Denial-of-services (DDoS) attack

Best practices & countermeasures

nexo

Milan Velev
Chief Information Security Officer, Nexo

- 10 years of experience in information security
- Lecturer in Penetration testing and information security
- Avid crypto and blockchain enthusiast

Nexo in the past four years

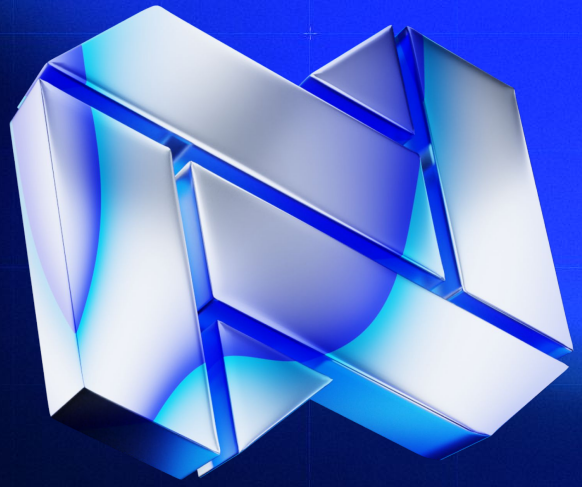
$130B+
Processed

5M+
Nexo users worldwide

600+
Top professionals

Licensed & Regulated
Digital Assets Institution

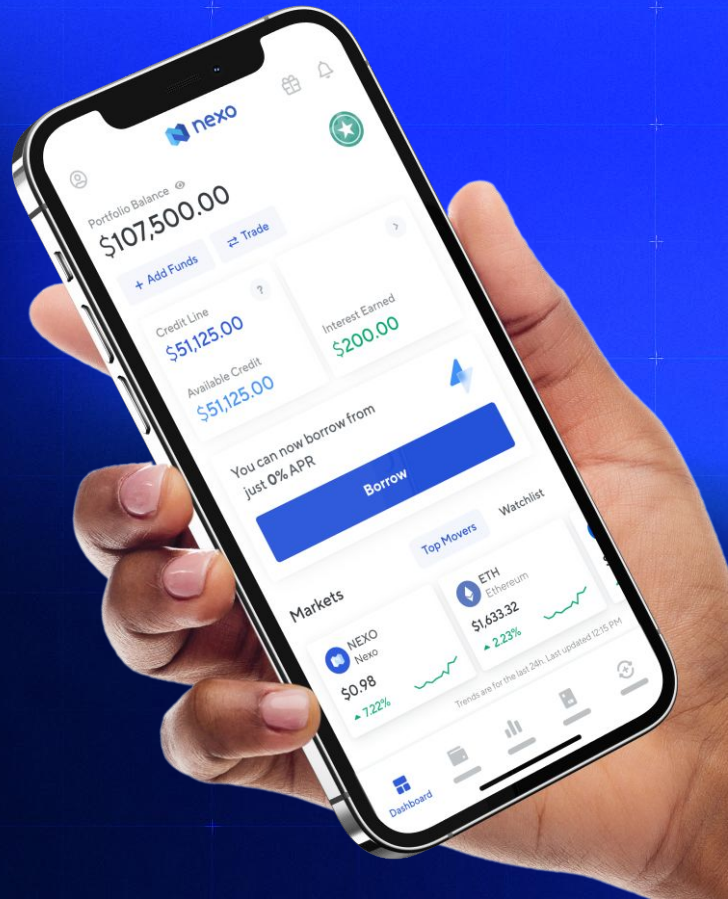
How we did it?



Products, created in Bulgaria, for the whole world

nexo

- Buy Crypto
- Earn Interest
- Exchange Crypto
- Borrow Funds
- Nexo Card
- Nexo Pro



Products, created in Bulgaria, for the whole world

nexo

2018

- The Nexo Platform

2019

- The Nexo App

2020

- Earn on Crypto
- $4B+ Assets Under Management

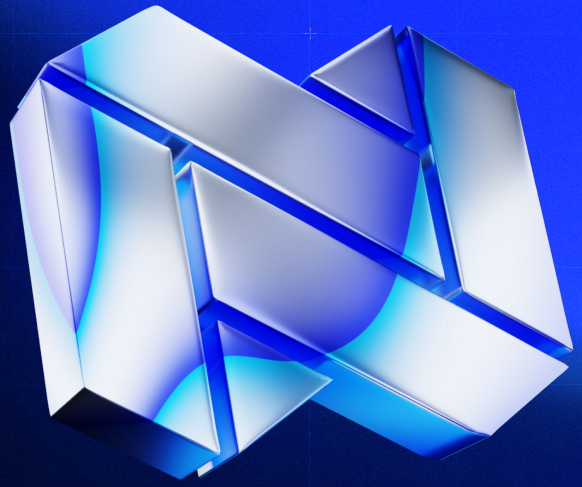
2021

- Nexo Exchange
- Nexo Pioneering a Real-Time Audit
- Nexo Booster

2022

- Nexo Ventures
- Nexo Prime
- The Nexo Card
- Nexo Pro

DDoS Attack



What is it?

- **Denial of Service (DoS)** is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.
- In a DoS attack, attackers flood the victim system with non-legitimate service requests or traffic to overload its resources.
- **Distributed denial of service (DDoS)** is a coordinated attack that involves a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system.

Types of DDoS Attack

F5 DDoS category	ATT&CK technique	Purpose of attack	ATT&CK sub-technique	Examples
Volumetric	Network Denial of Service T1498	Consume network bandwidth	Direct Network Flood T1498.001	TCP flood UDP flood ICMP flood
			Reflection Amplification T1498.002	DNS reflection NTP reflection memcache reflection
Protocol	Endpoint Denial of Service T1499	Overwhelm network device	OS Exhaustion Flood T1499.001	SYN floods ACK floods
Application	Endpoint Denial of Service T1499	Consume application resources	Service Exhaustion Flood T1499.002	HTTP flood Slowloris TLS renegotiation
			Application Exhaustion Flood T1499.003	Heavy URL Intensive SQL queries
			Application or System Exploitation T1499.004	Exploit a vulnerability to crash a system or service

Table 1. Mapping DDoS terminology to MITRE ATT&CK techniques.

*Source: www.f5.com

Major DDoS attacks

- **September 2017** – Largest disclosed attack - 2.54 Tbps against Google Cloud
- **February 2018** – 1.3 Tbps against Github
- **February 2020** – 2.3 Tbps against undisclosed AWS customer
- **April 2007** – Attack against Estonian government services, financial institutions, and media outlets

Actors & Consequences

- Botnets
  - Example: OVH Attack in 2016

- **Consequences:**
  - Financial Loss
  - Reputational Damage
  - Productivity Loss

Attack in motion

```
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            250
URL:                              http://10.0.2.4/dvwa/login.php
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          68
interval between follow up data:  10 seconds
connections per seconds:          50
probe connection timeout:         5 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Tue Nov 15 01:02:25 2022:
slow HTTP test status on 60th second:

initializing:         0
pending:              0
connected:            250
error:                0
closed:               0
service available:    NO
```

Trends in DDoS attacks 2022

- **Ransom DDoS**

- **Network Layer DDoS**: In Q2, the total amount of network-layer DDoS attacks increased by 109% YoY and 15% QoQ.

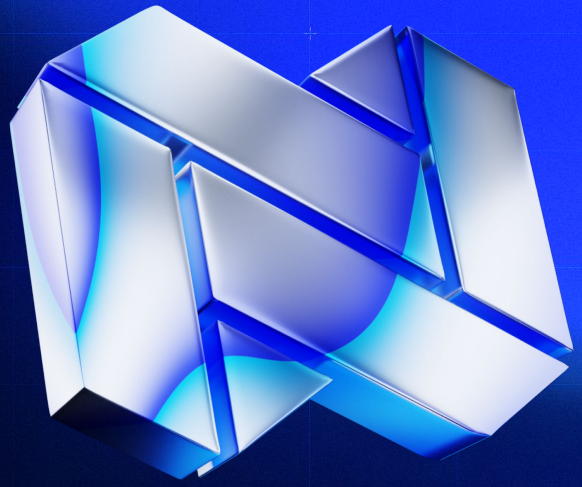
  Most targeted industries: Telecommunications and Gaming. 53% of all network-layer attacks were SYN floods.

- **Application Layer DDoS:** In Q2, the volume of application-layer DDoS attacks increased by 72% YoY, but decreased 5% QoQ.

  Most targeted industries: Aviation and Aerospace, Internet industry, Banking, Financial Institutions and Insurance (BFSI) industry, and Gaming / Gambling industry.

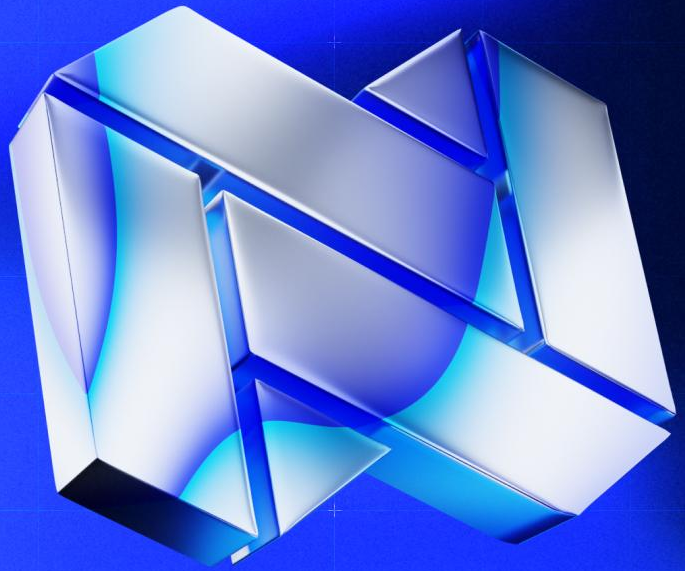
*Source: www.cloudflare.com

Protection & Best practices



Countermeasures

- Layered Defense
- Reducing Attack Surface
- Traffic Inspection
- DDOS Simulations



nexo