MYRA

WHITEPAPER BOT MANAGEMENT

Bot-generierten Traffic effizient steuern

Schutz und Kontrolle Ihrer Website und Ihres E-Business vor den Bedrohungen durch automatisierte Anfragen.

Ansturm im Onlineshop: Die Kehrseite

Website-Betreiber können sich heute nicht nur über Traffic-Zuwachs freuen, sondern müssen diesen genau analysieren und steuern, um ihr Business zu schützen.

Wer eine Website betreibt, macht seine Geschäftsdaten für die breite Öffentlichkeit zugänglich. Sie sind damit nicht nur für Kunden oder sonstigen gewünschten Besuch einsehbar, sondern auch für Dritte, die nicht immer nur Gutes im Schilde führen. Hier kommen Bots ins Spiel – automatisierte Computerprozesse, die sich wiederholende Aufgaben weitgehend automatisch abarbeiten.

Sie machen inzwischen rund die Hälfte des gesamten Web-Traffics aus. Dabei kann es sich um Suchmaschinen handeln, um Web-Monitoring Systeme, um Scraper, Crawler oder sonstige automatisierte Prozesse. Viele davon sind durchaus hilfreich – beispielsweise der Googlebot, der Webseiten durchleuchtet und damit den Suchmaschinenindex und das Ranking in den Suchergebnissen aktualisiert.

20 Prozent des Web-Traffics sind schädliche Bots

Ein erheblicher Anteil fällt jedoch in die Kategorie „schädlich". Über 20 Prozent des Traffics sind heute bösartige Bots, die dem Website-Betreiber gefährlich werden können. Getarnt als menschliche Nutzer oder gutartige Bots, greifen sie mit unterschiedlichen IP-Adressen und aus unterschiedlichen Netzwerken auf Websites zu. Systemadministratoren können zwar die einzelnen Zugriffe sehen, aber nicht den Zusammenhang dieser verteilten Zugriffe.

Die Ziele von Bad oder Evil Bots sind vielfältig: Sicherheitslücken ausspähen und ausnutzen, Webserver aus- bzw. überlasten, Inhalte kopieren und ungewünscht weiterverwenden, Blockieren von Warenkörben, großflächiges Testen von Nutzerdaten und Passwörtern, Preise ausspionieren, das Netzwerk infizieren bzw. kontrollieren etc. Im vorliegenden Whitepaper werden die einzelnen Bot-Typen mit ihren jeweiligen Spezifika dargestellt. Erklärt wird anschließend, wie man ihrer mittels der Fingerprint-Technologie von Myra Security sowie diverser abgestufter Maßnahmen Herr werden kann.

Diese Bots bedrohen Ihr Business

Credential Stuffing

Bots testen Nutzer-/Passwort-Kombinationen im großen Stil.
Ihr Ziel: Onlinebetrug.

Price Grabbing

Bots greifen Produktpreise oder ganze Preisgefüge ab.
Ihr Ziel: Konkurrenten zu schädigen.

Content- / Product Grabbing

In Sekundenschnelle kopieren Bots Produkt-beschreibungen oder ganze Websites.
Ihr Ziel: ein eigener Webshop.

Formular Spam

Über Kontaktformulare bombardieren Bots Unternehmen mit ihren Botschaften.
Ihr Ziel: Phishing.

Hype Sales

Bots stechen reale Kunden aus und sichern sich begehrte Artikel.
Ihr Ziel: Weiterverkauf mit hohem Gewinn.

Cart Abandonment

Bots füllen Warenkörbe ohne den Kaufprozess abzuschließen.
Ihr Ziel: Geschäftsschädigung.

Kreditkartentests

In Sekundenschnelle testen Bots Kreditkarten auf Ihre Gültigkeit.
Ihr Ziel: Betrügerischer Einsatz.

Account Creation & Takeover

Massenhaft neue Nutzerkonten zu erstellen ist für Bots ein Kinderspiel.
Ihr Ziel: Datenmissbrauch.

Skewing

Bots verfälschen Web-Analysen.
Ihr Ziel: Opfer zu falschen Entscheidungen zu verleiten.

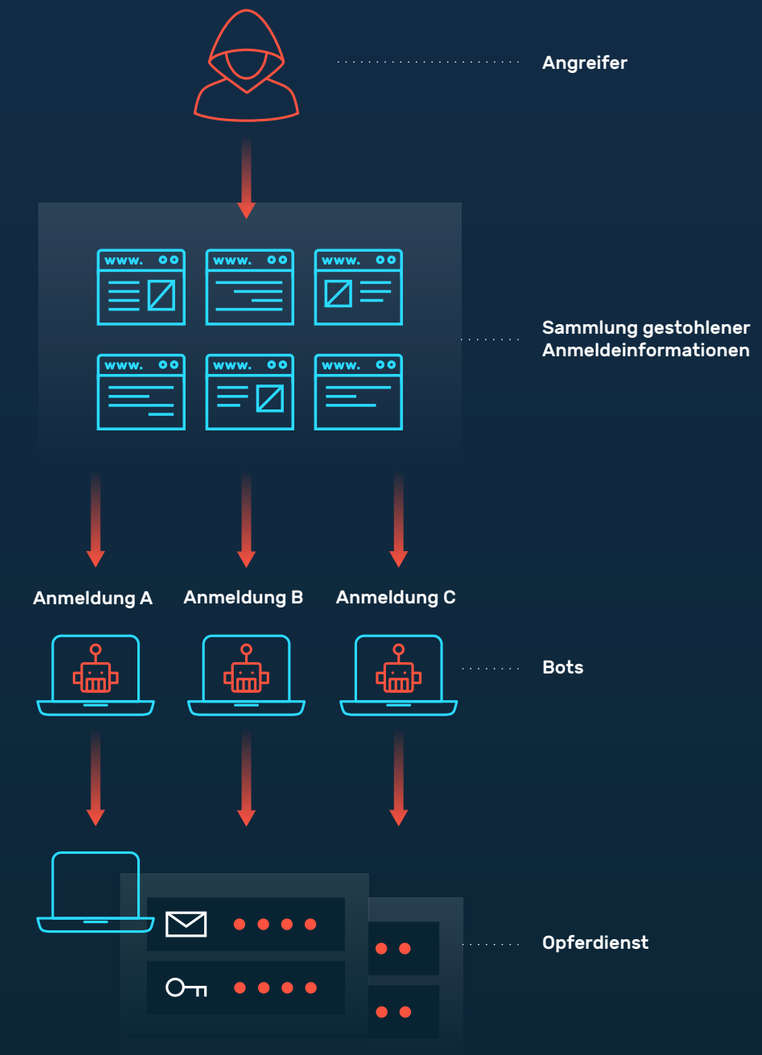
Credential Stuffing

Bots können in Sekundenschnelle Millionen Nutzerdaten auf Ihre Validität überprüfen.

