CASE STUDY: DDOS RANSOM INCIDENT RESPONSE

Handling a Ransom-Driven DDoS Attack on a Bank

RED BUTTON
DDoS Experts

BACKDROUND

A Latin America conglomerate, which includes a bank and several financial companies, received an extortion mail threatening to carry out a DDoS attack. The hacker group demanded Bitcoin payment and threatened to attack the company in one week if the payment was not received.

Nevertheless, the first DDoS attack started the same day that the threat mail arrived. After this, the company engaged with Red Button's Incident Response team to prepare for and mitigate further attacks.

ATTACK TIMELINE

July 12

Threat Mail and Attack #1

- Volumetric attack (60 Gbps)
- Duration: 6h
- 15 minutes service disruption

July 15

Incident Response Launch

- Analyze and map protection layers
- Build mitigation playbook
- Run DDoS test #1

July 16

DDoS Test #2

- Network level

July 17

Attack #2

- Volumetric attack (60 Gbps)
- Duration: 24h
- No service disruptions

August 7

DDoS Test #3

- Application level

Threat Mail and DDoS Attack #1

July 12

The first 60 Gbps DDoS attack was launched the same day that the ransom threat letter was received, using a UDP reflection attack vector.

The company's internal security and IT teams activated mitigation measures, which involved diverting traffic to the DDoS Mitigation provider Imperva Incapsula. A few network segments that were initially unprotected caused a 15-minute disruption of service due to pipe saturation. However, once all traffic was diverted, all services returned to the normal state.

Incident Response Launch and DDoS Test #1

July 15

Following the first attack, the company engaged with Red Button's Incident Response team. Our team met with all teams involved to review the DDoS protection architecture. Several hours later, we ran a controlled DDoS network attack simulation to detect and fix vulnerabilities with regard to a second attack.

The simulation attack uncovered multiple problems in infrastructure protection and the routing of traffic to Imperva Incapsula. The IT team spent time fixing all the routing problems.

Test #2

July 16

The next day, our team repeated the simulation and ran another controlled network DDoS attack. The routing problems were all fixed and the simulated attack was stopped successfully.

DDoS Attack #2

July 17

The attackers launched a second attack. While the team and the protection were fully prepared for a larger, more extensive attack, the attack was almost identical to the first one – a 60Gbps volumetric attack, which lasted 24 hours.

Thanks to the testing and fixes implemented earlier, as well as the collaboration between the IT team and our Incident Response teams, the attack was fully mitigated with zero service disruptions.

Test #3

August 7

After the threatened attack date (July 19th) had passed and no additional attacks were identified, our team ran another simulation, aiming to test the mitigation of application-level DDoS attacks. Our team identified and helped the IT team close configuration gaps in the Imperva web protection system.

CONCLUSION AND RECOMMENDATIONS

Following the handling of the attacks, our team provided the company with a detailed report containing conclusions and recommendations, including:

Running periodic DDoS simulations (including application protections)

Adding/Hardening application protections

Adding an external managed DNS service

Configuring automatic traffic diversion to reduce time to mitigation