DDoS VERSUS THE ONLINE GAMBLING INDUSTRY

THE HOUSE DOES NOT ALWAYS WIN

The online gambling industry has grown phenomenally over the last few years, tripling in size in the last decade itself.

A HIGH STAKES GAME

- There was a 350% increase in large-scale volumetric DDoS attacks in the first half of 2014 when compared to the previous year.
- Attacks of 20 Gbps and above now account for more than 1/3rd of all network DDoS events.
- DDoS attacks of over 100 Gbps increased to an overwhelming 100+ events in the first half of 2014 alone.

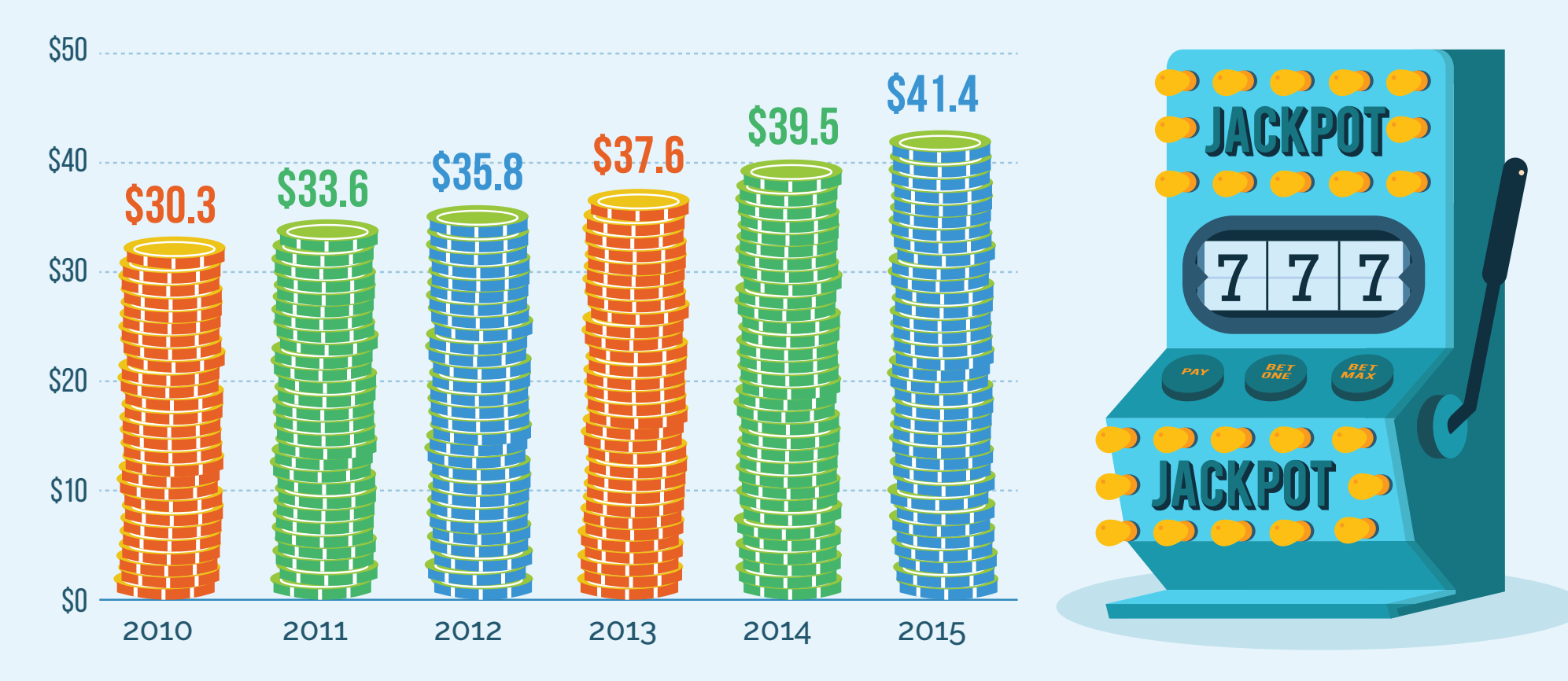
$40/hour VS **$40,000**

The average cost of hiring a Botnet is roughly $40/Hour

Every hour of unmitigated DDoS costs a business an average of $40,000 which is a 1000 times of what it costs a hacker to hire a Botnet.

