DDoS 방어: 측정 기반 접근 방식

마티즈 존커, 안나 스페로토, 아이코 프라스
트벤테 대학교, 엔쉐데, 네덜란드

요약-사회는 **글로벌 커뮤니케이션을 위해 인터넷에 크게 의존하고 있습니다. 동시에 인터넷의 안정성과 신뢰성은 고의적인 위협에 지속적으로 노출되어 있습니다. 이러한 위협에는 잠재적으로 치명적일 수 있는 (분산) 서비스 거부(DDoS) 공격이 포함됩니다. DDoS로 인해 기업은 매년 수억 달러의 손실을 입습니다. 또한 중요한 인프라의 경우 국가 안전과 생명까지 위태로울 수 있습니다. 따라서 효과적인 방어는 절대적으로 필요합니다. 하지만 쉽게 사용할 수 있는 방어 솔루션의 잠재적 사용자는 다양한 형태와 크기의 솔루션을 선택할 수 있으며, 그 중 적합한 솔루션이 항상 명확하지 않을 수 있습니다. 또한 완화 솔루션의 배포와 운영에는 더 잘 이해해야 하는 숨겨진 위험이 있을 수 있습니다. 또한 정책 입안자와 정부는 국가 차원에서 사이버 안전을 증진하기 위해 무엇을 해야 하는지에 대한 질문에 직면하게 됩니다. 따라서 DDoS에 대응하기 위한 최적의 행동 방침을 개발하는 것은 사회적으로도 어려운 과제입니다. DDoS 문제는 결코 새로운 문제가 아니지만, 그 규모에 대해서는 여전히 불분명합니다. 우리는 우리가 방어하고 있는 것이 무엇인지 정확히 알지 못하며, 문제를 정면으로 해결하기 위해서는 공격에 대한 이해를 높이는 것 이 필수적입니다. 상황 인식을 발전시키기 위해서는 여전히 많은 기술적, 사회적 과제를 해결해야 합니다. 전반적인 인터넷 보안을 개선하기 위해 DDoS 문제를 더 잘 이해하는 것이 중요하다는 점을 고려할 때, 이 백서에서 요약한 논문은 크게 세 가지 측면에서 기여합니다. 첫째, 공격과 공격 대상을 대규모로 엄격하게 특성화합니다. 둘째, 다양한 완화 솔루션의 인터넷 전반의 채택, 배포 및 운영 사용에 대한 지식을 발전시킵니다. 마지막으로, 방어 솔루션의 효과를 완전히 무력화시킬 수 있는 숨겨진 위험 요소를 조사합니다.**

색인 용어-서비스 거부**, 디도스, 공격, 완화, 인터넷 측정**

I. 소개

우리의 주요 통신망이 포위당하고 있습니다. 인터넷의 진화는 현대 사회에 혁명적인 영향을 미쳤습니다. 교육 기관, 연구 센터 등을 상호 연결하는 기술로 시작된 인터넷은 지난 30여 년 동안 전 세계 통신을 장악했습니다. 인터넷은 상거래, 기술, 엔터테인먼트 등 현대 사회에서 없어서는 안 될 중요한 부분이 되었습니다. 커뮤니케이션을 위해 인터넷에 의존하고 있는 오늘날, 많은 사람들이 당연하게 여기는 인터넷의 가용성은 매우 중요합니다. 인터넷의 핵심 구성 요소는 원래 복원력을 염두에 두고 설계되었지만, 오늘날 인터넷의 안정성과 신뢰성은 파괴적인 DDoS 공격을 비롯한 고의적인 위협에 지속적으로 노출되고 있습니다. DDoS 현상에 대한 엄격한 특성 분석과 관련 위험을 완화하기 위한 대응책이 부재하며 많은 분석적 과제에 직면해 있습니다. 이 논문은 이러한 미해결 문제를 정확하게 해결하기 위해 측정 기반의

공격과 방어 솔루션을 특성화하기 위한 접근 방식입니다. 저희의 연구는 상황 인식을 발전시키고 인터넷 연구, 네트워크 운영 및 정책 입안자들에게 증가하는 DDoS 위협에 대한 정보를 제공하는 능력을 입증하고 있습니다.

A. DDoS 공격

지난 수십 년 동안 DDoS 공격은 발생 빈도와 강도가 급격히 증가하여 인터넷의 안정성과 신뢰성을 위협하는 가장 큰 위협 중 하나로 자리 잡았습니다. 이름에서 알 수 있듯이 서비스 거부 공격은 공격자가 서비스 거부를 달성하기 위해 사용합니다. 즉, 가능한 모든 수단을 동원하여 네트워크, 즉 인터넷에서 네트워크 서비스를 차단하는 것입니다. 공격자의 동기는 매우 다양할 수 있으며, 다른 악의적인 활동(예: 데이터 도용[1], [2])으로부터 주의를 분산시키거나, 핵티비즘(예 : 정치적 동기에 의한 공격)[3], [4] 또는 사이버 갈취(예: 몸값을 내지 않으면 전자 뱅킹 애플리케이션을 다운시키겠다고 은행을 협박)[5] 등이 이에 국한되지 않고 있습니다. 공격이 성공하면 파급 효과가 발생하고 연쇄적인 장애가 발생하며 잠재적으로 인터넷에 막대한 영향을 미칠 수 있습니다[6]. DDoS 위협에 직면했을 때 효과적인 것은 자명합니다 .

