KASPERSKY lab

DENIAL OF SERVICE: HOW BUSINESSES EVALUATE THE THREAT OF DDOS ATTACKS

IT SECURITY RISKS SPECIAL REPORT SERIES

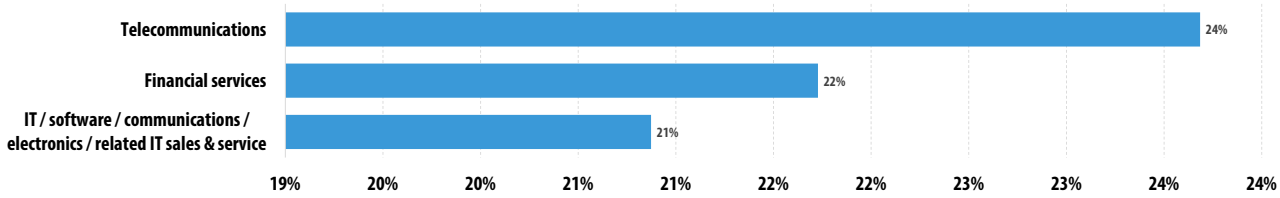
Kaspersky Lab

Corporate IT Security Risks Survey details:

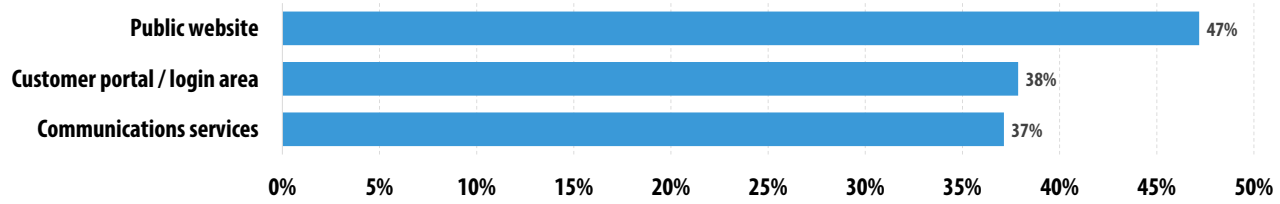
- More than 5500 companies in 26 countries around the world
- Top managers and IT professionals answered a series of questions about security, IT threats and infrastructure
- We asked them how they perceive the threat of potential DDoS attacks and what their typical losses have been from these attacks, in practice

What we have found:

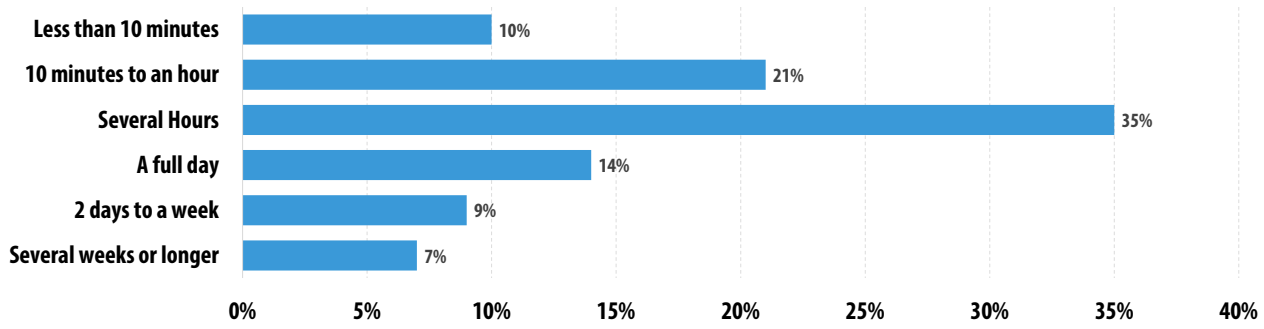
- **20%** of companies with 50 employees or more reported that they have been the victim of at least one DDoS attack
- The top three industries most likely to suffer from a DDoS attack are: telecoms, financial services and IT