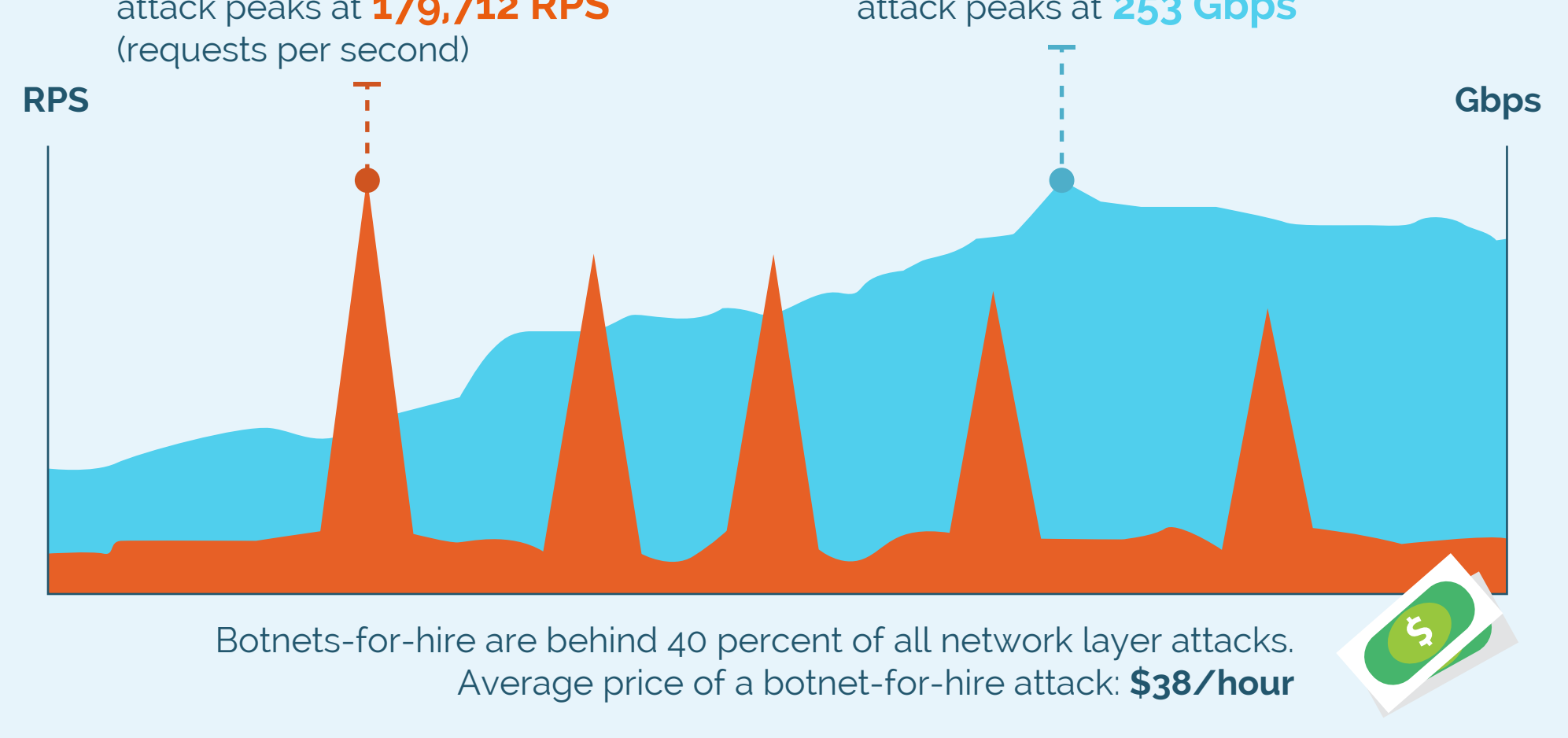
- 9 out of 20 online gambling businesses are attacked.
- 1 out of 2 attacks are launched or funded by rival businesses.
- 1 in 10 online gambling businesses was attacked in the last week.
- 3 out of 4 online gambling businesses are attacked more than once.
- 9 out of 10 online gambling businesses have been attacked in the last 12 months.