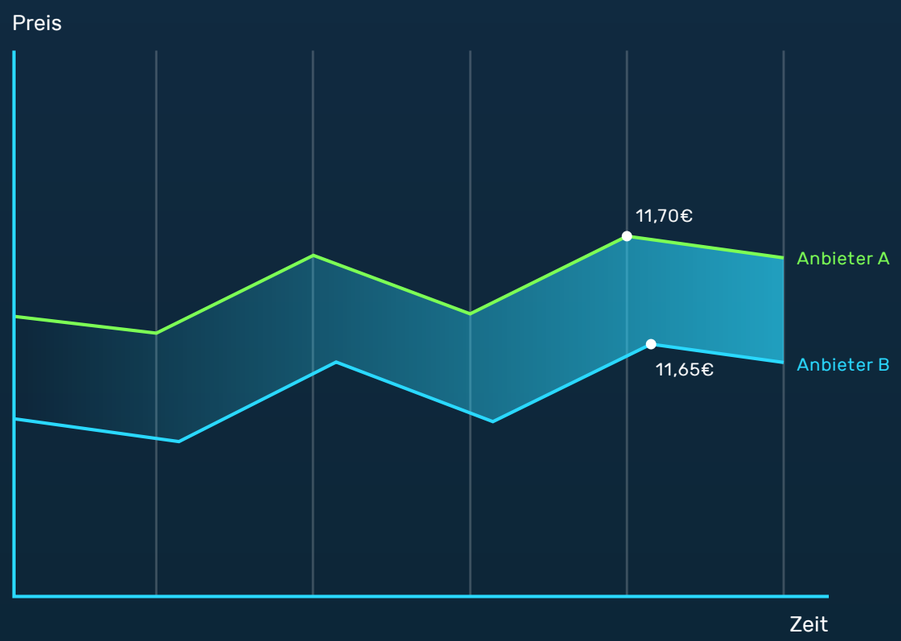
Werden gestohlene Nutzer/Passwort-Kombinationen auf Websites im großen Stil getestet, spricht man von Credential Stuffing. Betroffen ist im Prinzip jede Website, die über einen Log-in verfügt. Kriminelle greifen funktionierende Kombinationen aus Benutzername und Passwort von anderen Websites ab und können die gestohlene Identität dazu nutzen, die Website des anvisierten Unternehmens zu entern. Funktioniert von 10.000 Kombinationen nur eine einzige, ist der GAU für den attackierten Website-Betreiber bereits eingetreten. Im Onlineshop werden Einkäufe getätigt, im Onlinebanking Gelder umgeleitet oder im ERP-System eines Unternehmens vertrauliche Vertragsdaten eingesehen. Der Angreifer kann die gestohlenen Daten nicht nur selbst verwenden, sondern sie auch weiterveräußern.

Im Darknet kursieren zahllose Listen solcher Nutzer/Passwort-Kombinationen. Bots machen das systematische Abarbeiten von Passwortlisten unkenntlich. Probiert ein menschlicher Angreifer innerhalb eines kurzen Zeitfensters verschiedene Nutzer/Passwort-Kombinationen durch, ist das auffällig. Da alle Log-in-Versuche von derselben IP-Adresse stammen, kann ein Systemadministrator dieses Vorgehen leicht erkennen und gegensteuern. Anders bei der Bot-Attacke: Zum einen kann ein automatisches Programm solche Prozesse in unglaublicher Geschwindigkeit durchführen und Millionen von Anmeldedaten in kürzester Zeit testen. Zum anderen verschleiern sie ihr Tun: Der erste Rechner versucht es mit Nutzer/Passwort-Kombination Nummer 1, der nächste nutzt Nummer 2 usw.

> **Der Schaden ist riesig, nicht nur für den gehackten Website-Betreiber, sondern auch für solche Unternehmen, die ihre Daten nicht ausreichend schützen.**



Kriminelle testen Nutzer/Passwort-Kombinationen im großen Stil.



Beispiel: Anbieter B setzt Bots ein, um automatisch die Produktpreise von Anbieter A zu unterbieten.

Price Grabbing

Price Grabber spähen Produktpreise auf Ihrer Website aus, um sie automatisch unterbieten zu können.

Price Grabber gehören zweifelsohne zu den bösartigen Bots und sind insbesondere für E-Commerce-Anbieter ein Problem. Sie zielen auf die Tatsache ab, dass das nächste Angebot im Internet immer nur einen Mausklick entfernt ist. Preisvergleiche sind damit für Interessenten einfach. Es gilt also, die Preise aller Wettbewerber im Auge zu behalten und immer knapp darunter zu kalkulieren. Die mühselige Preisrecherche auf Wettbewerbsseiten müssen Unternehmen allerdings nicht selbst erledigen, sondern können dafür Bots einsetzen. Price Grabber werden demnach in der Regel von konkurrierenden Firmen losgeschickt, die ein ähnliches Produktportfolio wie die angegriffene Website anbieten. Sie greifen die Preise ab und passen den Preis im eigenen Onlineshop automatisiert so an, dass er permanent knapp darunter liegt.

Price Grabber analysieren komplette Preisgefüge

Für den Betreiber der angegriffenen Website ist dies aus mehreren Gründen schädlich: Nicht nur, dass er durchgehend unterboten wird. Der Angreifer kann zudem noch strategischer agieren und über Price Grabbing die Kalkulation seines Mitbewerbers analysieren. Er betrachtet dann nicht nur den isolierten Preis, sondern das komplette Preisgefüge. Daraus kann er Rückschlüsse auf die verhandelten Einkaufspreise des Unternehmens ziehen und diese als Basis für eigene Preisverhandlungen heranziehen.

Beanspruchte Serverkapazitäten

Bots interessieren sich für alles, egal ob populär oder nicht. Sie greifen auch die Daten solcher Produkte ab, die durch Ihre Kunden nie oder nur selten nachgefragt werden. Wenn ein Bot solche Informationen anfragt, dann befinden sich diese nicht im Cache der Auslieferungsschicht und müssen deshalb komplett vom Origin-Server bezogen werden. Dementsprechend ist Bot-Traffic vergleichsweise teurer als der Ihrer menschlichen Nutzer und kann zu Hochlastzeiten zu unerwünschten Verzögerungen im Seitenaufbau führen.

Content- / Product Grabbing

Bots kopieren Ihre gesamte Website und schädigen Ihr Google-Ranking.