방어는 절대적으로 필요합니다.

978-1-7281-4973-8/20/$31.00

B. 완화 솔루션

DDoS 문제가 급증하면서 다양한 방어 솔루션이 개발되었고 상용 제품 시장이 호황을 누리고 있습니다. 일반적으로 공격에 대한 방어는 공격 트래픽이 집중되어 해를 끼치기 시작하기 전에 소스 가까이에서 수행하는 것이 더 효과적입니다. 반면에 탐지는 일반적으로 피해가 발생하는 표적에 더 가까운 곳에서 더 잘 수행됩니다. 이 때문에 다양한 검증된 솔루션이 도메인 간에 사용되며, 이는 탐지를 위한 원격 측정 정보와 완화를 위한 사후 대응 제어 조치가 조직 경계를 넘어 교환된다는 것을 의미합니다. 인터넷에서 방어 솔루션 도입에 대한 정량적 지식은 제한적입니다. 또한 운영자가 공격을 받았을 때 이러한 솔루션이 어떻게 배포되고 운영되는지에 대한 이해가 부족합니다.

C. 숨겨진 위험

완화 솔루션은 쉽게 구할 수 있지만, 설정의 용이성과 사용자의 전문성 사이에 잠재적인 단절이 존재합니다. 솔루션 제공업체는 낮은 도입 장벽을 제공함으로써 이점을 얻을 수 있습니다. 위기 상황(즉, 공격을 받았을 때)에 필요한 것이 신속한 제품(또는 서비스) 배포이기 때문에 종종 이를 활용하려고 합니다. 하지만 숙련된 네트워크 전문가가 아닌 다른 사용자가 겪을 수 있는 잠재적 함정은 무엇일까요?

운영자와 보안 엔지니어가 특정 기능을 사용할 때 직면하는

완화 기술이 있나요? 솔루션의 효과를 떨어뜨릴 수 있는 숨겨진 위험 요소가 있나요?

D. 도전 과제

DDoS 방어와 관련해서는 다음과 같은 많은 과제가 있습니다: *(i)* 방어 대상을 정확히 파악하는 데 따르는 어려움, *(ii)* 방어 솔루션의 도입 및 운영과 관련된 어려움. 이 논문은 시작부터 우리가 직면한 기본적인 과제가 데이터에 관한 것임을 보여줍니다. DDoS 문제를 방법론적으로 연구하기 위해 다양한 (원시) 데이터 소스를 확보하고 개발하는 것은 그 자체로 어려운 과제입니다. 저희는 이러한 과제를 극복하는 데 크게 기여하고 있습니다.

E. 접근 방식

저희의 접근 방식은 측정 기반입니다. 전 세계의 다양한 지점에서 대규모 수동 및 능동 측정을 통해 다양한 독립적인 데이터 유형을 수집합니다. 이러한 데이터 처리의 어려움을 감안하여 빅 데이터 분석을 적용하여 데이터 세트를 융합, 도출, 분석합니다. 이 과정에서 기존의 측정 방법론을 적용하고 검증하며, 필요한 경우 새로운 측정 방법론을 고안하기도 합니다.

F. 기여

데이터를 성공적으로 융합함으로써 우리는 *(i)* 전 세계 공격 활동에 대한 놀라운 통계를 공개하고, *(ii)* 인터넷 전반의 완화 솔루션 도입과 사용자들의 운영 관행에 대한 인사이트를 확보하며, *(iii)* 배포 및 운영상의 실수로 인한 바람직하지 않은 부작용을 드러내고 조사할 수 있습니다. 또한, 기존의 방법론을 더욱 검증하고(즉, 이전의 검증 노력을 보완하는 작업), 일부 데이터를 연구 커뮤니티에 공개합니다.

무엇을 방어하고 있는지 파악하는 측면에서 공격의 대규모 특성을 제시합니다. DDoS 문제의 대규모 규모를 공개합니다. 약 2,100만 건의 공격에 대한 특성 분석을 통해 인터넷에서 활동 중인 것으로 추정되는 전체 /24 네트워크 중 1/3이 최근 2년간의 관찰 기간 동안 최소 한 번 이상 공격을 받았다는 사실을 밝혀냈습니다. 또한 방어 솔루션의 도입과 운영에 대한 이해도도 높아졌습니다. 특히 클라우드 기반 보호 서비스와 BGP 블랙홀링이라는 두 가지 도메인 간 솔루션에 초점을 맞추고, 도입 및 운영 관행에 대한 글로벌 동향을 공개합니다. 마지막으로, 배포 및 운영 과정에서 실수가 발생하여 일부 운영자와 사용자가 보안에 대한 잘못된 인식을 갖게 된다는 사실을 뒷받침합니다. 또한 공격자가 이러한 실수를 방어 체계를 우회할 기회로 삼을 수 있다는 사실을 입증합니다.

