ECONOMICS OF DDoS ATTACKS

A Buyer's Market: The Economics of DDoS Attacks

• • ○

These days, there are typically three parties to a distributed denial of service attack.

You probably know about two of them: the perpetrator and the target. What may surprise you, though, is the vast and growing number of third-party providers of DDoS attacks as a service. Brazenly advertising their wares online, these providers will either sell would-be attackers access to the tools to conduct an attack, or they will perform the attack themselves on the customer's behalf and provide detailed reports of their accomplishments. Their fees are shrinking due to rapidly expanding competition and the abundant supply of readily available attack resources such as botnets. As a result, the DDoS business is very much a buyer's market.

Prices for attack services, sometimes called "stressers" or "booters," vary widely, as do estimates of the total cost of an attack to the victim. But the economic model is very straightforward: DDoS attacks are cheaper than ever for the perpetrator, extremely lucrative for the attack service provider, and financially devastating for the target. Low prices and the turnkey nature of attack services — which require nothing to build or configure — have "democratized" DDoS attacks and the threat actor population.

ARBOR® NETWORKS
The Security Division of NETSCOUT

A VOLUME PLAY

Alarmingly, individual DDoS attacks can now be launched for as little as $5. As such, attack service providers look to make their money on volume — explaining why a DDoS attack occurs every six seconds. One case that recently came to light was a 20-year-old UK man who was convicted and sentenced to prison for operating and selling a service called "Titanium Stresser." As reported by security journalist Brian Krebs, the culprit originally built the service when he was a mere 15 years old. Since then, his "stresser" had been used in more than 1.7 million attacks around the world, netting him a cool $300,000.

To capitalize on increasingly lucrative opportunities to unleash DDoS attacks worldwide, more and more operators resemble legitimate service provider infrastructures with significant compute power. They typically run their own botnets — vast networks of internet connected computers, machines and devices infected with malware that turns them into "bots," or unwitting robotic accomplices — to unleash DDoS attacks. Perpetrators can essentially rent the providers' botnets by the hour, day or week, or in some cases can buy a specific number of bots outright. The mechanics of transactions follow a classic web service model, meaning the perpetrator and the provider need never come in contact.

A CHOICE OF ATTACK FLAVORS

Providers that conduct attacks-as-a-service boldly post their "menus" online with tiered pricing reflecting the many different flavors of attacks they offer. Prices are based on several factors. They can include the duration of the attack, the perceived value of the target, the country in which the attack takes place and/or the different methodologies employed. That said, other criteria can apply. For example, attacks on government agencies can command a significant premium. (Notably, providers charge a high multiple for attacks on organizations they deem to be using strong anti-DDoS protective measures.)

One threat actor tracked by the Arbor Security Engineering and Response Team (ASERT) offered $60 daily and $400 weekly pricing, as well as discounts on orders of $500 or $1000. ASERT's research pegged the mean cost at $66 per attack, compared to the potential cost to the victim of around $500 per minute.

PAYING A STEEP PRICE

For a large organization, the costs of being a target can run substantially higher. In Arbor Networks *12th annual Worldwide Infrastructure Security Report*, 59 percent of respondents estimated their downtime costs above $500/minute, with some indicating much greater expense. And that's just lost revenue. It does not factor in the sunk cost of building a robust e-commerce or service delivery platform, the cost of repairing the damage, or the potential legal costs of settling with customers denied service or otherwise compromised. Nor does it consider the long-term reputational damage that can erode market valuation.

All of this points to the need to invest wisely when protecting against DDoS attacks. A hybrid solution that combines on-premises and cloud-based protection is the industry best practice in DDoS defense and surprisingly affordable thanks to managed services and virtualized solutions.

With the attacker's costs diving and the victim's costs skyrocketing, the economics of DDoS attacks today clearly favor the attacker over the defender. That is why DDoS attacks aren't going away, and in fact are projected to escalate. But not every target has to be a victim. It's time to take action.

• • ○

Learn more about best practice hybrid defense and Arbor's DDoS mitigation solutions.

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

AI/ECONOMICS/EN/0617-LETTER

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842