DDos

Methods & Mitigations

HADESS

Forward

Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

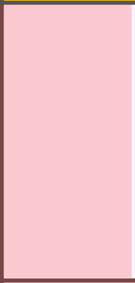
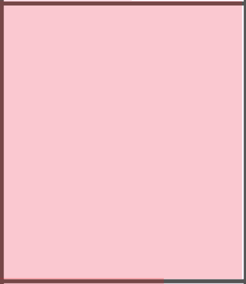
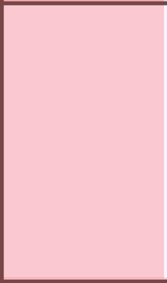
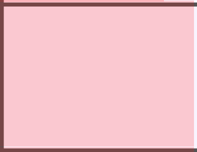
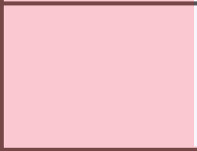
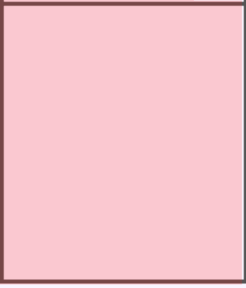
In June 2022 Cloudflare reported detecting and mitigating a 26 million RPS DDoS attack on an unnamed client's website.

This report was made by the Hadess About Trend Methods for DDos and data comes from various sources such as: Cloud Provider, Dark Web , Deep Web Forums, Sellers and etc.

