DDoS for Hire | Booter, Stresser and DDoSer | Imperva

Archived: 2026-04-05 23:34:46 UTC

DDoS stands for Distributed Denial of Service, a malicious attempt to make a server or a network resource unavailable to legitimate users, by overloading it with massive amounts of fake traffic.

Historically, DDoS attacks are associated with hacker and hacktivist groups and often considered to be a work of professional cyber crooks.

In recent years, with the emergence of DDoS-for-hire services (a.k.a. stressers or booters), the barriers to entry for a DDoS attacker has been significantly lowered, offering users the option to anonymously attack any target, for just a few dozen dollars.

> "With the increasing number of people on the internet we will see much, much more crime and it will be facilitated by cybercrime-as-a-service producers."
>
> Troels Oerting, head of EU cybercrime center

DDoS for hire: Subleasing infected computers

To understand the business of DDoS-for-hire let's take a look at what exactly the "product" is.

In a nutshell, what these DDoS services are usually selling is access to DDoS botnets: networks of malware-infected computers, which are in turn being "subleased" to subscribers.

Sadly, building such a botnet is simpler than you may think, considering the elaborate damage that can be caused a cluster of such "zombie" computers.

For instance, a quick Internet search by any would-be botnet creator will pull up several popular botnet builder kits, often complete with a set of tips and instructions.

Typically, such kits contain the bot payload and the CnC (command and control) files. Using these, aspiring bot masters (a.k.a. herders) can start distributing malware, infecting devices through a use of spam email, vulnerability scanners, brute force attacks and more.

With enough computers, mobile phones and other Internet-connected devices "enslaved", a new botnet is born—ready to do the dirty work of anyone willing to pay.

So what are these "Stressers" and "Booters"?

Though botnet building kits are widely available, most hackers will not make the effort to create a botnet overnight.

DDoS attacks are illegal and, subsequently subletting access to malware-infected computers is illegal as well. This situation poses a challenge to many DDoS-for-hire "service providers" who want to conduct their shady activities while still operating in the open and be able to reach the mass market.

In an attempt to reconcile these two contradictions, some DDoS-for-hire elect to euphemistically call their services "stressers"–the implication being that they can be used to test the resilience of your own server.

However, with no steps taken to actually verify your identity and your ownership of the target server, stressers allow you to "stress test" just about anybody, enabling cybercrime, cyber-vandalism and many other types of DDoS-related activities.

On the flip side, some botnet owners prefer to call a spade a spade, and offer "booter" or "ddoser" services. The services offered are exactly the same, so there's no actual difference between booter, stresser, or ddoser.

In the end, they all refer to DDoS for hire, with some exploiting the lack of regulation to remain vague about their intentions, allowing their "businesses" to fly under the radar.

