EDGE CENTER

# Modern Challenges and Defense: DDoS Attacks, Bots, and Hacktivists in the Context of Top-Level National Domain Registrars


## Artem Izbaenkov

Director of Cybersecurity Development

Board Member of ACISO

Member of ISDEF

# DDoS-attack

During a DDoS attack, infected hosts (bots) from various networks overload the server, channel, or application resources with illegitimate traffic, thereby preventing legitimate users from accessing the information.

# How do DDoS attacks affect national domain registrars?

Both volumetric attacks and application-level attacks can lead to service disruption at national domain registrars, thereby blocking access to numerous resources.

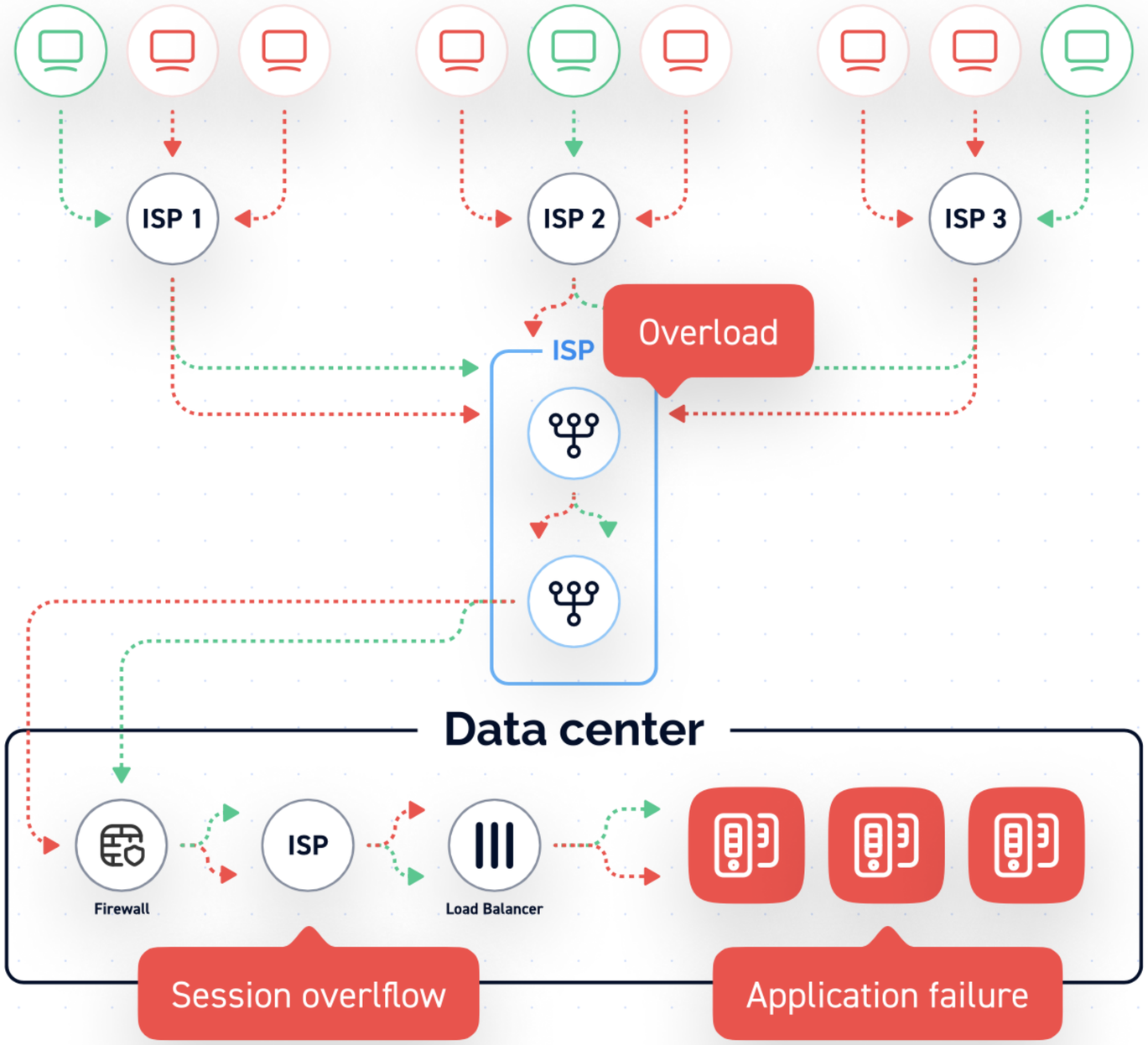
- Inaccessibility of client resources
- Inaccessibility of the call center
- Significant losses due to SLA violations
- Inaccessibility of all services

