Leitfaden

Der ultimative Leitfaden für die OWASP Top 21 der automatisierten Bedrohungen und die nötigen Schutzmaßnahmen

INHALTSVERZEICHNIS

Es gibt gute Bots, mit denen Online-Unternehmen ihr Ranking in Suchmaschinen und das Einkaufserlebnis der Kunden verbessern können. Aber es gibt auch bösartige Bots, die heute so diskret zu Werke gehen, dass sie sich mit herkömmlichen Sicherheitslösungen wie einer Web Application Firewall (WAF) oder CAPTCHAs nicht mehr erkennen lassen.

Von Web-Scraping und CAPTCHA-Umgehung über heimtückische Aktivitäten wie Spamming, Kontoübernahme und Credential-Stuffing bis hin zu Sniping und Carding: Automatisierte Bots stehen bei Angreifern, Betrügern, Konkurrenten und anderen Missetätern hoch im Kurs. Die Drahtzieher dieser Betrügereien verbessern ihre automatisierten Programme laufend, damit die Bots noch raffinierter und hartnäckiger werden und menschliches Verhalten so genau nachahmen können, dass ihre Angriffe unbemerkt bleiben.

Angesichts des Anstiegs der automatisierten Bot-Angriffe auf Webapplikationen erstellte das Open Web Application Security Project (OWASP) eine Top 21 der automatisierten Bedrohungen für Webapplikationen. Diese Übersicht soll Unternehmen helfen, die zunehmenden Bedrohungen durch automatisierte Bots besser zu verstehen und abzuwehren.

In diesem Leitfaden werden die einzelnen automatisierten Bedrohungen aus der OWASP-Liste erläutert, zusammen mit den Abwehrfunktionen, die eine spezialisierte Bot-Management-Lösung bieten sollte.

INHALTSVERZEICHNIS

OAT-01: Carding

Carding bezeichnet einen automatisierten Zahlungsbetrug, bei dem Kriminelle eine lange Liste von Kredit- oder Debitkartendaten im Zahlungssystem eines Händlers testen, um herauszufinden, wo die gestohlenen Daten akzeptiert werden. Die Kartendaten stammen aus verschiedenen Zahlungskanälen oder anderen Applikationen oder wurden auf Darknet-Marktplätzen gekauft. Hacker können sich die Kreditkartendaten auch mithilfe von Card-Cracking verschaffen (OWASP OAT-010).

Abwehr

Allgemein empfiehlt sich die Auslagerung aller Zahlungsvorgänge an Anbieter, die hinreichend gerüstet sind, um Carding-Angriffe abzuwehren. Weitere bewährte Best Practices sind die Festlegung eines höheren Mindestbetrags für Zahlungen und IP-Blacklisting.

Bot-Abwehrlösungen sollten einen anderen Ansatz verfolgen und auf einer detaillierten Benutzerverhaltens- und Intent-Analyse basieren, um Carding-Angriffen vorzubeugen.

OAT-02: Token-Cracking

Beim Token-Cracking erlangen Betrüger einen Zugriff auf Identifizierungs-Token, d. h. auf kryptografische Keys, die von Online-Diensten generiert werden. Token werden oft per SMS an die Mobilgeräte von Benutzern gesendet.

Token dienen zur Multi-Faktor-Authentifizierung (MFA), die einen zusätzlichen Authentifizierungsfaktor verlangt, damit Benutzer von einem unbekannten Gerät oder Standort auf Daten zugreifen können. Diese zweistufige Verifizierung soll den unerlaubten Zugriff auf vertrauliche Daten verhindern, aber Cyberkriminelle können sich mit Brute-Force-Methoden einen Zugang verschaffen. Mögliche Folgen sind Identitätsdiebstahl und andere Formen von Betrug. Wird das Token geknackt, erlangt der Angreifer die volle Kontrolle über das Konto des Opfers und kann alle Aktivitäten verfolgen und ändern oder Informationen löschen.

Abwehr

Sicherheitsexperten empfehlen für Benutzer eine Multi-Faktor-Authentifizierung (MFA), die zwei oder mehr Identifizierungsmerkmale nutzt anstatt nur eins. Neben MFA sollten Betreiber von Websites und Applikationen eine Bot-Abwehrlösung zur Erkennung und Blockierung von Bots implementieren, die Phishing-Methoden wie Robocalls verwenden, um Sicherheitsabfragen der Website oder Applikation vorzutäuschen. Solche Taktiken bringen ahnungslose Opfer dazu, ihre einmalig gültigen Passwörter oder Sicherheitscodes dem Angreifer zu übermitteln.

