Q2 2016 attack report

DDOS-GUARD

Jan. — Feb. — Mar. — **April** — **May** — **June** — July — Aug. — Sept. — Oct. — Nov. — Dec.

12 583
OVERALL NUMBER OF ATTACKS

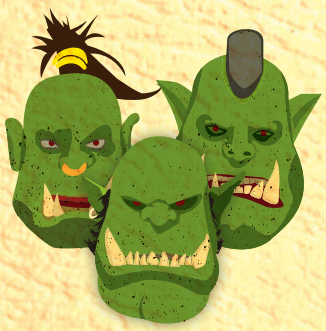
138 ATTACKS PER DAY (average)

5.7 ATTACKS PER HOUR (average)

The average power of attacks, however, has increased by 10%, reaching 1.15 Gbps. This proves the fact that hackers are expanding their opportunities

LARGEST ATTACK
217.7 Gbps

This attack was by 20% larger than the most powerful one detected during Q1 2016



LARGEST HIGH-PACKET-RATE ATTACK
145.3 Mpps

As for the packet attacks, the record of Q1 2016 — 259 Mpps — has not been beaten.

However the average attack power has been increased in 12 times as compared to the previous quarter, reaching 450 603 packets per second.

For the comparison, the average annual attack power of 2015 was tens of times less

ATTACK STATISTICS BY PROTOCOL

UDP

peaking at 217.7 Gbps

2 567 (20.4%) | ↑71% increase in power compared with Q1 2016

TCP

peaking at 119.8 Gbps

3 898 (30.9%) | ↑49% increase in power compared with Q1 2016

Others

peaking at 1.49 Gbps

6 118 (48.2%) | ↓3.8 times decrease in power compared with Q1

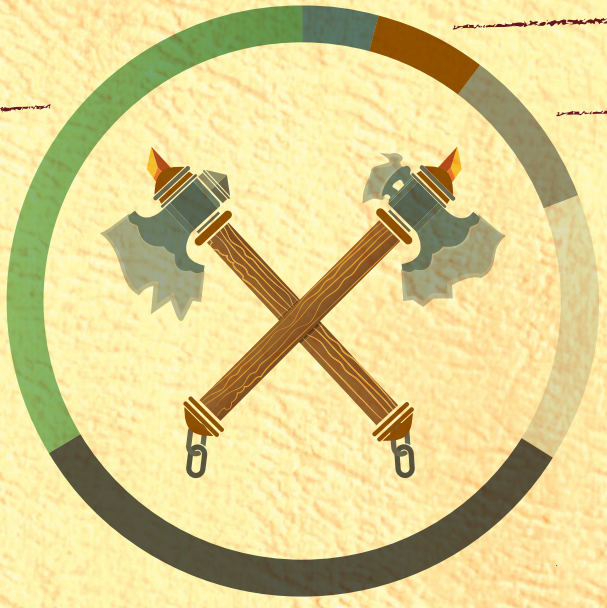
3 **SIGNIFICANT ATTACKS**
surpassing 100 Gbps
or 15 Mpps

1 **EXTREME ATTACK**
surpassing 200 Gbps
or 30 Mpps

For the first time our system has faced a type of attack,
where accounts and computing power of a social network were used.

In this quarter the cybercriminals have taken advantage of another DDoS technique, involving Facebook's servers to conduct an attack on ddos-guard.net. Having a large 'zombie army' botnet, the attackers had published a link to DDoS-GUARD's official website on profiles of multiple compromised users. As soon as the link was published, the Facebook bots generated requests to receive the content by the link, attempting to overwhelm all available bandwidth. Nevertheless, this attack didn't pass unnoticed. The engineers blocked the malicious traffic immediately, leaving the criminals no chance for victory.
This kind of attack is possible to be implemented by using standard Facebook API and lots of bot machines. Be advised that in order to conduct the attack, hackers use compromised accounts, which they gained access to by utilizing such fraud techniques as phishing, typosquatting, social engineering, etc. To protect your accounts, use strong passwords and do not autosave them when your browser suggests so. Two-factor authentication improves account's security as well.