G. 조직

이 백서의 나머지 부분은 다음과 같이 구성됩니다. II장에서는 저희가 식별, 개발, 사용한 주요 데이터 소스를 간략하게 설명합니다. II-A에서는 공격의 특징에 대해 설명합니다. 4장에서는 방어 솔루션으로 관심을 전환합니다. 다음으로, § V에서는 이러한 솔루션과 관련된 숨겨진 위험에 대한 분석을 제시합니다. 마지막으로 6장에서 저희의 연구 결과를 요약합니다.

II. 데이터 소스

A. (D)DoS 활동 데이터

저희는 (디도스) 활동의 글로벌 지표를 제공하는 두 가지 데이터 소스를 확인했습니다. 첫째, 무작위로 균일하게 스푸핑된 IP 주소를 사용하는 DoS 공격의 증거를 포착하는 UCSD 네트워크 텔레스코프(UCSD-NT)입니다. 둘째, 특별히 스푸핑된 IP 주소를 포함하는 공격 유형인 반사 및 증폭 DoS 공격을 캡처하는 AmpPot 허니팟입니다.

그림 1. 세 가 지 데이터 소스에 대한 측정 시스템의 배치에 대한 조감도. 특히, 공격 데이터와 블랙홀 관측입니다.

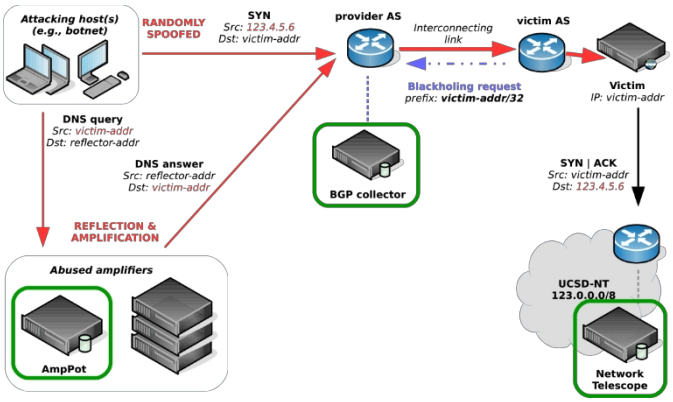
무작위 스푸핑 공격 UCSD-NT는 샌디에이고 캘리포니아 대학교에서 운영하는 `/8` 네트워크이지만 거의 사용되지 않는 라우팅된 네트워크입니다. [7] 네트워크 망원경, 즉 다크넷은 스캔, 잘못된 구성, 버그, 서비스 거부 공격으로 인한 후방 산란 등으로 인해 발생하는 원치 않는 트래픽을 수동적으로 수집합니다. - 호스트를 포함하지 않는 주소 공간의 라우팅된 영역으로 전송됩니다.

그림 1은 네트워크 망원경이 (D)DoS 후방 산란을 포착하는 방법을 보여줍니다(상단의 빨간색 선을 따라). 표시된 공격은 3자 TCP 핸드셰이크의 첫 번째 패킷 유형을 포함하는 `TCP SYN` 플러드 공격의 예입니다. 이 패킷의 소스 IP 주소는 공격자가 임의로 스푸핑한 IP 주소로 설정합니다. 피해자는 해당 링크가 공격으로 인해 포화 상태가 아닌 경우 `SYN` 패킷을 수신하면 핸드셰이크 응답, 즉 `SYN|ACK`으로 응답할 수 있습니다. 스푸핑된 주소가 네트워크 텔레스코프의 주소 공간 내에 있는 경우, 응답 패킷은 공격 패킷의 실제 소스가 아닌 텔레스코프로 전송되어 패킷을 수집하고 분석할 수 있습니다.

저희는 무어 등[8]이 설명한 탐지 및 분류 방법을 구현하여 UCSD-NT 데이터에서 무작위로 스푸핑된 공격을 식별했습니다. 이 과정과 데이터 소스에 대한 자세한 설명은 IMC 2017 논문 [9]에서 확인할 수 있습니다.

UCSD-NT는 IPv4 주소 공간의 약 *1/256을 차지합니다.* 즉, 무작위로 균일하게 스푸핑된 IP 주소를 가진 많은 패킷을 사용하는 공격과 같은 상당한 규모의 공격은 이 다크넷에서 탐지될 가능성이 높다는 뜻입니다.

반사 및 증폭 공격 공격에 대한 두 번째 데이터 소스는 AmpPot 프로젝트에서 제공합니다. 이



새로운 오픈 소스 허니팟은 반사기를 모방하여 반사 및 증폭 공격을 추적하는 것을 목표로 합니다. 공격자의 관심을 끌기 위해 AmpPot은 반사 공격에 악용되는 것으로 알려진 여러 프로토콜을 에뮬레이트합니다. 이러한 방식으로 공격자가 리플렉터를 스캔하여 AmpPot을 발견하고 후속 공격에서 "악용"할 수 있으며, 이를 유추하여 기록할 수 있습니다.

