Band 5, Sonderausgabe
„State of the Internet“-Sicherheitsbericht

Medien unter Beschuss

Inhaltsverzeichnis

Übersicht

Von Januar 2018 bis Juni 2019 erfasste Akamai mehr als 61 Milliarden Credential-Stuffing-Versuche und mehr als vier Milliarden Angriffe auf Webanwendungen. In dieser Sonderausgabe des „State of the Internet"-Sicherheitsberichts konzentrieren wir uns auf Daten aus den Sektoren Hightech, Videomedien und Unterhaltung – zusammengefasst als Medien- und Technologiebranche bezeichnet.

Auf diese drei Branchen zielten fast 35 % aller Credential-Stuffing-Angriffe ab und fast 17 % der Angriffe auf Webanwendungen, die Akamai während des 18-monatigen Reporting-Zeitraums beobachtet hat. Unsere Analyse zeigt, dass diese drei Branchen aus zwei Gründen eine stabile und konsistente Angriffsquelle sind: persönliche und geschäftliche Daten. Die anvisierten Marken sind bekannte Namen, und Kriminelle möchten von diesem Bekanntheitsgrad profitieren.

Durch direkte Angriffe auf Webanwendungen hoffen Kriminelle, Kunden- und Finanzdaten offenzulegen oder einen anfälligen Server zu nutzen, um schädlichen Code zu verbreiten – ebenfalls ein bekanntes Motiv, das Kriminelle zum Angriff auf den Einzelhandelssektor bewegt. Beim Credential Stuffing werden die anvisierten Marken und ihre Kunden angegriffen: Kriminelle verschaffen sich Zugriff auf persönliche Informationen und Unternehmensressourcen wie Medien und digitale Produkte.

Webangriffe in Zahlen
Januar 2018 bis Juni 2019

Gesamtzahl der Angriffe auf Webanwendungen: 4.068.741.948

- *Hightech: 609.117.260*
- *Videomedien: 143.308.490*
- *Unterhaltung: 51.464.909*

Angriffstypen:

- *SQL Injection (SQLi): 69,7 %*
- *Local File Inclusion (LFI): 21,6 %*
- *Cross-Site Scripting (XSS): 3,5 %*

Gleiche Angriffe, unterschiedliche Risiken, globale Auswirkungen

Jaspal Jandu

Group CISO

DAZN

Betrachten wir uns die grundlegenden Angriffsmethoden, die Kriminelle zum Kompromittieren von Unternehmen verwenden, zeigt sich Folgendes: Sendeanstalten und die Medienbranche insgesamt sind tagtäglich von denselben Angriffsmethoden wie auch viele andere Branchen betroffen. Diese Angriffe stellen für Medienunternehmen ein erhebliches Risiko dar – und genau darüber machen wir uns Sorgen.

Als die meisten Sendeanstalten nur linear waren und Sie zu einem bestimmten Zeitpunkt vor dem Fernseher sitzen mussten, um eine Sendung anzusehen, waren die mit der Technologie verbundenen Risiken relativ simpel im Vergleich zu den Auswirkungen, mit denen wir heutzutage konfrontiert werden. Wenn eine Live-Übertragung unterbrochen wurde, war der Fehler wahrscheinlich physischer Natur – entweder ein Kabelproblem oder ein Hardwarefehler. Angesichts der heutigen Umstellung auf IP-basiertes Fernsehen (IP-TV) und OTT-Streaming (Over-the-Top) sind die Risiken nicht nur drastisch angestiegen, sie sind auch komplexer zu managen.

Das Lieferkettenrisiko ist ein gutes Beispiel dafür, wie die Dinge immer komplexer geworden sind. In der heutigen Welt entwickeln sich herkömmliche Rundfunkanstalten zu Softwareunternehmen. Mechanismen zur Cloudbereitstellung wie Infrastructure as a Service (IaaS) haben diesen Wechsel in einigen Fällen vereinfacht. Dieser Ansatz birgt jedoch auch ein deutlich höheres Risiko für Dritte und Vierte, das Sendeanstalten jetzt bewältigen müssen. Dies ist ein völlig anderes Unterfangen als noch vor einem Jahrzehnt, als der Großteil der Sendekette über eine getestete und bewährte Senderinfrastruktur bereitgestellt wurde, die vollständig durch diese Sender kontrolliert wurde.

Aber fast die größte Furcht haben Sendeanstalten vor einem Komplettausfall, der dazu führt, dass die Zuschauer vor einem leeren Bildschirm sitzen. Aus Sicherheitsperspektive sind internetbasierte Angriffe wie Distributed Denial of Service (DDoS) Risiken, die Sendeanstalten nun in der gesamten Lieferkette berücksichtigen müssen. In Branchen wie dem Finanzdienstleistungssektor bestehen derartige Risiken seit Jahrzehnten. Die neue Welt von Live-IP-TV, in der ein Großteil der weltweiten Medien konsumiert wird, bedeutet, dass jeder Angriff auf die Verfügbarkeit zu Problemen bei der Kundenbindung, zu geringeren Werbeeinnahmen und zu geringeren Chancen auf künftige erfolgreiche Gebote für Rechte führen kann. Beim Live-TV gibt es keine zweite Chance. Den Zuschauern ist es egal, ob es sich um ein Lieferantenproblem handelt – es ist der Ruf der Sendeanstalt, der Schaden nimmt.

Die Medienbranche muss außerdem mit einer großen Menge kultureller Veränderungen im Bereich der Regulierung fertig werden. Die Integration von mehr Daten steht heute im Zentrum der strategischen Ziele vieler Sendeanstalten. Die Motivation besteht nicht nur darin, den Zuschaueranteil zu erhöhen, sondern auch darin andere Möglichkeiten zu finden, den Zuschauern ein maßgeschneidertes und relevanteres Erlebnis zu bieten. Es besteht ein schmaler Grat zwischen der legitimen geschäftlichen Nutzung von Kundendaten und der Überschreitung der zulässigen Nutzungsgrenzen – ein Limit, das nicht immer offensichtlich ist. Die Herausforderung für Medien besteht darin, die Notwendigkeit von Innovation und Flexibilität mit den Risiken abzuwägen, die durch Vorschriften entstehen, und zwar in einer Umgebung, in der Nutzer ständig Innovationen und modernste Unterhaltungsmöglichkeiten verlangen.