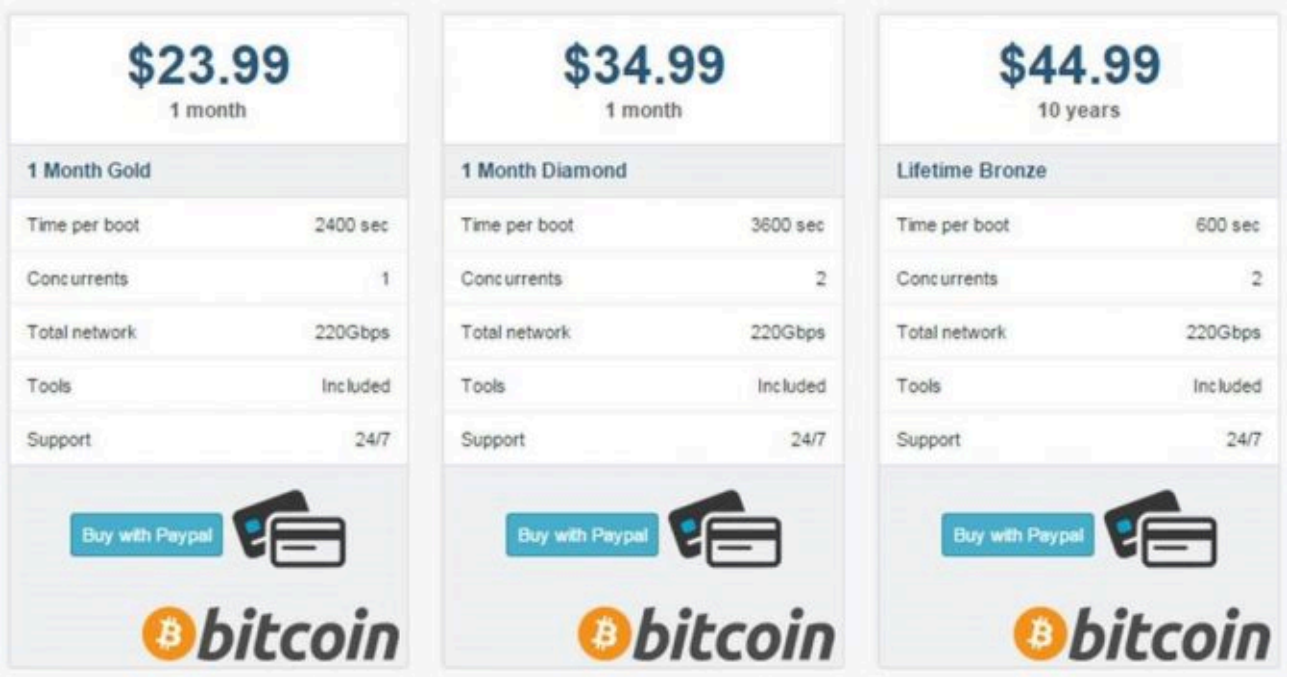
Regretfully, there is no mechanism along the way to examine the formation of such stresser services and the legitimacy of the "stress tests" they perform.

Renting a botnet is cheap, quick and easy

What would you need to rent a DDoS service, and how much does it cost?

It turns out, not much is needed to actually rent a botnet. Usually, it boils down to a PayPal account, ill-will towards the target and willingness to break the law.

As strange as it may sound, today just about anyone can use a stresser to paralyze an unprotected website for a small fee. To locate one of these you don't even need to school yourself in the mysterious ways of the Deep Web, just conduct a simple Google search.



Example of booter advertised prices and capacities.example of booter advertised prices and capacities.

When it comes to pricing, most stressers and booters have embraced a commonplace SaaS (software as a service) business model, based on subscriptions. As the DDoS report has shown, the average one hour/month DDoS package will set you back $38 (with $19.99 at the lower end of the scale).

The perils of booter services

Aside from the obvious threat of increased cybercrime, a key danger of widespread access to extremely capable DDoS services is the growth of a whole new class of cyber-criminals: numerous attackers who require very little knowledge, preparation and resources to cause a high degree of damage.

The danger of widely available botnets, however, runs deeper than their ability to cause grief to private users, or even the financial implications of DDoS attacks, no matter how destructive.

Fact is that, as long as they are allowed to operate with relative impunity, these DDoS-for-hire services can endanger entire online industries, especially SaaS and e-commerce that are built on user-trust and constant availability.

DDoS attackers undermine the very evolution of the Web, crippling the innovation of young online organizations that are less capable of dealing with DDoS threats and, as a result, far more exposed to DDoS extortion attempts.

Cybercrime cannot be viewed as a sub-class of crime, removed from the real world and existing only in cyberspace. If anything, it should be considered as a new, all-encompassing breed of criminal activity, one which disregards borders and can cripple billions of Internet users across the globe.

Stresser and booters services are just a byproduct of a new reality, where services that can bring down businesses and organizations are allowed to operate in a dubious grey area. All because of the inability to enforce effective global policies.

The fact remains that stressers, booters and other DDoS-for-hire tools are nothing more than cyber-weapons, whose growing popularity and remarkable availability demand strict and immediate action.