ONLINE GAMBLING INDUSTRY GROWTH



Largest **application layer** attack peaks at **179,712 RPS** (requests per second)

Largest **network layer** attack peaks at **253 Gbps**



Botnets-for-hire are behind 40 percent of all network layer attacks.
Average price of a botnet-for-hire attack: **$38/hour**

DDoS ATTACKS

Denial of Service attacks are meant to deny users access to the website, directly costing billions in downtime.

NETWORK (LAYER 3/4) DDOS ATTACKS: The majority of DDoS attacks target the network and transport layers. Such attacks occur when the amount of data packets and other traffic overloads a network or server and consumes all of its available resources.

APPLICATION (LAYER 7) DDOS ATTACKS: Breach or vulnerability in a web application. By exploiting it, the perpetrators overwhelm the server or database powering a web application, bringing it to its knees. Such attacks mimic legitimate user traffic, making them harder to detect.

"HIT AND RUN" ATTACKS ARE EVER PERSISTENT

What Are "Hit and Run" Attacks?

As their name suggests, hit and run attacks consist of short packet bursts at random intervals over a long period of time.

What makes these threats different from other DDoS attacks is that they can last for days or even weeks. Also, unlike other attacks, they are not continuous and are designed to specifically exploit slow-reacting anti-DDoS solutions. Despite the sophistication of other kinds of DDoS threats, hit and run attacks continue to be popular because of their low cost and ease of deployment.

Latest Trends

- Hit and run attacks typically last 20 – 60 minutes in duration.
- After causing some collateral damage to a target server, hit and run attacks usually occur again after another 12 – 48 hours.
- Traditional DDoS prevention solutions, such as GRE tunneling and DNS rerouting, have become ineffective in dealing with these types of attacks.

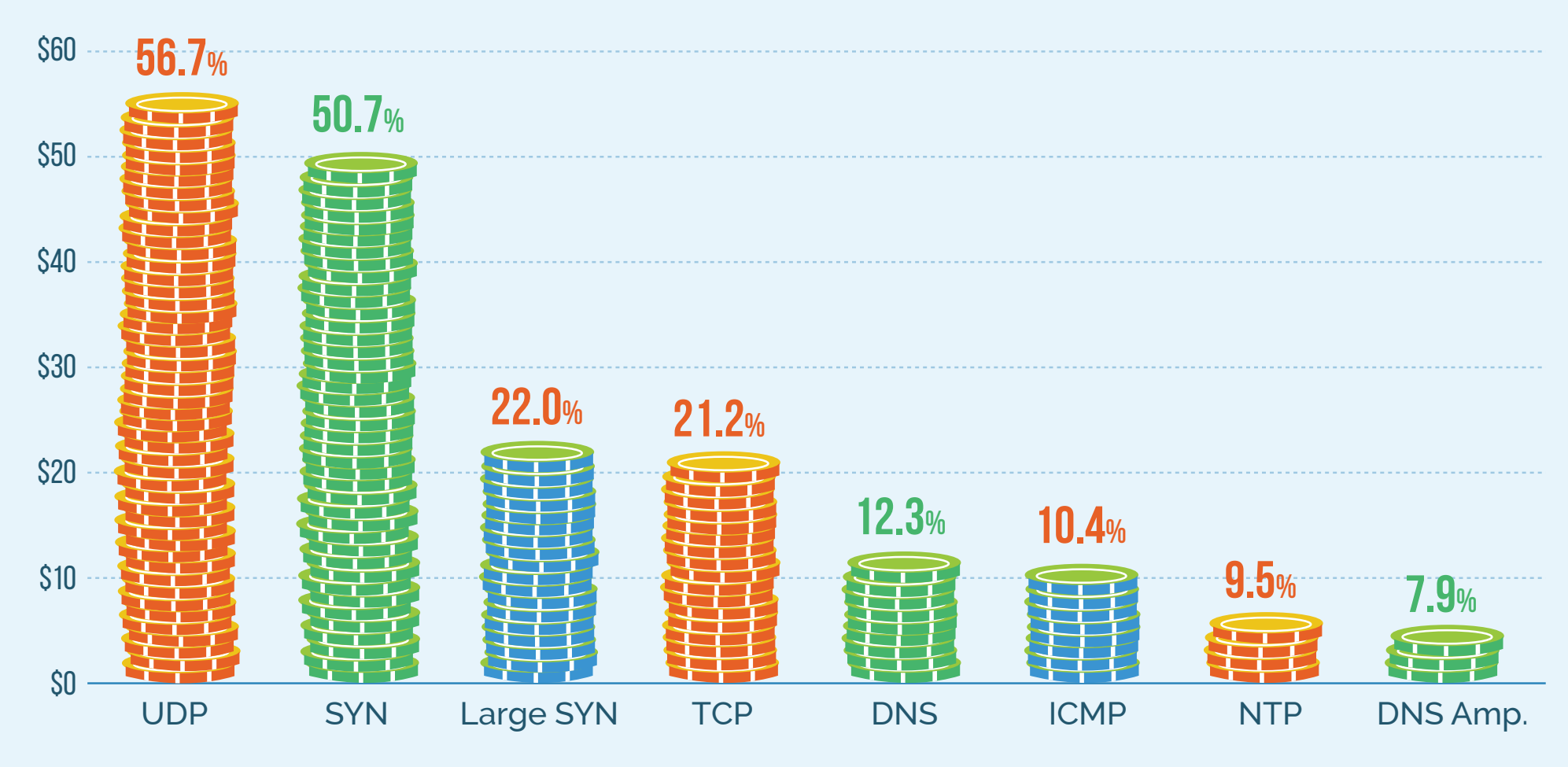
WHAT IS DDoS?

