서비스 거부(Denial-of-Service) 공격에 대한 대비 및 대응

최초 게시: 2011년 9월
최종 업데이트: 2025년 3월

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

서론

본 출간물은 서비스 거부(DoS) 공격이 우리의 지역 일대에서 증가하는 추세에 대응하기 위해 호주 신호국(Australian Signals Directorate, ASD)에서 뉴질랜드 국가 사이버 보안국(CSC-NZ), Akamai Technologies Ltd 및 Cloudflare Pty Ltd와 협력하여 제작되었습니다. 이는 DoS 공격에 대비하고 대응하기 위해 현대의 위협 거래 기술을 기반으로 한 모범 완화 방안에 대한 지침을 조직에 제공합니다.

본 기관은 본 지침을 ASD의 *'Internet of Things devices(사물 인터넷 기기)'* 및 *Secure your 'Wi-Fi and router(와이파이 및 라우터 보안 수행)'* 출간물과 함께 열람하는 것을 권장합니다. 이들 출간물은 개인들이 타인에게 해가 될 수 있는 DoS 공격에 의도치 않게 기여하는 것을 피할 수 있도록 돕습니다.

DoS 공격은 웹사이트, 이메일 및 도메인 이름 시스템(DNS) 서비스와 같은 온라인 서비스를 방해하거나 저해시키도록 설계된 사이버 공격으로 적법한 사용자들의 접근 권한을 막습니다. 이는 일반적으로 온라인 서비스를 대상으로 데이터, 접속 또는 요청을 퍼부어 해당 서비스를 과부하시키고 운영 기능을 저하시키는 방식으로 이루어집니다.

DoS 공격이 성공하기 위해서는 대개 대용량의 네트워크 트래픽이 요구됩니다. 이러한 공격은 점점 더 흔해지고 있으며, 그 부분적인 이유는 쉽게 침해당할 수 있는 사물 인터넷(IoT) 기기의 수가 증가하고 있기 때문입니다. IoT 제조업체들이 대개 사이버 보안보다 사용자 경험을 우선시함으로 인해, 스마트 TV, 주전자, 진공 청소기 및 보안 시스템 등, 인터넷에 연결되는 일반 가정 용품들이 취약 기기 대상이 될 수 있습니다. 이들 기기는 종종 악의적인 공격자가 원격으로 손상시켜 네트워크 트래픽을 생성하는 장치의 '봇넷'을 생성할 수 있으며, 이로 인해 대상 가정들과 조직들이 의도치 않게 DoS 공격이 발생할 수 있도록 하는 인프라에 기여하게 될 수 있습니다.

최근 사례들을 통해 알 수 있는 것은, 악의적인 공격자들이 대량의 IoT 기기를 한 번 손상시키게 되면, 이들은 해당 인프라를 사이버 범죄자 및 해커들에게 임대 또는 판매할 수도 있으며 이들 범죄자 및 해커들은 자신이 선택한 대상에 대해 DoS 공격을 수행하고자 한다는 것입니다. 대부분의 경우 DoS 공격은 조직을 대상으로 생산 및 금전적 피해를 초래하거나 어떠한 이유에서든 대중의 관심을 얻기 위해 수행됩니다. 이러한 활동의 예시는 ASD의 *'People's Republic of China-linked actors compromise routers and IoT devices for botnet operations(중화인민공화국과 연관된 공격자들에 의한 봇넷 운영 목적의 라우터 및 사물인터넷 기기 침해)'* 지침에서 확인할 수 있습니다.

경제가 더욱 디지털화되고 인터넷에 연결된 보안이 취약한 IoT 기기가 증가함에 따라 DoS 공격 또한 계속해서 증가할 가능성이 높습니다.

악의적인 공격자들은 조직의 온라인 서비스를 방해 또는 저해하기 위해 다음을 포함한 여러 접근 방식을 사용합니다:

- 사용 가능한 모든 네트워크 대역폭을 소모하기 위해 온라인 서비스를 대상으로 대량의 원치 않는 네트워크 트래픽을 유도하는 행위
- 온라인 서비스에 맞춤형 네트워크 트래픽을 유도하여 컴퓨터 처리 자원을 소모하는 행위
- 분산형 DoS(DDoS) 공격이라고 하는 흔한 유형의 DoS 공격 - 여러 컴퓨터, IoT 기기 또는 기타 인터넷 연결 기기를 사용하여 여러 방향에서 훨씬 더 큰 규모로 온라인 서비스에 네트워크 트래픽을 전송하는 행위
- 조직의 도메인 등록 또는 DNS 서버를 하이재킹하여 적법 사용자를 조직의 온라인 서비스에서 멀어지게 하는 행위

조직들은 DoS 공격의 대상이 되는 것을 피할 수는 없지만 이에 대비하고 피해 정도를 줄일 수 있는 여러 방안이 있습니다. DoS 공격이 일어나기 전에 이에 대비하는 것이 가장 좋은 전략입니다. 대비를 하지 않으면 일단 DoS 공격이 일어나고 있는 와중에는 대응하는 것이 어렵고 덜 효과적이기 때문입니다.

