MYRA

WHITEPAPER BOT MANAGEMENT

Efficiently managing bot-generated traffic

Protecting and monitoring your website and e-business from the threats of automated requests.

A rush in the online shop: The downside

Although website operators may be enjoying growth in traffic, they must also accurately analyze and manage it to protect their business.

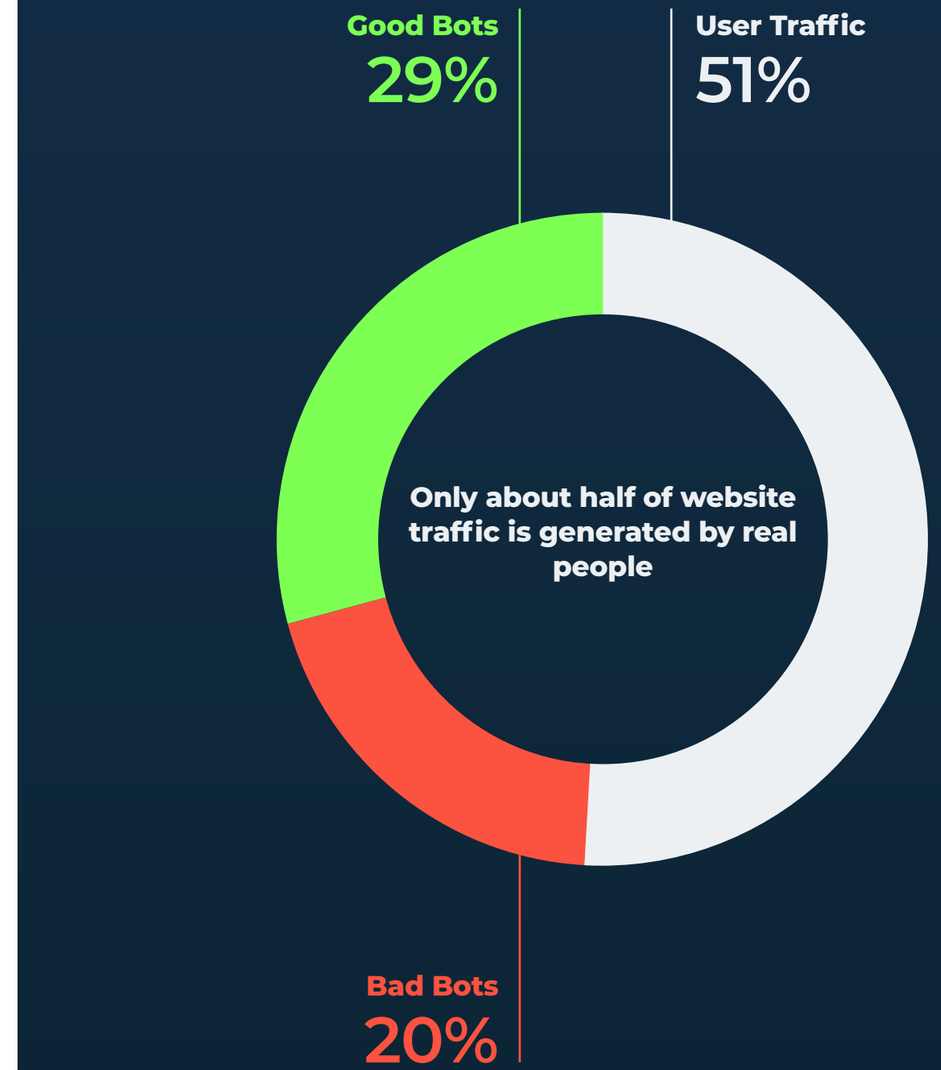
Anyone who operates a website is sharing their business data with the general public. This means that it is not only visible to customers and other desired visitors but also to third parties who do not always have the best intentions. This is where bots come into play – automated computer processes that perform repetitive tasks largely automatically.

They now account for roughly half of all web traffic. They can be search engines, web monitoring systems, scrapers, crawlers, or other automated processes. Many of these are quite helpful – such as the Googlebot, which crawls web pages, updating the search engine index and the ranking in search results.

20% of web traffic is malicious bots

However, a large part falls into the “malicious” category. Now, over 20% of traffic is malicious bots, which can pose a threat to website operators. Disguised as human users and benign bots, they access websites using multiple IP addresses from multiple networks. Although system administrators are able to see the individual requests, they are unable to see the context of these widely scattered requests.

Bad or evil bots have many different goals: Exposing and exploiting vulnerabilities, overloading and using web servers to full capacity, copying and reusing content without permission, blocking shopping carts, testing user data and passwords on a large scale, price grabbing, infecting or gaining control over the network, etc. This white paper describes the individual types of bots with their specific features. Following this, how you can get them under control using Myra Security’s fingerprint technology and a variety of graduated measures will be explained.



These bots threaten your business

Credential stuffing

Bots test user/password combinations on a grand scale.
Their objective: Online fraud.

Price grabbing

Bots grab product prices or entire pricing structures.
Their objective: To harm the competition.

