INDUSFACE™

WHITEPAPER

DDoS In The New Age World & How To Prevent Them.

With the advent of IoT, DDoS are attacks becoming more prominent and sophisticated. DDoS (Distributed denial of service) is an attack done from distributed machines to bring down the availability of service, temporarily or permanently. These attacks are done for varying reasons, ranging from cyberbullying or extortion tactics to some form of protest. Within days after DreamHost rejected a request from the Department of Justice to diverge visitor data for an anti-Trump website, the company has reported DDOS attacks. At times, DDOS attacks are also state sponsored, with widespread allegation of such DDOS attacks being done from China and Russia.

Whatever the reason behind the DDOS attacks, the reality is, with the cost of launching DDOS attacks coming down, these attacks are here to stay, and almost anyone can become a victim of DDOS attacks. These attacks are very cheap, easy to organise, and without proper defence, damn effective.

These attacks can be launched with no direct contact of attackers, and payment can be made using cryptocurrencies like Bitcoin. There are even review sites available for the same.

The best ip stresser/booter/ddoser on the market!

These have all been personally tested and chosen by multiple people. I personally was tired of weak ip stressers that couldn't knock down a stick. Luckily i found a few gems hidden away and i decided to make this list so that no one else has to waste money on a bad ip stresser. This ip stresser list was compiled by spending around 400 USD on dozens of booter sites so we could rank them. We rank each booter on a variety of factors. A booter may be stronger than one above it but ip stresser power isn't everything. As a customer you want an ip stresser that will last and be simple to use. So please enjoy our booter list, we updated it every few months so you don't have to waste your money on a bad ip stresser.

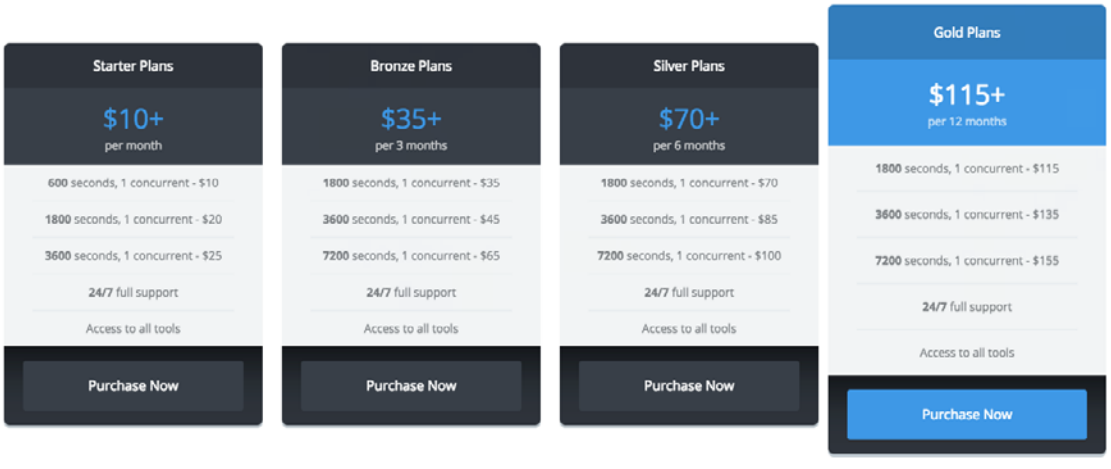
#1 – Webstresser.org (500GB/s of combined power)(Takes down everything)(Working Skype resolver)(Active support)(Accepts Paypal)(A lot of tools)

#2 – Freebooter.co (300GB/seconds)(Easy to use source)(Reliable)(20Gbps Per Boot)(Accepts Paypal/BTC)

#3 – Critical-boot.com (Good power) (Easy to use source) (PayPal/Credit cards and 15% off Bitcoin) (Build Your Plan)

Such services are a dime a dozen, and buyers of these services understand the efficacy of such attacks. A cost to launch a 5-minute attack is less than $5, but a 5-minute loss of service could be multi-fold for large organizations. We can only guess how many customers an online store loses if an attack lasts the whole day. For example, Amazon's loss for 40 minutes downtime was estimated to be around $4.8 million dollars.