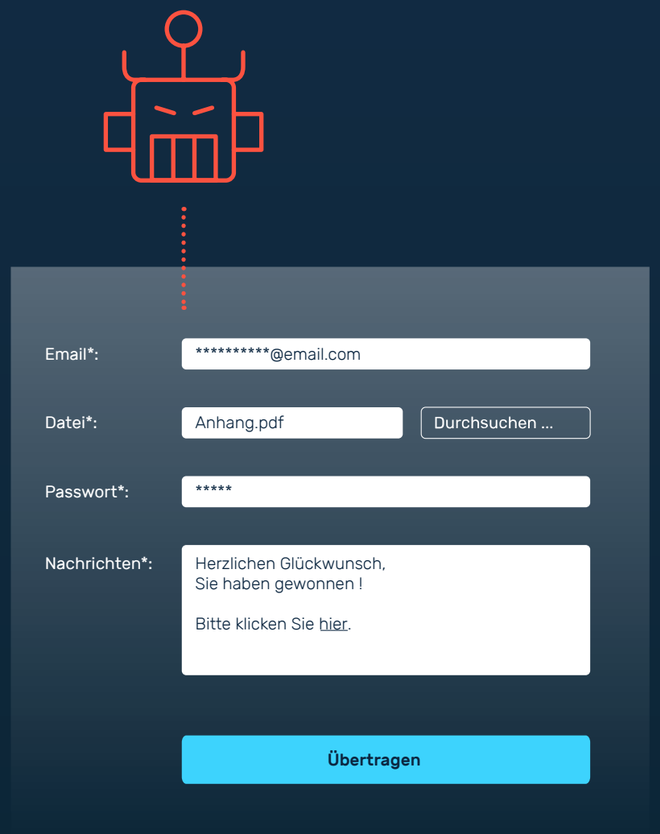
„Gut geklaut ist besser als schlecht erfunden“. Dieses Prinzip kultivieren die so genannten Content- oder Product Grabber. Sie sind eng verwandt mit Bot-Attacken vom Typ Price Grabbing. Statt Preise von bekannten Produkten zu beziehen, greifen sie die Produktbezeichnungen selbst ab - mit allen dazugehörigen Informationen. Bei der Bewertung des Schadenpotenzials kommt es darauf an, was der Bot-Betreiber mit dem abgegriffenen Content anstellt.

Bots als Parasiten

Kritisch wird es, wenn es ausschließlich darum geht, mit den kopierten Texten eine zweite identische Website aufzubauen. So spart sich der Angreifer das aufwändige Zusammentragen von Informationen und hat im Nu einen eigenen Onlineshop eingerichtet. Dies funktioniert auch auf fremdsprachigen Seiten. Der Original-Content ist damit nicht mehr „unique“, die mühevoll erstellten Texte sind zum „duplicate content“ degradiert.

SEO-Katastrophe: Geklauter Content verschlechtert Page Rank

Die Folge dieses parasitären Verhaltens ist eine Katastrophe für die Suchmaschinenoptimierung, denn der Page Rank der angegriffenen Seite sinkt damit fast automatisch. Für E-Commerce-Anbieter stellt dies ein gewaltiges Problem dar. Sie verwenden viel Zeit und Mühe darauf, mit einzigartigem Inhalt eine hohe Google-Platzierung zu erreichen. Je höher das Ranking, desto mehr Website-Besuche werden generiert und desto mehr Umsatz wird erzielt. Eine niedrigere Platzierung, verursacht durch Content-Dubletten, bedeutet daher zwangsläufig einen wirtschaftlichen Schaden. Nicht nur E-Commerce-Anbieter, sondern eine Reihe weiterer Websites sind im Visier von Product Grabbern: jede Art von Marktplätzen, Jobbörsen, Kleinanzeigen und sonstige Online-Verzeichnissen.



Nicht nur Menschen können Web-Formulare ausfüllen. Auch Bots sind dazu in der Lage und betreiben millionenfach Formular-Spam.

Formular Spam

Bots füllen Kontaktformulare mit unerwünschten Botschaften. Häufig im Gepäck: Links zu gefälschten Websites oder mit Schadsoftware verseuchte Dokumente.

Formulare auf der Webseite sind praktisch und schnell. Man kann über sie unkompliziert direkt Kontakt zum Unternehmen aufnehmen. Auch Bots lieben Formulare. Für einen automatisierten Computerprozess ist es ein leichtes, die einzelnen Felder auszufüllen und das Unternehmen mit unliebsamer Werbung zu bombardieren. Dafür zweckentfremden die Bots ohne Zögern Formulare und befüllen deren Freitextfelder mit ihren Botschaften. Der zusätzliche Arbeitsaufwand ist zum einen lästig, zum anderen funktionieren viele der Phishing-Methoden bei Formularen genau wie bei entsprechenden E-Mails. Auch hier sind Phishing-Links gut getarnt und mit einem falschen Klick beginnen die illegalen Machenschaften der Phishing-Seite.

Virenverseuchte Dokumente – per Formular direkt ins Netzwerk

Auch Personalabteilungen nutzen Formulare häufig. Interessierte können sich direkt über die Website des Unternehmens bewerben und im Zuge dessen sogleich Lebenslauf und Zeugnisse hochladen. Im Unternehmen werden die eingehenden Daten automatisiert in das HR-System übertragen – für beide Seiten praktisch und effizient. Nur öffnen solche HR-Formulare eben auch Tor und Tür für Fake-Bewerbungen.

> **Hochgeladene Office-Dokumente können Makros und Viren übertragen und der IT veritablen Schaden zufügen.**

Hype Sales

In Minuten ausverkaufte Konzerttickets oder vergriffene Sondereditionen. Hierfür können automatisierte Einkaufs-Bots der Grund sein. Gegen sie haben reale Kunden keine Chance.

So genannte Hype Sales werden von Unternehmen als gezieltes Marketinginstrument eingesetzt. Tickets für begehrte Events werden in nur begrenztem Kontingent auf den Markt geworfen, um den Anreiz zu erhöhen, unbedingt dabei sein zu wollen. Dies funktioniert analog mit beliebigen Produkt-Launches, ersten Auflagen, Sondereditionen etc. Ein Klassiker sind Sneaker-Hype-Verkäufe. Schon vor 30 Jahren prognostizierte Michael J. Fox alias Marty McFly in „Zurück in die Zukunft“, welche Blüten der Turnschuh-Wahn einmal treiben würde. Für bis zu 77.000,- Euro werden seine Original „Nike Mag“ heute auf Ebay gehandelt.

