuffing-Angriff das Ziel, unmittelbaren Schaden anzurichten. Oftmals geht es zunächst nur darum, die Funktionsfähigkeit der Logindaten zu bestätigen, um die Datensätze anschließend mit gesteigertem Wert weiterzuverkaufen.

Meist unauffällige Aktionen

Sobald die erfolgreich getesteten Anmeldedaten zum Login genutzt und anschließend weitere Daten gestohlen werden, spricht man von einem Credential-Abuse-Angriff. Im schlimmsten Fall kann es zum sogenannten Account Takeover kommen, wenn der Account eines Nutzers vom Hacker übernommen wird. In fast allen Fällen sind die Angriffe Bot-gesteuert: Ein Server, Open Proxy oder IoT-System wird verwendet, um mit einer möglichst großen Menge an IP-Adressen die Attacke auf die jeweilige Login-Seite zu starten.

Je mehr IP-Adressen dem Botnet zur Verfügung stehen, desto effizienter verläuft der Angriff. Denn der Ablauf ist denkbar einfach: Ein Bot mit einer IP-Adresse versucht, sich auf einer Website mit den Logindaten anzumelden. Gelingt es ihm nicht, startet er zunächst keinen neuen Versuch, sondern ein anderer Bot übernimmt. Solchen Botnets stehen oft unzählbare Mengen an IP-Adressen zur Verfügung und haben genug Zeit, um möglichst unauffällig und langsam die Kombinationen zu überprüfen. Zudem umgeht das Botnets so das Rate Limiting. Diese Sicherheitseinstellung dient dazu, IP-Adressen zu sperren, die wiederholt falsche Daten beim Login senden.

Drastischer Anstieg bösartiger Anmeldeversuche

In der Regel agieren die Botnets sehr unauffällig, dennoch gibt es immer wieder Credential-Stuffing-Angriffe, die schnell entdeckt werden. Wenn zum Beispiel der Bot-Betreiber seine Tools nicht vollständig beherrscht und vergisst, den Angriff möglichst dezent auszuführen und dadurch zu viel Traffic auf der Website stattfindet. Andere Angreifer probieren es mit einer Ablenkungstaktik: Während ein Botnet sehr auffällig vorgeht und die Aufmerksamkeit auf sich lenkt, führt ein

Gerhard Giese

Manager, Enterprise Security Team, Akamai, Ratingen

Die öffentliche Aufregung war groß, als zu Beginn dieses Jahres sensible Daten deutscher Politiker im Netz standen, und damit einmal mehr bewusst wurde, wie leicht sich Kriminelle Zugang zu IT-Systemen verschaffen können und wie nachlässig der Großteil der Bürger bei Schutzvorkehrungen seiner eigenen Daten agiert. Dabei war dieser Angriff auf die Prominentendaten offenbar nicht einmal das Ergebnis hochprofessioneller, sondern eher biederer Arbeit. Dass die Cyberkriminalität für die Finanzwirtschaft eine ernstzunehmende Herausforderung ist, zeigt der hohe Stellenwert, den sie seit einigen Jahren bei der Bankenaussicht einnimmt. Als besonders gefährlich für die Branche stuft der Autor Angriffe mit vernetzten Computern ein, die eine Schadsoftware transportieren und dabei vergleichsweise unauffällig agieren. Als besondere Gegenmaßnahmen sieht er Sicherheitslösungen, die weder dem Nutzer noch den Hackern auffallen. (Red.)

weiteres Botnet den eigentlichen Credential-Stuffing-Angriff aus. Es steuert den Login-Bereich seltener und mit vielen verschiedenen IP-Adressen an, bleibt dadurch länger unentdeckt und kann mehr Anmeldedaten überprüfen und gegebenenfalls verifizieren. Hinter solchen Ablenkungsmanövern steckt stets das klare Ziel, möglichst viele Daten abzugreifen.

Von diesen Botnets, die mit kleiner Frequenz und langsam agieren, geht die größte Gefahr aus: Sie haben zwar gegenüber einem einzelnen Ziel eine geringere Effizienz, sind aber besonders schlagkräftig gegen ein größeres Ökosystem, das aus verschiedenen Finanzdienstleistern besteht. Denn die IP-Adressen werden nur ein- bis zweimal täglich auf der Website bestimmter Banken oder Versicherungen eingesetzt, sie rotieren aber zwischen vielen verschiedenen Anmeldeseiten. Dadurch nutzt das Botnet seine Ressourcen optimal und reduziert gleichzeitig das Risiko, erkannt zu werden. Auf diese Weise kann das Credential-Stuffing-Botnet über einen langen Zeitraum aktiv und unentdeckt bleiben und hat bessere Chancen, gefährdete Konten aufzuspüren. Aber auch diese können erkannt und abgeschwächt werden.