- **50%** of DDoS attacks lead to a noticeable disruption of services. 24% of attacks lead to services being completely unavailable
- **74%** of attacks that lead to a noticeable disruption of service coincided with a different type of security incident, such as a malware attack, network intrusion or other type of attack
- **26%** of DDoS attacks lead to the loss of sensitive data
- The top three types of infrastructure targeted are: public websites, the limited access customer portal, general communications infrastructure



- A DDoS attack is most likely to last for several hours. But 7% of businesses reported attacks that latest a week, resulting in a severe impediment of services



- 12% of businesses are confident that a DDoS attack was initiated by their competition
- On average, enterprises lose $417,000 as a result of a denial of service attack and SMBs lose $53,000

DDoS: the menace is growing

In the overall corporate threat landscape DDoS attacks are noticeable, but not dominating. It's neither the top cause for data loss (6% of businesses reported loss of data due to a denial of service incident [1]), nor the most frequent type of an external threat experienced by companies (it's significantly behind malware, phishing attacks and network intrusions). While the share of companies reporting at least one DDoS attack was stable in the last few years (around 20%), the number of businesses naming such attack as their most serious and damaging security incident, has grown – from 4% last year to 6% in 2015.

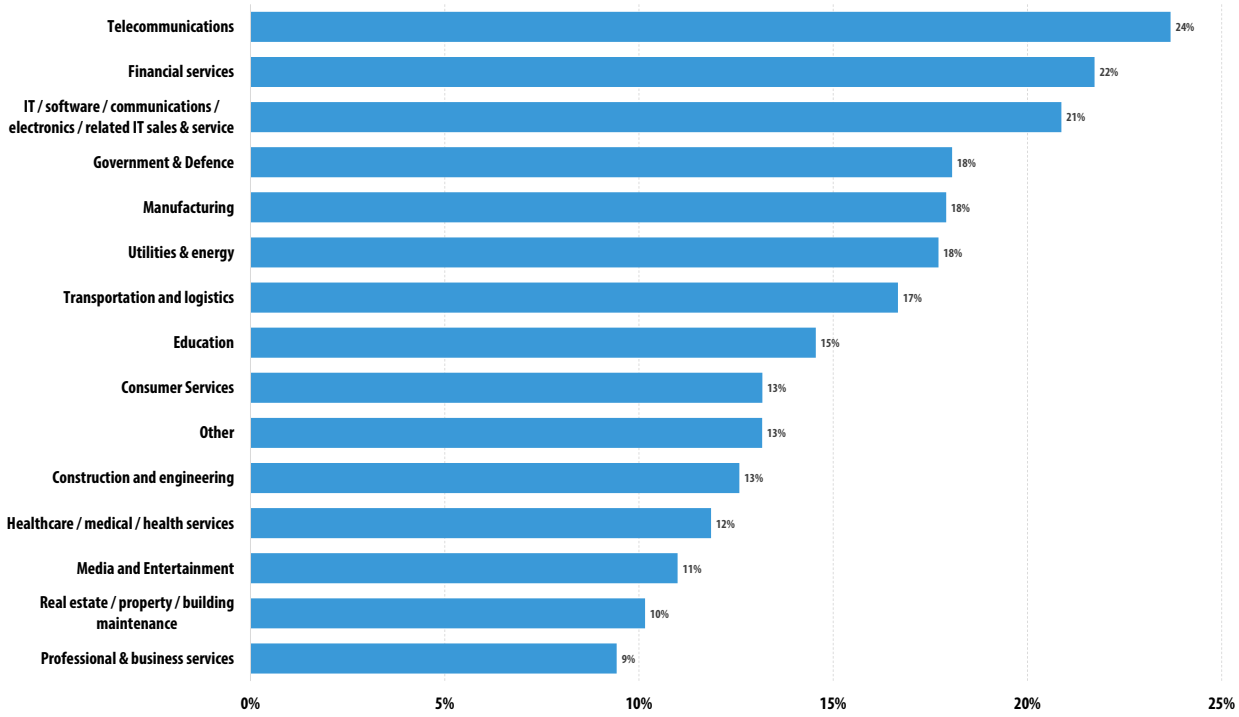
DDoS attacks may cost businesses a lot. More than two thirds of victims of a DDoS attack reported another type of security incident coinciding with an attack. Denial of service is frequently used as a decoy to distract IT staff from an intrusion taking place at the same time. Although the chances of a DDoS attack are stable, combining such an attack with another type of intrusion may increase the collateral damage, on top of already significant losses caused by downtime and reputational damage.