Table of Contents

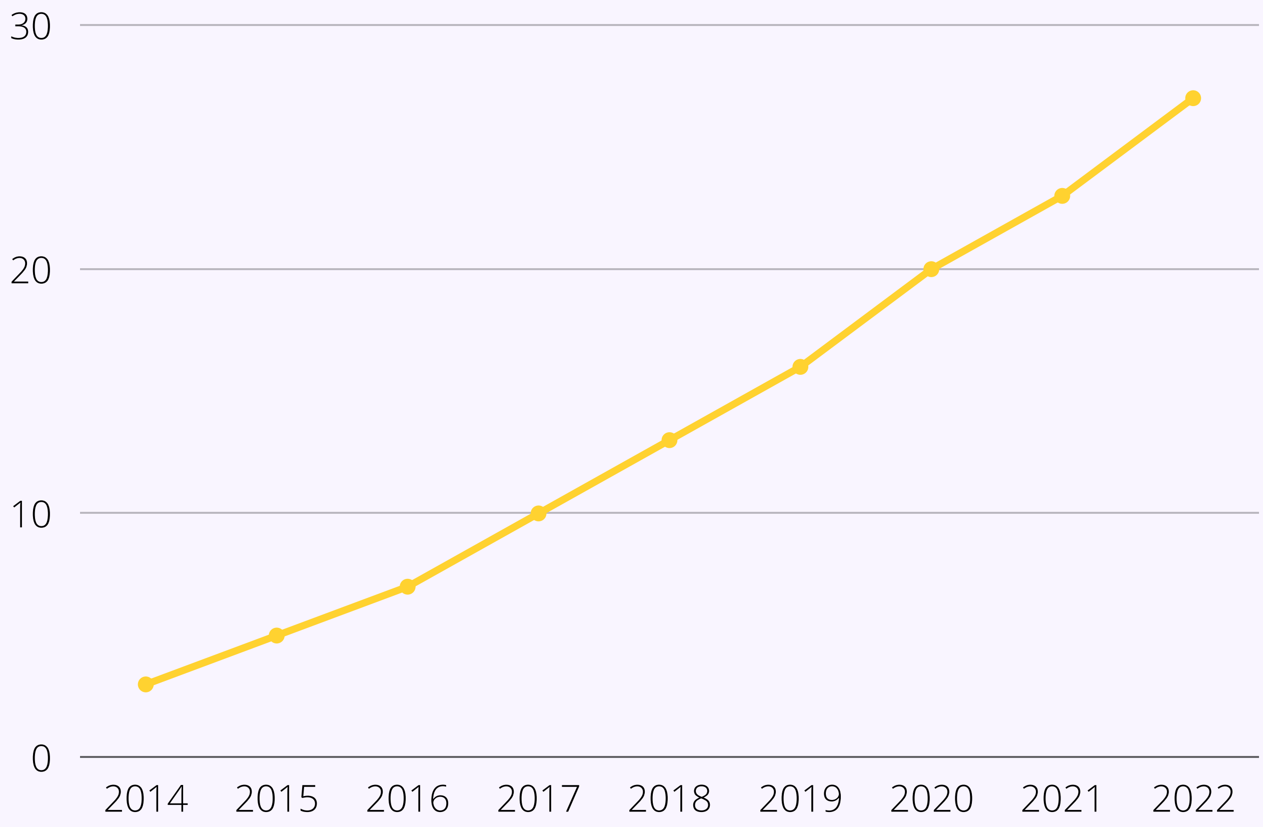
DDos Methods & Mitigations

🟪 Saddam
🟣 Ziyaettin
🟦 Cryptostresser
🟨 KARMA
🟩 MHDDoS
🟢 Fuxi Botnet
🩷 Hirestresser
🟧 DDOS-RootSec
🟥 Slowloris
⬛ R.U.D.Y.

Method Name	Summary	Mitigation Rate	Mitigation
🟨🟩🟢🟦🟣🩷 HTTP floods	exploits HTTP GET or POST		keeping track abnormal activity and employing progressive security challenges
🟥⬛🟧 Low and Slow	opening multiple connections and keeping them open as long as possible		Enable reverse proxy technology, used for inspection of all incoming requests
🟢🟣🟪 DNS Amplification	exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads		Blocking specific DNS servers or all open recursive relay servers, and rate limiting
🟨🟩🟣 UDP flood	overwhelms random ports with udp datagram		Limiting the rate of ICMP responses
🟨🟩🟣 SYN flood	exploits part of the normal TCP three-way handshake		Using cryptographic hashing
🟢🟣🟪 NTP amplification	exploits publically-accessible Network Time Protocol (NTP) servers		Reduce the number of NTP servers that support the monlist command

History of DDos

Check out our timeline to see the progression of the largest and most famous distributed denial of service attacks that have occurred within the past several years (both traffic-based and packet-based attacks)



2022

June — Cloudflare reported detecting and mitigating a 26 million RPS DDoS attack on an unnamed client's website.

April — Cloudflare reported the detection and mitigation of a 15.3 million RPS DDoS attack on a customer operating a crypto launchpad. The attack utilized a botnet consisting of an estimated 6,000 unique devices from 112 countries. Unlike many other DDoS attacks, this one was carried out via HTTPS, which is uncommon because it's more expensive for threat actors to use secure, encrypted connections.

2021

December — Microsoft reported two additional attacks against customers in Asia. The first was a 3.25 Tbps UDP attack that lasted more than 15 minutes; the second was a 2.55 Tbps UDP flood that lasted more than five minutes. While the latter might not sound like a long time, it's five minutes longer of unrelenting attack time than any organization wants to sustain.

November — Microsoft previously reported detecting and mitigating a whopping 3.45 Tbps DDoS attack against an Azure customer in Asia. This security incident had a packet rate of 340 million packets per second.

July — Cloudflare reported a DDoS attack that topped out at 17.2 million traffic requests per second against financial websites.

2020

February — Amazon Web Services (AWS) reported in their TLR for Q1 2020 that they observed and mitigated a 2.3 Tbps UDP reflection vector DDoS attack. Not only is this the largest DDoS attack that AWS reported ever facing, but it was also thought to be the largest DDoS attack in history on record at the time in terms of bit rate.

2019

April — Imperva reports one of their clients was able to thwart a DDoS attack that peaked at 580 million packets per second. To date, this is considered the largest DDoS attack by packet volume to date.