OAT-03: Ad Fraud (Klickbetrug)

Digitaler Ad Fraud bezeichnet vorsätzliche Handlungen, die eine Verfälschung oder Verschleierung der Kennzahlen von Werbeanzeigen bewirken. Dazu wird betrügerischer Traffic eingesetzt (Bots oder Menschen), der Dummy-Impressions generiert und die Click-Through-Rate (CTR) beeinträchtigt. Die ungültigen Aktivitäten von Bots überlasten die Anzeigenserver und untergraben die Bemühungen des Publishers, hochwertige Anzeigenbestände aufzubauen. Außerdem verzerrt nichtmenschlicher Traffic die Website-Analysen und erschwert somit Marketingkampagnen. Ferner schadet ungültiger Traffic dem Markenimage des Publishers, den Anzeigen-Überprüfungsberichten und der Qualitätsbewertung. Die meisten Sicherheitsmaßnahmen sind derzeit nicht in der Lage, menschenähnliche Bot-Aktivitäten herauszufiltern. Zu den verschiedenen Arten von Ad Fraud zählen Traffic Sourcing, Ghost Sites, Domain Spoofing, Ad Stacking, Pixel Stuffing und Ad Injection.

Abwehr

Publisher sollten eine Bot-Lösung mit Intent-Analyse und Pre-Bid-Filterung sowie Fingerprinting und kollektiver Bot Intelligence nutzen, um die Benutzerabsicht zu verstehen und SIVT (Sophisticated Invalid Traffic) herauszufiltern, bevor Anzeigen geschaltet werden, um Ad Fraud in Echtzeit zu verhindern. Eine Bot-Lösung hilft effektiv bei der Überwachung und Blockierung von synthetischem Traffic. So können Publisher ihren Werbetreibenden zusichern, dass die CTR-Statistik nur echte Impressions enthält.

Werbetreibende sollten Zugriff auf Bot-Intelligence-Berichte bekommen, in denen ungültiger Traffic genau kategorisiert wird, z. B. Crawler, Traffic aus bekannten Rechenzentren und SIVT. Dies ermöglicht einen detaillierten Einblick in die Qualität der Impressions und Klicks.

Die Bot-Management-Lösung sollte zudem CAPTCHAs, JavaScript-Challenges oder eine andere Challenge-Response-Technik mit High-Risk-Score bereitstellen.

Die Antworten auf diese Challenges fließen in ein geschlossenes Feedback-System ein, mit dem die Machine-Learning-Modelle dynamisch verbessert und Fehlalarme auf ein Minimum reduziert werden.

OAT-04: Fingerprinting

Mit Fingerprinting werden spezifische Anfragen an die Applikation gesendet, um ihr Informationen zu entlocken und ein Profil der Applikation zu erstellen. Dabei werden in der Regel die Namen und Werte von HTTP-Headern, Namen und Formate von Sitzungs-IDs, Inhalte von Fehlerseitenmeldungen, Groß- und Kleinschreibung im URL-Pfad, URL-Pfad-Muster, Dateierweiterungen und eventuelle softwarespezifische Dateien und Verzeichnisse ausgewertet.

Fingerprinting ist oft auf Datenlecks angewiesen, und die Profilerstellung kann auch Aufschluss über die Netzarchitektur/Topologie geben. Fingerprinting kann sogar ohne direkte Nutzung der Applikation erfolgen, d. h. durch Abfragen eines Speichers mit ungeschützten Applikationsattributen, wie beispielsweise im Index einer Suchmaschine.

Mögliche Symptome sind einzelne HTTP-Anfragen, oft gar keine, aber auch Anfragen für eine Vielzahl fehlender Ressourcen und Anfragen für selten angeforderte Ressourcen.

Abwehr

Zu den bewährten Best Practices zählen die Randomisierung der Inhalte und URLs von Zahlungsseiten und -formularen sowie die Begrenzung von Autorisierungsversuchen pro Sitzung, Benutzer, IP-Adresse, Gerät und Fingerprint.

Bot-Abwehrlösungen sollten Methoden zur Erkennung und Verhinderung von Fingerprinting-Angriffen verwenden, mit denen nach potenziellen Schwachstellen gesucht wird, die sich für schädliche Angriffe ausnutzen lassen.

OAT-05: Scalping

Scalping wird schon seit jeher von Schwarzhändlern und Wiederverkäufern praktiziert, die Veranstaltungstickets und heißbegehrte Waren aufkaufen, um sie später mit einem satten Gewinn weiterzuverkaufen.

Heutzutage findet Scalping hauptsächlich online statt, wobei Kriminelle raffinierte „All-in-one“-Bots einsetzen, die im Internet verkauft werden. Sie sind für das regelmäßige Scannen von E-Commerce-, Ticket- und anderen Websites und Applikationen programmiert, um beliebte Produkte aufzuspüren und in großen Mengen zu kaufen (z. B. bestimmte Sneaker-Marken oder Spielekonsolen), bevor normale Kunden überhaupt eine Chance haben, sich anzumelden und einen Kauf zu tätigen. Die gehorteten Produkte werden anschließend zügig über Websites wie eBay und andere Portale verkauft, die den Second-Hand-Markt bedienen.