그림 1은 AmpPot이 리플렉션 시도를 기록하는 방법을 보여줍니다(아래 빨간색 선 따라). 이 특정 예에서는 위조된 DNS 쿼리가 허니팟으로 전송되어 리플렉션 공격을 유추할 수 있도록 합니다. AmpPot에 대한 자세한 내용은 Kra¨mer 등의 논문을 참조하시기 바랍니다[10].

두 공격 데이터 소스 모두 표적 IP 주소를 제공하며, 이를 메타데이터로 보강하여 표적 특성을 연구할 수 있습니다. 저희는 지리적 위치 정보를 추가하기 위해 *넷어큐리티 엣지 프리미엄 에디션* 데이터[11]를 사용합니다. 또한 *라우트뷰 프리픽스-AS 매핑* 데이터[12]를 사용해 BPG 라우팅 메타데이터를 추가합니다.

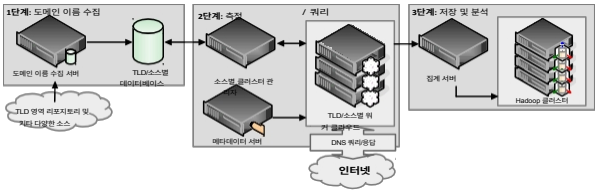


그림 2. OpenINTEL 측정 및 분석 아키텍처.

DNS 측정 데이터 UCSD-NT 및 AmpPot 데이터 세트에는 표적 IP 주소가 포함되어 있습니다. 웹 사이트를 이용한 공격의 잠재적 영향을 평가하려면 IP 주소와 웹 사이트 간의 과거 매핑이 필요합니다. 이 매핑을 얻기 위해 DNS 콘텐츠의 일일 스냅샷을 수집하는 대규모 활성 DNS 측정 플랫폼인 OpenINTEL 프로젝트의 활성 DNS 측정 데이터를 사용합니다[13]. 이 프로젝트는 전체 영역, 즉 최상위 도메인(TLD) 아래의 모든 도메인 이름에 대해 리소스 레코드(RR) 집합을 구조적으로 쿼리하여 스냅샷을 구축합니다. OpenINTEL은 수많은 TLD를 다룹니다. 결과 측정 데이터에는 특히 도메인 이름과 IP 주소 매핑(즉, `A` 레코드)이 포함됩니다.

저희는 OpenINTEL의 창립자 중 한 명으로, 처음부터 개발과 운영에 적극적으로 참여해 왔습니다. 당연히 다른 목적에도 OpenINTEL 데이터를 사용합니다(이에 대해서는 나중에 자세히 설명합니다). 또한 다양한 데이터를 융합하고 분석하기 위해 OpenINTEL 아키텍처를 활용하고 있습니다.

그림 2는 아키텍처를 간략하게 보여줍니다. 1단계는 영역(즉, TLD) 수집을 위한 단계입니다. 2단계는 일일 측정과 관련이 있습니다. 그리고 3단계는 데이터 저장 및 분석과 관련이 있습니다.

보호 서비스 사용 유추 DDoS 보호 서비스(DPS)의 사용에는 네트워크 트래픽을 우회하기 위해 DNS 또는 BGP를 사용하는 것이 포함됩니다. OpenINTEL은 다양한 DNS 기반 우회 메커니즘 기반 네트워크 트래픽 전환을 위해 BGP 라우팅 정보를 고려합니다. 이를 위해 OpenINTEL 데이터의 IP 주소 레코드를 자율 시스템 번호로 보완합니다. 이는 UCSD-NT 및 AmpPot 공격 데이터에서 공격 대상 IP 주소를 보강한 방법과 유사하게 수행됩니다. 방법론에 대한 자세한 내용은 IMC 2016 논문[14]에 설명되어 있습니다. 보호 서비스는 *상시* 또는 *온디맨드* 방식으로 사용할 수 있다는 점에 유의하세요.

BGP 블랙홀링 추론 사용 공개적으로 사용 가능한 BGP 라우팅 데이터에서 Giotsas 등이 설명한 방법론에 따라 구현된 확장 가능한 맞춤형 측정 시스템을 사용하여 BGP 블랙홀링 이벤트를 추론합니다[15]. 우리는 두 가지 프로젝트의 데이터를 사용합니다: *(i) 오리건* 대학교의 *RouteViews 프로젝트(RV)*; 그리고 *(ii)* RIPE NCC의 *라우팅 형성 서비스(RIS)*. BGP 데이터 내에서 블랙홀링 요청을 알 릴 가능성이 있는 커뮤니티로 태그가 지정된 BGP 공지를 찾습니다. 그림 1은 BGP 경로 수집기의 데이터를 통해 블랙홀링 활동(피해자의 AS에서 비롯된 파란색 점선)을 유추할 수 있음을 보여줍니다. 데이터의 각 블랙홀링 이벤트에는 특히 다음과 같은 내용이 포함되어 있습니다:

(i) 블랙홀 접두사, *(ii)* 활성화 시간, *(iii)* (선택적) 비활성화 시간. 자세한 내용은 IMC 2018 백서 [16]를 참조하시기 바랍니다.

