NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

JUNE 2017

Fact sheet: Distributed Denial of Service (DDoS)

A denial-of-service (DoS) attack is a resource consumption attack that has the primary goal of preventing legitimate activity of a victimized system. A DoS attack renders the target unable to respond to legitimate traffic. There are two basic forms of denial of services:

- Attacks exploiting a vulnerability in hardware or software;
- Attacks that flood the victim's communication pipeline with garbage network traffic.

Many DoS attacks begin by compromising or infiltrating one or more intermediary systems that then serve as launch points or attack platforms. The attacker installs remote-control tools, often called bots, zombies, or agents, onto these systems. Attacks involving these remote-control tools are known as distributed denial-of-service (DDoS) attack. (Stewart, 2016)

Key developments and trends related to DDoS:

- DDoS attacks are increasing in complexity and size, and as result, require more time and effort to mitigate. (Verisign, 2017)
- Multi-Vector DDoS attacks, targeting victim networks at multiple network layers and changing attack types over the course of DDoS events, dominates. (Verisign, 2017)
- UDP flood attacks – Domain Name System (DNS) reflection, Network Time Protocol (NTP) and Simple Service Discovery Protocol (SSDP) reflection – continue to lead in Q1 2017.
- The criminals are using the secure DNSSEC protocol against the industry by taking advantage of a common misconfiguration to amplify DDoS DNS attacks.
- The average DDoS attack size increased by 26% in the first quarter of 2017 compared to 2016, with 23% of these attacks hit over 10 Gbps and 36% over 5 Gbps.
- The large majority of DDoS attacks are fairly short in duration. In the first quarter of 2016, over 93% of attacks lasted under one hour, reports Imperva Incapsula.
- IT Services/Cloud/SaaS remained the sector with the largest number of DDoS attacks, followed by the financial sector.

Top 5 DDoS risks:

- DDoS effects primarily the availability of a service and therefore can lead to financial losses and reputational damage for organisations and its customers.
- As systems are highly connected and dependent on internal and external data, connection disruptions or delays in data processing can also impact data integrity and have impact on secondary target due because of co-hosting and partners in the economic value chain, which are dependent on the primary target.
- DDoS attack could also be used as a diversion to draw the attention from their actual goal, to commit a fraud attempt.
- DDoS attack are relative easy and cheap to execute, but is preventive measures are relative complex and expensive.
- The source of DDoS can be hard to determine, therefore prosecution is difficult.

Measures to mitigate DDoS attacks

Although there is no universal approach that can cover all DDoS security risks, there are a number of measures organizations can take in order to prevent or minimize risks from DDoS attacks. Based on researches and publications from Govcert, IntruGuard, Govcert.nl, National Cyber Security Centrum, National Cyber Security and Communication Integration Center, National Institute of Standards and Technology, Verisign, Drost (2015) developed a *dynamic DDoS Security Control Framework*. The framework contains procedural controls and technical controls divided over seven function levels: identify, protect, detect, respond, recover, assess and adjust. Some of the technical measures in this framework are:

- Protect level (focused on pre-emptive measures):
  - A SYN Proxy is implemented
  - Anomaly Recognition
  - Dark Address Prevention (block IP addresses that are not yet assigned by IANA)
  - White-list and black-list are maintained
  - Connection Limiting
  - Active verification through Legitimate IP Address Matching
  - Implementing anti-spoofing measures
  - Firewalls configured to apply filtering to monitor the traffic for certain protocols, maximum number of connections made from one IP-address
  - Implement adequate storage facilities to retain logging files
- Detect level (focused on being able to pinpoint abnormal behavior)
  - Setup of Intrusion Detection Systems (IDS) & Intrusion Prevention System
  - Flow-based accounting
  - Granular Rate Limiting
  - Dynamic Filtering
  - Source Rate Limiting
- Respond level (focused on respond in case of a DDoS attack)
  - Quality-of-Service (QoS)
  - Null-routing
  - ACL to block (or permit) certain source of destination IP-addresses and/or protocols
  - Aggressive aging
  - White-list and black-list are maintained
  - ‘DDoS wash street’
  - Specific DDoS appliances

Key focus areas for IT auditor:

- Start with a risk assessment. For this purpose, make use of well-known and accepted frameworks for risk assessment, for example, the ones mentioned in the ISACA’s Risk IT Practitioner guide. DDoS falls under the scenario for Logical Attacks. A number of selected COBIT Control Objective/Val IT Key Management Practices apply for this scenario.
- Further on, fill in this framework with the desired specific control and security measures (preventive/detective/corrective) for this given technology (see previous section).
- During this process, do not forget to take into account also the organization and the processes, together with the technology.
- Assess the control and security measures in place not only at the auditee’s company, but also on the ISP’s side.

- Assess the robustness of the auditee and the ISP’s infrastructures by asking the following questions:
  - Are these infrastructures vulnerable to DDoS-attacks? Consider for instance a pentest to demonstrate this;
  - Are there specific hardening and/or security tools and services implemented in order prevent and detect DDoS-attacks?
  - Determine whether specific DDoS attacks have taken place against the auditee (and ISP’s) infrastructure, and identify these (such as, for example, botnets);
  - Determine whether the follow-up to these attacks has been adequate (incident response mechanism);
  - Determine whether the improvements implemented will suffice to prevent DDoS-attacks in the future.

Conclusion:

DDoS attacks cannot be prevented, but organizations can become aware of the threat and work proactively to establish countermeasures and incident response plans to mitigate and minimize the potential impact of a determined and well-resourced attacker. Understanding the adversary's tactics, techniques, and procedures, as well as the options available for mitigating the effects, is vital to establishing a strong security posture and planning a rapid, effective response.

References and external links:

- BSI: Recommendations for the Protection against Distributed Denial-of-Service Attacks in the Internet
  www.bsi.bund.de/EN/Publications/RecommendationsDoS/RecommendationsDoS_node.html
- Drost L. (2015), A DDoS Security Control Framework
- ISACA – The Risk IT Practitioner Guide: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx
- Preparing for Distributed Denial of Service (DDoS) attacks, whitepaper from Dell SecureWorks
- Stewart J.M., Chapple Mike (2015, CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide
- Verisign, Distributed Denial of Service Trends Report, Vol 4, Issue 1 – 1st quarter 2017.