DDOS 사고 대응 방안 요점 정리

네트워크 분산 서비스 공격(DDoS)에 대응하는 팁 모음

일반적으로 고려할 것들

DDoS 공격은 원치 않는 많은 양의 트래픽을 보낸다. 일부 공격은 특정한 시스템에게 압도적인 부담을 준다.

ISP 및 장비의 도움 없이 공격을 막는 것은 쉽지 않다.

종종 너무 많은 사람들이 사고에 대응하려고 달려든다. 대응하는 사람의 수를 적절히 통제한다..

공격이 오랫동안 진행되기도 한다. 어떻게 대응을 이어갈지 고민한다.

소유하는 장비의 공격 차단 성능을 파악한다. 많은 사람들은 성능을 제대로 알지 못하거나, 과대평가한다.

다음 공격을 대비하기

공격에 대비하여 미리 준비한다. 해두지 않으면 공격이 진행되는 동안 중요한 몇 시간을 허비하게 될 것이다.

ISP 에 연락을 취해 공격을 막는 서비스가 유료인지 무료인지, 그리고 어떤 절차를 따라야 하는지 파악한다.

공격을 받는 동안에도 서버에 접근할 수 있는 IP 및 프로토콜 목록을 정리한다. 화이트 리스트는 중요한 파트너 회사 및 고객을 포함한다.

공격 당할 것 같은 시스템과 관련된 DNS TTL 설정을 확인한다. TTL 값을 낮추면 시스템이 공격 당할 때 손쉽게 DNS 설정을 바꿀 수 있다.

관련된 팀(ISP, 방화벽, 법률 등)들과 연락망을 만든다.

IT 인프라를 정리해둔 문서를 만든다. 이 문서엔 IP 주소, circuit ID, 소유자 등을 포함한다. 그리고 장비 목록 및 네트워크 구성도를 준비한다.

이러한 사고가 사업에 어떤 영향을 끼치는지 파악한다.

회사의 위기관리팀이 DDoS 사고를 바라보는 관점을 알아둔다.

DDoS 공격의 대상이 될 수 있는 네트워크, OS, 응용프로그램 등의 설정을 확실히 해둔다.

인프라 성능을 프로파일링하여 이후 공격 여부를 판단할 때 사용한다.

공격 분석하기

공격의 흐름을 파악하고, 영향을 받은 인프라를 확인한다.

서버, 라우터, 방화벽 그리고 공격의 영향을 받은 장비들의 로그 및 부하를 살펴본다.

정상, 비정상 트래픽의 차이를 확인한다. (IP, 포트 등)

가능하다면 tcpdump, ntop, MRTG 등의 네트워크 분석 도구를 이용해 트래픽을 살펴본다.

ISP 와 내부 팀으로부터 정황을 확보하고, 도움을 요청한다.

ISP 에 연락하기 전에, 트래픽 통제 방안을 결정한다. 어떤 네트웍을 막고, 어떤 IP 의 대역폭을 통제 할 것인지.

공격 이전에, 공격자에게 어떤 요구를 받았는지 확인한다.

가능하다면 NIDS 탐지 패턴을 만들어 정상적인 트래픽과 유해한 트래픽을 구분한다.

회사의 이사진과 법률팀에 연락한다. 지시에 따라, 법적 대응을 할지 고려한다.

공격의 영향 줄이기

공격을 완벽하게 막기는 힘들지만, 공격이 미치는 영향을 줄일 수 있다.

가급적 백본에 가까운 장비를 이용하여 DDoS 트래픽을 제어한다. (라우터, 방화벽, 로드밸런서 등)

서버와 라우터에서 세션을 끊고, TCP/IP 설정을 최적화 한다.

가능하다면, DNS 나 그 외의 방법을 이용해, 다른 서버나 네트워크로 트래픽을 옮긴다.

응용프로그램의 특정 기능이 병목이면, 그 기능을 임시로 비활성화한다.

가능하다면, 서버와 네트워크 대역폭을 추가한다.

가능하다면, DNS 와 라우팅 설정을 이용해 트래픽을 트래픽 검사 장비로 보낸다.

방어 시 한 번에 하나씩 진행해야 변화의 원인을 알 수 있다.

Egress 필터를 설정한다. 불필요한 DDoS 응답 트래픽을 차단한다.

사고 정리 및 조정

사고에 빠르고 효율적으로 대응하기 위해 어떤 준비단계를 취할 수 있었는지 살펴본다.

필요한 경우 DDoS 대응 준비에 영향을 미쳤던 가설을 조정한다.

DDoS 대응 과정, 참여자, 연락 방법이 효과적인지 평가한다.

내/외부의 어느 조직이 다음 사고에 도움을 줄 수 있을지 살펴본다..

DDoS 사고 대응 핵심 단계

1. 준비: 미리 연락처를 확보하고, 절차를 정의하고, 도구를 확보하여 대응 시간을 절약한다.
2. 분석: 사고를 탐지하고, 사고 범위를 파악하고, 관련 부서를 참석시킨다.
3. 퇴치: 공격의 영향을 줄인다.
4. 정리: 사고 내용을 정리하고, 얻은 교훈을 이야기한다. 그리고 대응 계획과, 방어 방법을 조정한다.

기타 DDoS 대응 자료

DoS 공격 탐지 기술
http://www.computer.org/portal/site/dsonline...

DoS/DDoS 방지 및 퇴치 기술에 관한 요약
http://sans.org/reading_room/whitepapers/intrusion/1212.php

네트워크 프로토콜 및 도구 요점 정리
http://packetlife.net/cheatsheets/

대응 담당자용 침해사고 초기 대응 요점 정리
http://nchovy.kr/forum/3/article/332