이 의존하는 DNS 레코드를 측정합니다. 이를 통해 OpenINTEL 데이터에서 DNS 기반 우회를 추론하는 방법론을 고안할 수 있습니다. 특히 A, CNAME 및 NS 레코드로부터 DPS 사용을 추론합니다. BGP-를 추론하려면

출처	#이벤트	#대상	#/24s	#/16s	#ASN
UCSD-NT	12.47 M	2.45 M	0.77 M	31057	25990
AmpPot	8.43 M	4.18 M	1.72 M	41678	24432
결합	20.90 M	6.34 M	2.19 M	43041	32580

표 I

DoS 공격 이벤트 데이터. 다음에서 2년간의 데이터를 고려합니다. UCD-NT 및 앰팟.

시작	#days	출처	#웹 사이트	#데이터 포인트	크기
2015-03	731	.com	173.7 M	1045.9 G	23.5TiB
		.net	21.6 M	121.0 G	2.8TiB
		.org	14.7 M	90.7 G	2.1 TiB
		결합	210.0 M	1257.6 G	28.4TiB

표 II

활성 DNS 데이터 세트. 당사는 오픈인텔 플랫폼에서 수집한 2년간의 DNS 데이터를 사용하여 .com, .net, .org gtld에 대한 웹 사이트 및 관련 IP 주소를 추론합니다.

III. 공격의 특성 분석

인터넷 전반의 공격 활동을 특성화하기 위해 이전에 확인된 DoS 활동에 대한 데이터 소스로부터 구축된 두 가지 데이터 세트를 분석합니다. 두 데이터 세트는 모두 2년(2015년 3월 1일~2017년 2월 28일)의 기간을 다루며, 설명하는 공격 유형 측면에서 서로를 보완합니다.

표 1은 두 데이터 세트를 요약한 것입니다. 두 데이터 세트를 합치면 2년 동안 *634만 개의* 고유 IP 주소를 대상으로 한 약 2,100만 건의 공격이 발생했습니다. 관찰된 공격은 다음과 같습니다.

하나 이상의 대상을 호스팅하는 고유한 /24 네트워크 블록은 219만 개로, 최근 인터넷에서 활성화된 것으로 추정되는 *~650만* /24 블록의 약 1/3에 해당합니다[17], [18].

특정 공격이 발생한 시점에 공격받은 IP 주소에 매핑된 www 레이블에서 A 레코드를 찾아 공격의 영향을 받을 가능성이 있는 웹사이트를 식별합니다. 당사는

의 하위 집합을 측정합니다. 특히 전 세계 도메인 네임스페이스의 약 *50%를* 차지하는 com, net, org의 세 가지 일반 TLD(gTLD)에 대한 데이터를 사용합니다. 표 II는 데이터 세트의 세부 사항을 보여줍니다. 총 2억 *1천만 개의* 웹사이트를 추론합니다.

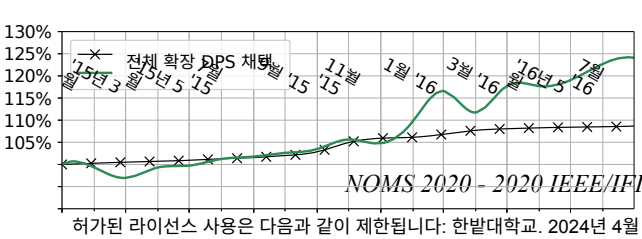
572k의 웹 사이트 연관성을 발견했습니다.
공격 데이터에 포함된 634만 개의 고유 표적 IP 주소. 이는 표적이 된 고유 IP 주소 중 최소 *9%가* 하나 이상의 웹사이트를 호스팅한다는 의미입니다.

여러 웹 사이트가 공격받은 IP 주소를 공유하는 경우가 종종 관찰됩니다. 따라서 단일 IP에 대한 공격은 잠재적으로 수백만 개의 웹 사이트에 동시에 영향을 미칠 수 있습니다. 추가 분석 결과, 많은 공격 대상 IP 주소가 대형 호스트에 속해 있으며 각각 최대 수백만 개의 웹 사이트를 매핑하는 것으로 나타났습니다. 극단적인 경우에는 한 번의 공격으로 최대 *360만 개의* 웹 사이트가 영향을 받을 수 있는 것으로 나타났습니다. 그리고 조사 기간인 2년 동안 2억 *1천만 개로* 추정한 웹 사이트 중 약 3분의 2(*64%*)가 공격의 표적이 된 IP 주소에서 호스팅된 것으로 나타났습니다. 공격의 특징과 공격 대상에 대한 자세한 내용은 이 섹션의 기반이 된 논문(또는 논문)을 참조하시기 바랍니다[9], [19].

IV. 완화 조치 도입 및 운영

이 논문은 클라우드 기반 보호 서비스와 BGP 블랙홀링이라는 두 가지 AS 간 완화 솔루션을 다룹니다.