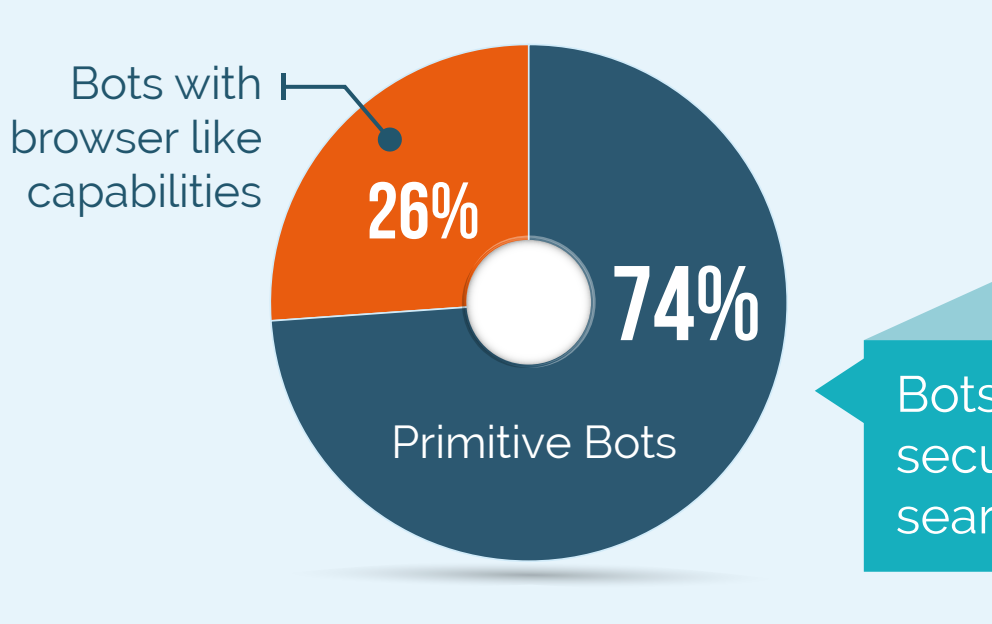
DDoS attack may sound complicated, but it is actually quite easy to understand. A common approach is to "swarm" a target server with thousands of communication requests originating from multiple machines. In this way the server is completely overwhelmed and cannot respond anymore to legitimate user requests. Another approach is to obstruct the network connections between users and the target server, thus blocking all communication between the two—much like clogging a pipe so that no water can flow through. Attacking machines are often geographically-distributed and use many different internet connections, thereby making it very difficult to control the attacks. This can have extremely negative consequences for businesses, especially those that rely heavily on its website

DDoS is a type of cyber attack which can:

- Force users to signup with competitors as an alternative
- Cause users to lose trust in the service
- Culminate in a massive loss of revenue
- Slow down a website's response
- Often time cripple the website to the point of being inaccessible
- Cause the loss of sensitive data in a real time situation like gambling rooms

NETWORK LAYER ATTACK TRENDS





Bots mimic browser capabilities to bypass security and there is also a steep drop in search engine impersonators.