Im Zuge der kulturellen Veränderung ist jedes Unternehmen, das digitale Ressourcen schützen muss, mit einem Mangel an Fähigkeiten konfrontiert. Es ist kein Kinderspiel, qualifizierte Sicherheitsexperten zu finden, die verstehen, wie wichtig es ist, Geschäftschancen gegenüber den Risiken einer sich schnell verändernden Welt abzuwägen. Vielen Sicherheitsexperten, die ihren Hintergrund in Branchen mit starken Compliance-Umgebungen wie Banken und Behörden haben, fällt es häufit schwer, sich an wechselnde Umgebung anzupassen. Es ist viel einfacher, auf eine Vorschrift zu verweisen, als die Risiken zu artikulieren, die eine bestimmte Entscheidung für ein kreatives Unternehmen bedeuten könnte.

Es gibt ein sehr strukturelles Risiko, das in der Medienbranche einzigartig ist und umfassende, komplexe gesellschaftliche Konsequenzen hat: Fake News. Sendeanstalten und soziale Medien haben einen erheblichen Einfluss auf die öffentliche Meinung. Während es zwar Debatten darüber geben kann, was Fake News sind bzw. nicht sind, stellen echte Fake News und die Möglichkeit, falsche Informationen zu verbreiten, die nicht von echten, vertrauenswürdigen Inhalten zu unterscheiden sind, eine erhebliche Bedrohung für die Branche dar. Diese Instrumente haben die Fähigkeit, Wahlergebnisse zu beeinflussen, und können toxische, spaltende Botschaften auf einer wirklich globalen Ebene Zugkraft verleihen. Dies wirkt sich auf das Urvertrauen und darauf aus, wie wir uns über die Welt um uns herum informieren.

Staaten achten nun deutlich stärker auf Sendeanstalten und Medienstellen, da auf diese Weise ein Publikum von Millionen erreicht werden kann. Dies geschieht nicht nur durch die Kompromittierung von Sendeplattformen, sondern auch durch die Präsenz in den sozialen Medien, die viele Sendeanstalten und Medienstellen nutzen. In den letzten fünf Jahren gab es mindestens zwei bekannte Fälle von landesweiten Angriffen auf die Medienbranche.

Vertrauen ist für die Zukunft der Medienbranche von entscheidender Bedeutung. Das Verbrauchervertrauen wird nicht nur durch die Schnelligkeit gefährdet, mit der wir bekannte Risiken angehen, sondern auch durch die Art und Weise, wie wir auf Risiken reagieren, die für uns einzigartig sind und von denen viele vor einem Jahrzehnt einfach noch nicht existiert haben. Wir wissen, dass ein bedeutender kultureller Wandel erforderlich ist, um mit den Bedrohungen umzugehen, und dass es nicht genug der richtigen Fähigkeiten gibt, um sie zu umgehen. Die Dinge werden sich in naher Zukunft nicht ändern. Zumindest werden wir vorerst weiterhin mit einer schwierigen Entwicklung konfrontiert, und die Risiken, denen wir uns heute ausgesetzt sehen, könnten uns sogar stärker treffen, als wir je zuvor erwartet hätten.

Jaspal ist ein leitender Sicherheitsexperte mit mehr als 20 Jahren Erfahrung. Im letzten Jahrzehnt hat er sich hauptsächlich auf den Mediensektor konzentriert. Er bietet erstaunliche Einblicke in die Risiken, mit denen Medienunternehmen konfrontiert werden, denn er war an der Abwehr einiger der wichtigsten Angriffe auf den Sektor beteiligt.

Die in diesem Beitrag geäußerten Ansichten sind die Ansichten des Autors. Sie spiegeln nicht notwendigerweise die Ansichten von Akamai wider.

Angriffe auf Webanwendungen

Angriffe auf den Hightech-Sektor, der neben der Herstellung von Geräten und Software auch Technologie- und Serviceanbieter (wie Cloud-, Mobil-, Telekommunikations- und Kabelanbieter) umfasst, machten den Großteil der Angriffe in der Medien- und Technologiebranche aus, wie in Abbildung 1 gezeigt.

Im Gegensatz dazu blieben Angriffe auf Unterhaltungsmedien, zu denen Unternehmen wie Content-Anbieter, Sendeanstalten, Postproduktion, Content-Entwicklung, Forschung und Analyse gehören, weitgehend stabil, mit einem sehr signifikanten Anstieg am 22. September 2018. Die vertikalen Videomedien, zu denen Vertrieb und Lieferung gehören, sowie die Filmindustrie verzeichneten ebenfalls einen stetigen Strom von Angriffen, der im Laufe der Zeit zunahm und im zweiten Quartal 2019 zu einigen Spitzen führte.

Das konsistente Volumen zeigt, dass die Medien- und Technologiebranche ein attraktives Ziel für Kriminelle darstellt. Personenbezogene Daten können verkauft oder gehandelt werden, sobald sie kompromittiert wurden, während Unternehmensdaten für weitere Angriffe genutzt werden können. Dieselben Daten können auch von Angreifern verwendet werden, um Medienstreams zu stehlen – ein Problem, das bei Sportveranstaltungen häufig zu auftritt.

Genauso viel Schaden verursachen Kriminelle, die versuchen, Originalinhalte zu stehlen, um sie vor dem geplanten Sendedatum zu veröffentlichen oder auf verschiedenen kriminellen Märkten zu verkaufen. Dies kommt häufig bei Vorabversionen von Software und Spielen (in einigen Kreisen als *Warez* bezeichnet) vor, während Musik und Filme gehandelt werden.

Die Angriffsspitze im September 2018 richtete sich gegen eine bekannte internationale Marke und bestand nur aus SQLi-Angriffen (SQL Injection). Es ist nicht klar, worauf es die Kriminellen bei diesem Angriff abgesehen hatten, aber SQLi ist normalerweise ein direkter Angriff auf Anmeldedaten und andere Informationen. Es ist ungewöhnlich, aber nicht vollkommen neu, dass eine Website von einem Brute-Force-SQLi-Angriff von dieser Intensität betroffen ist.