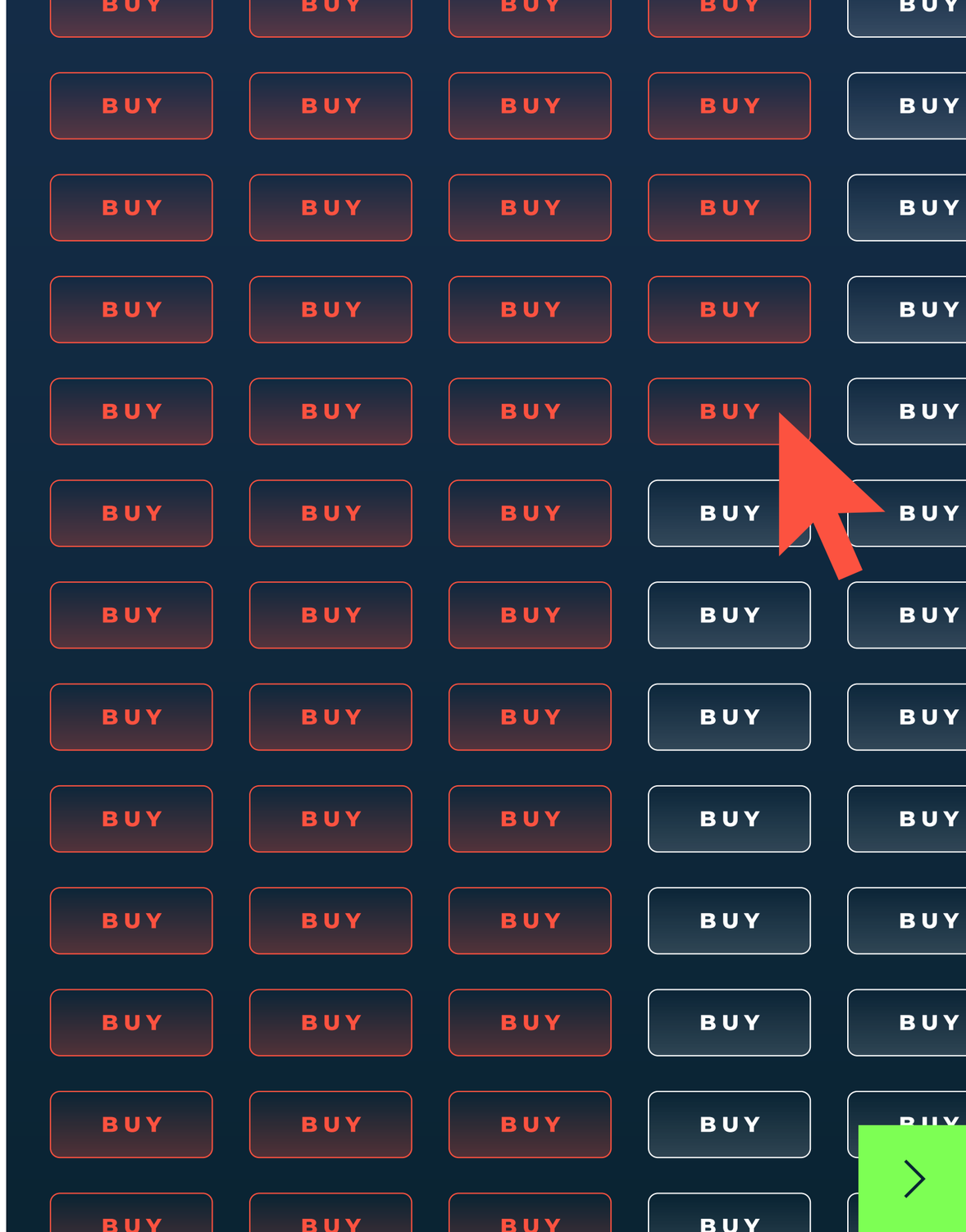
Eine ordentliche Gewinnspanne, die Bot-Betreiber auszunutzen wissen und Online-Händler damit massiv schädigen können. Deshalb ist Bot-Management zur Erkennung von Hype-Sales-Bots für sie so wichtig. Kriminell sind Bots nicht, sondern sie überlisten ihre Mitbieter mit ganz legalen Mitteln und 100 % validen Kreditkartennummern.

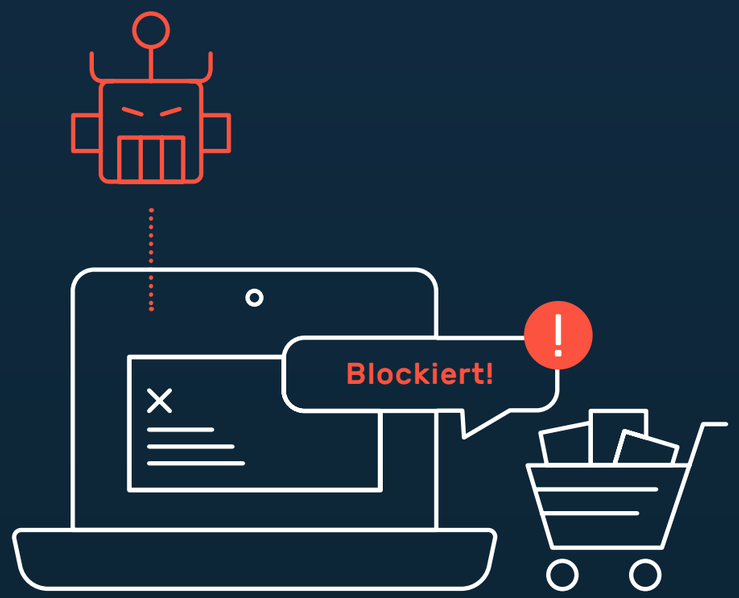
Ganze Heerscharen automatisierter Computerprozesse schickt ein Bot-Betreiber parallel mit unterschiedlichen Identitäten und Zahlungsmitteln los und umgeht damit geschickt maximale Abgabemengen: Während sich der reale Kunde maximal ein oder zwei Exemplare sichern kann, kauft der Bot-Betreiber erfolgreich große Stückzahlen.

Geschäftsmodell: Maximale Gewinnmarge

Für den Online-Händler sind diese Bot-Aktivitäten nicht auf Anhieb erkennbar, denn die Artikel werden an unterschiedliche Adressen verschickt: Die günstig erworbenen Produkte veräußert der Bot-Betreiber anschließend zum Vielfachen des Ausgabepreises. Gewinnmargen von 1.000 % sind dabei üblich.

Eine völlig legale Aktion, für das Marketing des Verkäufers jedoch der GAU. Der Werbeeffekt verkehrt sich ins Gegenteil. Zurück bleiben enttäuschte Kunden, und das Image des Online-Händlers nimmt Schaden.





Bots blockieren Artikel für reale Kunden in Online-Shops

Cart Abandonment

Füllen Bots den digitalen Einkaufswagen, ohne den Kaufprozess abzuschließen, blockieren sie die Produkte für tatsächliche Kunden. Der Umsatz sinkt und Kunden wandern ab.