Finanzielle Verluste und Imageschaden

Im „State of the Internet"-Bericht werden zwei Fälle geschildert, bei denen das Unternehmen Credential-Stuffing-Angriffe erfolgreich abwehren konnte. Im ersten Fall wurde ein Fortune-500-Finanzdienstleister aufmerksam, als der Traffic auf seiner Website rapide in die Höhe schnellte. Innerhalb von 48 Stunden wurden über ein Botnet 8,5 Millionen maliziöser Anmeldeversuche generiert – gewöhnlich verzeichnet die Website nur rund sieben Million Anmeldeversuche pro Woche. Über 20 000 Geräte waren an dem Botnet beteiligt, das Hunderte Anfragen pro Minute gesendet hat.

Noch aggressiver verlief der Angriff auf eine Kreditgenossenschaft: Hier stiegen die böswilligen Anmeldeversuche ebenfalls stark an, denn – wie man später herausfand – griffen drei Botnets gleichzeitig die Website an. Während ein Botnet den Traffic auf der Website deutlich erhöhte und damit die Aufmerksamkeit auf sich zog, arbeitete eines der anderen beiden Netze langsam und methodisch und verursachte dadurch den größten Schaden. Die beiden Fälle verdeutlichen, wie variabel die Hacker heutzutage Botnets für Credential-Stuffing-Angriffe einsetzen und wie gefährlich solche Methoden sind.

Credential Stuffing verursacht im Finanzsektor jedes Jahr einen Schaden in Milliardenhöhe. So verzeichnete einer der weltweit größten Finanzdienstleister über 8 000 Kontoübernahmen pro Monat, was zu täglichen Verlusten in Höhe von 100 000 Dollar führte. Durch die Implementierung eines Bot-Management-Systems bei dem Unternehmen gingen die Kontoübernahmen sofort auf eine bis drei monatlich und die betrugsbezogenen Kosten um 98 Prozent zurück.

Neben finanziellen Verlusten droht aber auch ein Imageschaden, da im Finanzsektor besonders viele sensible Informationen online gespeichert sind. Hacker könnten nicht nur Kreditkartendaten erbeuten, sondern auch Informationen über den Kontostand, Versicherungsschutz oder auch monatliche Einnahmen und Ausgaben. Mit einem einzigen Angriff können Hacker viele verschiedene Daten abgreifen und anschließend als Datensatz weiterverkaufen. Das betroffene Unternehmen erleidet dann neben einem Vertrauensverlust auch finanzielle Einbußen und einen großen Imageschaden.

Bot-Management-Systeme zum Schutz vor Credential Stuffing

Unternehmen sind den Credential-Stuffing-Angriffen allerdings nicht schutzlos ausgeliefert, sie können Maßnahmen ergreifen, um die Daten ihrer Kunden abzusichern. Mit einem Bot-Management-System können der Traffic auf der Website sowie die Login-Versuche genau beobachtet und analysiert werden. Das System führt verhaltensbasierte Analysen beim Login-Vorgang durch und kann so erkennen, ob die Eingabe der Anmeldedaten von einem Menschen oder einem Bot stammt.

Ein Beispiel: Visualisiert man die Mausbewegungen und Tastaturanschläge von Menschen, ergibt sich ein uneinheitliches Muster, während Bots bei der Eingabe der Login-Daten gleichförmige, gerasterte Muster erzeugen. Automatisierte Requests kann das System deshalb schnell anhand einer Analyse der Bewegungsmuster identifizieren. Dadurch können Veränderungen sofort entdeckt und Bot-gesteuerte Angriffe gezielt abgewehrt werden.

Liegt tatsächlich ein Credential-Stuffing-Angriff vor, gibt es verschiedene Möglichkeiten, um dagegen vorzugehen. Eine Möglichkeit besteht darin, die IP-Adresse, die den schädlichen Login-Vorgang vornimmt, zu blockieren. Da Botnets aber oftmals Tausende verschiedene IP-Adressen nutzen, ist dieses Verfahren nicht immer effektiv. Mitunter ist es sinnvoll, den Angreifer auf ein anderes System weiterzuleiten, um zum Beispiel falsche Informationen weiterzugeben. Letztlich geht es aber immer darum, Attacken zu neutralisieren, ohne dass der Botnet-Betreiber es bemerkt und einen neuen Angriff starten kann.

Uneingeschränkte Usability

Trotz der bekannten Risiken und Gefahren zögern Unternehmen, Schutzmaßen zu ergreifen. Sie begründen dies mit fehlendem Budget oder damit, dass Credential-Stuffing-Angriffe keinem Zuständigkeitsbereich innerhalb der Firma zuzuordnen seien. Darüber hinaus glauben laut einer Studie des Beratungsunternehmens Ponemon Institute 70 Prozent der Befragten, dass die Tools, die sie zur Verteidigung benötigen, das Weberlebnis legitimer Nutzer beeinträchtigen würden. Doch das Risiko eines Schadens ist vor allem im Finanzsektor zu groß, um Credential-Stuffing-Angriffe lediglich als Grundrauschen auf der Website abzutun.