ATTACK FREQUENCY AND DURATION

DDoS attacks have begun to resemble advanced persistent threats with attackers using multiphase, multi-vector assaults which can last for days or even months.

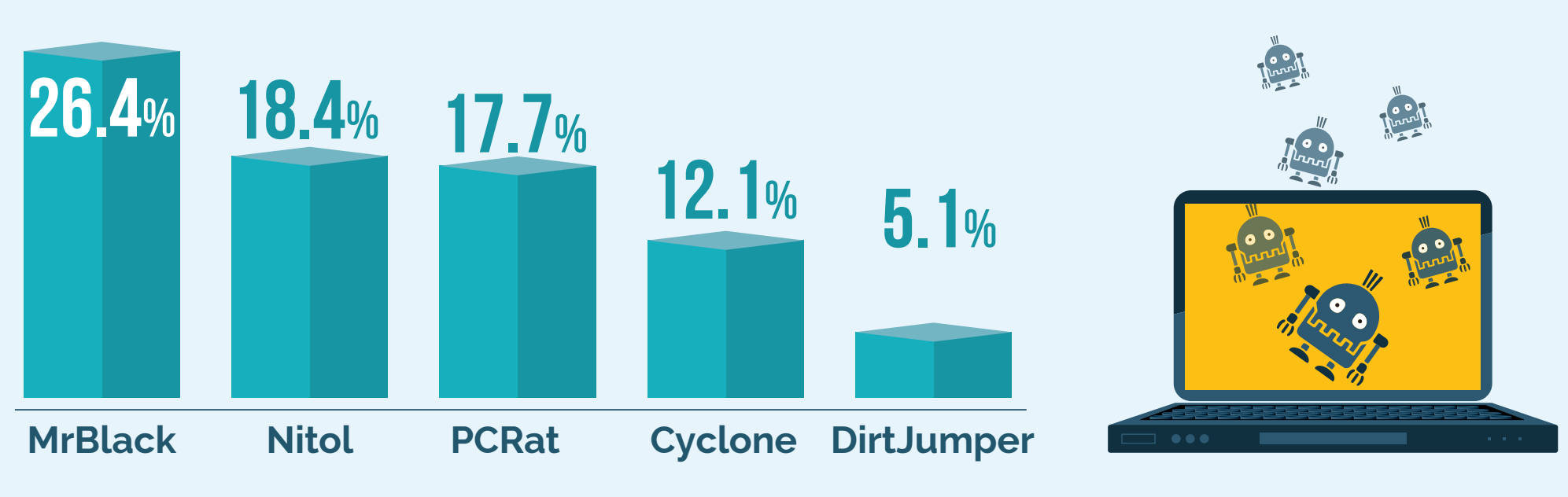
On an average, a target is hit at least once a week.

20% of all network layer DDoS attacks last for over 5 days.

17% of targets are hit more than 5 times.