Scalping-Bots besuchen immer wieder in kurzen Zeitabständen populäre E-Commerce-Portale und lauern auf Produktlaunches, d. h. die Einführung sehnlichst erwarteter Artikel wie Sneaker oder Spielekonsolen, Veranstaltungstickets und andere Produkte in begrenzter Auflage. Dazu müssen die Betrüger hinter diesen Bots zunächst Benutzerkonten in Online-Shops erstellen. Dafür verwenden sie verschiedene Identitäten, IP-Adressen, Zahlungskarten, Lieferadressen oder Kombinationen davon, um Betrugserkennungssysteme zu überlisten.

Abwehr

Viele E-Commerce-Portale setzen Höchstgrenzen für die Anzahl der Artikel fest, die Käufer in ihren Warenkorb legen können. Andere verlangen die persönliche Abholung von Produkten aus ihren Shops oder haben „Reibungspunkte“ eingebaut, um Scalping-Aktivitäten auszubremsen (was aber auch echte Käufer verärgern kann). Beispiele dafür sind das Anfordern von Identitätsnachweisen, das Lösen von CAPTCHAs oder die Ausgabe von Tokens, mit denen Bestandskunden oder Mitglieder des Treueprogramms Priorität erhalten. Leider lässt sich keine dieser Methoden für große E-Commerce- und Ticket-Portale skalieren, wodurch es Schwarzhändlern meist gelingt, die Abwehrmaßnahmen zu umgehen.

Scalping-Bots sind problemlos im Internet erhältlich, und moderne Bot-Entwickler bieten sogar Kundenservice und ausgelagerte CAPTCHA-Löseverfahren, damit ihre Nutzer die Bots optimal einsetzen können. Wenn ein Unternehmen versucht, die Bots durch traditionelle Methoden wie das Blockieren bestimmter IP-Adressen, Regionen oder Rechenzentren aufzuhalten, schalten Scalping-Bot-Betreiber einfach auf gekaperte private Geräte und Proxy-IP-Adressen um, sodass sie herkömmlichen Abwehrsystemen durch die Lappen gehen.

Eine ausgefeilte Bot-Management-Lösung nutzt verschiedene Methoden, um den Betrügern das Handwerk zu legen. Durch eine Kombination von Verhaltensanalyse und Machine Learning mit Device-Fingerprinting wird der Traffic in Echtzeit analysiert, um bösartige Bots zu erkennen und zu blockieren. Bot-Anbieter, die eine Challenge-Response-Authentifizierung wie die Krypto-Challenge „Proof-of-Work“ unterstützen, können den mehrschichtigen Schutz vor automatisierten Programmen ergänzen.

OAT-06: Expediting

Expediting bezeichnet einen beschleunigten Prozess, mit dem explizite oder implizite Annahmen über die normale Nutzung der Applikation verletzt werden, um unfaire individuelle Vorteile zu erzielen. Dies ist oft mit Täuschung und Verlusten für andere Parteien verbunden.

Im Gegensatz zu Skewing (OAT-016), das sich auf Kennzahlen auswirkt, bewirkt Expediting nur die schnellere Abwicklung einer Reihe von Applikationsprozessen. Spamming (OAT-017) unterscheidet sich von Expediting darin, dass bei Spam das Hinzufügen von Informationen und nicht der Prozessfortschritt im Fokus steht.

Ein typisches Symptom von Expediting ist das ungewöhnlich schnelle Durchlaufen mehrstufiger Prozesse.

Abwehr

Unternehmen können automatisierte Nutzung durch Device-Fingerprinting präzise erkennen und einschränken, um bösartige Bots zu blockieren. Eine hochwertige Bot-Management-Lösung erkennt Taktiken, mit denen Angreifer ihre Device-Fingerprints verschleiern wollen, und nutzt kollektive Bot Intelligence und KI zur Bot-Erkennung in Echtzeit.

OAT-07: Credential-Cracking

Mit Credential-Cracking, das auch als „Brute-Forcing“ bezeichnet wird, versuchen Betrüger, gültige Zugangsdaten herauszufinden, indem sie verschiedene Benutzernamen und Passwörter eingeben (meist aus Listen gestohlener Kontozugangsdaten, die von Kriminellen offengelegt wurden). Hacker dringen mithilfe von Bots in Kundenkonten ein, wobei sie Brute-Force-Angriffe, Wörterbuchangriffe (Eingabe langer Zahlen oder Wörter) und Guessing-Angriffe verwenden, um gültige Zugangsdaten herauszufinden. Zu den Symptomen von Brute-Force-Angriffen gehören ein plötzlicher Anstieg fehlgeschlagener Anmeldeversuche und viele Kundenbeschwerden wegen geknackter Konten.