Wie Cart-Abandonment-Attacken funktionieren, verdeutlicht ein Vergleich mit dem Supermarkt: Der Kunde befüllt seinen Wagen randvoll mit Artikeln. Statt aber zur Kasse zu gehen, lässt er ihn anschließend in einer Ecke stehen und verlässt den Laden. Bis dem Personal der verwaiste Einkaufswagen auffällt und die Artikel wieder zurück in die Regale geräumt sind, kann es dauern. Solange ist die Ware für den Verkauf an die übrige Kundschaft gesperrt. Analog funktionieren Bot-Angriffe vom Typ „Cart Abandonment“ in der virtuellen Welt. Man versteht darunter das Blockieren von Inventar in „geparkten“ Warenkörben, um dadurch den Abverkauf der angegriffenen Seite zu verlangsamen oder zu erschweren.

Geblocktes Inventar verlangsamt E-Commerce

Zwischen 40 und 80 Prozent der Besucher eines Webshops brechen ihren Einkauf ab. Beim bot-betriebenen Cart Abandonment ist das Blockieren von Inventar von vornherein das Ziel. Für Produkte, die in beliebiger Menge zur Verfügung stehen, stellt dies zunächst kein Problem dar. Kritisch wird das Parken von Warenkörben dann, wenn die Produktmenge begrenzt ist oder wenn nur für eine bestimmte Zeit hohe Nachfrage herrscht. Setzt ein Online-Anbieter einen solchen Bot erfolgreich beim Wettbewerber ein, wird dessen Kunden das Produkt als nicht lieferbar angezeigt. Dadurch könnte er selbst derjenige sein, der den großen Käuferansturm abbekommt.

Kreditkartentests

Das Testen von Kreditkarten gehört zu den besonders lukrativen Aktivitäten und bereitet Online-Betrug vor. Für Unternehmen sind die Machenschaften kaum nachvollziehbar.

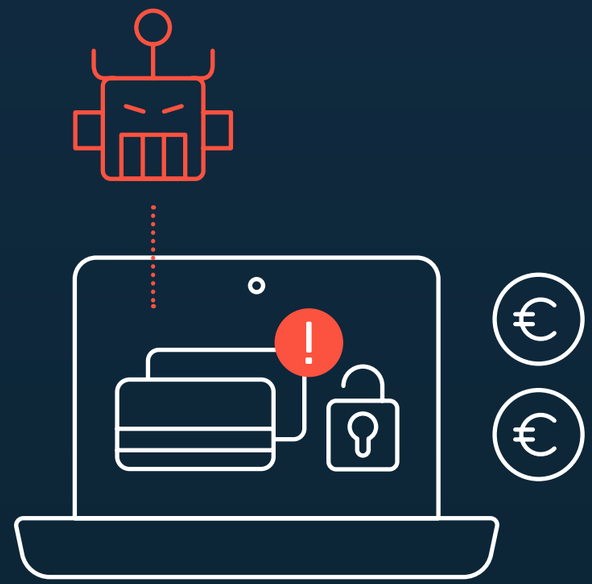
Dieser spezielle Bot-Typ hat den Zweck, im großen Stil Kreditkartendaten zu testen. Üblicherweise werden diese Daten auf E-Commerce-Seiten nicht direkt verarbeitet, sondern die Shops beauftragen damit Zahlungsdienstleister wie PayPal.

Vorbereitung zum Betrug

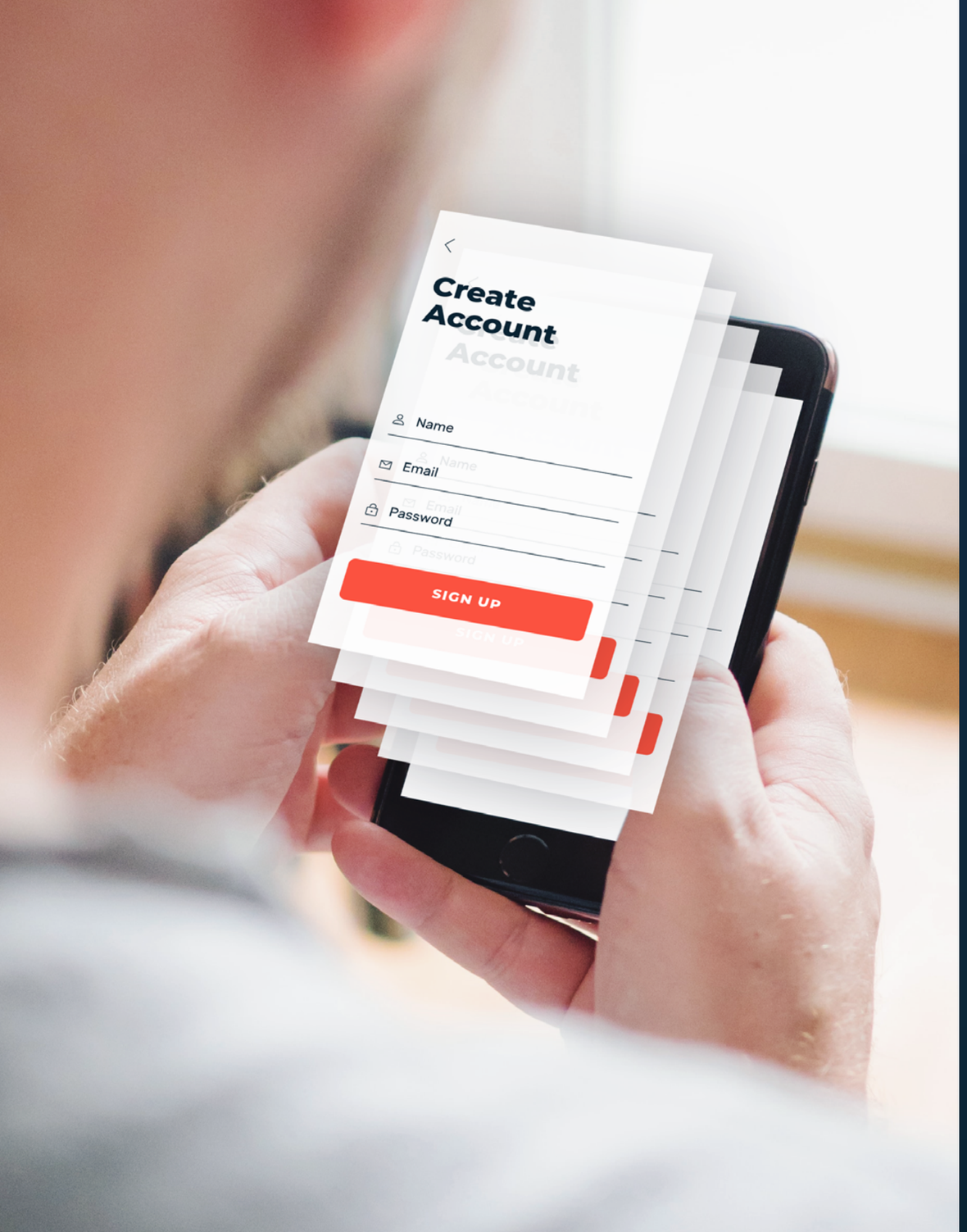
Um zu testen, ob sich mit Kreditkartendaten ein Einkauf tätigen lässt, erwerben Angreifer im Internet blockweise eine große Menge an Kreditkarteninformationen. Dazu müssen sie nicht einmal auf das Darknet zurückgreifen; es gibt zahlreiche einschlägige Seiten, auf denen dies möglich ist. Anschließend schicken sie Bots los, welche bei mehreren Online-Shops testen, ob mit den Daten Einkaufstransaktionen möglich sind.