Content/product grabbing

Bots copy product descriptions or entire websites in just seconds.
Their objective: A new online shop.

Form spam

Bots exploit contact forms to bombard companies with their messages.
Their objective: Phishing.

Hype sales

Bots are able to beat out real customers and purchase highly coveted products.
Their objective: Resale at a high profit.

Cart abandonment

Bots fill up shopping carts without completing the checkout process.
Their objective: To harm the business.

Credit card testing

Bots test the validity of credit cards in a matter of seconds.
Their objective: Fraudulent use.

Account creation & takeover

For bots, creating massive numbers of new user accounts is a piece of cake.
Their objective: Data misuse.

Skewing

Bots falsify web analyses.
Their objective: To mislead victims into making the wrong business decisions.

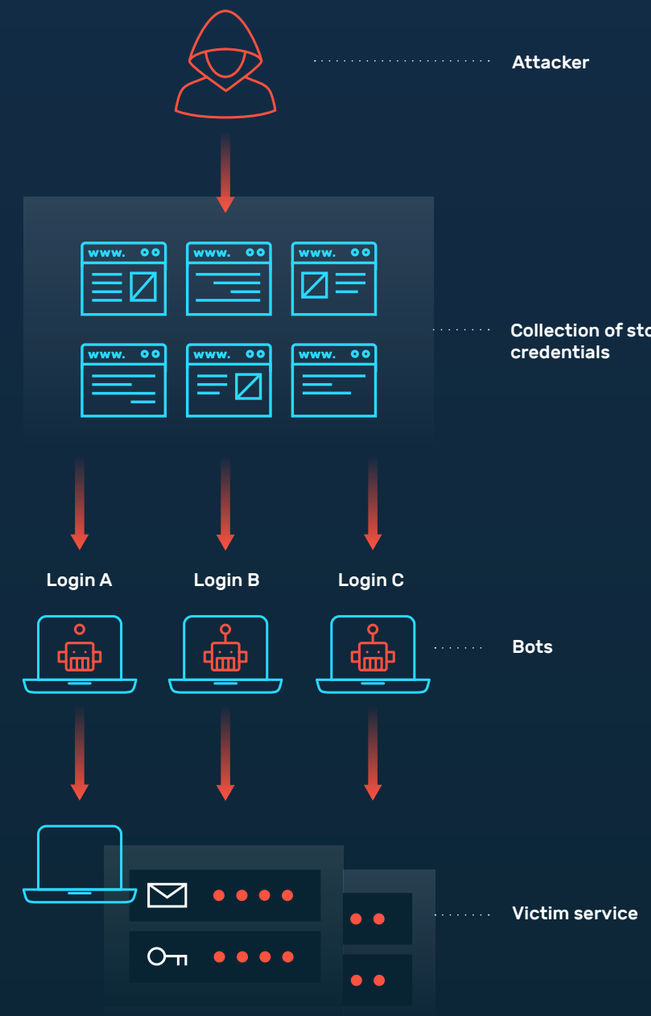
Credential stuffing

Bots can check the validity of millions of user credentials in a matter of seconds.

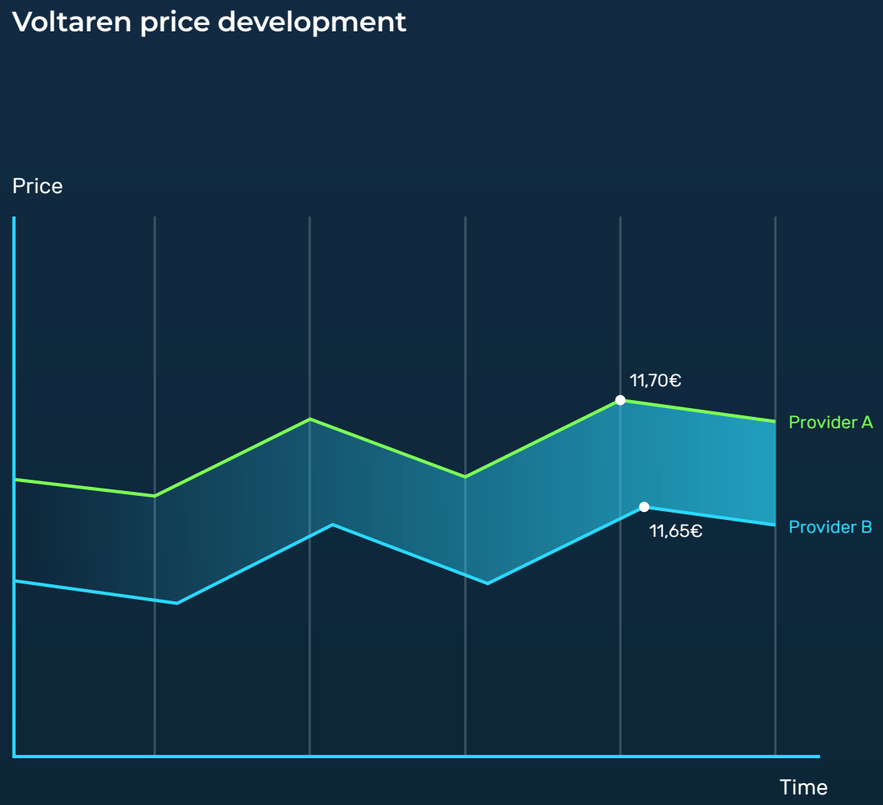
When large-scale testing of stolen user/password combinations is performed on websites, it is called credential stuffing. Any website that provides a login option is potentially at risk. Criminals grab working user name/password combinations from other websites and are then able to use a stolen identity to gain access to the website of the company being targeted. If only one of 10,000 combinations works, the game is already over for the website operator under attack. Purchases are made in online stores, money is rerouted in online banking, or confidential contract data in a company's ERP system can be viewed. The attacker may use the stolen data himself or resell it.