Abwehr

Online-Unternehmen nutzen zahlreiche Methoden, um Bot-Traffic auszuschalten und Kontoübernahmen zu verhindern. Dazu gehören altbewährte Verfahren wie die Beschränkung der Anmeldeversuche, ein robuster Authentifizierungsprozess, IP-Blacklisting, die Konfiguration von WAF-Regeln und CAPTCHAs.

Lösungen für Bot-Erkennung und -Abwehr sollten Verhaltens- und Intent-Analysen, Machine Learning sowie Device- und Browser-Fingerprinting nutzen, um schädliche Bots abzufangen, die Credential-Cracking-Angriffe mit dem Ziel der Kontoübernahme ausführen wollen. Idealerweise sollten diese Lösungen auch spezielles Machine Learning für URL- und API-Schutz sowie neuartige Krypto-Challenges zur Erkennung und Blockierung bösartiger Bots umfassen.

OAT-08: Credential-Stuffing

Beim Credential-Stuffing wird die Tatsache ausgenutzt, dass viele Menschen gerne dieselbe Kombination aus Benutzername und Passwort auf mehreren Websites verwenden. Hacker testen Listen mit Zugangsdaten, die sie sich durch Datenschutzverletzungen verschafft (oder im Darknet gekauft) haben, mithilfe von Bots auf einer Reihe von Websites. Dabei hoffen sie darauf, dass ein Opfer auf verschiedenen Websites dieselben Zugangsdaten gewählt hat.

Im Gegensatz zu Credential-Cracking werden bei Credential-Stuffing keine Brute-Force-Angriffe eingesetzt, und Werte müssen nicht erraten werden. Vielmehr werden mit den gestohlenen Kombinationen aus Benutzername und Passwort massenweise Anmelde-versuche gestartet. Ein typisches Symptom von Credential-Stuffing sind aufeinanderfolgende Anmeldeversuche mit unterschiedlichen Zugangsdaten über denselben HTTP-Client.

Abwehr

Online-Unternehmen nutzen diverse Methoden, um Bot-Traffic auszuschalten und Kontoübernahmen zu verhindern. Zum Beispiel die Beschränkung der Anmeldeversuche, ein robuster Authentifizierungsprozess, IP-Blacklisting, die Konfiguration von WAF-Regeln und CAPTCHAs.

Lösungen für Bot-Erkennung und -Abwehr sollten nicht-intrusive API-basierte Verfahren nutzen, um schädliche Bots abzuhalten, die Credential-Stuffing-Angriffe zwecks Kontoübernahme ausführen wollen. Idealerweise sollten diese Lösungen auch Intent-Analysen zur Bot-Erkennung beinhalten.

Progressive JavaScript-Challenges können helfen, die Angriffe schneller einzudämmen, da sie den Ressourcen-bedarf bösartiger Bots erhöhen und damit den Abbruch des Angriffs erzwingen.

OAT-09: CAPTCHA-Umgehung

CAPTCHAs dienen zur Unterscheidung zwischen legitimen Benutzern und Bots, doch Bedrohungsakteure können CAPTCHAs mit Bots umgehen, die visuelle und/oder akustische CAPTCHAs und ähnliche Rätsel/Challenges automatisch analysieren und die Antworten finden.

Typische Symptome sind hohe Erfolgsquoten bei der CAPTCHA-Lösung durch betrügerische Konten oder verdächtig schnelle/gleichmäßige CAPTCHA-Lösungszeiten.

Abwehr

Unternehmen können eine Überwachung und Beschränkung der Anzahl an Kartenautorisierungsversuchen pro Sitzung, Benutzer, IP-Adresse, Gerät und Fingerprint einrichten. Dadurch werden verdächtige Autorisierungsversuche und bösartige Benutzer blockiert, sobald sie beim Testen verschiedener Kartennummern eine bestimmte Anzahl Fehlversuche erreicht haben.

Automatisierte Nutzung lässt sich durch reputationsbasierte Verfahren erkennen und einschränken. Insbesondere können Unternehmen den geografischen Standort und/oder die IP-Adresse heranziehen, um Listen zu erstellen, mit denen der Zugriff auf Zahlungsvorgänge in der Applikation blockiert wird.

Unternehmen können Bot-Lösungen mit Krypto-Challenge einsetzen, die CAPTCHA-fähige Bots erkennen und blockieren. Mit der Krypto-Challenge „Proof of Work“ wird dem Benutzer kein CAPTCHA angezeigt, sodass es für Bots wesentlich schwieriger ist, das CAPTCHA zu lösen.