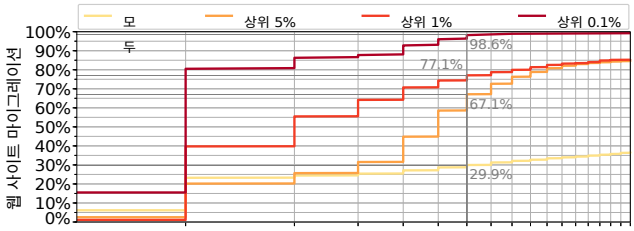
클라우드 기반 보호 서비스 2015년 *Forrester Wave* 보고서 [20]에 나열된 9개 보호 서비스 모두를 중심으로 클라우드 기반 방어 서비스를 제공하는 주요 업체를 연구합니다.[1] 구체적으로 Akamai, CenturyLink, Cloudflare, DOSarrest, F5 Networks, Incapsula, Level 3, Neustar, Verisign이 이에 해당합니다. 당사는 1.5년 동안의 사용량 증가를 연구하고 com, net, org의 세 가지 gTLD를 사용하는 사용자(즉, 웹 사이트)를 고려합니다.



의 대형 업체들이 하루에도 수백만 개의 도메인에 대한 보호를 활성화 또는 비활성화합니다. 또한 보호 서비스가 선택적 권한 있는 네임서버 보호 사용 등의 측면에서 어떻게 사용되는지도 알아봤습니다. 분석에 대한 자세한 내용은 논문 [14]에서 확인할 수 있습니다.

또한 공격을 받은 경험이 DPS 도입에 어느 정도 영향을 미치는지도 조사했습니다. DoS 공격의 표적이 된 후 운영자는 DPS에 보호를 아웃소싱하기 시작할 수 있습니다. DPS 사용에 대한 데이터를 통해 웹 사이트가 DPS를 도입했는지 여부와 시기를 분석할 수 있습니다. 섹션 III에서 이미 공격과 웹사이트를 연결했습니다. 이러한 데이터 세트를 융합하면 어떤 공격이 채택으로 이어지는지 확인할 수 있습니다. 이 프로세스를 *마이그레이션이라고 합니다.*

공격 특성이 마이그레이션에 미치는 영향을 조사했습니다. 그림 4는 공격 강도(가장 느린 CDF)와 정규화된 공격 강도 분포의 *95번째*, *99번째*, *99.9번째* 백분위수에 해당하는 강도로 공격을 받은 웹 사이트에 대해 각각 웹 사이트를 마이그레이션하는 데 걸린 일수의 누적 분포 함수를 보여줍니다. 이러한 CDF를 비교하면 공격과 영향을 받은 사이트가 DPS로 마이그레이션하는 데 걸리는 지연 시간이 크게 줄어든 것을 알 수 있습니다. 공격 이벤트의 강도는 특히 속도 측면에서 DPS로의 이전과 밀접한 상관관계가 있으며, 이는 DDoS 피해와 위험을 완화하는 데 있어 시급함을 직관적으로 시사합니다. 자세한 조사 내용은 [9]를 참조하시기 바랍니다.



100%
95%
90%

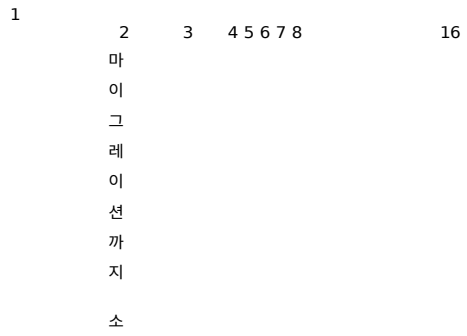


그림 3. DNS의 50%(com, net, org) 에서 DPS 사용량 증가율

그림 3은 데이터 세트 시작 시점과 비교한 9개 제공업체의 성장률을 보여줍니다. 관련된 영역의 전반적인 확장도 보여줍니다. DPS 도입의 추세가 분명해집니다. DPS 사용은 1.5년에 걸쳐 1.24배 증가했으며, 이는 고려된 네임스페이스의 전체 확장(1.09배)을 초과하는 수치입니다. 이 분석을 위해 몇 주 동안의 고객 수를 합친 중간값을 사용하여 사용량의 최고점과 최저점을 평활화했습니다.

또한 웹 호스트와 도메인 소유자 등 제3자가 사용자 기반과 DPS 제공업체 채택에 큰 기여를 하고 있다는 사실도 알게 되었습니다. 일부

1공개적인 방법론을 따르는 자문형 시장 조사 회사입니다.

그림 4. 정규화된 공격 강도의 백분위수에 대한 마이그레이션 지연 시간.

BGP 블랙홀링 BGP 블랙홀링에 초점을 맞춥니다. 섹션 II에서 설명한 대로 생성된 블랙홀링 데이터 세트는 2015년 3월부터 3년 동안의 데이터를 포함합니다. 표 III에 요약이 나와 있습니다.

수집가	#이벤트	#접두사	#출처	#AS 경로
34	1.30 M	146193	2682	31493

공개 BGP 데이터에서 추론한 블랙홀링 데이터 세트.