January — Another Imperva client sustained a 500 million packets per second DDoS attack.

2018

March — NETSCOUT reported that its Arbor ATLAS global traffic and DDoS threat detection system confirmed a 1.7 Tbps memcached reflection/amplification attack on an unnamed U.S.-based service provider.

2018

February — The GitHub DDoS attack inundated the company with 1.35 Tbps of data (129.6 million PPS) — the largest DDoS attack on record as of that time — via memcaching. This means that the attackers spoofed GitHub's IP address to send small inquiries to several Memcached servers to trigger a major response in the form of a 50x data response.

2017

October — The Czech statistical office websites relating to the Czech Republic's parliamentary elections — volby.cz and volbyhned.cz — failed temporarily due to DDoS attacks during the vote count.

August — Web host company DreamHost, which was said to host the Nazi-advocate website Daily Stormer under its new name Punished Stormer, suffered a DDoS attack of unannounced proportion. This attack followed a Department of Justice request for visitor data relating to the stormer site.

June — Throughout the second half of the year, video game software developer Square Enix's Final Fantasy XIV online role-playing game (RPG) sustained intermittent DDoS attacks via botnets. The attacks spanned the summer and another set of attacks occurred during the fall.

2016

October — The Dyn DDoS attack, which measured in at 1.2 Tbps and was considered the largest DDoS attack at the time, brought down much of the internet across the U.S. and Europe. Using the Mirai botnet, the attack targeted Dyn, a company that controls much of the domain name system (DNS) infrastructure of the internet.

September — French web host OVH experienced a DDoS attack measuring in at nearly 1 Tbps. The attackers used a botnet of hacked IoT devices (CCTV cameras and personal video recorders) to launch their attack.

2015

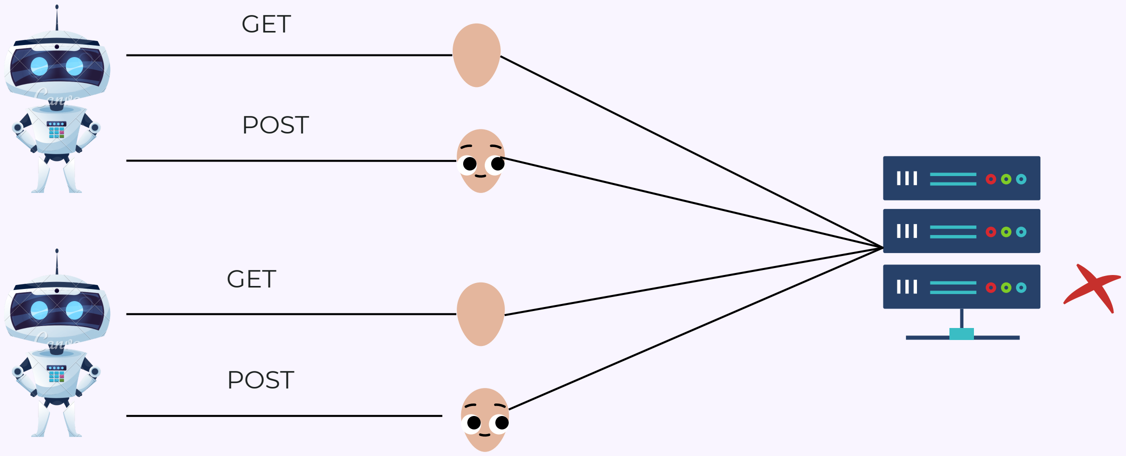
March — GitHub sustained a DDoS attack that was thought to be politically motivated because it focused on two GitHub projects that aimed to provide Chinese citizens with a way to circumvent Chinese state web censorship.

2014

November —The website for Occupy Central in Hong Kong, which was campaigning for a more democratic voting system, experienced a 500 Gbps DDoS attack that was executed via five botnets. Also targeted were the online news site Apple Daily and PopVote, a mock election site, both of which supported OC's message.

