CZ.NIC | SPRÁVCE DOMÉNY CZ

Recap of the (D)DOS Attacks of 4-7 March

This document provides insight into the period between 4 and 7 March, which saw a series of (D)DOS attacks launched against www services operated in the Czech Republic, as seen from the perspective of the CZ.NIC Association and CSIRT.CZ (the national CSIRT of the Czech Republic).

Despite our great effort to collect as much information and data as possible and to continuously monitor the situation, we are aware that we do not have all the information at our disposal and that our overview may not be complete.

Description of the Events

On Monday, 4 March 2013 a series of (D)DOS attacks was launched against web servers operated in the Czech Republic. The attacks were usually carried out in two waves – in the morning, between 9-11am, and in the afternoon between 2-4pm. Each day the attack targeted a different group of servers:

Monday, 4 March – the attacks are directed against Novinky.cz, iDNES.cz, IHNED.cz, Lidovky.cz, Denik.cz, Csfd.cz; around noon, the websites E15.cz, Živě.cz, Mobilmania.cz were also inaccessible.

Tuesday, 5 March – the services of Seznam.cz are unavailable around 10am. Seznam.cz reports the situation on its Facebook profile. Seznam.cz is operational again around 11:30am. The attack is repeated around 1:30pm, with observed intermittent server downtime.

Wednesday, 6 March – from approximately 9:30am to 11am, the web servers of the following banks are inaccessible: Česká spořitelna, Komerční banka, FIO banka, ČSOB, Raiffeisen banka, Czech National Bank (www.cnb.cz). As a consequence of these attacks, Česká spořitelna's e-commerce services failed and some payment terminals were paralysed. At 2pm, a second wave of attacks targeted the websites of Česká spořitelna.

Thursday, 7 March – beginning at about 9:30am, the servers of two mobile phone carriers Telefónica O2 and T-Mobile were under attack. Telefónica eliminated the attack around 10am, T-Mobile at about 11am.

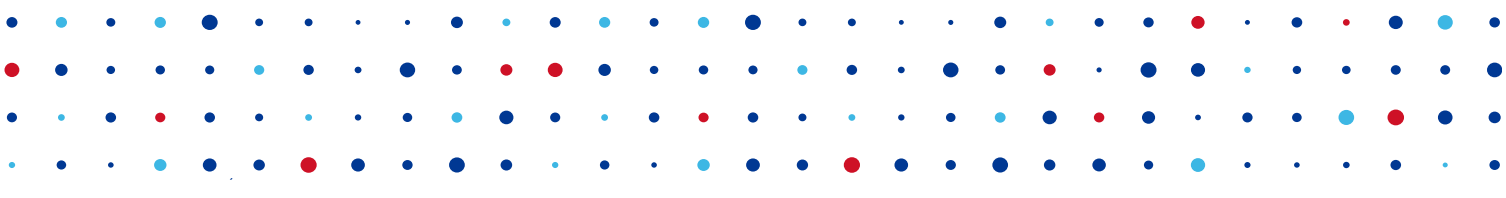
During the attack, some other services were also occasionally unavailable, such as the vehicle register or the website of Prague Public Transport, dpp.cz. There were reports that the service for purchasing public transport tickets via SMS was unavailable for some time during the attack.

Around 8pm, websites of Czech Television became unavailable; according to the latest information, however, their issues were not related to the attacks.

On Friday, 8 March, no further (D)DOS attacks of this type (disrupting the availability of frequently visited and highly visible websites) was observed or reported. The situation gradually calmed down both on the side of network operators and the media.

Characteristics of the Attacks

During the attacks, they were generally referred to as DDOS (Distributed Denial of Service). At this moment, after having collected a large amount of information and related data, we are not entirely sure whether the attack was of the DDOS or DOS type. Most attacks targeted www services.



Most of the attack traffic came over the RETN network (http://www.retn.net/en/). Even though the attacked parties, ISPs and CSIRT.CZ tried contacting the operator of this network, no one managed to secure relevant assistance (data, blocking the attackers). It is likely however that RETN possesses data that could help in specifying the attacker (MRTG traffic charts, ratio of sent packets to bandwidth, etc.).

The attacks utilised a combination of the SYN Flood mechanism and IP spoofing. The aim of such attacks is to overwhelm the machine they are targeting or its network infrastructure (e.g. a front-end equipment firewall) and exhaust their system resources.

Another employed variant of the attack added the technique known as bounce traffic. In these cases, the mechanism of the entire (D)DOS attack was such that the attacking machines emitted a large amount of packets with a spoofed source address. The used source address was the IP address of the machine targeted by the attack. The packets were sent to other machines, which then returned the communication to the fake source address. This technique, based on emitting a large amount of packets with spoofed source addresses and utilising a bouncing mechanism, makes the attack even stronger.