Die beiden genannten Fallbeispiele zeigen, dass Unternehmen schnell zur Zielscheibe werden können. Deshalb ist es elementar zu reagieren, bevor die Website angegriffen wird. Bei Unternehmen, bei denen sensible Informationen so gebündelt vorliegen wie im Finanzsektor, ist das Risiko, attackiert zu werden, signifikant höher als in Branchen, in denen nur wenige Kundendaten verarbeitet werden. Aus diesem Grund sollten Lösungen für Credential Stuffing fest im IT-Sicherheitsplan eines Unternehmens integriert sein. Denn anders als DDoS-Angriffe können Credential-Stuffing-Angriffe über einen langen Zeitraum hinweg unerkannt bleiben und dadurch gravierende Schäden anrichten. Solange Botnet-Betreiber wissen, wie sie ihre verfügbaren Tools einsetzen können, ist es entscheidend, es dem Hacker so schwer wie möglich zu machen.

Unauffällige Abläufe im Hintergrund

Das gelingt aber nur, wenn ein Unternehmen weiß, was auf seiner Website passiert, den Traffic entsprechend analysieren und bei einem Angriff reagieren kann. Bei der Integration eines Bot-Management-Systems müssen sich Unternehmen auch keine Sorgen bezüglich der Usability machen. Denn anders als bei umständlichen Captcha-Abfragen oder Zwei-Wege-Identifizierungen bemerkt der User das Bot-Management-System nicht einmal. Der Bot-Manager läuft unauffällig im Hintergrund und beeinträchtigt auch die Performance der Website nicht. Schließlich ist die beste Securitylösung die, die gar nicht – also weder dem Nutzer noch dem Hacker – auffällt.

Zeitschrift für das gesamte KREDITWESEN

IMPRESSUM

Verlag und Redaktion:

Verlag Fritz Knapp GmbH
Aschaffenburger Straße 19, 60599 Frankfurt am Main
Postfach 70 03 62, 60553 Frankfurt am Main

Telefon +49 (0) 69 97 08 33 - 0
Telefax +49 (0) 69 7 07 84 00
E-Mail: red.zfgk@kreditwesen.de
Internet: www.kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser (Mo), Philipp Otto (P.O.)

Redaktion: Swantje Benkelberg (sb), Philipp Hafner (ph), Hanna Thielemann (ht), Frankfurt am Main

Redaktionssekretariat und Lektorat: Volker Schmidt

Satz und Layout: Patricia Appel

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Manuskripte: Mit der Annahme eines Manuskripts zur Veröffentlichung erwirbt der Verlag vom Autor das ausschließliche Verlagsrecht sowie das Recht zur Einspeicherung in eine Datenbank und zur weiteren Vervielfältigung zu gewerblichen Zwecken in jedem technisch möglichen Verfahren.

Die vollständige Fassung der Redaktionsrichtlinien finden Sie unter www.kreditwesen.de.

Verlagsleitung: Philipp Otto

Anzeigenleitung: Timo Hartig

Anzeigenverkauf: Hans-Peter Schmitt, Telefon +49 (0) 69 97 08 33 - 43

Zurzeit ist die Anzeigenpreisliste Nr. 61 vom 1.1.2019 gültig.

Zitierweise: KREDITWESEN

Erscheinungsweise: am 1. und 15. jeden Monats.

Bezugsbedingungen: Abonnementspreise inkl. MwSt. und Versandkosten: jährlich € 628,35, bei Abonnements-Teilzahlung: 1/2-jährlich € 322,85, 1/4-jährlich € 164,69. Ausland: jährlich € 650,67. Preis des Einzelheftes € 25,00 (zuzügl. Versandkosten).

Verbundabonnement mit der Zeitschrift »bank und markt«: € 957,76, bei Abonnements-Teilzahlung: 1/2-jährlich € 502,88, 1/4-jährlich € 263,76. Ausland: jährlich € 985,12.

Studenten: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt. Bestellungen direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter Telefon +49 (0) 69 97 08 33 - 25

Bei Nichterscheinen ohne Verschulden des Verlags oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindung: Frankfurter Sparkasse, IBAN: DE68 5005 0201 0200 1469 71, BIC: HELADEF1822

Druck: Hoehl-Druck Medien + Service GmbH, Gutenbergstraße 1, 36251 Bad Hersfeld

ISSN 0341-4019

Fotonachweise für Heft 4/2019 – Seite 2: Fritz Knapp Verlag GmbH; Seite 9: B. Keese/Andreas Pohlman, Renaud de Planta/Pictet, Dr. H. Sepp/Hauck & Aufhäuser, Michael Breuer/RSGV; Seite 11: P. Büttel/PwC, W. Sawahn/PwC; Seite 21: LBBW, Seite 24: Muzinich & Co; Seite 27: Dr. A. Wiedemann/A. Wiedemann, J.H. Wilhelms/ J.H. Wilhelms, Seite 32: Dr. Th. Metzner/Th. Metzner, Dr. M. Pooria/ M. Pooria; Seite 37: WCG-Wiesbaden; Seite 40: Akamai Technologies GmbH; Seite 47: Verlag Dr. Schmidt; Seite 48: nwb-Verlag Herne