REPORT ON ATTACKS FROM 10.10.2023

Incident report

Version: 1.0
Date: 27/10/23
Classification: Public

1. Executive summary

On the dates of the 10th to 13th of October 2023, the Restena Foundation suffered waves of attacks on its network. The attack patterns were identified of DDoS type. The Restena crisis team being on site, was active to mitigate the incident in short time. After 2 waves of attacks the mitigation measures took over and the incident was managed. The duration of the outage was approximately 30 minutes in all.

2. Description of incident

On October 10, 2023 around **15:12** a first attack wave of a duration of 4 to 5 minutes hot the network. The attack announced itself by triggering some symptoms, such that public services on a VLAN were impacted. The impacted services covered principally email, webhosting and the DNS resolver. The crisis team was activated to speed up mitigation and investigations started.

At **15:32** a second wave with same duration of 4 to 5 minutes, with almost identical attack pattern occurred. The attack ran at 1-1,5Gbps with a 3Gbps peak at the end. It targeted the IP address of the Webhosting service.

The attack of DDoS type consisted of a UDP fragmentation attack, with 50% DNS and 50% QUIC. The DDoS attack had an impact on the Firewall that was not able to cope with the amount of open connections.

At **15:35** (approx.) the mitigation processes were in place at about the same time as the 2nd attack wave was ending. By setting up simple ACLs on the routers enabled to drop fragmented udp packets before they could even reach to firewall.

On **15:45**: the communication team informed on the Restena website that there are technical problems and investigations are ongoing. The reason we stated technical problems was that we expected more attacks to come, due to our CyberDay.lu conference speakers two days later.

At **15:58**: the communication team updated the Restena website that all services were back to normal. At the same time, the attack was still ongoing on but mitigated by the ACL on the routers.

The crisis team was up for two additional days, as stronger attack waves were expected for the conference. For this a closer monitoring of the traffic was performed and the attack waves were still hitting the matches on the ACL in place, but without impact on the services.

On October 13, 2023, after the CyberDay.lu conference event, the crisis was declared over.

3. Aftermath

After the investigations were concluded, some additional restrictions have been put in place on the technical side to further reduce the attack surface.