There are countless lists of such user/password combinations circulating on the Darknet. Bots make the systematic processing of password lists impossible to detect. If a human attacker were to try out different user/password combinations within a short window of time, this would attract attention. Since all login attempts would come from the same IP address, it would be easy for a system administrator to detect this and take countermeasures. This is different in a bot attack: For one, an automated program can perform these types of actions at an incredible speed and test millions of credentials in a very short time. For another, they conceal what they do: The first computer tries out the first user/password combination, the next uses the second combination, and so on.

> **The harm is immense, not only for the hacked website operator, but also for companies that fail to adequately protect their data.**



Criminals test user/password combinations on a grand scale.



Example: Retailer B uses bots to automatically undercut the product prices of retailer A.

Price grabbing

Price grabbers snoop through product prices on your website to automatically beat them.

Price grabbers are undoubtedly among the most malicious bots and are a major problem for e-commerce providers. They target the fact that the next deal on the internet is always just a mouse click away. This makes price comparisons easy for prospective customers. That is why it is important to keep an eye on the prices of all competitors and always set prices just below them. Companies do not have to laboriously search for prices on competitor sites themselves, but instead use bots for this. Price grabbers are therefore usually sent out by competing companies offering a product range similar to the website being attacked. They grab prices and automatically adjust the respective prices in their own online shop to be permanently just below them.

Price grabbers analyze entire pricing structures

This is harmful to the operator of the attacked website for several reasons: Not just by being continuously undercut. The attacker can also take even more strategic action and use price grabbing to analyze his competitor's pricing calculations. He then looks at not only the individual prices, but the entire pricing structure. From this he can draw conclusions about the company's negotiated purchase prices and use them in his own price negotiations.

Server capacities used

Bots are interested in everything, whether popular or not. They also grab data on products that are never or only rarely in demand by your customers. When a bot requests such information, it is not in the delivery layer cache and must therefore be obtained in its entirety from the origin server. As a result, bot traffic is comparatively more costly than that of your human users and can cause unwanted delays in page loading at peak load times.

Content- / product grabbing

Bots copy your entire website and harm your Google ranking.

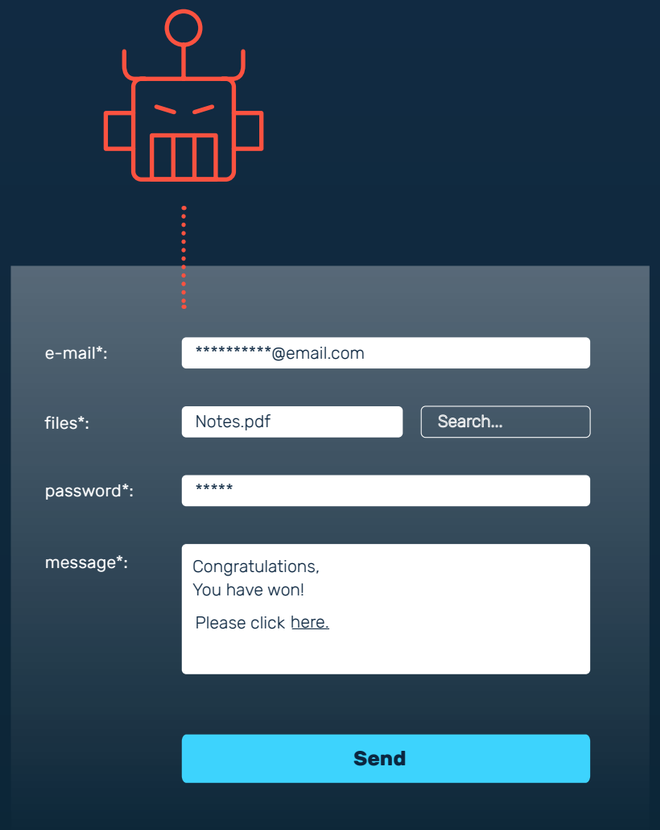
“Good artists borrow, great artists steal.” This is the principle cultivated by content and product grabbers. They are closely related to bot attacks of the price grabbing variety. Instead of obtaining the prices of known products, they grab the product names themselves, along with all associated information. When evaluating the potential for damage, it is important to know what the bot operator is doing with the grabbed content.