저희는 공격과 블랙홀 데이터를 공동으로 분석하여 *'블랙홀 공격'을* 찾아냅니다. 공격 대상 IP 주소와 블랙홀 접두사를 대조하여 공격 시작 시간이 블랙홀이 활성화되기 최대 24시간 전이어야 합니다. 이를 통해 공격에 직면했을 때 운영자가 어떻게 행동하는지 연구할 수 있습니다. 이 섹션의 나머지 부분에서는 논문의 일부 결과를 중점적으로 살펴보겠습니다.

그림 5는 블랙홀이 작동하는 데 걸리는 시간을 보여줍니다. 블랙홀 공격의 거의 절반*(44.4%)*이 1분 이내에 블랙홀이 활성화되고 *84.2%가* 활성화되는 것으로 나타났습니다.

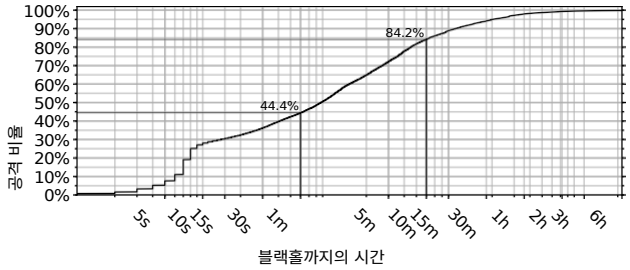


그림 5. UCSD-NT 및 AmpPot 데이터 세트의 블랙홀 공격에 대한 공격 시작과 블랙홀링 발생 사이의 시간 분포.

10분 이내입니다. 이러한 시간은 자동화된 탐지 및 완화 기능을 사용해야 함을 시사합니다. 블랙홀 공격의 *0.02%만이* 블랙홀이 활성화되는 데 6시간 이상이 걸립니다.

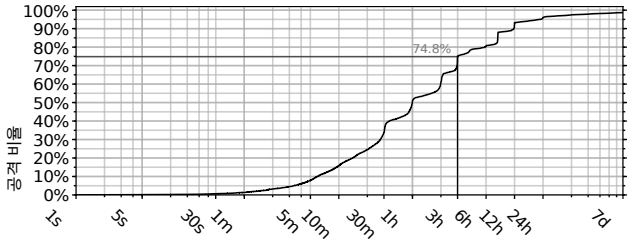


그림 6. AmpPot 데이터 세트에서 공격 종료 시점과 상관관계가 있는 블랙홀 이벤트 종료 시점 사이의 시간 분포.

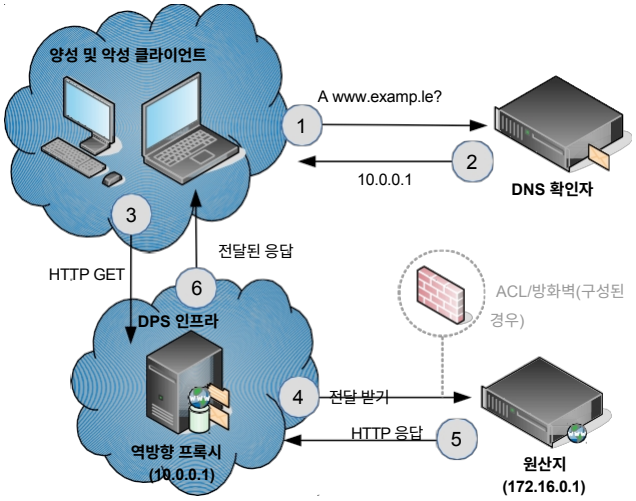
그림 6은 AmpPot 데이터 세트에서 블랙홀 공격이 종료된 시점과 관련 블랙홀 이벤트의 비활성화 시간 사이의 시간을 보여줍니다.[2] *96.1%의 블랙홀* 공격의 경우 24시간 이내에 비활성화됩니다. *3.9%의* 경우 며칠이 걸릴 수도 있습니다. 이러한 결과는 블랙홀링 복구에 자동화가 부족하다는 것을 시사하며, 블랙홀링의 부작용(블랙홀링 접두사로 향하는 *모든* 트래픽을 완전히 차단)이 공격 지속 시간 이상으로 확대되어 자해성 DoS에 해당할 수 있음을 강조합니다.

곡선)의 강도는 최대 $100ps_{max}$ 이며, 이는 대략 *300Mbps의* 공격 트래픽 양에 해당합니다. 이는 전체 공격의 *91.1%에* 해당합니다(검은색 곡선). 무시할 수 없는 비율의 블랙홀 공격은 강도가 낮습니다. 특히 *13.1%는* 최대 $1ps_{max}$ *(3Mbps)*의 강도를 보입니다. 이 결과는 운영자가 블랙홀링과 같은 극단적인 방법으로 무작위 스푸핑 공격의 강도를 완화한다는 것을 보여주며, 공격자가 DoS를 자행하기 위해 얼마나 적은 노력을 기울여야 하는지에 대한 의문을 제기합니다. 우리의 앰프팟 데이터 세트의 블랙홀 공격 분석에서도 비슷한 결과가 나왔습니다. 여기서 다룰 수 없는 이러한 결과와 그 밖의 다른 결과에 대해서는 백서를 참조하시기 바랍니다[16].