Ob Kreditkartendaten valide sind, prüfen Bots auch bei Reservierungen von Mietwagen oder Hotels. Dort muss der Besteller in der Regel eine Kreditkarte als Sicherheit hinterlegen. Es kommt zu keiner Buchung, sondern nur zu einer Sicherheitsüberprüfung, im Verlaufe derer der Betrag vorreserviert wird. Für den Karteninhaber ist dies gar nicht sichtbar.

Für das Testen von Kreditkartendaten greifen Bots von verschiedenen IP-Adressen auf die Website zu. Daher lassen sich solche Vorgänge nur sehr schwer nachvollziehen. Das Ende vom Lied: Angreifer finden heraus, ob eine Kreditkarte funktioniert und können anschließend Listen mit „guten“ und „schlechten“ Karten erstellen. Das Munitionslager für betrügerische Bezahltransaktionen in größerem Maßstab ist damit gut gefüllt – für die eigene Verwendung oder auch attraktiv für den Weiterverkauf.



Bots testen Kreditkartendaten schnell, effektiv und oft unentdeckt



Account Creation & Takeover

Angreifer nutzen Botnetze auch für Angriffe auf die Verfügbarkeit von Websites und IT-Infrastruktur. Ihr Ziel ist das Lahmlegen der attackierten Seite.

Manche Bots erstellen unbemerkt massenhaft neue Konten auf der Webseite für den späteren Missbrauch. Dieser kann im Erzeugen von Content-Spam oder der Verbreitung von Malware bestehen. Auch kann Geldwäsche betrieben werden oder die Suchmaschinenoptimierung des angegriffenen Unternehmens wird verzerrt – die Schäden für den Website-Betreiber sind vielfältig.

Betroffene Website-Betreiber erkennen das Problem in der Regel, wenn eine anormale Zunahme der Erstellung neuer Konten oder ein erhöhtes Aufkommen von Kommentar-Spam festzustellen ist. Weitere Anzeichen für Anomalien sind Konten mit unvollständigen Informationen oder auch solche, die erstellt wurden, aber nicht verwendet werden. Zu den typischerweise missbrauchten Daten für die Kontoerstellung zählen Authentifizierungsinformationen, Kreditkarten- und andere Finanzdaten, aber auch medizinische oder weitere persönliche Daten.

Account Creation Bots stellen den Betreiber einer Webseite vor eine unangenehme Situation, denn die Menge an neu erstellten und aktiven Accounts ist eigentlich ein Performance-Indikator und unterstreicht den Wert einer Webseite. Abgesehen davon ist beim Eliminieren automatisiert erstellter Accounts noch mehr darauf zu achten, dass die Anzahl der False Positives, also die irrtürmlich als Bot-Traffic eingestuften Anfragen, wirklich bei Null ist: Eine abgebrochene Transaktion mag von einem treuen Kunden noch verziehen werden: das Blockieren oder gar Löschen des Accounts nicht.

Skewing

Geschäftsentscheidungen basieren zunehmend auf der Analyse von Nutzerdaten. Bots verzerren diese Statistiken. Planen Unternehmen aufgrund falscher Annahmen z. B. Werbebudgets, wird viel Geld fehlinvestiert.

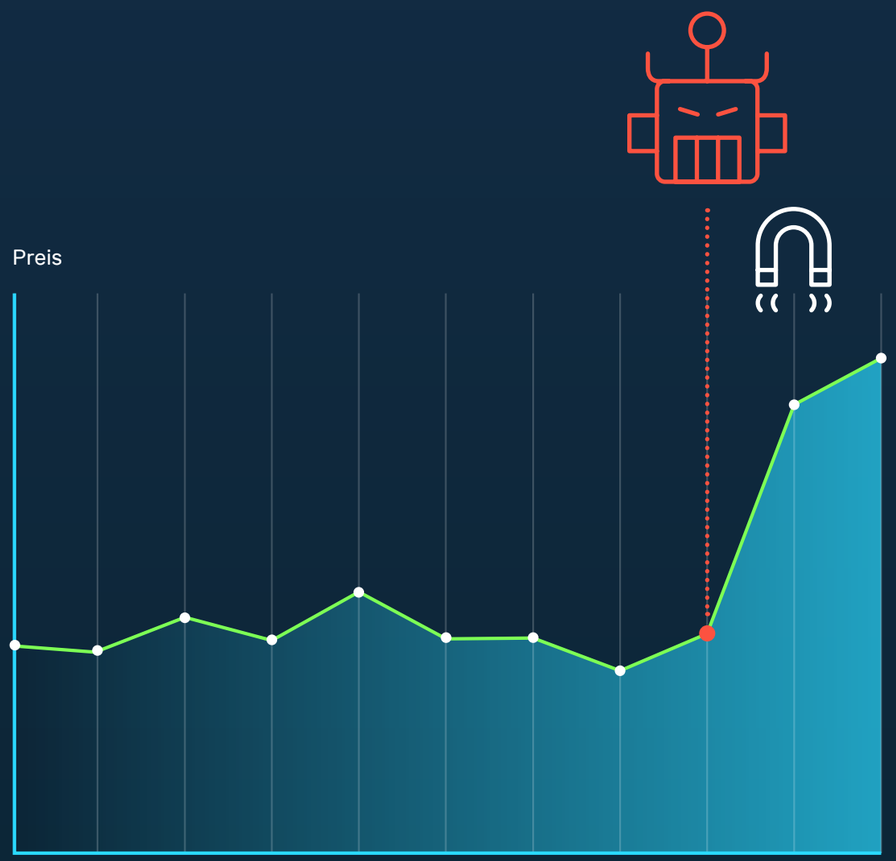
Marketingspezialisten untersuchen permanent, wie die Website ihres Unternehmens angenommen wird, wie sich Conversion-Rates entwickeln und warum User an welcher Stelle wie reagieren. Auf Basis dieser Analysen planen sie ihre Marketingaktivitäten und budgetieren Werbeaktivitäten.

Was aber, wenn die Aktivität auf der Website von keinem Menschen stammt, sondern einem Bot – der von vornherein nicht die Absicht hat, einen Kauf zu tätigen? Im Bereich der sozialen Medien ist ein solches Vorspiegeln falscher Identität heute ganz normal, Stichwort Fake-Follower auf Twitter.