# The complexity of modern

# DDoS attacks

**Today, DDoS attacks can be divided i three types:**

1. Channel congestion
2. Session table overflows
3. Service (application) failure



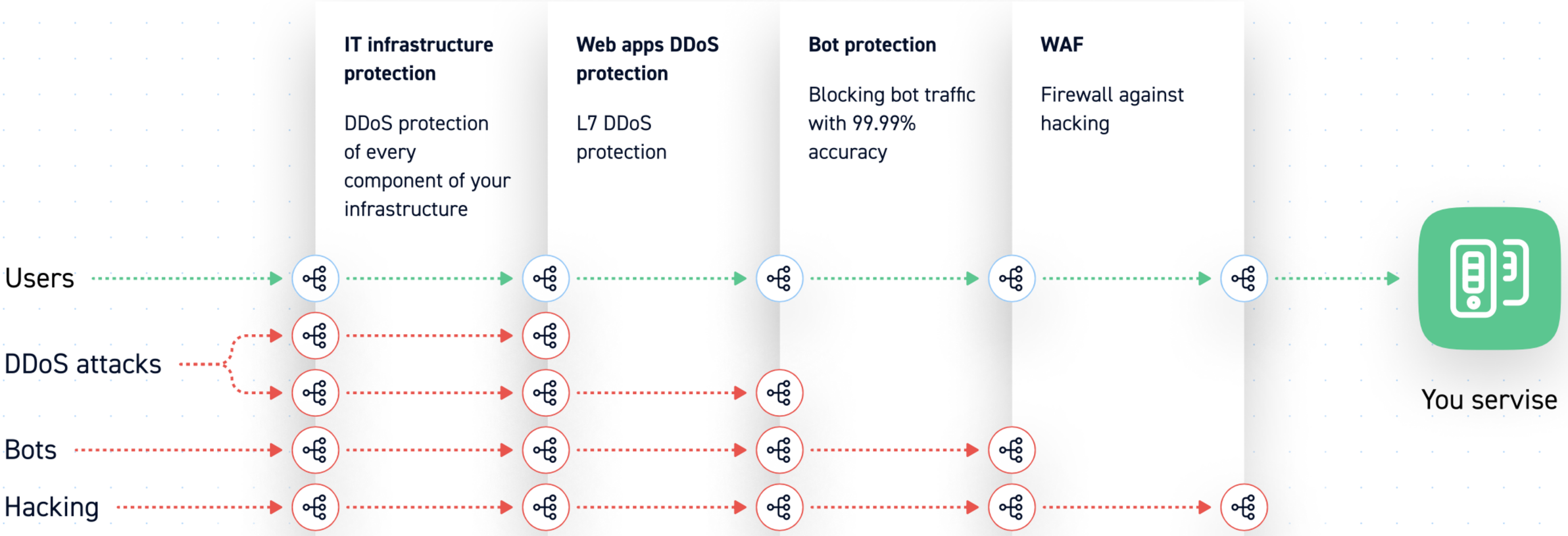
# The First World Cyber War

- National domain registrars
- Banks
- Hosting companies
- Cargo carriers
- Payment systems
- Information portals
- E-commerce platforms
- Government structures
- Metallurgy
- Large-scale E-commerce
- Telecommunications
- Electric power industry
- Mechanical engineering
- Oil and gas industry
- Airlines

# DDoS Attack Trends in 2023

- L7 (Application) layer attacks on web infrastructure
- Targeted attacks on company DNS servers
- Botnet attack volumes on Russia easily crossed the 1.2 Tbps and 500 Mpps threshold
- Increase in attack power and duration exceeding 1 Tbps and 10 days
- A significant portion of bots originate from Russia
- Utilization of cloud data centers for organizing and monetizing DDoS attacks
- Attacks on APIs

# We offer comprehensive protection



# Interesting cases

# Government Data Center

## Problem

Following the events of February 24th, the Data Center's cybersecurity team changed providers and implemented secure solutions. However, during the setup of secure channels, vulnerabilities remained that could allow malicious actors to launch a small DDoS attack and disrupt the entire region's infrastructure.

## Solution

Stress testing was conducted, and a vulnerability report was provided. A collaborative solution was developed based on two independent operators with DDoS attack protection. There are plans to deploy cleansers directly within the region.

# National Domain Registrar

## Problem

At a certain point, the national domain registrar faced a large-scale DDoS attack that severely impacted its operations. The attack was persistent and employed various methods to overload the registrar's infrastructure. This multi-vector DDoS attack consisted not only of L7 application layer attacks and significant distributed amplification but also included a pronounced attack on the root DNS servers using pre-prepared valid packets. This led to a significant unavailability of their systems and services, resulting in damage to clients and a disruption of the integrity of top-level national domains.

## Solution

1. Monitoring and Detection: The registrar promptly activated EdgeCenter DDoS monitoring and detection systems to identify anomalous activity in the network. This allowed them to quickly detect the attack and begin analyzing its characteristics.

2. Traffic Filtering: The registrar decided to implement traffic filtering solutions at the network infrastructure level. They utilized multi-zone protection mechanisms that automatically recognized and blocked malicious traffic, allowing only legitimate traffic to pass through.

3. Increased Bandwidth: To enhance future resilience, the registrar increased the bandwidth of its network by adding additional resources and planning more flexible scaling measures in the event of similar attacks.

4. Crisis Readiness: The registrar developed a crisis response plan, including a dedicated team to respond to DDoS attacks. This enabled them to react quickly and cohesively to the threat.

EDGE CENTER

edgecenter.ru

**8 800 775 08 54**