Methods

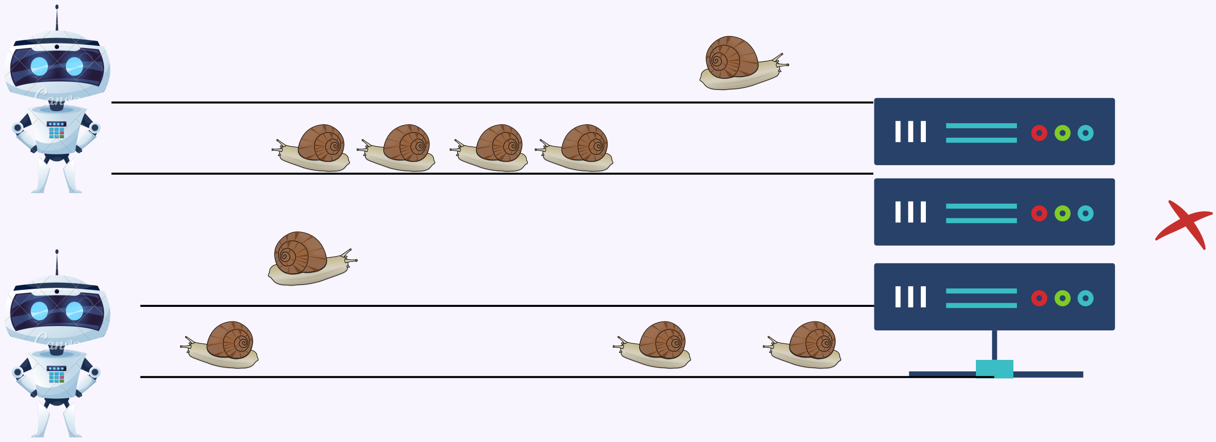
HTTP floods



Attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application.

Mitigation: The most highly-effective mitigation mechanism rely on a combination of traffic profiling methods, including identifying IP reputation, keeping track abnormal activity and employing progressive security challenges (e.g., asking to parse JavaScript).

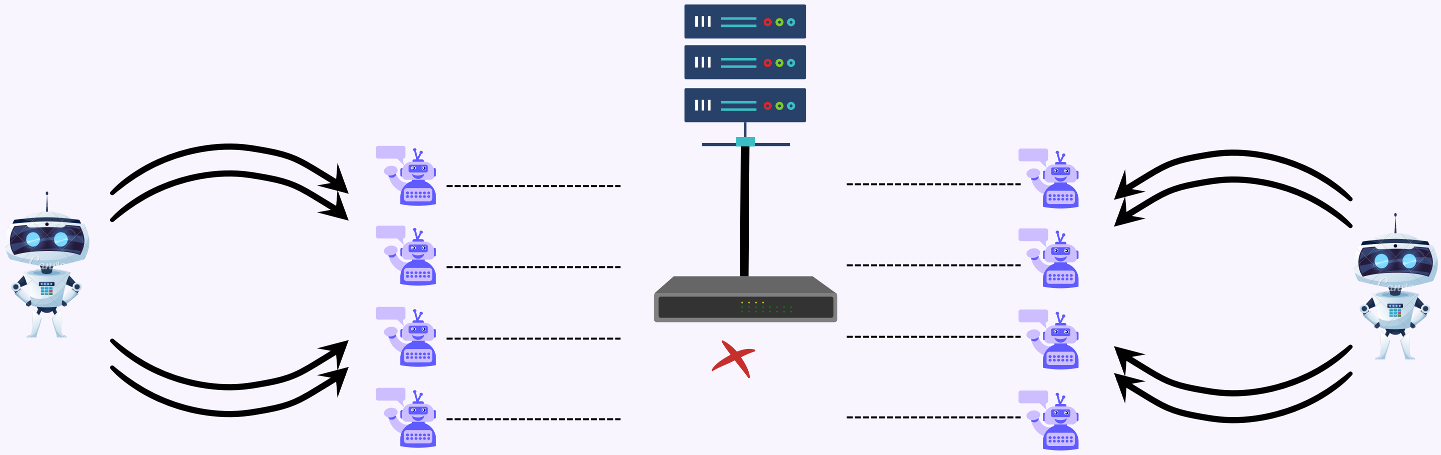
Low and Slow



opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, waiting for each of the attack requests to be completed.