In terms of the real spend required to recover from a DDoS attack, an average figure for large companies (1500+ seats) is US$417,000, including direct and indirect losses. SMBs report an average loss of $53,000. Compared to the average losses connected with other types of security breaches, we clearly see that DDoS attacks damage small and medium companies more than enterprises, most likely due to the limited budget they have available for DDoS prevention services. For large companies DDoS is the 9th most expensive type of a breach, but for SMBs it's the fourth most expensive, and the amount of loss is comparable to such incidents as network intrusion ($56K) and cyber espionage ($69K - the largest average recovery budget for SMBs).

Practice: Who is targeted and how

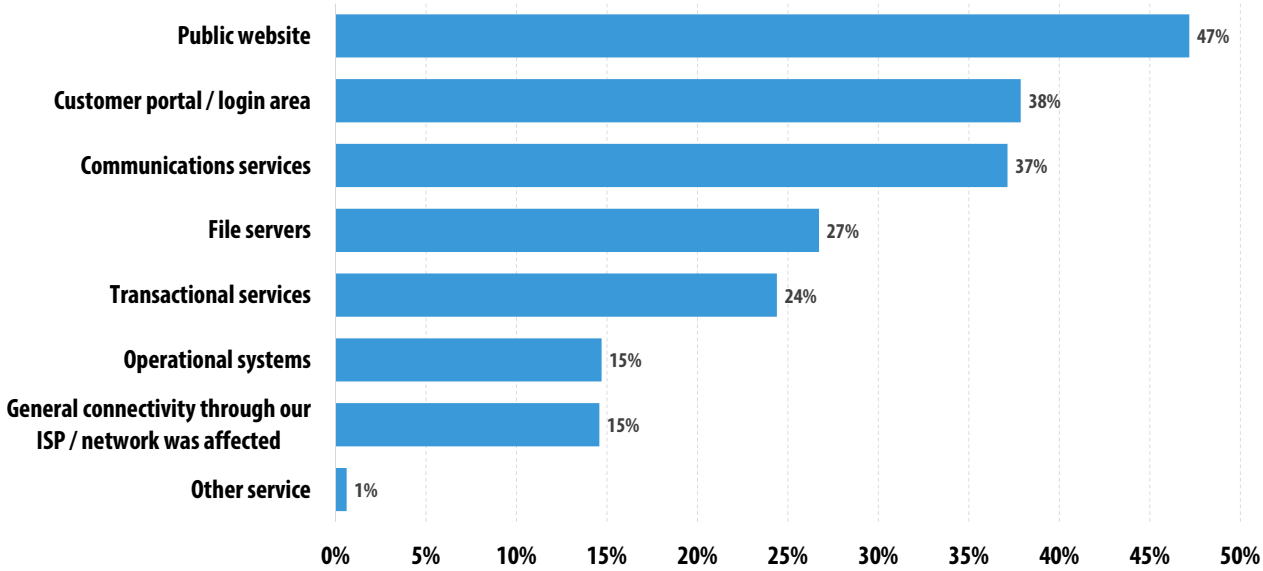
20% of companies with 50 or more employees admitted to at least one DoS or DDoS attack. This proportion varies from industry to industry, and those with the highest chances of being hit with such an attack are telecommunications companies (24%) and financial services organizations (22%). At the lower end of the scale, 11% of media and entertainment companies, 10% of real estate businesses and 9% of professional services have suffered from an attack.

1 Figures in this section are taken from Kaspersky Lab's "Damage Control: The Cost of Security Breaches" report, also based on Global It Security Risks Survey. More details here.