Die zweite Angriffsspitze gegen die Hightech-Branche im November 2018 ist wesentlich interessanter. Dieser Angriff richtete sich gegen eine andere bekannte Marke – eine Art hochwertiges Ziel, das im Ganzen zu betrachten ist. Die Kriminellen zielten auf die vertraulichen Informationen dieses Unternehmens ab. Dieser Angriff bestand aus Local File Inclusion (LFI) (82,3 %), PHP-Injektion (9,3 %), Command Injection (7,6 %) und SQLi (0,7 %).

Tägliche Angriffe auf Webanwendungen in der Medienbranche
Januar 2018 bis Juni 2019

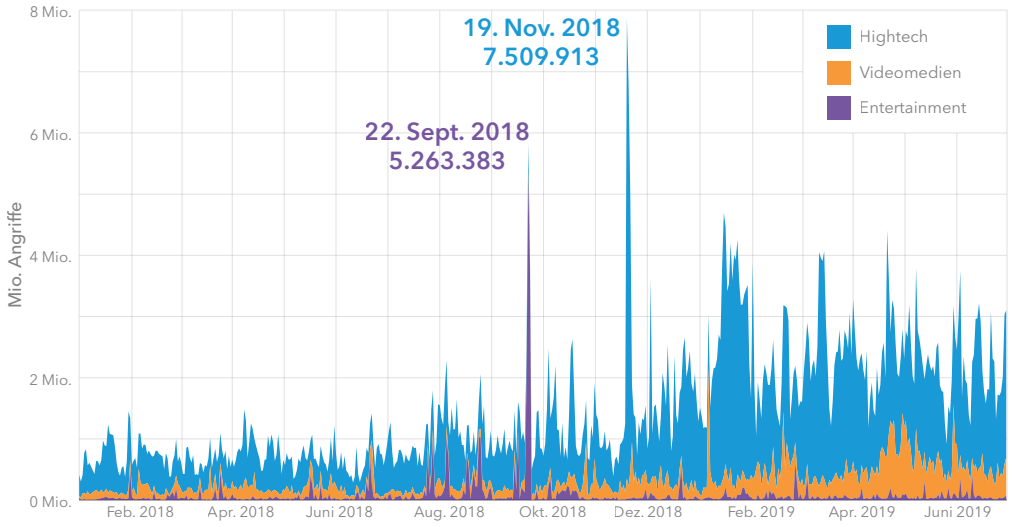


Abb. 1 – Anwendungsangriffe haben seit der zweiten Hälfte des Jahres 2018 ein spürbares Wachstum hingelegt – ein Trend, der sich voraussichtlich fortsetzen wird.

SQLi blieb während des 18-monatigen Zeitraums mit mehr als 70 % der Angriffe die wichtigste Angriffsmethode, gefolgt von Local File Inclusion (LFI) mit 19,3 %, Cross-Site Scripting (XSS) mit 3,9 %, PHP-Injektion mit 3,3 % und Remote File Inclusion (RFI) mit weniger als 1 %.

SQLi-Angriffe sind eine sehr beliebte Angriffsmethode für Kriminelle, die Anmeldedaten, Finanzinformationen und andere Daten stehlen möchten, die in Unternehmensdatenbanken gespeichert werden. Die Injection-Angriffe als Ganzes, wie in Abbildung 2 dargestellt, machten jedoch mehr als 98 % der Angriffe gegen die Medien- und Technologiebranche aus.

Code-Injection-Angriff, einschließlich SQLi, LFI, RFI und XSS, ist ein allgemeiner Begriff für Angriffstypen, mit denen ein Angreifer schädlichen Code in Anwendungen einfügen kann, der dann interpretiert oder anderweitig ausgeführt wird. Im Unterschied zu Command-Injection-Angriffen verwenden Kriminelle hierbei ihren eigenen Code verwenden. Hingegen ist der Gegner bei Command-Injection-Angriffen auf die Standardfunktionen der Anwendung oder des Service beschränkt.

Injection-Angriffe profitieren im Wesentlichen von einer mangelhaften Datenvalidierung und -verarbeitung. Solche Schwachstellen wurden auf Plattformen wie .NET, PHP, Java, JavaScript und Ruby on Rails entdeckt.

Schwachstellen bei der Codeinjektion können in Gruppen oder einzeln ausgenutzt werden (wie in den in Abbildung 1 hervorgehobenen zwei Tagen zu sehen ist), und die Fähigkeiten, die erforderlich sind, um solche Fehler zu finden und auszunutzen, sucht man vergebens. Im Internet gibt es mehrere Tools, die das Scannen auf Schwachstellen bei der Codeinjektion automatisieren. In einigen Fällen automatisieren diese Tools auch die Ausnutzung und Exfiltration.