Bots as parasites

Things become critical when the sole purpose is to create a second, identical website using the copied texts. This saves the attacker the time-consuming process of gathering all the information he needs and he is able to set up his own online shop in no time at all. This also works on foreign language sites, making original content no longer “unique” and degrading painstakingly created texts to “duplicate content.”

An SEO catastrophe: stolen content lowers page ranking

The consequence of this parasitic behavior is a catastrophe for search engine optimization, because the page ranking of the site being attacked drops almost instantly. This is a huge problem for e-commerce providers. They spend a lot of time and effort to get a high Google ranking with unique content. The higher the ranking, the more website visits are generated and the more revenue is earned. A lower ranking, caused by content duplicates, thus inevitably means an economic loss. It is not e-commerce providers alone that are targeted by product grabbers, but a number of other websites as well: all kinds of marketplaces, job exchanges, classified ads, and other online directories.



Humans are not the only ones who can fill out web forms. Bots are also capable of this and engage in form spam millions of times over.

Form spam

Bots fill contact forms with unwanted messages.And they frequently include links to fake websites or documents infected with malware.

Forms on websites are practical and fast. They allow you to easily get into direct contact with the company. Bots also love forms. It is easy for an automated computer process to fill in the individual fields and bombard the company with unwanted advertising. For this, bots do not hesitate to abuse forms, filling up the text fields with their messages. The additional work this causes is bothersome, and many phishing methods work just as well with forms as they do with e-mails. Phishing links are also well concealed here and one wrong click is all it takes for the unlawful machinations of the phishing page to begin.

Documents infected by viruses—from a form straight to the network

HR departments also frequently use forms. Prospective employees can apply directly via the company's website and can upload their CVs, diplomas, and references while doing so. Within the company, the incoming data is automatically transferred to the HR system, which is practical and efficient for both sides. However, these HR forms also open the door to fake applications.

> **Uploaded Office documents can spread macros and viruses and cause serious damage to IT infrastructure.**

Hype sales

Concert tickets sold out in minutes or special editions that are out of stock. Automated shopping bots can be the reason for this. Real customers have no chance against them.

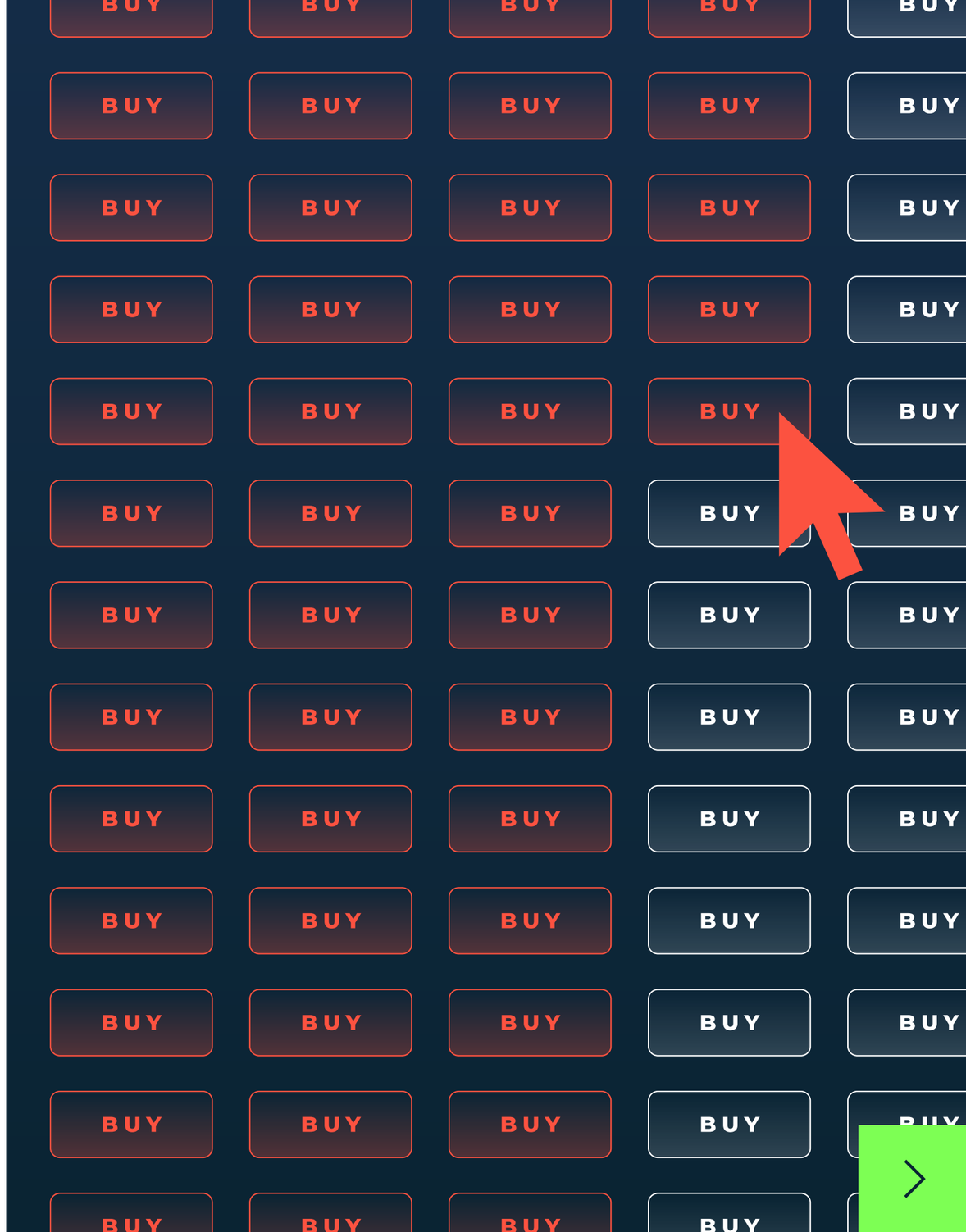
"Hype sales" are used by companies as a targeted marketing instrument. Limited numbers of tickets for coveted events are thrown onto the market to increase the desire of wanting to be there at any cost. This works the same way with any number of product launches, new editions, special editions, and the like. Sneaker hype sales are a classic. 30 years ago, Michael J. Fox (alias Marty McFly) predicted in "Back to the Future" the seeds of the sneaker mania that would one day blossom. His original "Nike Mags" are now being traded on Ebay for up to €77,000.