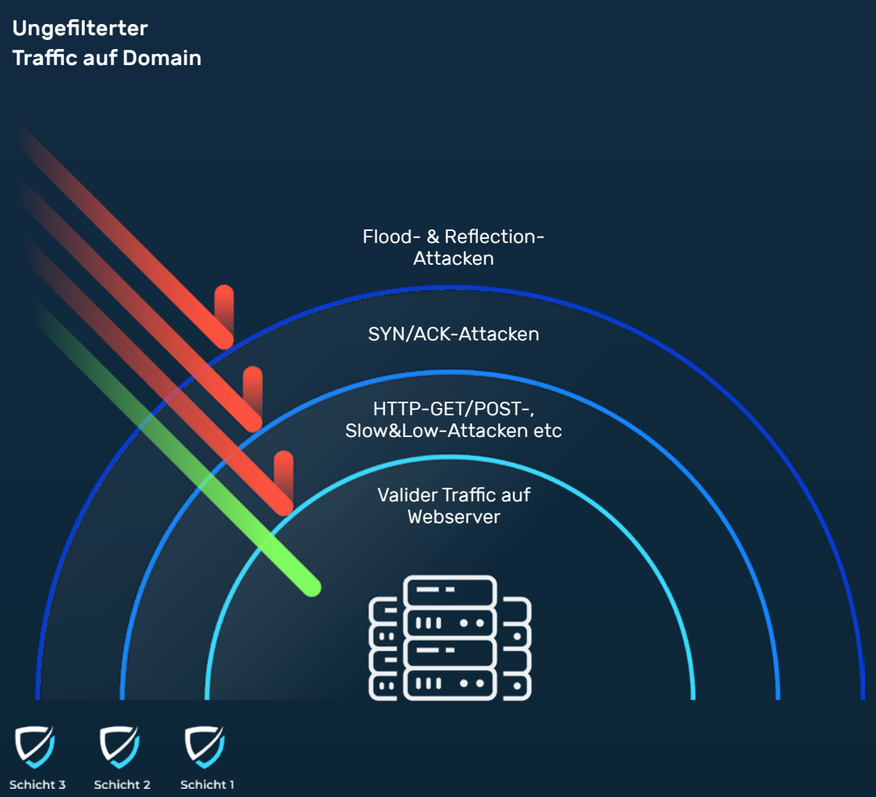
Bot-Betreiber sind hier äußerst kreativ und können ihre Computerprozesse so programmieren, dass sie auch etwas länger auf der Seite verweilen und damit perfekt das Verhalten eines menschlichen Besuchers imitieren.

> **Dann sorgt Bot-Traffic dafür, dass falsche Geschäftsentscheidungen getroffen werden.**

Die User-Situation wird anders wahrgenommen als sie in Wirklichkeit ist, die mühsam erstellten Statistiken sind schlichtweg falsch – eine Verzerrung, engl. Skewing, findet statt.



Bots täuschen starkes Nutzerinteresse vor und verzerren damit Analysedaten.



Die Myra DDoS Protection filtert schädlichen Traffic in Echtzeit heraus. Den Webserver erreichen ausschließlich valide Anfragen.

Dienstblockade: Denial of Service

Angreifer nutzen Botnetze auch für Angriffe auf die Verfügbarkeit von Websites und IT-Infrastruktur. Ihr Ziel ist das Lahmlegen der attackierten Seite.

Die im vorliegenden Whitepaper beschriebenen Bots haben eines gemeinsam: Sie erwarten, dass die angegriffene Website antwortet. Ein Interesse daran, sie zum Stillstand zu bringen, haben sie nicht.

Insofern unterscheiden sich die hier behandelten Bot-Typen grundlegend von DDoS-Angriffen. Auch diese funktionieren bot-basiert durch Botnetze. Sie führen aber anderes im Schilde. Nicht die einzelne Aktion als solches steht im Vordergrund, sondern die schiere Masse an Zugriffen. Sie soll eine Website lahmlegen und dafür sorgen, dass diese ihren Service einstellt: Eine Dienstblockade oder auch „Denial of Service“ ist die Folge.

Damit sind auch sie zweifelsohne den schädlichen Bots zuzurechnen. Für ihre Bekämpfung werden jedoch andere Instrumente herangezogen als gegen die hier behandelten Bots. Myra Security bietet einen DDoS-Schutz, der Websites und andere Applikationen vor DDoS-Angriffen schützt, in dem er die Applikationen hinter einem dreischichtigen Filtersystem verbirgt. Dieses basiert auf eigens von Myra entwickelten Hard- und Softwarekomponenten.

> **Schadhafte Traffic-Ströme werden über die komplexen, intelligenten und selbstlernenden Myra-Filterschichten abgewehrt.**

Myra Web Security

Das Myra Web Application Security Portfolio enthält alle Produkte und Dienstleistungen für einen effektiven Schutz von Websites und Anwendungen.

Myra Bot Management

Das Myra Bot Management ist modular aufgebaut und gibt Ihnen als Kunde volle Flexibilität bei der Erkennung und Kontrolle von Bots: entweder basierend auf den Bot-Kategorien, oder als Gesamtpaket.

Integraler Bestandteil ist das Myra Multi-Fingerprinting zur zuverlässigen Erkennung der automatisierten Bot-Zugriffe.

Myra Web Application Firewall

Die Myra Web Application Firewall filtert, überwacht und kontrolliert ein- und ausgehenden Web-Traffic auf der Inhaltsebene. Damit schützt sie Applikationen u. a. vor dem Einschleusen schädlicher Daten und dem Ausspähen sensibler Informationen.

Myra Malware Protection

Die Myra Malware Protection bietet einen zusätzlichen Schutz vor einem Befall mit Schadsoftware durch infizierte Benutzerdateien. Sie überprüft Dateien, noch bevor sie Ihre Infrastruktur erreichen.

Bots hinterlassen Fingerprints

Bots greifen mit unterschiedlichen IP-Adressen und aus unterschiedlichen Netzwerken auf die Webseite zu.

Sie geben vor, ein normaler Browser zu sein und fälschen weitere Informationen, um wie ein regulärer Benutzer auszusehen. Weil die Zugriffe verteilt stattfinden, ist auf den ersten Blick kein Zusammenhang zwischen ihnen zu erkennen.

Genau diesen Kontext stellt das Myra Bot Management mit Hilfe des passiven Multi-Fingerprintings her. Bei jedem Zugriff auf die Webseite gehen über 50 Attribute des Zugriffs zur eindeutigen Identifikation der verwendeten Software in diesen Fingerprint ein. Über drei Millionen solcher digitalen Fingerabdrücke hat Myra inzwischen gespeichert.