조직들은 자사를 DoS 공격으로부터 보호하는 데 초점을 두지만, 이와 더불어 악의적인 공격자가 타인을 표적 삼아 조직의 온라인 서비스와 인터넷 연결 기기를 남용하는 것을 방지하기 위한 조치도 취해야 합니다.

DoS 공격에 대비하기

우리의 지역 일대에서 DoS 공격이 증가하는 상황에서 DoS 공격에 대비하기 위한 조치를 구현하기 전에, 여러분의 조직은 DoS 공격 시 제공하는 각 온라인 서비스가 계속해서 가동되어야 하는지 또는 일시적인 서비스 중단이 허용되는지 여부를 판단하기 위해 전체적인 사업 요건을 먼저 평가해야 합니다.

만약 조직이 DoS 공격에 대한 대응 능력을 향상시키길 원한다면, DoS 공격이 발생하기 전에 적절하고 실행 가능한 경우 다음 조치를 사전에 시행해야 합니다.

- 조직에서 콘텐츠 전송 네트워크(CDN)를 사용한다면, 적절하고 실행 가능한 경우 다음과 같은 추가 조치를 마련해야 합니다.
  - 원본 웹 서버를 다양한 애플리케이션 및 네트워크 레이어 공격으로부터 보호하는 기능이 탑재된 CDN 사용을 고려해 보세요. 일부 CDN은 이러한 기능을 엣지 웹 애플리케이션 방화벽의 일부로 포함할 수도 있습니다.
  - 원본 웹 서버의 인터넷 프로토콜(IP) 주소가 불필요하게 대중에 공개되는 것을 피하고, 대중 노출 시 DoS 공격으로부터 보호되도록 하세요.
  - 악의적인 공격자가 예측할 수 있는 원본 웹 서버 IP 주소를 사용하지 마세요. 예를 들어, 공개적으로 알려진 조직의 온라인 서비스 IP 주소와 동일한 네트워크 서브넷 IP 주소를 사용하지 마세요.
  - 네트워크 접근 제어 장치(예: 방화벽)를 사용하여 CDN 및 귀하 조직의 승인된 관리 네트워크만 귀하의 원본 웹 서버에 접근할 수 있도록 하세요.
  - 원본 웹 서버에 대해 더 높은 수준의 보호가 필요하다면 원본 웹 서버와 CDN 제공자 간에 개인 네트워크 연결을 포함한 복원력 있는 다양한 네트워크 연결을 사용하는 것을 고려해 보세요.
  - 캐싱 작업량을 최적화하기 위해 CDN, 원본 웹 서버 및 클라이언트 HTTP 헤더를 구성하세요.
  - 더 높은 수준의 가용성이 필요하다면 원본 웹 서버에서 위험성이 낮은 IP 주소와 위험성이 높은 IP 주소의 요청이 별도로 처리되는 분리 기능을 고려해 보세요.