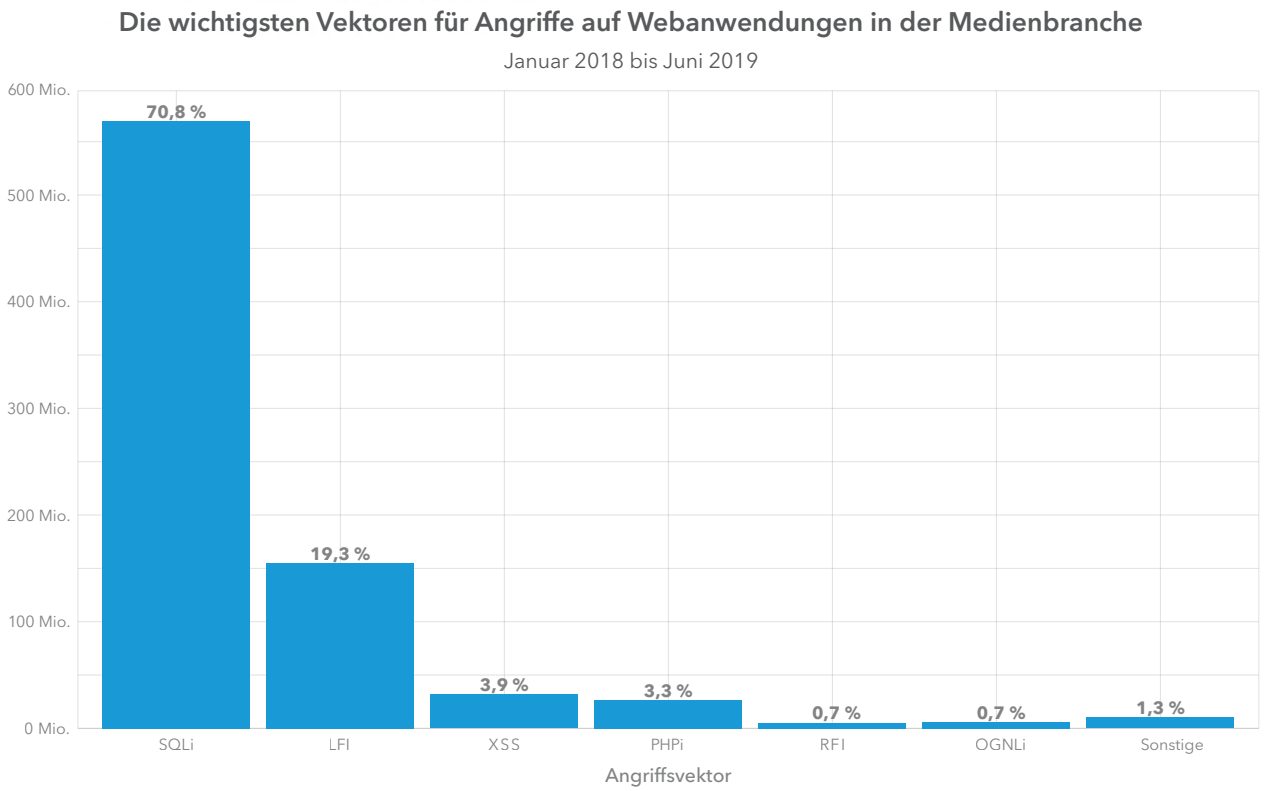


Abb. 2 – Injection-Angriffe haben insgesamt mehr als 98 % der Angriffe auf die Medien- und Technologiesektoren ausgemacht

In diesem Zusammenhang ist erwähnenswert, dass die meisten Kriminellen keine ausgeklügelten oder spezialisierten Tools verwenden. Sie verwenden im Allgemeinen dieselben legitimen Programme, die in zahlreichen Sicherheitsangeboten weit verbreitet sind, darunter Metasploit und Kali Linux. Kriminelle mit der Fähigkeit, maßgeschneiderte Tools zu entwickeln, sind selten so auffällig, dass sie in volumenbasierten Metriken auftauchen – doch sie sind sehr aktiv.

Erfolgreiche Injection-Angriffe können zu kompromittierten Daten und Unternehmensressourcen führen, z. B. Kundendatensätze, interne Kommunikation, Pläne zur Geschäftsentwicklung, Nutzernamen und Kennwörter. Aktivisten der Gruppe LulzSec nutzten im Jahre 2010 XSS, RFI, LFI und SQLi, um eine Reihe von Angriffen zu starten, die Dutzende von Websites und Organisationen beeinträchtigten. Injection-Angriffe können jedoch auch ein Einstiegstor für Kriminelle sein und die Voraussetzungen für größere Probleme schaffen, wie beispielsweise bei dem Angriff auf Heartland Payment Systems im Jahr 2009.

Warum nutzen Kriminelle also Angriffe auf Injection-Basis? Erstens bieten sie aufgrund der automatisierten Tools eine niedrige Einstiegsbarriere für Kriminelle, denen es an fortgeschrittenen Fähigkeiten mangelt. Der zweite Grund, warum diese Angriffe stark bevorzugt werden, besteht darin, dass sie schlichtweg gut funktionieren.

Bei Betrachtung der globalen Sichtweise auf die Quelle von Webangriffen belegten die Vereinigten Staaten in allen Branchen weltweit den ersten Platz, gefolgt von Großbritannien und Deutschland. Das Hauptziel für Angriffe auf die Medien- und Technologiebranche waren auch die Vereinigten Staaten, wobei Frankreich auf dem zweiten Platz lag. Wie in Abbildung 3 zu sehen ist, waren 18,63 % aller Angriffe, die Akamai innerhalb des 18-monatigen Zeitfensters in den USA verzeichnete, tatsächlich gegen die Medien- und Technologiebranche gerichtet.

Es ist interessant festzustellen, dass kein anderes nordamerikanisches Land unter den Top-10-Zielen liegt, wenn die vertikale Ausrichtung der Medien- und Technologiebranche betrachtet wird. Frankreich (34,78 %), Japan (22,96 %), Deutschland (11,09 %) und Indien (10,55 %) vervollständigen die Top 5. Korea ist ein interessanter Ausreißer in diesem Datensatz, denn 64 % aller Angriffe auf Unternehmen in Korea richteten sich gegen Medienunternehmen.

Anwendungsangriffe – Top-Ziele

ANVISIERTE BEREICHE	MEDIENBRANCHEN	ALLE BRANCHEN	GLOBALER RANG IN ALLEN BRANCHEN
USA	636.551.596	3.416.411.545	1
Frankreich	27.995.960	80.501.396	8
Japan	25.417.099	110.691.972	6
Deutschland	16.896.288	152.341.265	3
Indien	15.116.167	143.323.371	4
Niederlande	12.968.664	52.918.175	11
Korea	11.007.413	17.307.359	18
Australien	10.837.898	61.597.371	10
Großbritannien	7.662.747	243.559.654	2
Hongkong Sonderver-waltungszone	6.503.057	27.502.462	15

Abb. 3 – Fast 20 % aller Angriffe auf die USA zielten auf die Medien- und Technologiebranche ab

Die Vereinigten Staaten stehen bei den Herkunftsländern und Angriffen nur in der Medien- und Technologiebranche erneut an der Spitze (Abbildung 4). Die Niederlande (31,23 %) folgen mit deutlichem Abstand auf Platz zwei.

Die größte Überraschung ist jedoch Belize, das während des Reporting-Zeitraums auf dem dritten Platz landet. Belize ist nicht nur die elftgrößte Angriffsquelle insgesamt, sondern 68 % dieser Angriffe zielen auf die Medien- und Technologiebranche ab. Nach einigen zusätzlichen Recherchen scheint der hohe Rang im ersten Quartal 2019 mit kompromittierten ISP-Routern und -Services verbunden zu sein. In diesen Monaten haben Kriminelle Kundengeräte kompromittiert und Services missbraucht, um Botnet-Command-and-Control-Server (C2) zu hosten. Diese Server wurden dann zum Starten von Angriffen verwendet.