Resolving the Situation

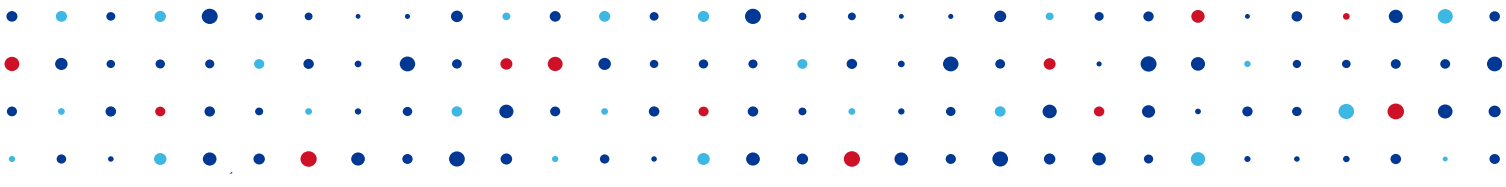
Beginning Monday, 4 March, the CSIRT.CZ team was contacted by the operators of networks and services targeted by the attacks with requests for assistance, cooperation and the exchange of information. In our opinion, the administrators of the attacked networks performed well in their roles and the downtime of the individual websites was only a matter of hours. We also found the approach of the ISPs through which the attacked sites were connected to be professional. They provided support to the targeted networks and were able to deploy effective defence mechanisms. It seems likely that the unavailability of the websites was caused by errors in configuration and under-dimensioned network elements and the servers themselves.

We particularly appreciate the ability and willingness of all stakeholders to communicate and share their experience, information and recommendations.

During the strongest attacks against Česká spořitelna on Wednesday, 6 March, a workgroup was formed by experts from CZ.NIC (CSIRT.CZ), CESNET, GTS and Česká spořitelna, who organised an ad-hoc videoconference meeting. At this meeting, the group discussed the current attacks, analysed traffic and looked for and tested the most efficient defence mechanisms. This workgroup remained on alert throughout Thursday and Friday.

Another workgroup established directly at CZ.NIC was composed of members of the CSIRT.CZ team, CZ.NIC network administrators and PR staff. This group was, as part of the *incident handling* process, responsible for communication with network and service operators, collecting and sharing information, data and experience, communication with the network workgroup, NSA (National Cybernetic Security Centre), security forces or foreign parties and communication with the media.

On Thursday, employees of companies and organisations worried that they might be the next target of the attack (e.g. PRE, ČEPS) started contacting CSIRT.CZ, asking for information and cooperation. They were given basic information about the attacks and contact details of their connection providers and transit operators, to make sure they and we were prepared and knew which ISP to turn to, if required.



Technical Recommendations

There are many methods and technologies protecting against (D)DOS attacks, but it is usually necessary to employ a combination of several of them instead of relying on just one. On the network infrastructure level, defence mechanisms include RTBH (remotely triggered black hole) filtering, using Load Balancer equipment, a Scrubber-type equipment (cleaners separating most bad traffic from good), prefix lists (limiting AS propagation), rate limits, access lists on the network layer, firewall, IDS, IPS etc.

The availability of a particular service may be further increased by strengthening the robustness of the entire architecture using the anycast, DNS round-robin technology which can distribute load between multiple machines with the same content, etc.The next step may be placing servers providing the same service in multiple networks.

Any decisions on the architecture of services and related network infrastructure should, however, always consider if the additional protection is worth the cost. The key factors in this decision are the character of the service and its importance for the user.

Within the CZ.NIC security team, a solution was built during the week of the attacks which can generate traffic of approximately ten million packets per second, several times more than what was employed in the attacks.

This solution is currently being used to test CZ.NIC's own infrastructure. It was also offered as a tool for free infrastructure testing to other interested parties.

Observations and Lessons Learned

The (D)DOS attacks launched against Czech targets between 4 and 7 March were rather weak in character, at least from the perspective of ISPs, who only encountered issues in end networks.

The magnitude of the attack did not in any way disrupt the operation of the providers' backbone networks and their infrastructure.

According to available information, the encountered data flows were under 1 Gbps (the maximum recorded flow being 1.5 million packets per second). The attacks only caused issues in end networks.

According to information available to us, the attacks did not actually reach their target server in most cases, but instead overloaded a front-end system – usually a firewall, load balancer or similar equipment.

Without any doubt, the attacks revealed a number of weaknesses in the network architecture of end networks.

The series of attacks was well prepared, with interesting and highly visible targets, the unavailability of which would be noticed both by users and the media; various techniques and their combinations were utilised.

Knowledge of the environment is confirmed by the distribution of attacks between targets – while Monday's attack had multiple victims, on Tuesday there was only a single one which could be expected to employ a more robust solution than news sites. Similarly, Thursday's attack "omitted" the third major mobile carrier – again presumably because the attacker decided to concentrate forces on a smaller number of targets.

It is therefore likely that the attacks were initiated by someone with good knowledge of the Czech internet.

Conclusion

The events of last week confirmed one basic fact – network and service administrators both on the ISP and end network levels are able and willing to cooperate effectively and exchange experience and certain information.

As the national CSIRT team, we consider it useful to further promote communication and the exchange of information on the technical level, ideally from the very first moments of similar attacks, and improve the means and tools for this communication.

We believe that the course of the attacks confirmed that the CSIRT.CZ team is well-established in the Czech environment and plays an important part in similar incidents.

It was shown that ISPs in particular are well-prepared for such situations, both in terms of technical equipment and organisation.

One of the negative experiences confirmed in this event is the presence of an unpleasant barrier preventing the sharing of relevant information about the attacks. One of the ISPs referred to Act No. 127/2005 Coll., on electronic communication, as amended, and Decrees No. 335/2005 Coll. and 357/2012 Coll., governing the conditions of providing operational or location data and lawful interception. This directly prevents effective cooperation between ISPs and security teams.