- 조직의 온라인 서비스를 이용하는 적법 사용자에게 허용되는 기능과 서비스 품질 정도, 해당 기능을 유지하는 방법, 그리고 DoS 공격 시의 불필요한 기능을 파악하세요.
- 클라우드 기반 DoS 공격 완화 서비스를 구입하여 활용하세요.
- 조직의 공격 대상 영역을 줄일 수 있는 다음 조치를 고려해 보세요:
  - DoS 공격을 견딜 수 있는 평판 좋은 서비스 제공자에게 기초 온라인 서비스(예: DNS)를 외주 주세요.
  - 핵심 온라인 서비스(예: 이메일)를 표적이 될 가능성이 더 높은 다른 온라인 서비스(예: 웹사이트)와 분리하세요.
  - DoS 공격 완화 서비스가 온라인 서비스의 네트워크 포트와 관련된 네트워크 트래픽만 허용하도록 확인하세요.
- 서비스 제공업체와 DoS 공격 방지 및 완화 전략의 세부 사항에 대해 논의하세요. 다음은 특히 중요한 논의 항목들입니다:
  - 전 세계의 DoS 공격을 견뎌낼 수 있는 입증된 능력
  - DoS 공격에 대한 대응 그리고 포괄적이고 승인된 DoS 공격 테스트에 대한 처리 경험 및 기록
  - 인간의 개입(네트워크 트래픽에 대한 수동 분석 등) 없이 대다수 유형의 DoS 공격을 자동으로 완화할 수 있는 기능
  - 비용이 고정되어 있는지 혹은 네트워크 트래픽 및 컴퓨터 처리 자원 사용량에 따라 가격이 변동하는지, 그리고 청구 한도를 설정할 수 있는지 등 서비스 가격 책정에 대한 접근 방식
  - DoS 공격 발생 시 이에 대해 고객에게 고지 또는 온라인 서비스를 끄는 임계값
  - DoS 공격 발생 시 수행할 수 있는 사전 승인된 작업
  - 업스트림 공급업체와의 DoS 공격 예방 협력 조치
- 시스템 가용성, 네트워크 트래픽, 컴퓨터 처리 자원, 관련 비용에 대한 실시간 모니터링 및 경고 등 DoS 공격을 탐지하기 위한 조치를 마련하세요.
- DoS 공격 발생 시에도 서비스가 중단되지 않고 최소한의 프로세싱과 대역폭만으로 운영되는 웹사이트의 정적 버전을 준비하세요.
- 대역폭이 크고, 컴퓨터 처리 자원이 충분하고, 호스팅 위치가 지리적으로 분산되어 있고, 원하지 않는 네트워크 트래픽을 제거하기 위한 클라우드 기반 트래픽 스크러빙을 갖춘 복원성 높은 온라인 서비스를 마련하고 사용하세요. 이는 대개 정적 웹사이트 콘텐츠를 캐시하기 위해 평판 좋은 CDN을 사용하고 원본 웹 서버를 원하지 않는 네트워크 트래픽으로부터 보호하는 조치 등을 포함합니다.
- 도메인 잠금을 사용하고, 도메인 등록 관련 연락처 및 기타 세부 정보가 정확한지 확인하고, ASD의 'Domain Name System security for domain owners(도메인 소유주들을 위한 도메인 이름 시스템 보안)' 출간물에 설명된 추가 지침을 참고하여 귀하 조직의 도메인 이름을 보호하세요.
- 서비스 제공업체의 연락처 정보를 최신 상태로 유지하고, 조직의 연락처 정보를 서비스 제공업체와 공유하여 조직의 관련 내부 조건(예: 주 7일, 하루 24시간)에 따라 모든 연락처를 관리하고 유지하세요.
- 정상적인 통신 채널이 막힐 경우를 대비해 서비스 제공업체에 신뢰할 수 있는 통신망을 위한 조직의 별도 연락처 정보를 제공하세요.
- DoS 공격을 견뎌내야 하는 조직의 각 온라인 서비스에 대한 다양한 유형의 DoS 공격을 포함하여 사이버 보안 사고 대응 계획을 개발, 구현 및 유지하고, 이를 매해 최소 1회 실행하세요.
- 컴퓨터 처리 자원의 소모가 늘어나거나 추가 재정적 비용이 발생하는 일반적으로 남용되는 기능(예: SMS 전송)을 보호하기 위한 애플리케이션을 설계하세요.
  - 레이트 리미팅 및 사람이 요청을 전송한 것인지 확인하는 기능이 포함된 보호 기능
  - DoS 공격 테스트 수행(애플리케이션 기능 관련 잘못된 로직 흐름 타겟팅 등)
  - DoS 벡터를 식별하고 해결하기 위한 더 광범위한 부하 테스트 수행

DoS 공격에 대응하기

조직이 DoS 공격에 대비하지 않았더라도 DoS 공격 발생 시 위에 나열된 내용과 같은 조처를 시도할 수 있습니다. 그러나 그 효과가 덜할 수 있고 구현하는 데 시간이 걸릴 수 있기 때문에 결과적으로 조직의 대응 능력을 저하시킬 수 있습니다.

DoS 공격 발생 시 적절하고 실행 가능한 경우, 다음 조치를 취해야 합니다.

- 사이버 보안 사고 대응 계획을 실행하세요.
- 서비스 제공업체에 대응책을 즉시 적용할 수 있는지 여부를 확인하세요. 제공업체의 대응 능력을 사전에 논의하지 않으면 그들이 응답할 수 없거나, 응답하고 싶어하지 않거나, 추가 비용을 청구하는 상황이 발생할 수도 있습니다.
- 현재 DoS 공격을 효과적으로 만드는 필수적이지 않은 기능을 비활성화하거나 온라인 서비스에서 필수적이지 않은 콘텐츠를 제거하세요. 예를 들어, 검색 기능, 동적 콘텐츠 또는 대용량 파일이 없는 웹사이트 버전을 전개하세요.
- DoS 공격 완화 서비스 제공업체 등을 포함한 서비스 제공업체 및 고객과의 소통망을 유지하고 온라인 서비스 사용 가능성 여부를 계속해서 모니터링 하세요.
- 원본 웹 서버가 직접적인 표적이 된 경우, 그 서버의 IP 주소 변경을 고려하고, 관련 보호 장치가 구현되지 않은 한, 새로운 IP 주소를 대중에 공개하는 것을 피하세요.
- 본 출간물 'Contact details' 부분에 따라 관련 이해당사자(ASD 및 NCSC-NZ 등)에게 DoS 공격 상황을 고지하세요.