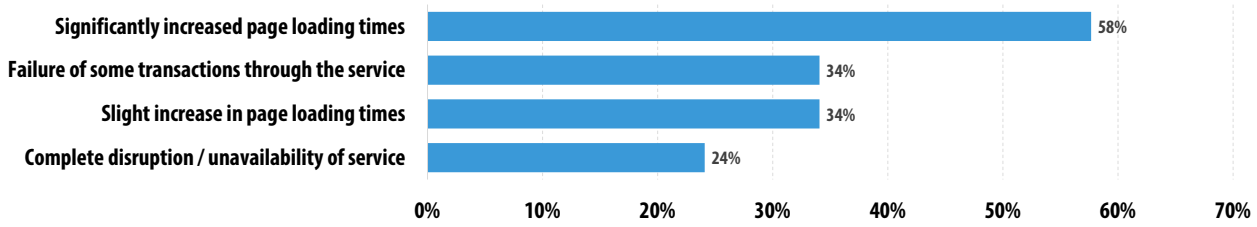


Share of companies affected by a DDoS attack, by industry/type

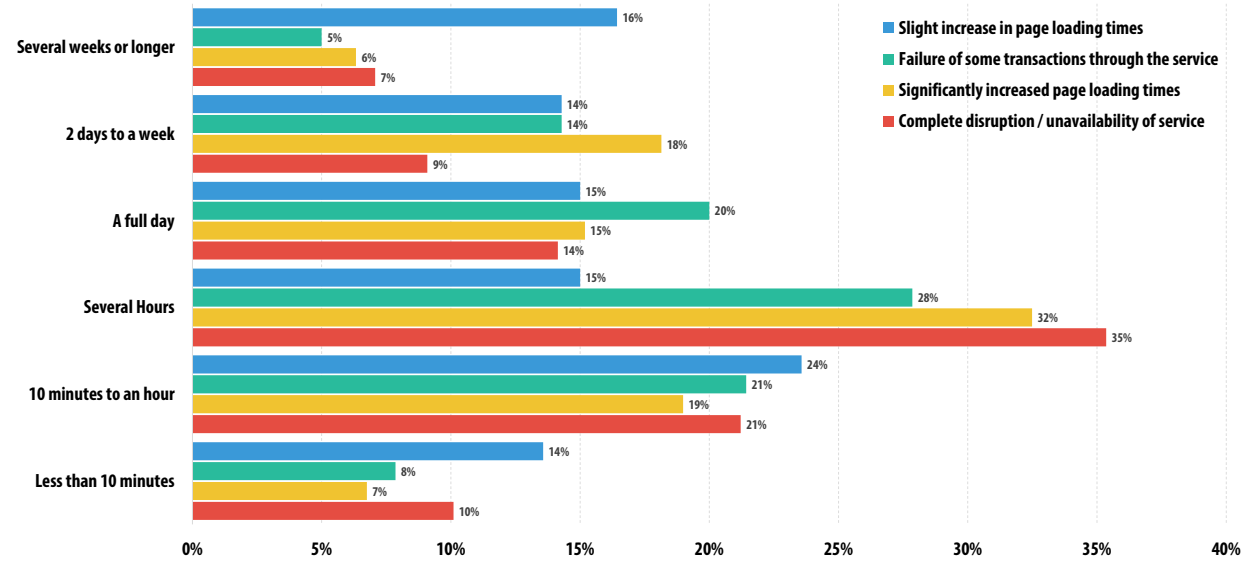
The survey shows that the most commonly affected service is a business's public website, with almost half of surveyed businesses (47%) citing their website's inability to function during a DDoS attack. At 38%, the customer portal or login area was the second most affected area, while issues with communications services (37%) were the third most affected service.



The most common form of disruption for a business was increased page loading times. 34% reported a partial failure of transactions that depended on an affected service. 24% of DDoS attacks lead to the complete unavailability of services.

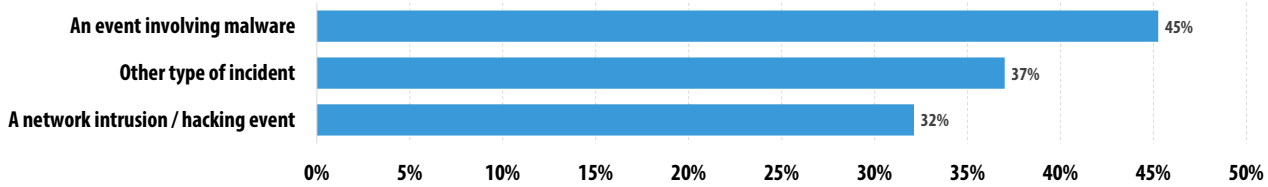


To analyze the typical time frame of a DDoS attack we also had to take into account the severity of an attack: for obvious reasons, attacks that cause only minor delays to service, are not considered critical, even if they last for a few days. On the contrary, an attack causing a complete unavailability of a website or a customer-facing service, leads to a significant damage even if it only lasts for a few hours. Having said that, the typical length of a serious attack, causing complete unavailability, is several hours (35% of severe attacks), although 7% of companies reported being the victim of a severe attack that lasts for several weeks.



DDoS as a decoy

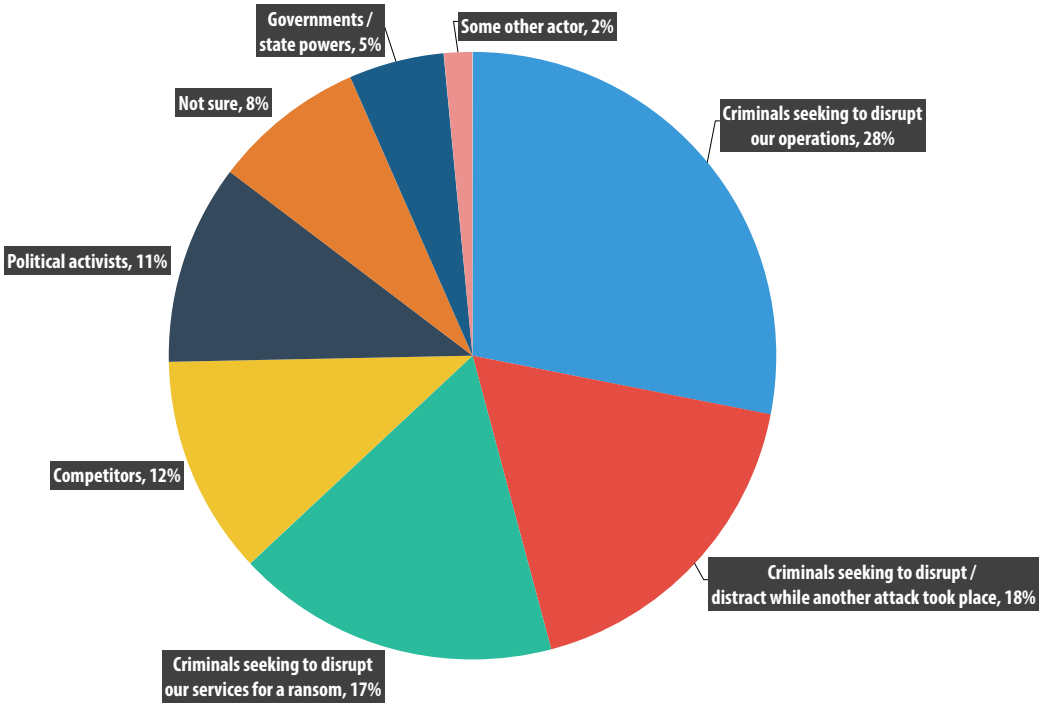
50% of those who experienced a DoS/DDoS attack reported a noticeable disruption of services. Of those, 74% registered other cyber-security incidents at the same time as the DDoS attack. Although it is often impossible to attribute two types of a security breach to a single source, we see that it is highly likely that DDoS attacks are being used as a decoy – to disrupt the IT and/or IT security teams, while cybercriminals try to breach the company's perimeter. Typical examples of attacks experienced by businesses at the same time as the DDoS attack are malware attacks and network intrusion.