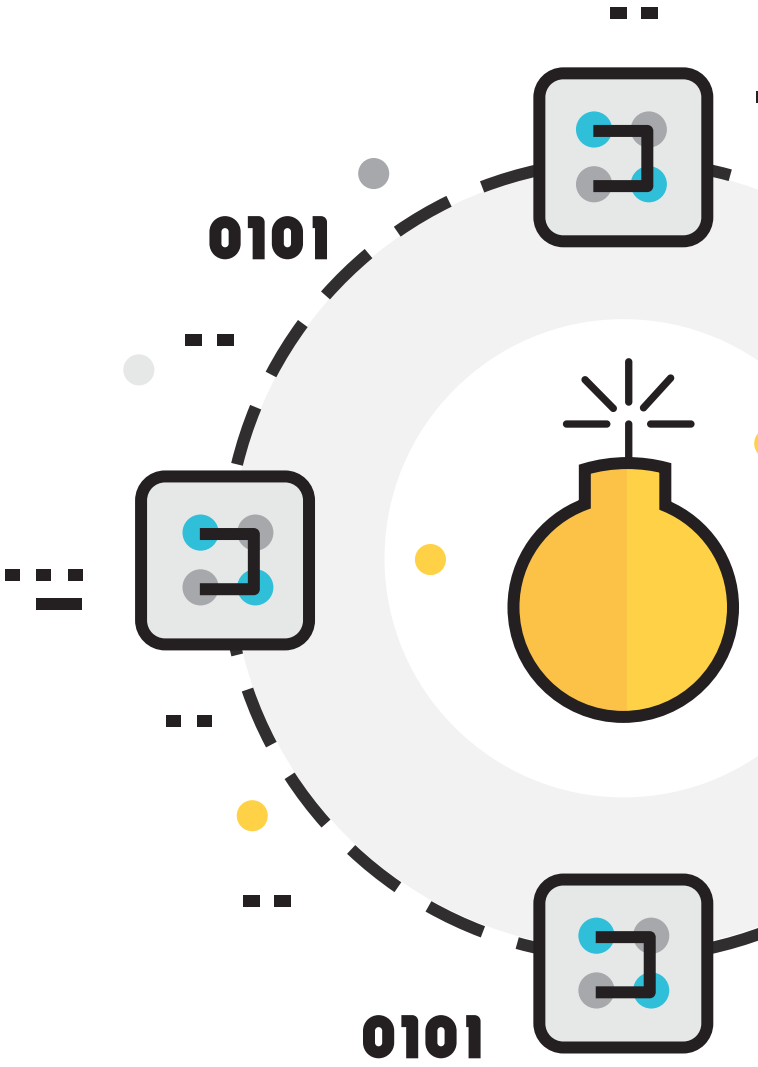
Nowadays, DDOS attacks are available as a service that can be ordered online. When you dig deeper and look at the DDOS services available, you will feel like you are ordering a legitimate SaaS service with various plans, ranging from free to premium service.



Extra concurrents cost an +$25 on any plan.