DoS 공격에 기여하는 것을 피하기

타인에게 해가 될 수 있는 DoS 공격에 의도치 않게 기여하는 것을 피할 수 있도록 귀하의 조직은 다음 조치를 취해야 합니다.

- 불필요하거나, 또는 안전하지 않게 구성되었거나 유지 관리가 부적절한 서비스와 IoT 기기 그리고 인터넷에 연결된 기타 기기가 인터넷에 노출되지 않도록 하세요.
- 인터넷에 노출된 서비스와 IoT 기기 그리고 인터넷에 연결된 기타 기기를 안전하게 설정, 관리 및 모니터링하세요.
  - 소사업체를 위한 추가 지침은 ASD의 *'Internet of Things devices(사물 인터넷 기기)'* 및 *'Secure your Wi-Fi and router(와이파이 및 라우터 보안 수행)'* 출간물에 포함되어 있습니다.

만약 여러분의 조직이 온라인 서비스를 운영하고 있다면 다음 추가 조치를 취해야 합니다.

- 미국 사이버 보안 및 인프라 보안 기관(CISA)의 *'UDP-Based Amplification Attacks(UDP 기반 증폭 공격)'* 지침의 프로토콜을 우선적으로 검토하세요.
- 새로운 증폭 벡터가 식별되면 이를 모니터링하고 이에 대비해 온라인 서비스를 보호하세요.
- 인바운드 및 아웃바운드 네트워크 접근 제어 장치를 구성하여 승인된 온라인 서비스와 조직에 대한 접근을 제한하세요.
- 필요하지 않다면 증폭되기 쉬운 온라인 서비스에 대한 익명의 공개 접근을 차단하세요.
- 차단 또는 접근 제어 적용이 불가능하거나 적절하지 않은 경우 남용의 가능성을 줄이기 위해 레이트 리미팅 장치 구현을 고려하세요.

추가 정보

ASD의 *'Information security manual(정보 보안 매뉴얼)'*은 조직들이 자사의 시스템 및 데이터를 사이버 공격으로부터 보호하기 위해 적용할 수 있는 사이버 보안 프레임워크입니다. *'Strategies to mitigate cyber security incidents(사이버 보안 사고 완화 전략)'* 출간물과 *'Essential Eight (8가지 필수)'* 출간물에 포함된 지침은 이 프레임워크를 보완합니다.

*'New Zealand Information Security Manual(뉴질랜드 정보 보안 매뉴얼)'*은 뉴질랜드 정부에서 제작한 정보 보장 및 정보 시스템 보안에 대한 지침입니다. 이 지침은 기관 정보 보안 임원은 물론, 기관에 서비스를 제공하는 공급업체, 계약자 및 컨설턴트의 요구를 충족하도록 고안된 실무자 매뉴얼입니다.

다양한 DoS 공격 유형에 대한 더 자세한 정보는 CISA의 *'DDoS Quick Guide(DDos 간단한 가이드)'* 및 *'Understanding and Responding to Distributed Denial-Of-Service Attacks(분산된 서비스 거부 공격 이해 및 대응)'* 출간물에서 확인할 수 있습니다.

연락처

호주에서 본 지침에 대한 문의가 있는 경우, ASD에 서면으로 문의하거나 1300 292 371(1300 CYBER1) 번으로 전화하세요.

뉴질랜드에서 사이버 보안 사고를 신고하려면 incidents@ncsc.govt.nz로 이메일을 전송하거나 NCSC-NZ의 'Report an incident(사고 신고)' 웹페이지를 방문하세요.

면책 조항

본 지침의 자료는 일반적인 성격을 지니며 법률 자문으로 간주되거나 특정 상황 혹은 긴급 상황에서 도움을 받기 위해 의존되어서는 안 됩니다. 모든 중요한 문제에 대해서는 자신의 상황과 관련해 적절하고 독립적인 전문가의 조언을 구해야 합니다.

연방정부는 본 지침에 포함된 정보에 의존한 결과로 발생한 어떠한 손상, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

더 자세한 정보를 원하시거나 사이버 보안 사고를 신고하시려면 다음으로 저희에게 연락주시기 바랍니다.

cyber.gov.au | 1300 CYBER1 (1300 292 371)

이 번호는 호주 내에서만 사용 가능합니다.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre