imperva

Cheap and Nasty: The Anatomy of a DDoS Attack

Distributed Denial of Service (DDoS) attacks capable of crippling websites and network resources for days can be bought online for as little as $5 an hour[1].

With consequences including significant financial losses, damaged client relationships and lost productivity, that's a lot of bang for the cybercriminal's buck.

Protecting your business starts with understanding the DDoS ecosystem - and how your organization is impacted...

Cyber arms dealers
sell ready-made DDoS 'services' to

Sells Services

Cybercriminals
who can attack their targets, even if they don't know how to code

Attacks Targets

Victims
can be anyone.

Recruits botnet

High-profile DDoS targets make the headlines daily, but the truth is that anyone with a public web presence is a target...

1. Large Corporations
2. Mid-sized Corporations
3. Small Businesses
4. Online Retailers
5. Financial Services Providers
6. Online Gaming/Entertainment Providers
7. Healthcare providers/hospitals

...and anyone with the inclination and a target can launch an attack — Arms dealer "service providers" even offer live chat support for unskilled attackers who are willing to pay.

Most Targeted Industries

DDoS attacks on some industries increased significantly during the COVID-19 pandemic[2].

A typical DDoS attack is executed using a **botnet**.

A **botnet** is a group of malware-infected devices that cybercriminals can use like an enslaved army of cyber weapons to launch DDoS attacks, without the device-owners even knowing they're infected.

Historically, DDoS attacks were associated with hacktivists and professional cybercriminal gangs. Today, anyone can hire an attack - and automate it - without needing any programming skills whatsoever.

+108% Automobile

+53% Telecomunications / Internet Service Providers

+43% Marketing

+32% Gambling

+30% Financial Services

The Cyber Arms Dealers

Tools of the trade vary, but there's a botnet to suit every type of attacker....

What They Are	What They Do
The Kit Maker	Builds user-friendly toolkits that make botnets accessible to anyone.
The Builder	Uses malware kits to build botnets for herders and booters.
The Bot Herder	Controls botnets using remote command-and-control servers.
The Booter	Sells botnets and toolkits under the guise of legitimate server stresser tools.

The Cybercriminals

Who buys these weapons, and why might they attack you?

The Hacktivist
To promote political, social or other causes by defacing targeted websites, leaking information etc.

The Intimidator
To suppress free speech and political discussions

The Bully
To harass and intimidate online users

The Extortionist
For money (**Pro tip**: Don't give it to them)

The Hired Gun
Like assassins, it's how they earn their living.

The Script Kiddie
To show off to their peers or just for the heck of it.

Operation Overload: DDoS and the Bottom Line

Even a few minutes of downtime can have far-reaching effects for your business. It can take days, or even weeks, to recover from a DDoS attack.

91% **of organizations have experienced downtime from DDoS**

90% of companies have experienced at least one DDoS attack over a 12 month period

25% of DDoS attack targets are hit **10 times or more**

Counting the Cost

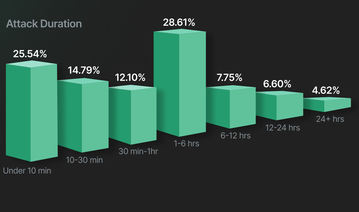
$100k is the average cost of just **one hour of downtime.**

34% report costs in excess of $1m for an hour of downtime[3]

545 hours of staff productivity lost to IT downtime every year[4]

72 most DDoS attacks stop within 72 hours, some last just minutes

10 Days the longest DDoS attacks in 2020 lasted over 254 hours



Big Bang for Small Bucks

A 24-hour DDoS attack costs cybercriminals **just $540 to execute[5].**

24 hours DDoS Attack

$ 540

The Hidden Cost

From helpdesk meltdowns to reputational damage, the costs of a cyberattack are far-reaching...

The hidden cost of a 12 hour outage...

39 engineers working to mitigate the damage

30 minute status updates, impacting resources across the business

$42 K / hour website down

$44 K x 12 centers contact center chaos

$616 K lost productivity[6]

DDoS attacks come in many shapes and sizes and are almost impossible to prevent on your own.

Learn more about protecting your organization from DDoS attacks here:

imperva.com

[1] Imperva, *Global DDoS Threat Landscape Report 2020*
[2] Imperva, *DDoS Attacks during Covid-19*
[3] *ITIC Global Server Hardware Reliability Survey*
[4] *EMA IT, The Costs of IT Downtime*
[5] Imperva, *DDoS Attacks: How Imperva Mitigates Increasingly Powerful and Sophisticated Attacks*
[6] *Real stats from Imperva analysis of an attack on a multinational entertainment company*