Mitigation: Enable reverse proxy technology, used for inspection of all incoming requests on their way to the clients' servers and do not forward any partial connection requests.

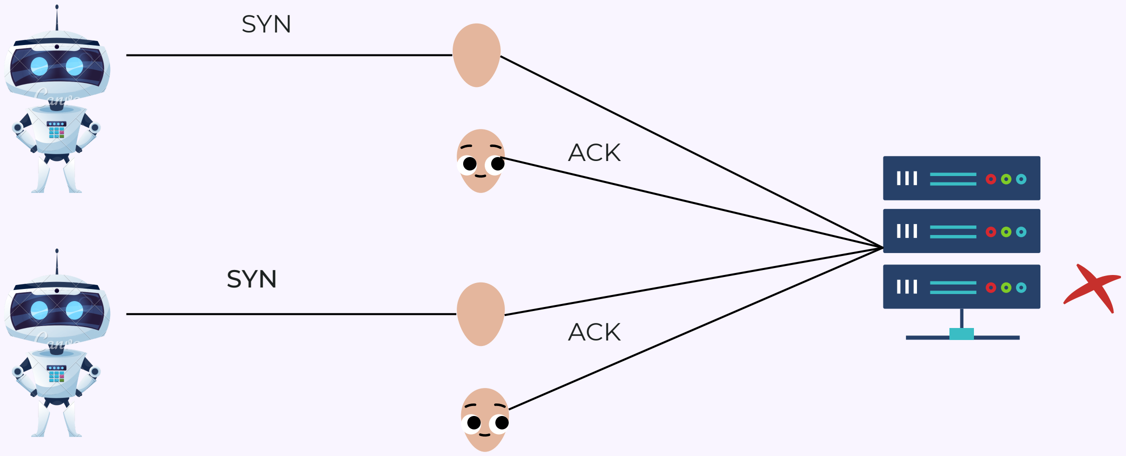
UDP flood



Attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.

Mitigation: Limiting the rate of ICMP responses.