Der aktuelle *Botnet Threat Report* von Spamhaus führte ISPs in Belize unter den Top 20 für Botnet-C2-Hosting, kompromittierte Server und Websites. Die Daten des Spamhaus-Berichts entsprachen den von Akamai in Belize beobachteten Spitzenwerten im schädlichen Traffic, was unsere Schlussfolgerung untermauert.

Anwendungsangriffe – Top-Quellen

QUELLBEREICH	MEDIEN-BRANCHEN	ALLE BRANCHEN	GLOBALER RANG IN ALLEN BRANCHEN
USA	177.678.990	1.041.639.431	1
Niederlande	90.602.359	290.096.974	3
Belize	71.054.852	103.372.849	11
Russland	54.058.380	822.468.109	2
China	51.751.691	240.602.133	4
Indien	40.352.673	173.637.873	7
Deutschland	28.651.918	147.644.005	8
Irland	28.172.199	82.245.577	13
Ukraine	19.804.493	181.211.429	6
Frankreich	16.400.882	128.396.046	9

Abb. 4 – Aufgrund einer Zunahme der Bot-bezogenen Aktivitäten in Belize sprang das Land auf den dritten Platz auf der Quellliste und insgesamt auf den 11. Platz, wenn es um Internetangriffe geht

Credential Stuffing in Zahlen
Januar 2018 bis Juni 2019

Schädliche Anmeldeversuche insgesamt: 61.192.394.742

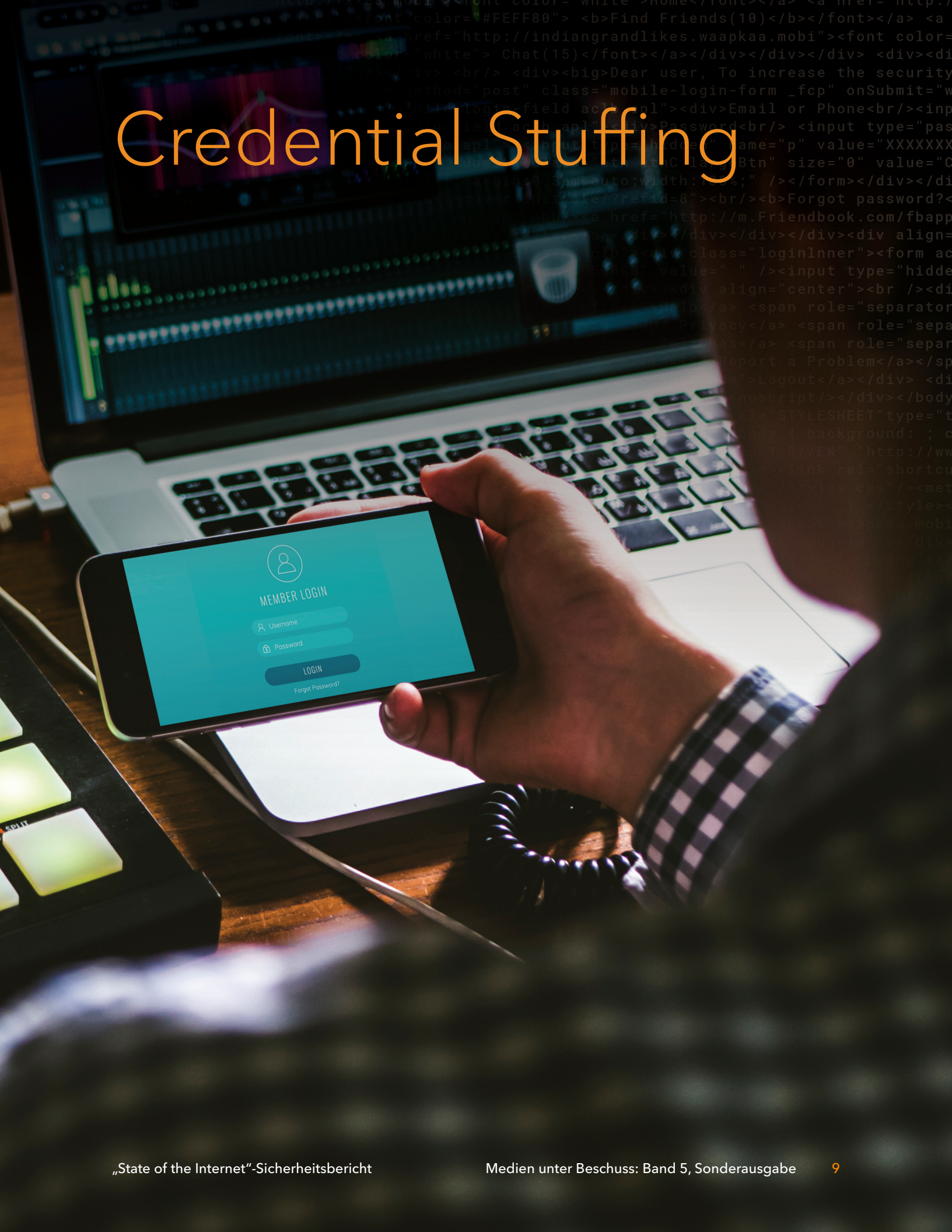
- *Videomedien: 13.760.213.425*
- *Hightech: 7.533.980.169*
- *Unterhaltung: 77.292.308*

Durchschnittliche Anzahl schädlicher Anmeldungen pro eindeutigem Host:

- *SQL Injection (SQLi): 69,7 %*
- *Local File Inclusion (LFI): 21,6 %*
- *Cross-Site Scripting (XSS): 3,5 %*

Fast 35 % aller schädlichen Anmeldungen zielen auf die Medien- und Technologiebranche ab

Credential Stuffing



Der Missbrauch von Anmeldedaten, häufig als Credential Stuffing bezeichnet, ist eine Art von Angriff, der in letzter Zeit viel Aufmerksamkeit erregt hat. Der Grund für die Aufmerksamkeit liegt nicht darin, dass Credential Stuffing neu ist, sondern dass die Anzahl der Angriffe in diesem Bereich in den letzten Jahren exponentiell gestiegen ist.

Akamai hat in diesem Jahr ausführlich über Credential Stuffing berichtet. In diesem Bericht untersuchen wir, wie sich diese Angriffe auf die Medien- und Technologiebranche auswirken.

Hintergrund

Beim Credential Stuffing wird eine gestohlene Liste von Nutzernamen und Kennwörtern ungehindert freigegeben, verkauft oder getauscht. Dabei wird jede Kombination bei der Authentifizierungsplattform des Ziels versucht. Häufig haben es die Kriminellen auf Authentifizierungs-APIs abgesehen, aber es gibt einige, die direkt auf Anmeldeformulare abzielen. Während die meisten Kombinationslisten kostenlos heruntergeladen werden, können andere Listen, z. B. solche, die sich auf einen bestimmten Service oder eine bestimmte Region beziehen, mit 50.000 Nutzernamen und Passwörtern für ca. 5 US-Dollar verkauft werden.

Abb. 5 – Die STORM AIO-Software ist einfach zu verwenden und kostenlos. Daher ist sie bei Kriminellen, die Credential-Stuffing-Angriffe durchführen, sehr belielbt.

Credential-Stuffing-Angriffe sind fast vollständig automatisiert und werden von AIO-Anwendungen (All-in-One) mit Namen wie SNIPR und STORM gesteuert. Einige AIO-Programme sind kostenlos, für andere fällt vorab eine Registrierungsgebühr an. SNIPR, eines der beliebtesten Programme, wird für ca. 20 US-Dollar angeboten, während STORM (siehe Abbildung 5) online kostenlos erhältlich ist.

AIO-Plattformen wie STORM und SNIPR arbeiten mit Konfigurationsdateien, durch die sie verschiedene Services (wie die in der Medien- und Technologiebranche) nutzen können, ohne sich um Raten- oder andere Sicherheitsbeschränkungen zu kümmern. Die Konfigurationsdateien werden manchmal einfach kostenlos zur Verfügung gestellt; andere kundenspezifische Konfigurationen werden jedoch für mehr als 50 US-Dollar angeboten.

Diese Anwendungen wurden so entwickelt, dass sie die Aktionen eines normalen Nutzers nachahmen. Daher sind für den Schutz dagegen eine entsprechende Planung und die Fähigkeit erforderlich, Angriffe schnell zu erkennen. Die meisten AIOs weisen vorgefertigte Ausweichtechniken für viele standardmäßige Abwehrmaßnahmen auf. Daher sind nutzerdefinierte Lösungen ein Muss, die auf die Anforderungen des Unternehmens zugeschnitten sind. Darüber hinaus muss jeder Abwehrplan Bewusstseinsschulungen für Endnutzer beinhalten, da Kriminelle den gemeinsamen Zugriff auf Konten und recycelte oder schwach und leicht zu erratende Kennwörter ausnutzen.

Sobald die Kriminellen ihre Konfigurationsdateien und Kombinationslisten in die AIO geladen haben, leiten sie die Verbindungen per Proxy auf die Website des Ziels um und versuchen, sich anzumelden. Erfolgreiche Eingaben werden aufgezeichnet, und der Zugriff auf das Konto wird entweder getauscht oder verkauft. Komprommittierte Konten in der Medien- und Technologiebranche können bereits für 5 US-Dollar verkauft werden, einige Konten können jedoch je nach ihren Eigenschaften bis zu 15 US-Dollar einbringen. Rundfunk und Content-Entwicklung sind wichtige Ziele für das Credential Stuffing, weshalb die Konten in diesem Bereich zu einem höheren Preis verkauft werden.

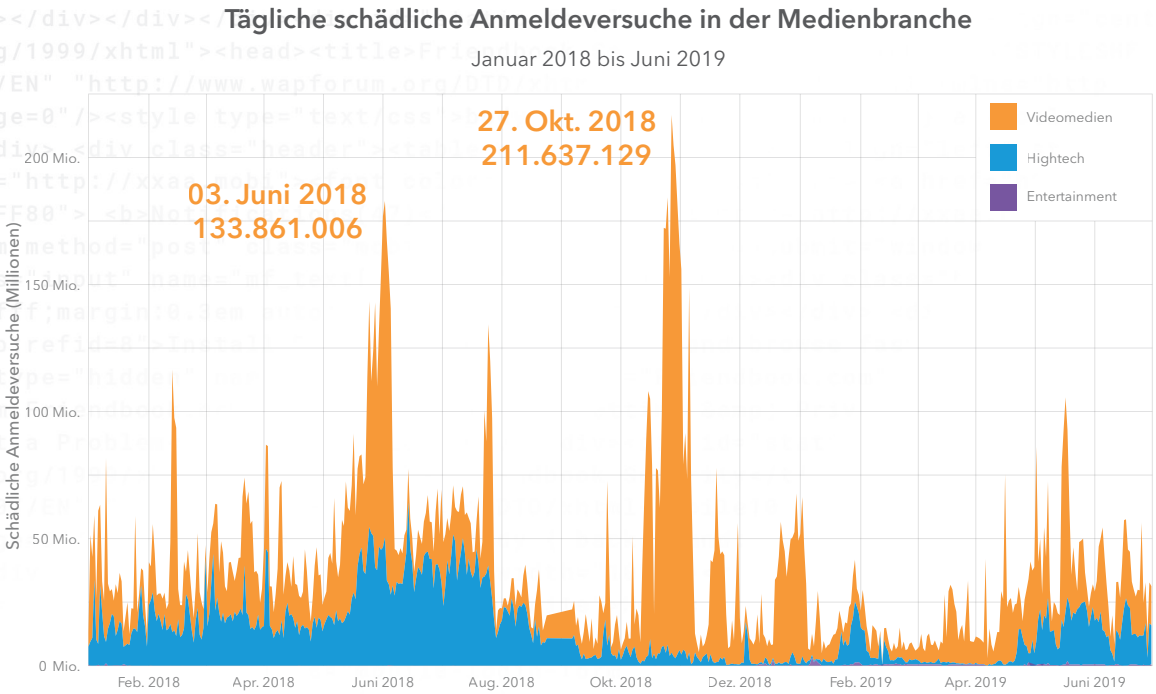


Abb. 6 – Zwei Angriffe im Jahr 2018 führten zu mehr als 340 Millionen Credential-Stuffing-Versuchen

In Abbildung 6 können Sie im selben 18-monatige Zeitrahmen deutlich sehen, dass es die überwältigende Mehrheit der Angriffe auf die Videomedien- und Hightechbranche abgesehen hatte. Die Unterhaltungsbranche ist zwar vertreten, aber im Vergleich zu den beiden anderen Branchen kaum wahrnehmbar. Wie bereits erwähnt, sind Konten in diesen beiden Bereichen Hauptziele, die schnell und mit einem satten Gewinn weiterverkauft werden können.