OAT-10: Card-Cracking

Ähnlich wie Carding (OAT-1) basiert auch Card-Cracking auf Bots, die betrügerische Aktivitäten mit Kreditkarten und anderen Zahlungsmethoden ausüben, indem sie Zahlungsdetails erraten oder bereits bekannte (meist gestohlene) Zahlungsdetails missbrauchen. Card-Cracking ist ein gängiges Beispiel für den Missbrauch von Webapplikationen, in diesem Fall mit Kreditkartendaten. Dabei wird versucht, gestohlene Zahlungskartendaten zu validieren.

Zu den Symptomen von Card-Cracking gehören das Zurücklassen nicht bezahlter Warenkörbe, ein geringerer durchschnittlicher Warenkorbwert, ein höherer Anteil fehlgeschlagener Zahlungen bzw. Zahlungsautorisierungen sowie vermehrte Rückbuchungen.

Abwehr

Unternehmen müssen sicherstellen, dass sie ungewöhnliches Verhalten speziell bei Zahlungs-Gateways erkennen und Card-Cracking-Versuche blockieren können. Darüber hinaus sollte eine Bot-Management-Lösung in der Lage sein, mehrere Datenströme zu kombinieren, darunter Mausbewegungen, Tastatureingaben und URL-Folgen. Dies hindert Bots am systematischen Knacken von Zahlungskarten.

OAT-11: Scraping

Content-Scraping (auch als Web-Scraping oder Data-Scraping bezeichnet) bedeutet, dass einzigartige/originale Inhalte von Websites gestohlen und anderweitig veröffentlicht werden. Content-Scraper kopieren in der Regel den gesamten Inhalt und geben ihn als eigenen aus, z. B. Blogs, Studien, Produktbewertungen, Finanzinformationen usw.

Im einfachsten Fall erfolgt Content-Scraping durch manuelles Kopieren und Einfügen. Fortschrittlichere Methoden beruhen auf Bots, die Websites durchsuchen und innerhalb weniger Sekunden Tausende von Seiten kopieren.

Content-Scraping wird häufig von Online-Publishern praktiziert, die ihre Websites durch Werbeeinnahmen finanzieren. Drittanbieter-Scraper durchsuchen und kopieren hochwertige Inhalte anderer Websites, die viele Keywords enthalten. Weitere Opfer, deren Website-Inhalte häufig gestohlen werden, sind Blogger und Medienunternehmen.

Abwehr

Eine Bot-Abwehrlösung sollte Intent-Analysen und teilüberwachtes Machine Learning, Device- und Browser-Fingerprinting, Verhaltensmodellierung und dynamische Turing-Tests nutzen, um Scraping-Bots zu blockieren.

API-Schutz spielt ebenfalls eine kritische Rolle. Scraper und Konkurrenten nutzen API-Schwachstellen aus, um mithilfe von Bots sensible Daten zu stehlen. Dabei ist erneut Machine Learning von Bedeutung, verbunden mit proprietären Modellen wie API-Ablaufsteuerung, Authentifizierungssteuerung, absichts-basierter Verhaltensanalyse und Aufrufkontext, um bösartige API-Aufrufe präzise zu erkennen und abzuwehren.

OAT-12: Auszahlung

Auszahlung (Cashing Out) bezeichnet einen Vorgang, der gestohlene und zuvor validierte Zahlungskarten oder andere Kontozugangsdaten in einer Applikation nutzt, um sich Geld oder wertvolle Waren zu verschaffen. Manchmal erfolgt diese Auszahlung in Verbindung mit Betrug bei der Produktrückgabe.

Häufige Symptome sind vermehrte Rückbuchungen, die verstärkte Nutzung verknüpfter Konten und eine höhere Nachfrage nach hochwertigen Waren oder Dienstleistungen.

Abwehr

Unternehmen können die Anzahl der Transaktionen pro Benutzer, IP-Adresse, Sitzung oder Gerät beschränken oder eine strengere Überprüfung auf Zahlungsseiten einrichten, um Betrüger abzuschrecken.

Neben der Erkennung und Blockierung von ungewöhnlichem Verhalten oder Traffic bietet eine Bot-Management-Lösung einen weiteren Vorteil, nämlich kollektive Intelligence (Bedrohungsinformationen aus mehreren Datenbanken). Damit lassen sich Bot-Netzwerke über verschiedene geografische Regionen hinweg schneller aufdecken. Außerdem werden neue Angriffsmuster erfasst und geteilt, damit auch andere davon profitieren.

OAT-13: Sniping

Beim Sniping wird in allerletzter Minute ein Gebot bzw. Angebot für eine bestimmte Ware oder Dienstleistung gemacht. Dadurch bleibt anderen Benutzern keine Zeit mehr, selbst noch zu bieten.

Sniping kann auch darin bestehen, Systemlatenzen mithilfe von Timing-Angriffen automatisiert auszunutzen. Dabei kommt es auf richtiges Timing und sofortiges Handeln an. Am häufigsten ist Sniping bei Auktionen anzutreffen, aber diese Bedrohung nimmt auch andere Arten von Applikationen ins Visier. Sniping geht in der Regel zulasten anderer Benutzer und kann als eine Form von Denial of Service betrachtet werden.

Häufige Symptome sind zunehmende Beschwerden von Benutzern, die sich keine Waren oder Dienstleistungen sichern können, oder unerwartet hohe Erfolgsquoten bestimmter Benutzer.

Abwehr

Sniping-Bots lassen sich auf intelligente Weise erkennen und stoppen, indem überwacht wird, ob Benutzer die Schritte zum Ausfüllen von Zahlungs-/Bestätigungsseiten umgehen. Diese Überwachung auf unvollständige Schritte gibt Einblick in ungewöhnliche Trends und auffällig hohe Erfolgsquoten.

Mithilfe eines speziellen API-Machine-Learning-Moduls in Verbindung mit Intent-Analyse kann eine hochwertige Bot-Management-Lösung alle Anomalien im API-Ablauf und Aufrufkontext erkennen.

OAT-14: Schwachstellen-Scans

Mit Schwachstellen-Scans wird eine Applikation überwacht und durchsucht, um ihre empfindlichen Stellen zu finden. Durch eine systematische Auflistung und Untersuchung von identifizierbaren, erratbaren und unbekannten Inhaltsorten, Pfaden, Dateinamen und Parametern sollen Anfälligkeiten und wunde Punkte bestimmt werden. Manche Schwachstellen-Scans sind bösartiger Natur, während andere von befugten Engines durchgeführt werden und hilfreiche Informationen liefern.

Zu den Symptomen gehören eine erhöhte Fehleranzahl, eine extrem hohe Applikationsnutzung von einer einzigen IP-Adresse aus, ein hohes Verhältnis von GET/POST- zu HEAD-Anfragen für einen Benutzer, eine Sitzung oder IP-Adresse und wiederholte Missbrauchsversuche an Einstiegspunkten der Applikation.

Abwehr

Unternehmen können zum einen fehlgeschlagene Autorisierungen oder Authentifizierungen überwachen. Zum anderen empfiehlt es sich, die Anzahl an Fehlversuchen bei der Eingabevalidierung oder Autorisierung pro Benutzer, Sitzung, IP-Adresse oder Gerät zu beschränken.

Die Einführung spezieller Tools für Schwachstellen-Scans hilft Unternehmen bei der Kontrolle und Eindämmung dieser Scans. Mithilfe einer Bot-Manager-Lösung lassen sich Angriffe vermeiden, bei denen diese Schwachstellen ausgenutzt werden.

OAT-15: Denial of Service

Diese Bots stellen eine neue Version eines altbekannten Angriffsvektors dar. Sie nehmen Web- und mobile Applikationen sowie Websites ins Visier mit dem Ziel, ihre Ressourcen lahmzulegen, damit ein Denial of Service (DoS) entsteht. Klare Anzeichen für einen DoS-Angriff auf eine Website oder Webapplikation sind eine nachlassende Website-Leistung und eine Verschlechterung ihrer Dienste. Ebenso eindeutige Symptome sind der Ausfall einer Applikation oder ein plötzlicher Anstieg an Benutzerkonten, die keinen Zugriff mehr haben.

Abwehr

Stellen Sie sicher, dass Ihre Bot-Management-Lösung einen plötzlichen Anstieg automatisierter Aktivitäten bei kritischen Applikationsressourcen präzise erkennen kann, um das betrügerische Ausnutzen von Sicherheitsschwachstellen in der Geschäftslogik zu unterbinden. Wählen Sie für Bot-Management einen Anbieter, der über Bedrohungsinformationen aus Tausenden von Interneteigenschaften verfügt und Angriffe mithilfe von Device-Fingerprinting erkennt.

Ferner sollte jede Bot-Management-Lösung Teil einer mehrschichtigen Integration mit anderen DDoS-Abwehrsystemen (Distributed Denial of Service) sein. Bot-Management-Lösungen eignen sich hervorragend zum präzisen Erkennen und Analysieren bösartiger Bots, um sie von legitimem Traffic zu unterscheiden, aber wenn Sie auch die Verfügbarkeit Ihrer Online-Dienste sicherstellen möchten, benötigen Sie darüber hinaus eine DDoS-Abwehrlösung. Die Bot-Management-Lösung ergänzt deren Funktionen, indem sie die DDoS-Lösung und/oder WAF in Echtzeit mit Datenfeeds für umfassenden Schutz versorgt.