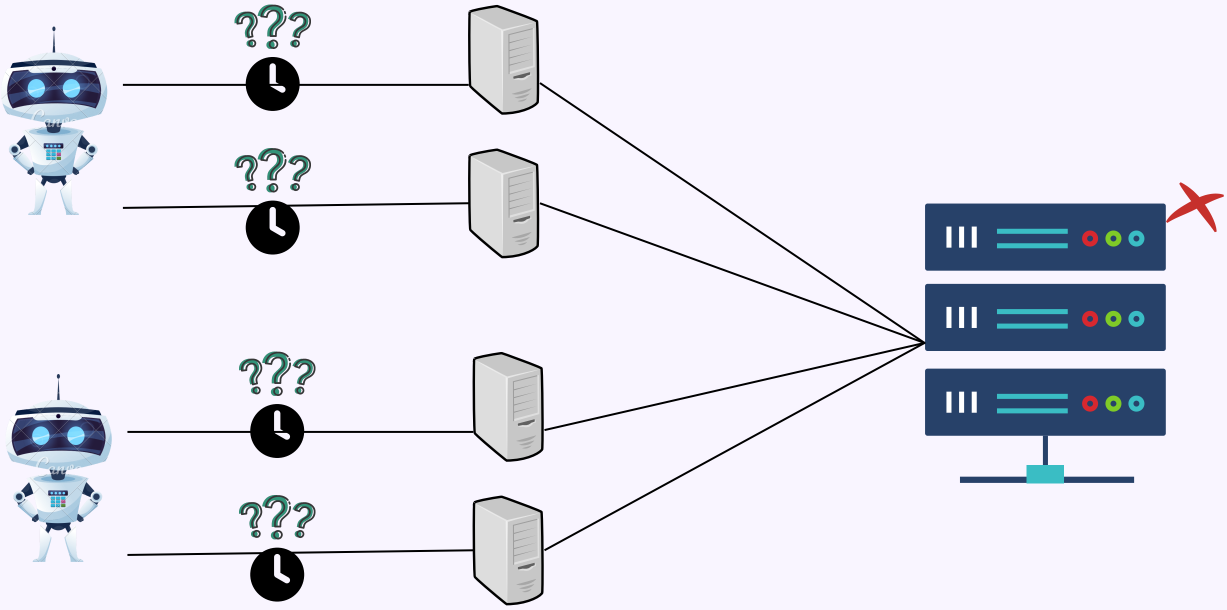
SYN flood



Attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

Mitigation: Using cryptographic hashing, the server sends its SYN-ACK response with a sequence number (seqno) that is constructed from the client IP address, port number, and possibly other unique identifying information. When the client responds, this hash is included in the ACK packet. The server verifies the ACK, and only then allocates memory for the connection.

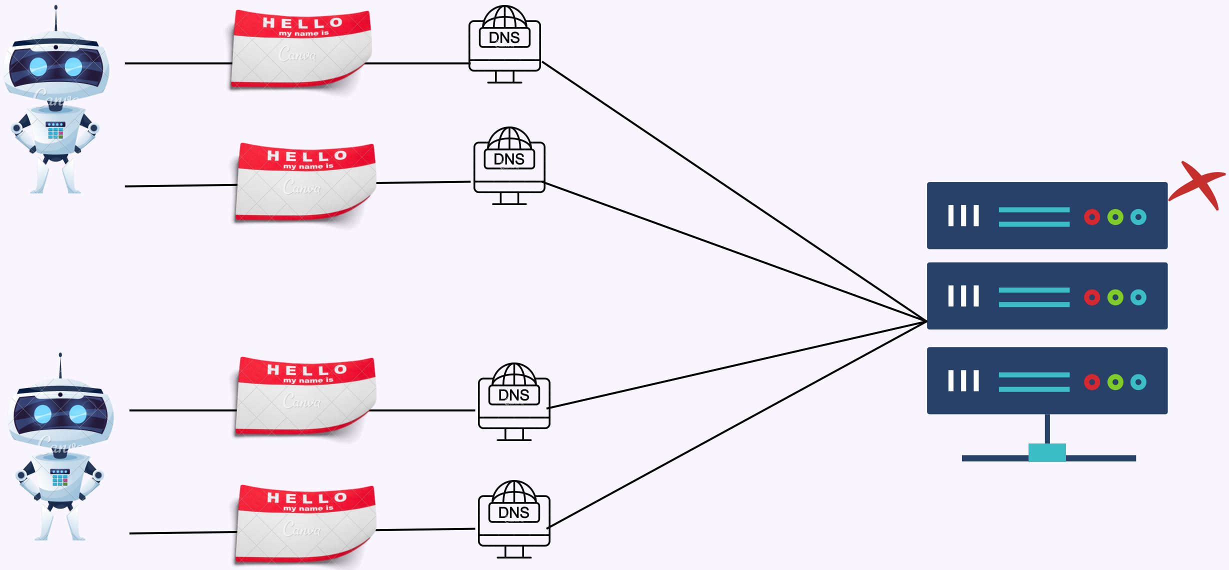
NTP amplification



Attack in which the attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.

Mitigation: Reduce the number of NTP servers that support the monlist command

DNS amplification



Attack in which the attacker exploits vulnerabilities in domain name system (DNS) servers to turn initially small queries into much larger payloads, which are used to bring down the victim’s servers.

Mitigation: Blocking specific DNS servers or all open recursive relay servers, and rate limiting.