Wir haben die beiden Monate Juni 2018 und Oktober 2018 herausgegriffen, da beide aus Sicht des Angriffs interessant waren.

Im Juni haben Angreifer sieben verschiedene Organisationen und 14 eindeutige Hosts angegriffen. Das Ziel bestand anscheinend darin, Zugriff auf Daten und Konten mit umfangreichen Inhalten zu erhalten, die später weiterverkauft werden sollten. Bei Betrachtung der anvisierten Kunden ist festzustellen, dass es die Kriminellen auf den Weiterverkauf von Konten in der Videomedienbranche und den Diebstahl neuer Anmeldedaten und anderer Informationen im Hightechsektor abgesehen hatten, die weiterverkauft werden können. Im Oktober griffen Angreifer 18 verschiedene Organisationen und 28 eindeutige Hosts an. Wieder einmal waren die Ziele offensichtlich identisch.

In beiden Fällen wurde die häufigste Angriffsquelle nach Russland zurückverfolgt. Dies ist wahrscheinlich auf die hohe Anzahl von Proxy-Services in diesem Land zurückzuführen. Bei den Angriffen auf alle Bereiche in der Medien- und Technologiebranche folgten auf Russland Kanada, Brasilien, Malaysia und China. Jeder dieser Standorte ist für Proxy-Services, Piraterie sowie für den Kontoweiterverkauf und -handel bekannt.

Durchschnittliche Anzahl schädlicher Anmeldungen nach Branche

BRANCHE	BÖSWILLIGE ANMELDEVERSUCHE	DURCHSCHNITTLICHE ANZAHL SCHÄDLICHER ANMELDUNGEN PRO EINDEUTIGEM ZIEL
Einzelhandel	24.245.971.895	26.556.377
Videomedien	13.760.213.425	151.211.137
Hightech	7.533.980.169	35.537.642
Hotel- und Reisebranche	4.860.206.037	23.941.902
Finanzdienstleistungsbranche	3.900.240.393	27.466.482
Fertigungsindustrie	2.615.438.681	74.726.819
Konsumgüter	1.560.726.138	18.803.929
Soziale Medien	1.079.139.624	37.211.711
Gaming	645.181.719	25.807.269
Andere digitale Medien	331.455.583	5.815.010
Dienstleistungen für Verbraucher	311.243.282	14.147.422
Automobilindustrie	97.816.354	13.973.765
Medien und Entertainment	77.292.308	4.294.017
Öffentlicher Sektor	75.116.539	4.694.784
Unternehmensdienstleistungen	35.908.816	1.158.349

Abb. 7 – Die durchschnittlichen Angriffe pro Host in der Videomedienbranche liegen weit vor jeder anderen Branche

In Abbildung 7 wird die Anzahl der schädlichen Anmeldungen pro eindeutigem Opfer untersucht. Basierend auf den Daten können wir sehen, dass der Einzelhandel zwar die führende Branche ist, die Videomedien- und die Hightech-Branche aber im Durchschnitt härter getroffen werden. Tatsächlich ist die Rate von Angriffen pro Host gegen Videomedien fast fünfmal so hoch wie die der Angriffe gegen die anderen, wenn alle Branchen berücksichtigt werden.

Auffällig in Abbildung 6 ist auch die konsistente Angriffsstufe. In den Sommermonaten, in denen neue Versionen auf verschiedenen Plattformen veröffentlicht werden, steigen die Angriffe sprunghaft an – genauso wie in den Herbstmonaten – aber das ganze Jahr über gibt es Millionen und Abermillionen von Credential-Stuffing-Angriffen im gesamten Internet. Dieses Problem wird natürlich nicht einfach von alleine verschwinden.

Die Hauptziele für Credential-Stuffing-Angriffe während des 18-monatigen Zeitraums waren, wie in Abbildung 8 dargestellt, die USA, Indien, Kanada, Singapur und Australien. Zu den Unternehmen, die an diese Standorte gebunden sind, gehören einige der weltweit führenden Marken im Bereich der Medien- und Technologiebranche. Die Konten und Daten, die die Unternehmen in diesen Bereichen pflegen, sind wertvoll und können leicht gehandelt oder mit Gewinn verkauft werden – und die Kriminellen sind hinter Geld her.

Zu den wichtigsten Quellen für Credential-Stuffing-Angriffe gehörten die USA, Russland, Kanada, Deutschland und Indien. Der Grund dafür, dass Russland und Indien so hoch auf der Liste gelandet sind, waren Proxy-Services, die das Verbergen des wahren Ursprungs von Angriffen vereinfacht haben. Akamai sieht nur das letzte System, das bei einem Angriff verwendet wurde, und nimmt keine weitere Zuordnung vor.

Schädliche Anmeldeversuche – Top-Ziele

ANVISIERTER BEREICH	MEDIENBRANCHEN	ALLE BRANCHEN	GLOBALER RANG IN ALLEN BRANCHEN
USA	17.554.816.847	46.897.833.276	1
Indien	2.455.628.895	3.702.332.247	3
Kanada	1.156.597.318	1.487.337.095	4
Singapur	47.008.228	55.117.432	18
Australien	42.773.334	198.379.421	9
Tschechische Republik	36.139.380	36.139.380	19
Niederlande	15.614.129	15.770.397	22
China	15.105.040	4.758.443.883	2
Deutschland	12.683.512	1.280.565.528	5
Italien	7.532.004	106.015.785	14

Abb. 8 – Die Vereinigten Staaten und Indien waren die Top-Ziele für Credential-Stuffing-Angriffe

Nur weil sich die IP-Adresse eines Angreifers in Russland befindet, bedeutet dies nicht, dass auch der Angreifer dort ist. Kriminelle, die Credential-Stuffing-Angriffe durchführen, verlassen sich nicht nur auf Proxy-Einstellungen, um die Sicherheitsmaßnahmen zu umgehen, sie bieten auch eine Maskierungsebene für ihre Identität.