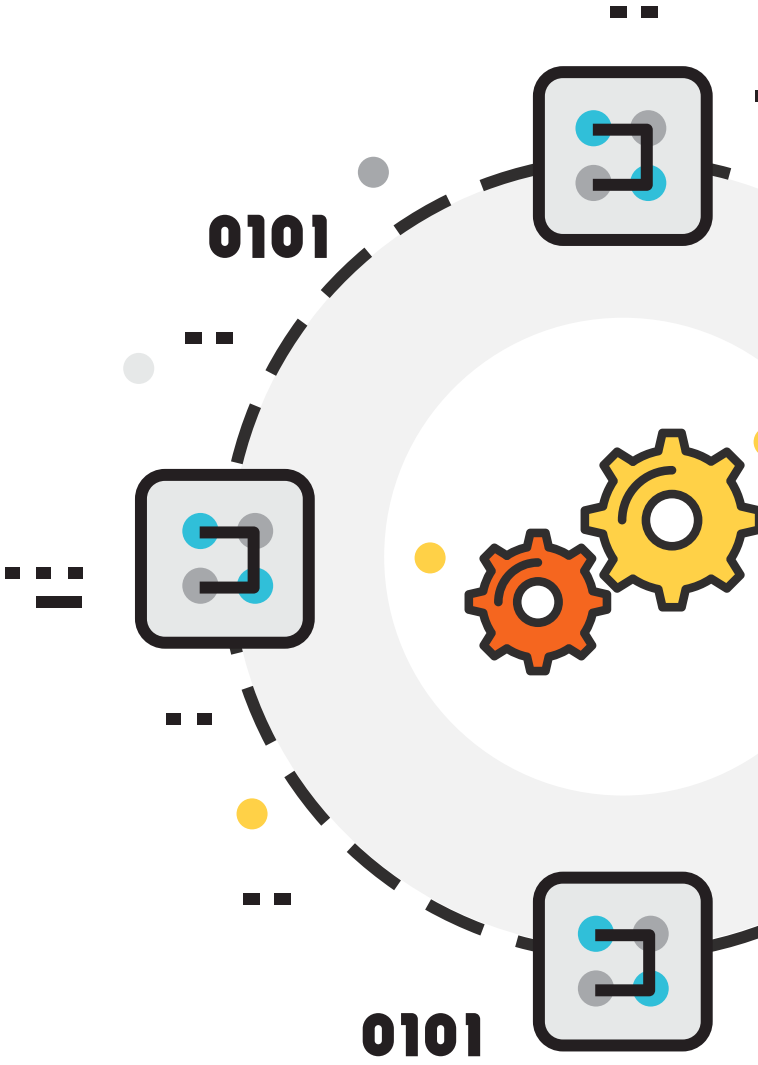
BOTNETS

Cybercriminals are seeking new and cheaper ways to make the attacks more effective, and IOT is making their life easier. These criminals are turning IOTs into botnets (bots on networks) to launch distributed attacks. Sometimes called zombie armies, botnets are a bunch of connected devices hijacked by cybercriminals and controlled remotely to use the device resources for malicious purposes, like spam or DDOS.



Internet of Things (IOT) lends automatically for these type of attacks, as they are inter-connected and public most of the time and are not built with great defences. Usually, even the default passwords of these IOTs are not even changed, making them easy targets for hackers to take control of. The last time botnets made news was last year, when a massive DDoS attack on Dyn (an internet infrastructure provider) knocked out access to Amazon, Netflix, eBay and Twitter, to name just a few. This attack was unusual not only for its scale – blocking services for millions of online users – but because internet of Things devices, such as DVRs and alarm systems, were used to create the botnet.

NEW AGE DDOS ATTACKS



You may be thinking, all right, I understand DDOS is here to stay; cyber-criminals can launch huge attacks to bring down service using botnets easily, so I need a basic solution that can deny distributed attacks. Yes, that might have been true even a year ago, but unfortunately, the landscape is changing, and these attacks are becoming very sophisticated.

Earlier this month, a huge IOT based DDoS attack was predicted after publication of code that could exploit Huawei HG532 routers. Similar warnings were made after the publication of Mira malware code in Oct 2016. The truth is, with botnets being prevalent, cyber criminals are becoming very sophisticated and have started using botnets to exploit vulnerabilities in applications/devices as they get published, and such attacks can unfortunately be not stopped by existing out of the box d DDoS solutions that may work for rudimentary volumetric attacks.

HOW TO PREVENT THEM?

To build defences against these sophisticated DDOS attacks, the rudimentary traditional out of box defences that existing cloud vendors provide are insufficient. For one, they only address one part of the problem, namely certain classes of bot attacks but not web application, DDOS, and business logic attacks launched by bots or humans.

At Indusface, through our revolutionary AppTrana solution, we offer a solution that is radically different and builds defence around an application after understanding the security posture of the application. With us, organizations can identify the vulnerabilities in the application through the automated and premium scans. This guarantees that organizations understand the risk posture of their application upfront. AppTrana, through a fully managed detection module, ensures vulnerabilities reported have zero false positives.