That is a respectable profit margin—one which bot operators know how to exploit and which can cause massive damage to online retailers. That is why bot management to recognize hype sales bots is so important for them. Bots are not criminal, but they outwit their fellow bidders using completely legal means and 100% valid credit card numbers. A bot operator sends out a whole host of automated computer processes along with different identities and payment methods, thus skillfully circumventing maximum purchase quantities. While a real customer is able to secure a maximum of one or two items, the bot operator successfully buys large quantities.

Business model: maximum profit margin

These bot activities are not immediately apparent to the online retailer, because the items are shipped to different addresses. The bot operator then sells the cheaply purchased products at a multiple of the original price. Profit margins of 1,000 percent are not unusual.

This is a perfectly legal activity, but a disaster for the seller's marketing. The advertising effect is reversed, leaving disappointed customers behind and damaging the image of the online retailer.



Bots block products from real customers in online shops.

Cart abandonment

When bots fill a digital shopping cart without completing the purchasing process, they block products for actual customers. Sales drop and customers leave.

A comparison with supermarkets illustrates how cart abandonment attacks work: The customer fills his cart up with items. But instead of going to the check out, he just leaves it in a corner and departs the shop. It can take some time for staff to notice the abandoned cart and put the items back on the shelves. Until then, the goods are blocked from being sold to other customers. Bot attacks of the “cart abandonment” type work similarly in the virtual world. They involve blocking inventory in “parked” carts to slow down or hinder sales on the site under attack.

Blocked inventory slows e-commerce down

Between 40 and 80 percent of the visitors to a web shop abandon their purchase. In bot-driven cart abandonment, blocking inventory is the goal from the outset. For products available in large quantities, this is not a problem at first. Parking carts becomes critical if the quantity of products is limited or if there is high demand for a certain time only. If an online provider successfully uses such a bot against a competitor, the competitor’s customers will be informed that the product is not available. As a result, he himself could be the one who gets the big rush of buyers.

Credit card testing

Testing credit cards is one of the most lucrative activities and is preparation for online fraud. Unfortunately it generally goes unnoticed by retailers.

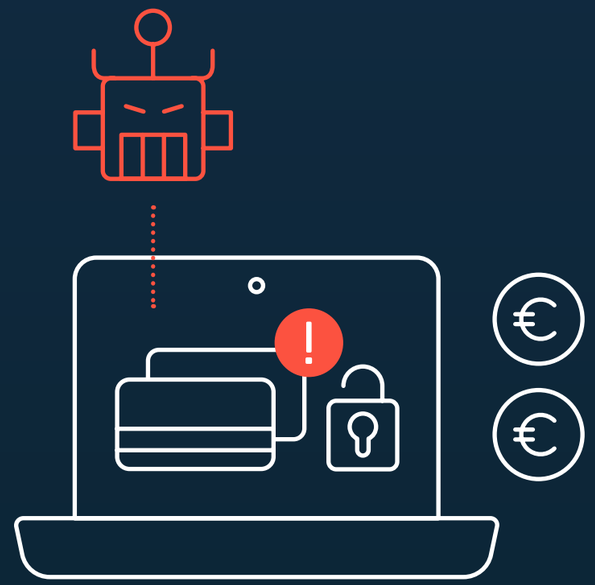
This particular type of bot is designed to test credit card data on a grand scale. This data is not usually processed directly on e-commerce sites, but instead by payment service providers, such as PayPal, commissioned by the shops.

Preparation for fraud

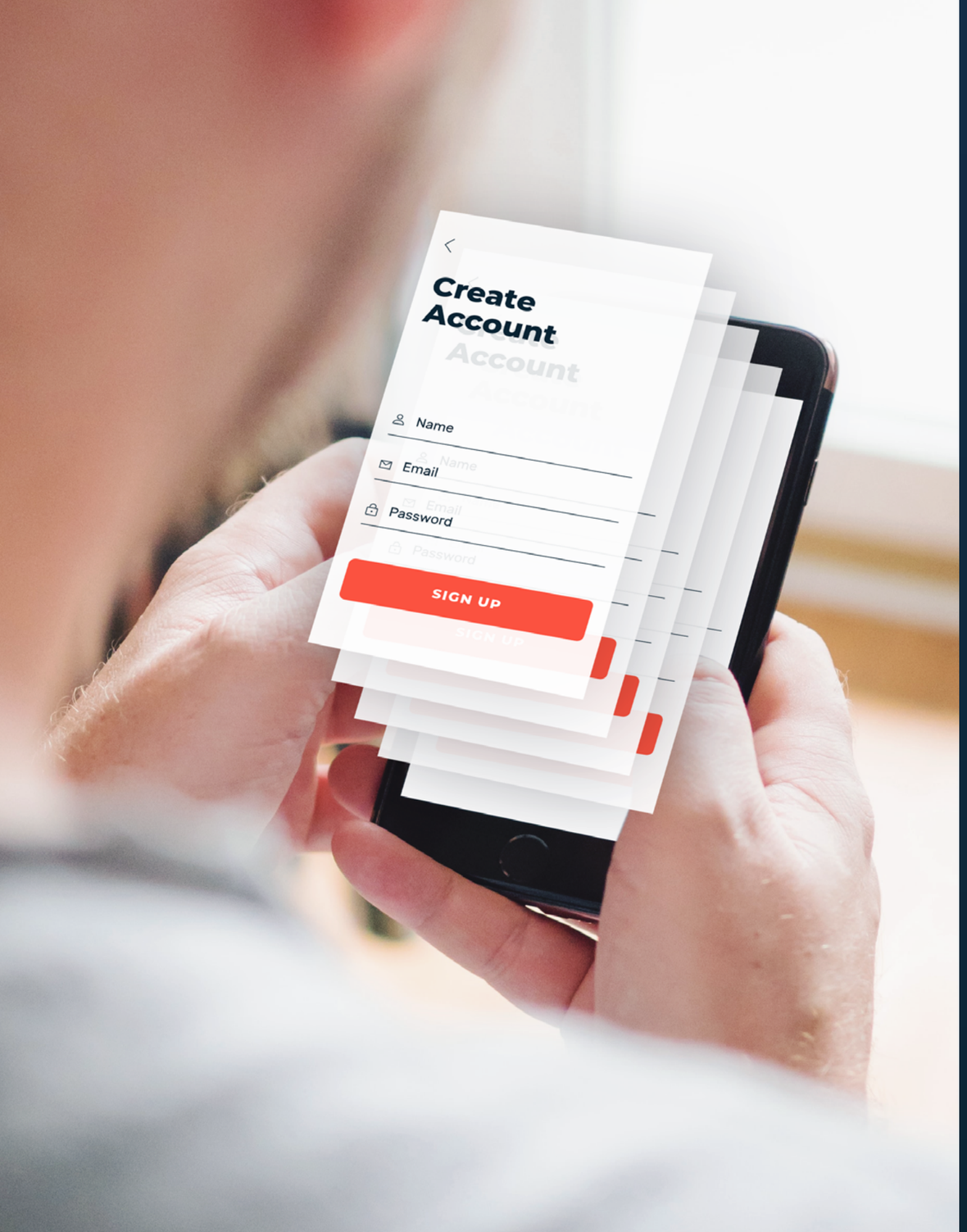
In order to test whether a purchase can be made with credit card data, attackers on the internet purchase a large amount of credit card information in blocks. They do not even have to use the Darknet for this; there are plenty of websites where this can be done. They then send bots to multiple online stores to test whether the information can be used to make purchases.

Bots also check whether credit card details are valid when making reservations for rental cars or hotels. The customer usually has to provide a credit card as security. There is no booking, but only a security check during which the amount is pre-booked. This is not even apparent to the card holder.

Bots access the site from a variety of IP addresses to test credit card information. This makes it very difficult to track transactions of this kind. The end of the story: Attackers find out whether a credit card works and are then able to create lists of “good” and “bad” cards. The ammunition depot for large-scale fraudulent payment transactions is thus well stocked, for personal use or for resale.



Bots test credit card information quickly, effectively, and often undetected.



Account creation & takeover

Fake profiles or spam with malicious software: automated requests specifically try to manipulate web services, causing harm to users and companies alike.

Without being noticed, some bots create massive numbers of new accounts on the website for later misuse. This can involve generating content spam or spreading malware. Money laundering can also be carried out or the search engine optimization of the company under attack distorted, with wide-ranging harm to the website operator.

Affected website operators usually recognize the problem when there is an abnormal increase in the creation of new accounts or an increase in comment spam. Other signs of anomalies include accounts with incomplete information or accounts that have been created but are going unused. Typically misused information for account creation includes authentication credentials, credit card and other financial information, but also medical or other personal information.