Overall, 26% of those who suffered from a DDoS attack said that sensitive business data was lost as a result, and 31% said that non-sensitive business data was lost.

Attribution

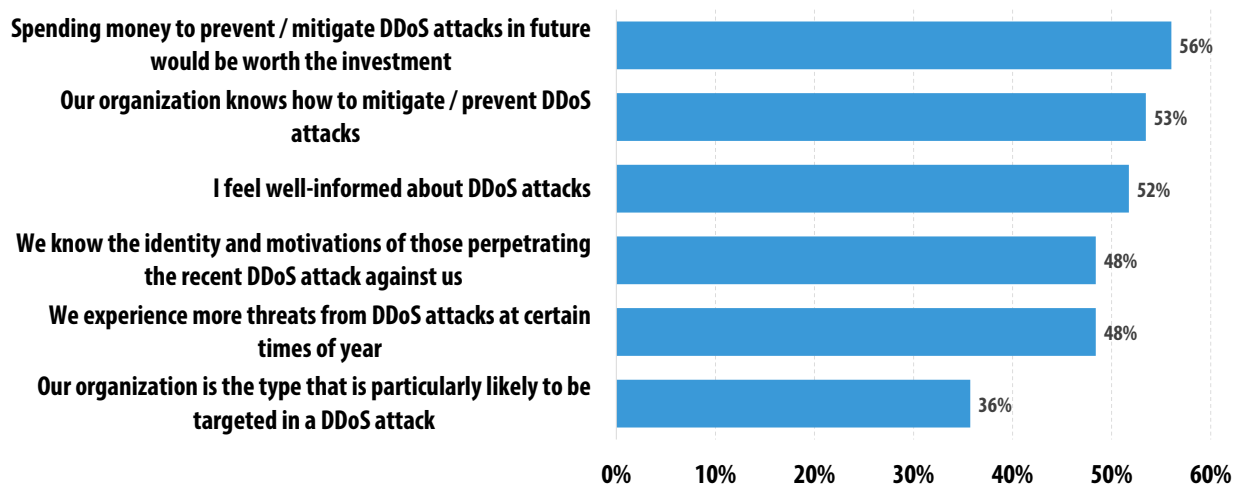
When asked whether businesses are aware of who was behind the attack, 48% said they knew the identity and motivations of those perpetrating recent DDoS attacks against them. In most cases IT professionals believe it was criminals seeking to disrupt their operations. But in 12% of attacks their victims are confident they were organized by a competitor.



Theory: perception of DDoS attacks by businesses

In general, companies have become more alarmed about the growth of DDoS attacks. In the 2015 survey, 6% stated that DDoS attacks are the most serious threats. In the past two surveys (2013 and 2014) this point of view was shared by only 4% of respondents.

Attitudes towards DDoS attacks are mixed, to say the least. 56% of IT professionals believe that spending money to prevent or mitigate an attack in the future would be worth the investment. Only 34% of respondents have fully implemented DDoS prevention systems of any type. At the same time, 12% list DDoS prevention as one of their top priorities for the next year.



Conclusion

In many ways denial of service resembles ransomware attacks. They are not as overwhelming as malware and spam, they may be targeted, and smaller companies with limited IT budget suffer from them frequently. The technology behind DDoS attacks may be simple, but measures to avert them are quite complex and often require additional staff and/or training. No wonder almost half of businesses do not think that preventing future DDoS attacks is worth the investment.

The Global IT Security Risks Survey proves quite the opposite. Firstly, a significant number of DDoS attacks were simply a tool, which, combined with other cybercriminal toolkits may lead to data leaks and intrusion of the network perimeter – while a DDoS attack alone does not lead to such dire consequences. Secondly, the average financial damage of a DDoS attack is significant, especially for SMBs, and is definitely higher than the cost of a service designed to reduce the effect of such attacks. DDoS prevention is almost always a third party service, and outsourcing this trouble to experts not only reduces the damage, but also frees up IT personnel to deal with a probable complementary attack on a company infrastructure, which will have much worse consequences.