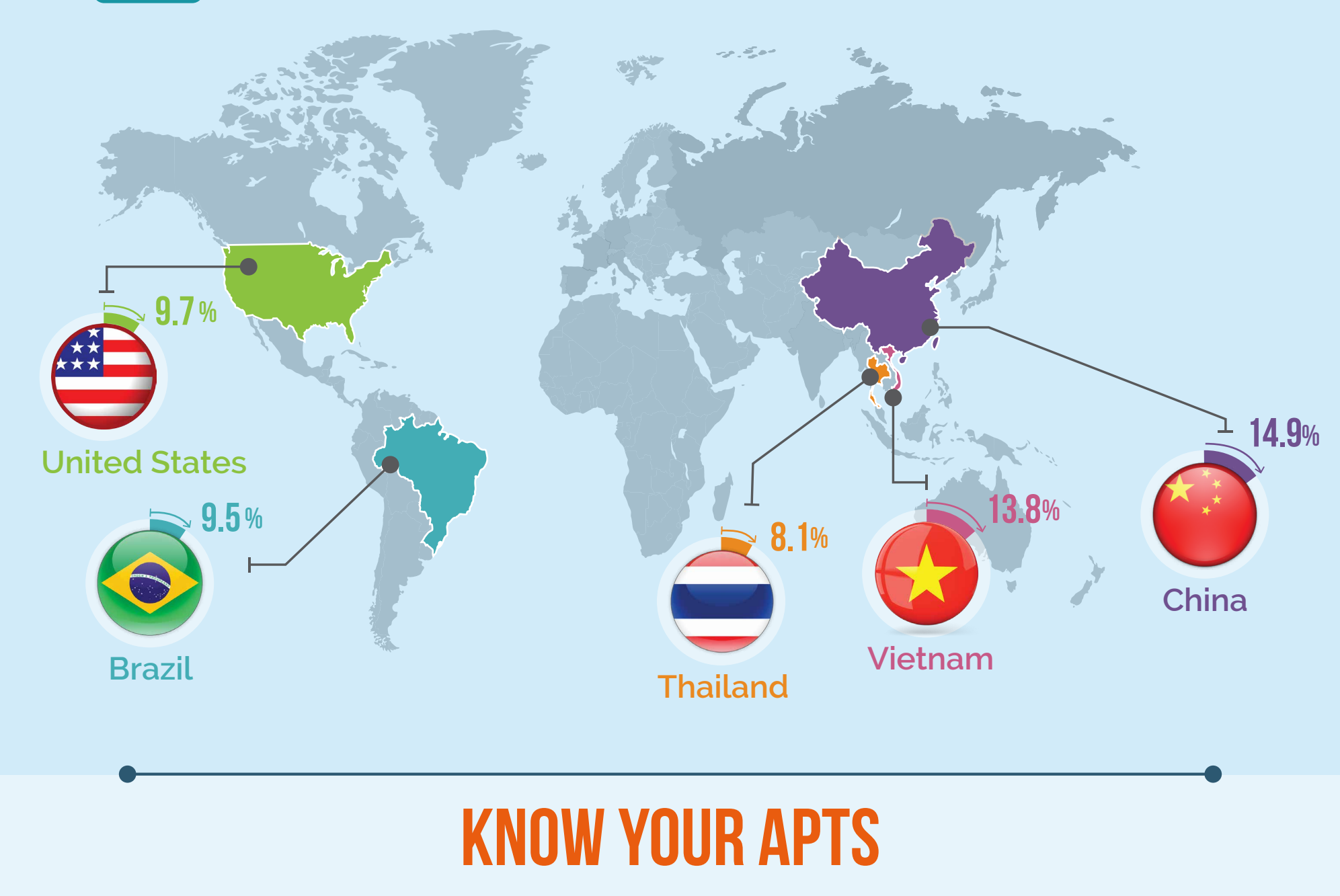
47% of all targets are hit again within 60 days.

DEADLIEST BOTNETS



DDoS ATTACK ORIGIN SUMMARY

Out of the global total of DDoS attacks documented every year, as much as 56% of bot traffic can be traced back to China, United States, Brazil, Thailand and Vietnam.



KNOW YOUR APTS

APTs or advanced persistent threats are what modern DDoS attacks are evolving towards. The level of planning an organization that goes into a DDoS attack is staggering.

TARGETED
Early reconnaissance paired with careful target pre-selection enables attackers to expose weaknesses in the target system.

PERSISTENT
Advanced attacks are asymmetrical in nature and do not follow any set pattern or last for a fixed duration.

ADVANCED
Stealth tactics combined with an extremely well connected network allows attackers to roll in swiftly & securely bypass security countermeasures.

DETAILS OF THE ANALYSIS

Analysis data based on:

- **1572** network layer attacks
- **2714** application layer attacks
- **Time Perid:** March 1st to May 7th, 2015
- **Sample Size:** 60 million DDoS work sessions

RIGGING THE GAME

Service outage during sporting events can cause users to go to competitors' sites to place bets.

Latency means loss
Online gaming, including sports betting and poker, can be crippled by even slight latency.

60% of online gaming is real time in nature

FREQUENCY HIGH AND DURATION LONG

- On average, targets are hit **once a week**
- **20 percent** of all network layer DDoS attacks last **over 5 days**
- 17 percent of targets hit **more than 5 times**
- 47 percent of all targets are **hit again within 60 days**

Every hour of unmitigated DDoS costs a business **$40,000.** Persistent attacks entail losses of hundreds of thousands-if not millions.

Sources:
Global Betting and Gambling Consultancy
The Top 10 DDoS Attack Trends by Incapsula
Incapsula Enterprise for Gold Security