Sobald der Fingerprint vorliegt, können entsprechende Maßnahmen durchgeführt bzw. Schutzmechanismen gestartet werden. Unerwünschte und verbotene Zugriffe können eindeutig identifiziert, geblockt, mit Human-Interaction-Challenges (z. B. CAPTCHA) konfrontiert oder anderweitig kontrolliert bzw. umgeleitet werden.

Auch Bots hinterlassen Spuren. Ihre eindeutige Identifikation ist die Basis für ihr effektives Management.

Myra nutzt mehr als 50 Attribute zur Identifikation von Bots.

Abgestufte Bekämpfung: vom Blocken bis zum Honeypot

Alle automatisierten Anfragen einfach zu blocken, ist keine gute Strategie. Auch gute, erwünschte Bots würden damit ausgesperrt werden. Vielmehr kommt es darauf an, für jede Anfrage eine geeignete Antwort zu liefern.

Myra rät grundsätzlich zur Wahl des mildesten effektiven Mittels, um Bots von ihrem Tun abzuhalten. Dazu gehören Human Interaction Proof-Verfahren. Sie dienen dem Ziel, automatisierte Eingaben von solchen zu unterscheiden, die von Menschen stammen.

CAPTCHA ist heute Standard auf vielen Websites und dennoch kein Allheilmittel. Denn wird jemand abgelehnt, obwohl er ein Mensch ist, ist er damit als Kunde/Käufer für den Website-Betreiber verloren – das Problem der False Positives. Ein CAPTCHA-Mechanismus kann auch als Schutz vor Formularmissbräuchen installiert werden.

Eine weitere Möglichkeit der Bot-Bekämpfung ist dessen Reglementierung. Hier wird der Bot erkannt und man erlaubt ihm, eine nur begrenzte Zahl an Zugriffen pro Zeiteinheit zu starten (Rate Limiting).

Angewandt wird die Reglementierung, wenn es sich um grundsätzlich „gute“ Bots handelt, die jedoch viel Last erzeugen und daher die Performance der Website schwächen.

> **Als probates Mittel hat sich außerdem der „Honeypot“ erwiesen – quasi eine zweite Variante der Website, die dem Bot suggeriert, sie sei das Original.**

Dort werden dann aber vollkommen andere Inhalte angegeben. Um etwa Price Grabber auszubooten, enthält der Honeypot Preise, die niedriger, höher oder auch gleich den originalen sind. Eine Irritationsmaßnahme, die der automatisierten Unterbietung um wenige Cent auf der Seite des Angreifers den Garaus macht.

Unsere Kernbereiche

Schützen und beschleunigen Sie Ihre Applikationen, Websites und IT-Infrastrukturen. Unsere smarten Produkte und Lösungen basieren auf selbst entwickelter Software und erfüllen auch zukünftige Anforderungen an IT-Sicherheit und -Performance.

Myra Plattform

Die Myra Plattform ist die Basis für alle Produkte und Dienste. Sie bietet Zugang zum Kundenbereich mit nutzerfreundlicher Konfigurationsoberfläche.

DDoS Protection

Die Myra DDoS Protection sichert Web-Anwendungen, Websites, DNS-Server und IT-Infrastrukturen zuverlässig und vollautomatisiert vor Überlastungsangriffen.

Web Application Security

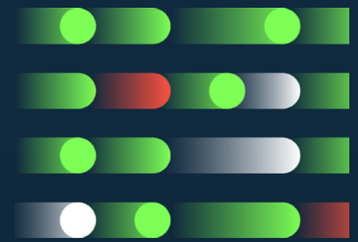
Die Myra Web Application Security schützt als vorgelagerte Instanz Ihre Anwendungen vor Angriffen. Bösartiger Traffic wird gefiltert, bevor er Ihre Server erreicht.

Load Balancing

Das Myra Multi Site Load Balancing sorgt für eine ideale Verteilung der Anfragen auf eine beliebige Anzahl an Servern und macht Ihre Dienste ausfallsicher. Ihre Website und Applikationen laufen durch verringerte Ladezeiten hoch performant.

Content Delivery Network

Das weltweite Myra Content Delivery Network (CDN) mit eigener globaler Infrastruktur liefert alle statischen und dynamischen Elemente Ihrer Website blitzschnell aus.



Web Intelligence

Myra bietet eine 100%ige Transparenz über den eingehenden Traffic. Dies erlaubt eine Visualisierung der Anfragen in Echtzeit und eine auf Ihre Bedürfnisse angepasste Datenanalyse.

Warum Myra

Technischer Vorreiter
Myra erfüllt alle 37 Leistungsmerkmale des BSI für qualifizierte DDoS-Mitigation-Dienstleister.

Made in Germany
Wir schützen Ihre Daten nach strengsten Standards – garantiert.

Zertifiziert
Myra setzt auf höchste Qualitäts-standards und Zertifizierungen wie ISO 27001 und PCI-DSS.

Zukunftssichere Technologie
Unsere Systeme sind für künftige Anforderungen gerüstet z. B. durch native IPv6-Unterstützung.

Einfaches Setup
Sie benötigen keine zusätzliche Hard- oder Software-Installation.

Hohe Skalierbarkeit
Unsere Systeme passen sich dem Wachstum Ihres Unternehmens an.

Echtzeit-Schutz
Unsere Filter blockieren bösartige Anfragen, bevor sie Schaden bei Ihnen anrichten.

Kurze Reaktionszeiten
Sie fragen. Wir antworten sofort.

Eigenes, globales CDN
Unser Servernetz gewährleistet eine zuverlässige, schnelle und weltweite Auslieferung Ihrer Daten.

Maßgeschneiderte Lösungen
Wir bieten individuell auf Ihre Branche angepasste Lösungen und Produkte.

Echter 24/7-Support
Sie sprechen direkt mit unseren IT-Experten.

Garantierte Servicequalität
Sie benötigen ein Service-Level-Agreement von 99.999 Prozent? Wir sorgen dafür.

Weltweit vertrauen international bekannte Unternehmen und Institutionen auf Myra Security.

Bundesministerium für Gesundheit

flatex DEGIRO

msc Munich Security Conference

STADT REGENSBURG

CANCOM

Liechtensteinische Landesbank 1861

BIOSCIENTIA MEDIZIN. LABOR. SERVICE.

Hugendubel Die Welt der Bücher

breuninger

DSV IT Service

Barmenia EINFACH. MENSCHLICH.

klöckner & co

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Myra bietet als deutscher Technologiehersteller eine sichere, zertifizierte Security-as-a-Service-Plattform zum Schutz digitaler Prozesse.

Die smarte Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic, noch bevor virtuelle Angriffe einen realen Schaden anrichten.

Myra Security GmbH

Telefon +49 89 414141 - 345

www.myrasecurity.com

info@myrasecurity.com