Once risk posture is identified, AppTrana enables organizations to patch vulnerabilities virtually through its WAF module. For this, AppTrana provides-

- Advance Rules
  Out of the box protection Rules with zero false positive guarantee
- Premium Rules
  Rules that are experimental in nature, monitored by security experts and fine-tuned to meet application need before they are put in block mode. No action is required from customer
- Custom Rules
  Application specific rules written by security experts with zero false positive guarantee based on customer request

With this approach, AppTrana ensures security is tuned to meet specific application need, guaranteeing zero false positive. These rules are constantly monitored and updated as new vulnerabilities are published, ensuring customers' applications are always protected against vulnerabilities. These rules also act as a starting point for further advancement of protection. We constantly monitor these rules, and if anyone is trying to exploit the vulnerabilities protected by the patches, we gather valuable information about the hackers and their behaviour, which helps us further strengthen the rules/protection. There is a lot of talk of Deep learning and Machine learning. At the core, an intelligent system can determine a bad intent of a hack attempt and learn on its own. A managed service with historical information as the baseline, combined with human intervention for analyses, enables us to do this without getting too caught up in the technical details of deep learning and machine learning.

With bot/DDOS protection, Indusface takes a multi-pronged strategy. For automated protection, we have rate based DDOS/BOT mitigation, specific bot signatures, brute-forcing, behavioural rules, like anomaly scoring and self-learning rules, which track the activity of users uniquely through machine fingerprinting, allowing us to granularly flag suspect users by their behaviour. Actions that can be taken vary from customer to customer, depending on the security posture of the company, where they can block the users automatically or show a captcha page. In our experience, we see that customers want to vet anything that is even a little intrusive (e.g., landmine planting or script injection), so options like log, captcha, and expert monitoring is key.

As discussed, Indusface protection uniquely takes advantage of the detect + protect components of our solution. Protection is inline, which gives it complete visibility to all web application

traffic, good and bad, and makes use of scan data (automated and manual Pen Testing) and specialized rules. We can check if known vulnerabilities are being targeted and take an aggressive security posture towards clearly malicious actors. Our algorithms automatically tune the rules and share intelligence across customers by learning from traffic and scans.

What we have learned over the years is that, when sophisticated denial of service attacks is in play, only specific, fine-tuned rules can protect customers. This is something we provide and none of our competitors or specialist bot protection vendors do. Our automated protection is augmented by human intelligence from our Signature Development team, who constantly monitors new threats through third party feeds, scripts, vulnerabilities, and tools, writing custom rules for any new attacks, and our manual pen testing team keeps abreast of the latest in new vulnerabilities. A purely automated solution will not stand up to a sophisticated targeted attack. We have an in-house 24*7 team that steps in case of DDOS /BOT attacks and writes custom rules to avoid advance layer 7 attacks. This is a huge differentiator, since it is always an arms race between malicious actors (humans and bots) and protection, and with Indusface's unique approach, we ensure our customers are always ahead in this race.

AppTrana is built bottom up on AWS, adhering to AWS DDOS resilient architecture. This intern inherently protects any application behind AppTrana from infrastructure level DDOS attacks and volumetric attacks, making us the only vendor capable of protecting applications from all types of DDOS attacks, ranging from network/infrastructure level attacks and protocol attacks to sophisticated application level DDOS attacks.

ABOUT INDUSFACE

Indusface is an award-winning application security leader protecting 1000+ global customers with our unique Total Application Security platform that detects, protects, and monitors applications. Our Total Application Security solution is available On-Premise, As A Service and through the AWS Marketplace.

Mentioned in the Gartner Magic Quadrants for Application Security Testing and Web Application Firewall, Indusface has won all major startup awards in the last 12 months including the NASSCOM-DSCI 'Security Product Company' Award, iSpirit's 'InTech50 Most Innovative Products from India' and AWS 'Regional Innovation Partner: Technology Award'.