Im Rahmen unserer Recherchen haben wir einen Proxy-Service gefunden, der Zugriff für einen Preis von 30 US-Dollar bis zu 200 US-Dollar pro Woche bietet. Die Kosten hängen vom Standort des Proxy-Servers und von den Einschränkungen des Kontos ab. Die günstigste Option, die sich in Australien befindet, hat eine Begrenzung von 50 gleichzeitigen Verbindungen (Threads) und verfügt über mehr als 200 Server, die für Verbindungen (genannt Pool) verfügbar sind. China bot eine der teureren Optionen: eine Thread-Grenze von 500 und mehr als 20.000 Server im Pool.

Schädliche Anmeldeversuche – Top-Quellen

QUELLBEREICH	MEDIENBRANCHEN	ALLE BRANCHEN	GLOBALER RANG IN ALLEN BRANCHEN
USA	5.978.803.240	19.946.636.280	1
Russland	2.811.700.327	5.080.433.712	2
Kanada	1.767.056.222	2.423.776.410	4
Deutschland	883.080.860	1.727.582.602	8
Indien	790.854.971	2.167.920.536	5
Vietnam	750.780.050	1.618.414.860	10
Brasilien	692.183.261	2.834.964.769	3
Frankreich	518.293.553	1.358.495.125	13
Niederlande	448.213.143	1.386.280.155	12
Vereinigtes Königreich	424.914.180	1.140.233.591	14

Abb. 9 – Die Vereinigten Staaten und Russland waren während des 18-monatigen Reporting-Zeitraums immer noch die Hauptquellen für Credential-Stuffing-Angriffe.

Fazit

Es kann nicht häufig genug betont werden: Webangriffe und Credential Stuffing sind echte, langfristige Bedrohungen. Sie sind beide Teil einer größeren kriminellen Wirtschaft, die durch ihre symbiotische Beziehung angetrieben wird. Die gängigste Methode für die Entwicklung von Kombinationslisten für Credential Stuffing, besteht darin, die Daten aus einer frisch kompromittierten Datenbank herunterzuladen. Daher kann ein SQLi-Angriff in wenigen Augenblicken zu einem Credential-Stuffing-Angriff werden. Aber der Umgang mit diesen Bedrohungen ist nicht einfach. Unternehmen müssen mit ihren Sicherheitsanbietern und Kunden zusammenarbeiten, um die Ursachen dieser Angriffe anzugehen.

Methodik

Webangriffe

Die Akamai Intelligent Edge Platform ist ein Netzwerk aus mehr als 240.000 Servern in Tausenden von Netzwerken auf der ganzen Welt. Zum Schutz dieses Traffics wird die Kona WAF verwendet und Informationen zu den Angriffen werden in ein internes Tool namens Cloud Security Intelligence (CSI) eingespeist. Anhand dieser Daten, die in Petabyte pro Monat gemessen werden, untersuchen wir Angriffe, analysieren Trends und speisen zusätzliche Informationen in die Lösungen von Akamai ein. Bei den Daten handelt es sich um Millionen täglicher Warnungen auf Anwendungsebene, die aber nicht auf einen erfolgreichen Angriff schließen lassen.

Die Darstellungen und Tabellen in diesem Abschnitt sind auf Aufzeichnungen zwischen Januar 2018 und Juni 2019 beschränkt.

Missbrauch von Anmeldedaten

Die Daten für diesen Abschnitt wurden ebenfalls aus dem CSI-Repository abgerufen. Versuche, Anmeldedaten zu missbrauchen, wurden als fehlgeschlagene Anmeldeversuche für Konten identifiziert, bei denen eine E-Mail-Adresse als Nutzername verwendet wird. Zur Abgrenzung von Missbrauchsversuchen gegenüber Aktivitäten von echten Nutzern, die Tippfehler machen, haben wir zwei verschiedene Algorithmen verwendet. Der erste ist eine einfache volumetrische Regel, die die Anzahl der fehlgeschlagenen Anmeldeversuche für eine bestimmte Adresse zählt. Dieser Vorgang unterscheidet sich insofern von dem, was ein einzelnes Unternehmen ermitteln könnte, als dass Akamai Daten über Hunderte von Unternehmen hinweg korreliert.

Der zweite Algorithmus verwendet Daten aus unseren Bot-Erkennungsservices, um Missbrauch von Anmeldedaten durch bekannte Botnets und Tools zu identifizieren. Mit einem gut konfigurierten Botnet kann eine volumetrische Erkennung vermieden werden, indem der Traffic auf viele Ziele verteilt wird. Erreicht wird dies beispielsweise durch eine große Anzahl von Systemen im Scan oder durch Verteilen des Traffics über einen bestimmten Zeitraum hinweg.

Diese Aufzeichnungen wurden zwischen Januar 2018 und Juni 2019 erfasst.

Herausgeber- und Mitarbeiterverzeichnis

„State of the Internet“-Sicherheitsbericht – Mitwirkende

Omri Hering
Data Analyst Senior –
Missbrauch von Anmeldedaten

Lydia LaSeur
Data Scientist –
Missbrauch von Anmeldedaten, Web-Angriffe

Redaktionsteam

Martin McKeay
Editorial Director

Amanda Fakhreddine
Sr. Technical Writer, Managing Editor

Steve Ragan
Sr. Technical Writer, Editor

Lydia LaSeur
Data Scientist

Marketing

Georgina Morales Hampe
Project Management, Creative

Murali Venukumar
Program Management, Marketing

Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben, und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet”-Sicherheitsberichte von Akamai unter akamai.com/soti.

Weitere Informationen zur Bedrohungsforschung bei Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden akamai.com/threatresearch

Akamai

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai hält Angriffe und Bedrohungen fern und bietet im Vergleich zu anderen Anbietern besonders nutzernahe Entscheidungen, Anwendungen und Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter @Akamai und @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: September 2019


Akamai
Intelligent Security
Starts at the Edge