Account creation bots put website operators in an unpleasant situation, because the amount of newly created and active accounts is actually a performance indicator and underscores the value of a website. Apart from that, when getting rid of automatically created accounts, extra care must be taken to ensure that the number of false positives, i.e. requests erroneously classified as bot traffic, is really zero: an aborted transaction may still be forgiven by a loyal customer, but blocking or even deleting the account will not be.

Skewing

Business decisions are increasingly based on the analysis of user data. Bots distort these statistics. If a company's planning, e.g., for advertising budgets, is based on improper assumptions, a lot of money will be incorrectly invested.

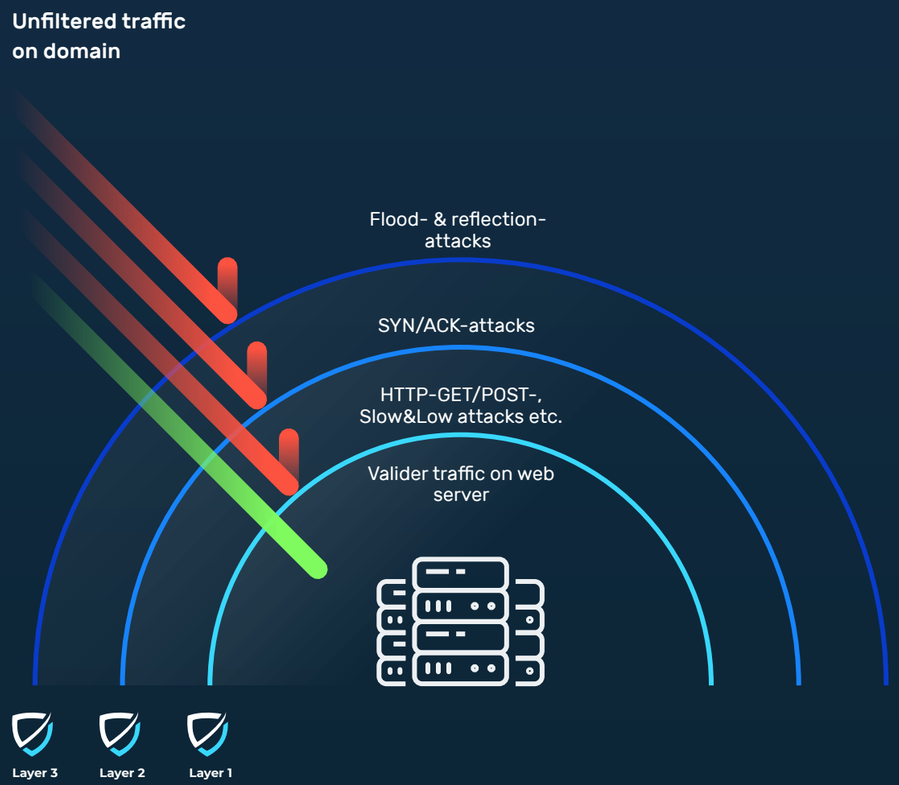
Marketing specialists are constantly studying how their company's website is being received, how conversion rates are developing, and why users respond in a particular way at specific times. They use these analyses to plan their marketing and budget advertising activities.

But what if the activity on the website is not coming from a human, but from a bot with no intention of making a purchase in the first place? In social media, the assumption of a false identity is quite normal today, one prime example being fake followers on Twitter. Bot operators are extremely creative and can program their computer processes to remain on the site a while longer, perfectly imitating the behavior of a human visitor.

> **Bot traffic then ensures that wrong business decisions are made.**

The user situation is seen differently from what it actually is and the painstakingly compiled statistics are simply wrong. A distortion or skewing has taken place.

Bots mimic strong user interest, distorting analysis data.



Myra DDoS Protection filters out harmful traffic in real time. Only valid requests reach the web server.

Denial of Service

Hackers also use botnets to attack the availability of websites and IT infrastructure. Their goal is to cripple the site under attack.

The bots thus far described in this white paper have one thing in common: they expect a response from the website being attacked and they have no interest in bringing it to a complete stop.

In this respect, the previously discussed types of bots are fundamentally different from DDoS attacks. These attacks also operate through botnets, but they are up to something else: Their focus is not on the individual action as such, but on the sheer mass of access requests. They are intended to cripple a website and make sure that it stops providing its services. A service blockade or “Denial of Service” is the result.

This means that they too, without doubt, can be classified as harmful bots. However, different instruments are used to combat them than those used against the bots discussed here. Myra Security offers DDoS protection that protects websites and other applications from DDoS attacks by hiding applications behind a three-layer filter system. This system is based on hardware and software components developed by Myra.

> **Harmful traffic flows are blocked via complex, intelligent, and self-learning Myra filter layers.**

Myra Web Security

The Myra Web Application Security portfolio includes all of the products and services needed to effectively protect websites and applications.

Myra Bot Management

Myra Bot Management is modular and gives you, the customer, full flexibility in detecting and controlling bots: either based on bot categories or as a complete package.

Myra Multi-Fingerprinting is an integral part of the system for reliably detecting automated bot accesses.