Zudem verstärken Bot-Management-Lösungen die Cloud-DDoS-Abwehrsysteme und WAFs durch ihre Verhaltens- und Intent-Analyse, um automatisierte Programme zu erkennen und zu blockieren.

OAT-16: Skewing

Bots können Systeme und Prozesse zur Geschäftsanalyse beeinträchtigen, die z. B. für digitale Werbung, Treueprogramme und Pay-per-Click (PPC) eingesetzt werden. Dadurch erhält das Opfer verfälschte Berichte und Daten, die letztendlich zu Fehlentscheidungen führen. Skewing, Ad Fraud (Klickbetrug) und Spamming sind Paradebeispiele für diese Art von Applikationsmissbrauch. Bei Skewing und Ad Fraud werden die Klickzahlen manipuliert, was sich auf die Webleistung und Werbekennzahlen und folglich auf den Umsatz auswirkt. In beiden Fällen zeigt sich ein Rückgang der Klicks/Impressions und der Konversionen. Gleichzeitig werden stark verzerrte Messwerte verzeichnet, die erheblich von den typischen Schwellenwerten abweichen.

Abwehr

Machine Learning ist ein zentrales Instrument zur Abwehr dieser Bedrohungen. Gegen Skewing helfen domänenspezifische Machine-Learning-Methoden, die ungewöhnliches Benutzerverhalten erkennen und Bots an der Manipulation von Geschäfts-KPIs hindern. Eine Bot-Management-Lösung der Enterprise-Klasse kann mithilfe von JavaScript-Tags Hunderte von Parametern erfassen, um raffinierte Bot-Muster zu erkennen und Skewing zu unterbinden. Außerdem erleichtert eine solche Lösung die Schätzung und Filterung von nichtmenschlichem Traffic in Berichten für bezahlte und organische Nutzerakquise. Stellen Sie dazu sicher, dass sich die Bot-Management-Lösung auch mit Marketing-Analyseplattformen integrieren lässt.

OAT-17: Spamming

Spamming dient zum Veröffentlichen falscher und fragwürdiger Informationen in Foren, Kommentarbereichen, Blogs, Wiki-Webseiten, öffentlich zugänglichen Webseiten und Content-Contribution-Plattformen.

Abwehr

Genau wie Skewing lässt sich auch Spamming am besten durch zeitreihenbasiertes Machine Learning abwehren. Damit können betrügerische Formulareinreichungen und Spam-Kommentare in Online-Portalen und Foren erkannt werden.

OAT-18: Footprinting

Footprinting ist eine Online-Sicherheitsbedrohung, die Informationen sammelt mit dem Ziel, möglichst viel über die Zusammensetzung, Konfiguration und Sicherheitsvorkehrungen einer Applikation zu lernen. Im Gegensatz zu Scraping liefert Footprinting einen Überblick über die Applikation selbst, d. h. nicht ihre Daten. Mithilfe von Footprinting werden alle URL-Pfade, Werte, Parameter und Ad-Prozessabläufe ermittelt. Beim Durchforsten der Applikation werden weitere Pfade erkannt und ebenfalls untersucht.

Footprinting kann auch Brute-Force-Angriffe und Wörterbuchangriffe beinhalten. Ferner kann Fuzzing zum Einsatz kommen, um weitere Applikationsressourcen und -funktionen ausfindig zu machen.

Typische Symptome sind ein Anstieg der System- und Applikationsfehlercodes, z. B. die HTTP-Statuscodes 404 und 503, oder ein ungewöhnliches Benutzerverhalten.

Abwehr

Der Schutz von URLs und wichtigen APIs hat für Unternehmen hohe Priorität. Durch die Unterscheidung zwischen legitimen und schädlichen Aufrufen können Missetäter schnell erkannt und blockiert werden, bevor sie Schwachstellen ausnutzen. Neben Intent-Analysen eignen sich spezielle Machine-Learning-Module für APIs, wie z. B. Ablaufsteuerung, Aufrufkontext oder Analyse der Authentifizierungsabläufe.

OAT-19: Kontoerstellung

Bei dieser Online-Sicherheitsbedrohung erstellen Einzelpersonen oder Unternehmen in einer Applikation eine Vielzahl von Konten, mit denen sie anschließend Missbrauch betreiben. Beispiele dafür sind Content-Spam, Verbreitung von Malware, Geld- und Warenwäsche, störende Aktionen, Schädigung des Markenimages oder Verfälschung von SEO, Bewertungen und Website-Analysen.

Zu den Symptomen zählen ungewöhnlich viele Kontoeinrichtungen, Konten mit wenig Informationen im Vergleich zum typischen Kontoinhaber sowie Konten, die nach der Erstellung nicht sofort genutzt werden.