«VICTIMS» RANKING BY TYPE
(percentage of attacks against a target)



4.3% Others

6.2% Governmental authorities

8.7% Hosting services

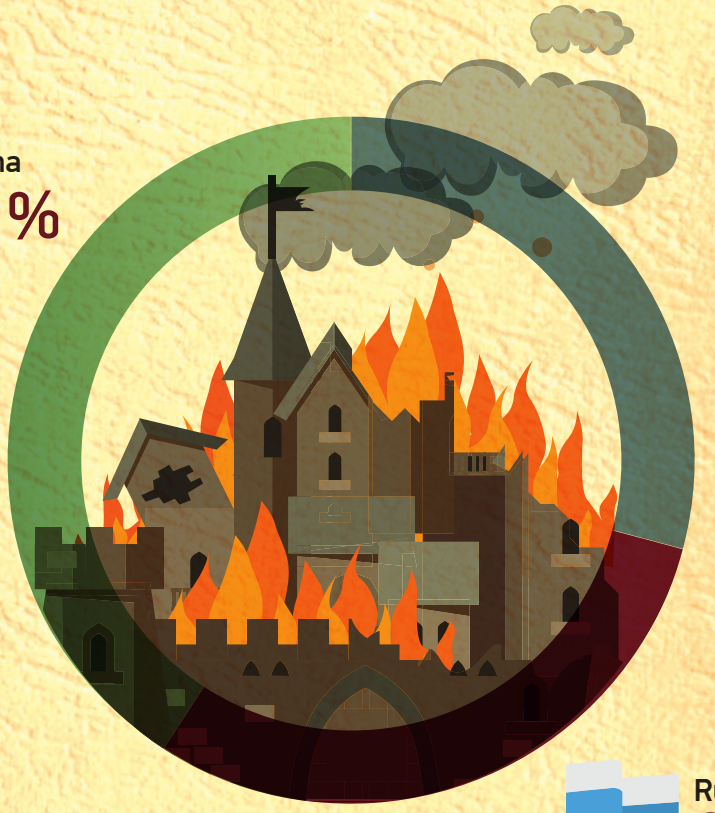
14.9% Multimedia services

33.5% Online stores

32.3% Game servers

A significant increase in attacks on online stores and game servers has been monitored during the 2nd quarter. This can be explained by the fact that in anticipation of summer vacation people spend more time on shopping, which leads to increased competition among the online stores and DDoS attack frequency

TOP TARGETED COUNTRIES*



China
41%

USA
29%

Russia
30%

*among DDoS-GUARD's customers

Compared with the previous quarter, the number of attacks on Russian and Chinese resources has been slightly reduced, but the top three mostly targeted countries have kept their leading positions

The specified percentage ratio of attacks quantity has been calculated on the basis of attacks conducted on the three mentioned above countries only. In total, these countries were the target of 70% DDoS attacks occurred

GENERAL TRENDS

A significant increase in DDoS attack power was observed during the spring period, caused by the 'arms race' between cybercriminals and the DDoS-GUARD team. Along with the attack power growth, a decrease in attack frequency has been noticed, which is due to summer vacation period and a temporary decline in demand for some resources.

UDP-based attacks have become larger, and as compared with TCP, their power increased by 22%. In this quarter cybercriminals gave preference to the flooding attacks combined with non-standard high-packet-rate attacks

PREDICTION

The percentage of UDP flood — one of the simplest kinds of DDoS attacks — is decreasing. This allows us to predict further sophistication of attacks along with combined use of botnets and dedicated servers for generating parasitic traffic.

The «needle» attacks are still popular. These are large but short bursts that occur at regular intervals

ABOUT US

DDoS-GUARD is a licensed communications service provider specialized in DDoS protection services. The statistical information presented in this report is relevant for our customers from all over the world