Myra Web Application Firewall

The Myra Web Application Firewall filters, monitors, and controls incoming and outgoing web traffic on the content level. It thus protects applications against being infected by harmful data and sensitive information against being spied upon.

Myra Malware Protection

Myra Malware Protection provides additional protection against malware infection from infected user files. It scans files before they reach your infrastructure.

Bots leave fingerprints behind

Bots access the website from multiple IP addresses and networks.

They pretend to be a normal browser and fake other information to appear like a regular user. Because access is distributed, no connection between them is apparent at first glance.

Myra Bot Management creates exactly this context with the help of passive multi-fingerprinting. Each time the website is accessed, more than 50 access attributes for the unique identification of the software used are included in the fingerprint. Myra has now stored over three million of these digital fingerprints.

As soon as the fingerprint is available, appropriate measures can be taken or protective mechanisms can be initiated. Unwanted and prohibited access can be clearly identified, blocked, confronted with human interaction challenges (e.g., CAPTCHA), or otherwise controlled or redirected.

Even bots leave traces behind. Their unique identification is the basis for managing them effectively.

Myra uses more than 50 attributes to identify bots.

Tiered combat system: from blocking to the honeypot

Simply blocking every automated request is not a good strategy. That would also block good, desired bots. It is much more important to provide a suitable response for each request.

Myra generally advises choosing the mildest effective means to prevent bots from doing what they do. This includes human interaction verification to tell automated input apart from input originating from real people.

CAPTCHA is now standard on many websites and yet it is no panacea. Because the problem with false positives is that if someone is turned away, even though he is a real person, he is lost as a customer/buyer to the website operator. A CAPTCHA mechanism can also be installed to protect against form abuse.

Another option for fighting bot abuse is to rate limit it. Here, the bot is recognized and allowed to start a limited number of access requests per time unit (rate limiting).

This type of rate limiting is used when the bots are basically "good," but are generating a lot of traffic and lowering performance of the website.

> **The "honeypot" has also proven to be an effective tool—more or less a second version of the website, which suggests to the bot that it is the original.**

The content is displayed there is completely different, however. For example, in order to kick out price grabbers, the honeypot includes prices that are lower, higher, or even the same as the original. This measure is an irritant that puts a stop to automated price undercutting by a few cents on the attacker's website.

Our key areas

Protect and speed up your applications, websites, and IT infrastructures. Our smart products and solutions are based on software developed in-house and are designed to meet current as well as future IT security and performance requirements.

Myra Platform

The Myra Platform is the basis for all our products and services. It provides access to the customer area with an easy-to-use configuration interface.

DDoS Protection

Myra DDoS Protection reliably and fully automatically protects web applications, websites, DNS servers, und IT infrastructures against overload attacks.

Web Application Security

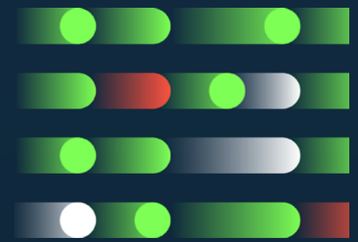
Myra Web Application Security protects your applications against attacks as an upstream protective filter. Malicious traffic is filtered before it reaches your servers or cloud infrastructure.

Load Balancing

The Myra Multi-Site Load Balancer ensures an ideal distribution of requests onto any number of servers, making your services fail-safe. Your website and applications perform excellently due to reduced loading times.

Content Delivery Network

The worldwide Myra Content Delivery Network (CDN) with its own global infrastructure delivers all static and dynamic elements of your website with lightning speed.



Web Intelligence

Myra offers 100% transparency with respect to incoming traffic. This allows for visualizing requests in real time and for data analysis adapted to your needs.

Why Myra?

Technical pioneer

Myra fulfills all 37 performance requirements of the BSI (German Federal Office for Informations Security) for qualified DDoS protection providers.

Future-proof technology

Our systems are designed for future requirements, e.g., through native IPv6 support.

Real-time protection

Our filters block malicious requests before they cause any damage.

Custom solutions

We offer solutions and products specifically tailored to your industry.

Made in Germany

We'll protect your data in line with the strictest standards. Guaranteed.

Easy to set up

No additional installation of hardware or software is required.

Quick response times

You ask. We answer right away.

Real 24/7 support

You talk directly to our IT experts.

Certified

Myra is committed to the highest quality standards and certifications, such as ISO 27001 and PCI-DSS.

High scalability

Our systems adapt to the growth of your business.

Our own global CDN

Our server network guarantees reliable, fast, and worldwide delivery of your data.

Guaranteed service quality

Do you need a service level agreement of 99.999%? We will take care of it.

Internationally reputed companies and institutions throughout the world rely on Myra Security.

Bundesministerium für Gesundheit

flatexDEGIRO

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 is the new standard for global IT security.

The German technology manufacturer Myra offers a secure, certified Security-as-a-Service platform for protecting digital business processes.

The smart Myra technology monitors, analyzes, and filters harmful Internet traffic before virtual attacks cause any real damage.

Myra Security GmbH

Telefone +49 89 414141 - 345

www.myrasecurity.com

info@myrasecurity.com