Abwehr

Unternehmen können die Funktionen, die für neu erstellte Konten verfügbar sind, vorübergehend einschränken. Fortschrittliche Bot-Lösungen, die abnormales Kontoverhalten mithilfe von Intent-Analysen oder progressiven JavaScript-Challenges überwachen und erkennen, können die Applikation vor unerwünschtem Zugriff schützen.

OAT-20: Konto-Aggregation

Bei der Konto-Aggregation werden Informationen aus verschiedenen Konten, wie z. B. Kreditkartenkonten, Bankanlagekonten oder andere Geschäftskonten, an einem zentralen Ort gesammelt. Diese Aggregation kann zum Ziel haben, Informationen eines Benutzers aus mehreren Applikationen oder aber Informationen mehrerer Benutzer einer einzigen Applikation zusammenzuführen.

Zu den häufigen Symptomen gehören fehlende Endbenutzer-Interaktion, Verhaltensmuster beim Kontozugriff, die nicht dem Benutzerprofil entsprechen, und auffällige Aktivitätsspitzen.

Abwehr

Jedes Unternehmen muss prüfen, wo Konto-Aggregation für eine Applikation zur Bedrohung werden kann, und mit Testfällen für Konto-Aggregation nachweisen, dass eine Applikation jede Form von Aggregation durch Benutzer erkennt und verhindert. Beispielsweise müssen IP-Adressen bekannter Aggregationsdienste erkannt und blockiert werden.

Konto-Aggregation ist eine Sonderform der Kontoübernahme und erfordert möglicherweise spezielle Tools wie einen Bot-Manager, der zwischen legitimem und nicht legitimem Traffic unterscheidet und Schadprogrammen den Zugang zur Applikation verweigert. Des Weiteren werden dedizierter API- oder URL-Schutz und innovative Abwehrmethoden wie progressive JavaScript-Challenges empfohlen, um selbst ausgefeilte Bots abzuhalten.

OAT-21: Denial of Inventory

Durch Denial of Inventory werden die Bestände von Waren oder Dienstleistungen reserviert, ohne jedoch den Kauf zu tätigen bzw. die Transaktion abzuschließen. Mit dieser Bedrohung sollen ganz gezielt die Bestände von E-Commerce-Händlern, Ticketverkäufern, Fluggesellschaften usw. „als Geisel genommen“ werden. Dazu wird ein Kaufprozess eingeleitet, ohne zur Kasse zu gehen, und sobald die zulässige Zeit für die Bezahlung verstrichen ist, beginnt der Vorgang von Neuem. Andere Bots hingegen kaufen den gesamten Bestand auf einmal auf, damit Cyberkriminelle die Waren weiterverkaufen können. Dies wird als Scalping bezeichnet (OAT-5). Das Ergebnis sind direkte finanzielle Verluste.

Abwehr

Abwehrmaßnahmen für Denial-of-Inventory-Angriffe hängen davon ab, welche Art von Bot eingesetzt wird. Ältere Bots der 1. und 2. Generation lassen sich durch individuell angepasste Regeln für Bezahlseiten/APIs abfangen, die jeden Versuch unterbinden, Produkte systematisch in den Warenkorb zu legen. Die Abwehr fortschrittlicher Bots der 3. und 4. Generation erfordert jedoch die bereits erwähnte absichtsbasierte Verhaltensanalyse. Die Validierung von Abläufen und Besucheraktionen trägt entscheidend dazu bei, Bedrohungen unterschiedlicher Komplexität abzuwehren und gleichzeitig Fehlalarme zu minimieren.

Über Radware

Radware® (NASDAQ: RDWR) ist ein weltweit führender Anbieter von Lösungen zur Cybersicherheit und Applikationsbereitstellung für physische, cloudbasierte und softwaredefinierte Rechenzentren. Das preisgekrönte Lösungsportfolio sichert durch die Bereitstellung von Infrastruktur, Applikationen und Dienstleistungen zum IT-Schutz und zur Verfügbarkeit für Unternehmen weltweit die digitale Erfahrung. Die Lösungen von Radware versetzen mehr als 12.500 Unternehmens- und Netzbetreiber-Kunden weltweit in die Lage, sich schnell an Herausforderungen am Markt anzupassen, die Geschäftskontinuität zu wahren und maximale Produktivität bei niedrig gehaltenen Kosten zu erreichen. Weitere Informationen finden Sie unter www.radware.com.

Schließen Sie sich der Radware-Community an und folgen Sie unseren Aktivitäten hier: Radware-Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube und Radware Connect (iPhone®-App). Zudem stellt DDoSWarriors.com, unser Sicherheitscenter, umfassende Analysen zu Tools, Trends und Bedrohungen rund um DDoS-Angriffe bereit.