Services & Tools

Ziyaettin Botnet Services

Its a botnet with +27K devices all over the world with a power of +300 GB TCP/UDP:

- Big raw Layer 4 service
- TCP/UDP attack support
- Layer 7 service
- Cloudfare bypass 100K + RQS

Cryptostresser

TLS v3 and floods HTTPS requests in a secure tunnel through HTTP proxies
node tls.js GET https://target.com 120 64

KARMA DDoS

DDoS Script (DDoS Panel) with Multiple Bypass (Cloudflare UAM,CAPTCHA,BFM,NOSEC / DDoS Guard / Google Shield / V Shield / Amazon / etc..)

MHDDoS

- Layer 7
  - get GET | GET Flood
  - post POST | POST Flood
  - ovh OVH | Bypass OVH
- Layer 4
  - tcp TCP | TCP Flood Bypass
  - udp UDP | UDP Flood Bypass
  - syn SYN | SYN Flood

Fuxi Botnet

- 700GB UDP Flood
- 400GB TCP/ACk Flood

Hirestresser

We guarantee a minimum of 500k-1m+ pps per concurrent for Layer 4 (the Gbps will depend on the method) and minimum 300Gbps of valid.

- HTTPS-BEAST
- Bypass Security Protection Like:
  - Cloudflare (free-enterprise) Cloudflare Bot-Fight mode, and javascript detection,
  - Cloudflare UAM (js challenge), Cloudflare Captcha (hcaptcha & recaptcha)
  - DDoS-Guard (JS challenge)
  - Sucuri
  - Stormwall(recaptcha v2 & v3)
  - Amazon CDN Cloudfront
  - Imperva Incapsula
  - Akamai
  - Fastly
  - Blazingfast
  - Nooder(recaptcha v3)
  - React.su
  - Qrator
  - Arvan Cloud
  - ...

DDOS-RootSec

DDOS Archive by RootSec (Scanners, BotNets (Mirai and QBot Premium & Normal and more), Exploits, Methods, Sniffers)

Saddam

DDoS Tool that supports:

- DNS Amplification (Domain Name System)
- NTP Amplification (Network Time Protocol)
- SNMP Amplification (Simple Network Management Protocol)
- SSDP Amplification (Simple Service Discovery Protocol)

Slowloris

Slowloris is a type of denial of service attack tool invented by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

R.U.D.Y.

R.U.D.Y. is a denial-of-service attack tool that aims to keep a web server tied up by submitting form data at an absurdly slow pace. A R.U.D.Y. exploit is categorized as a low-and-slow attack, since it focuses on creating a few drawn-out requests rather than overwhelming a server with a high volume of quick requests. A successful R.U.D.Y. attack will result in the victim’s web server becoming unavailable to legitimate traffic.

Resources

- https://www.imperva.com/
- https://www.thesslstore.com/
- https://www.artstation.com/latkowski

About **Hadess**

Savior of your Business to combat cyber threats
Hadess performs offensive cybersecurity services through infrastructures and software that include vulnerability analysis, scenario attack planning, and implementation of custom integrated preventive projects. We organized our activities around the prevention of corporate, industrial, and laboratory cyber threats.

Contact Us

To request additional information about Hadess's services, please fill out the form below. A Hadess representative will contact you shortly.

Website:

www.hadess.io

Email:

Marketing@hadess.io

Phone No.

+989362181112

Company No.

+982177873383

hadess_security

Hadess

Products and Services

→ **RASP | Protect Applications and APIs Anywhere**

Identifying and helping to address hidden weaknesses in your organization's security

→ **Penetration Testing | PROTECTION PRO**

Fully assess your organization's threat detection and response capabilities with a simulated cyber-attack.

→ **Red Teaming Operation | PROTECTION PRO**

Fully assess your organization's threat detection and response capabilities with a simulated cyber-attack.

→ **Blockchain Security | Smart Audit and Protection**

Identifying and helping to address hidden weaknesses in your organization's security

HADESS

www.hadess.io