V. 완화 솔루션을 통한 숨겨진 위험

여기에서는 클라우드 기반 보호 서비스 사용의 주요 단점인 공격자가 소위 "오리진 노출"로 인해 보호 기능을 우회하고 비효율적으로 만든다는 사실을 강조하고 정량화합니다.

2장에서 처음 설명한 것처럼 보호 서비스에는 *트래픽 우회가* 필요합니다. 즉, 트래픽은 보호 서비스의 보안 인프라를 통해 라우팅되어야 합니다. 그림 8은 DNS를 사용할 때 이것이 어떻게 작동하는지에 대한 개략도를 보여줍니다.



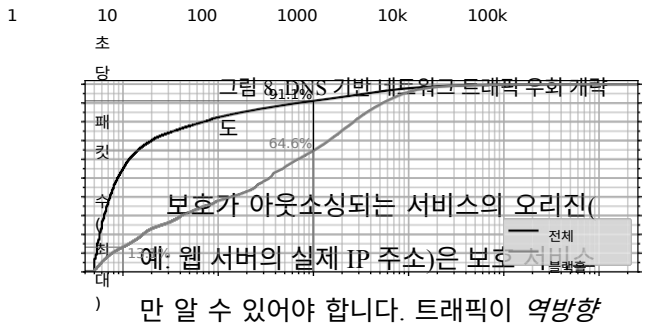


그림 7. UCSD-NT 데이터 세트의 모든 공격(검은색 곡선)과 블랙홀이 적용된 공격(회색 곡선)에 대한 강도 분포.

UCSD-NT 데이터 세트에는 초당 관측된 최대 후방 산란 패킷 수로 표시되는 공격 강도 측정값(pps_{max})이 포함되어 있습니다. 그림 7은 모든 공격과 블랙홀 공격에 대해서만 이러한 강도의 분포를 보여줍니다. 블랙홀 공격의 *64.6%*(회색

2블랙홀링은 UCSD-NT 데이터에서 공격 종료 시간을 "잘라내기" 때문에 무작위로 스푸핑된 공격에 대한 비활성화 지연은 분석하지 않습니다[16].

그림 8. DNS 기반 네트워크 트래픽 우회 개략도

보호가 아웃소싱되는 서비스의 오리진(예: 웹 서버의 실제 IP 주소)은 보호 서비스만 알 수 있어야 합니다. 트래픽이 *역방향 프록시를* 통과해야 하기 때문입니다(그림 8 참조). 원본 IP 주소를 학습할 수 있는 다양한 '벡터'가 있습니다.

DNS 구성 측면에서 이는 DNS 구성에 출처의 흔적을 남기거나 OpenINTEL이 제공하는 기록 DNS 데이터를 통해 노출되도록 하는 것으로 요약됩니다. 저희는 다양한 DNS 기반 벡터를 조사하며, 이에 대한 자세한 설명은 CNSM 2017 논문[21]에서 확인할 수 있습니다. 이러한 벡터와 OpenINTEL 데이터를 사용하여 Alexa 상위 100만 목록에 있는 웹 사이트의 출처에 대한 *후보* IP 주소를 찾고 클라우드 기반 보호를 사용합니다. 웹 사이트는 § IV의 9개 보호 서비스 중 8개 서비스의 보호를 받는 것으로 간주합니다(CenturyLink는 DNS 기반 보호 서비스를 지원하지 않습니다.

우회). 후보 주소를 확보한 후 직접 HTTP 요청을 전송하여 보호 우회를 시도합니다. 그런 다음 결과 HTTP 콘텐츠를 일반 요청(즉, 역방향 프록시를 통해)을 통해 검색된 콘텐츠와 비교합니다. 한 트리에서 다른 트리로 이동하는 편집 작업(삽입, 삭제, 대체)의 수를 계산하는 Zhang과 Shasha의 트리-편집 거리 알고리즘에 기반한 DOM-트리 비교 방법을 사용하여 전체 웹사이트의 *40.5%에서* 보호를 우회할 수 있는 것으로 간주되는 것을 발견했습니다. 이는 10884개 웹 사이트 중 4408개에 해당합니다.

또한 노출된 웹 사이트와 공격 데이터를 대조한 결과, 4408개의 웹사이트 중 843개의 출처가 DPS로 보호를 시작한 후 공격을 받은 것으로 나타났습니다. 이는 노출된 전체 웹사이트의 *19%에 해당하는 수치입니다.* 이러한 결과는 보호 서비스를 효과적으로 사용하려면 올바른 관리와 구성이 필요하다는 것을 뒷받침합니다.

VI. 요약

DDoS 공격이 급증하면서 개인 사업자부터 정부에 이르기까지 많은 사람들이 DDoS 문제에 가장 효과적으로 대처하는 방법에 대해 의문을 품고 있습니다. 우리는 정확히 무엇을 방어하고 있을까요? 방어 솔루션은 실제로 어떻게 운영되고 있을까요? 그리고 운영자, 즉 최종 사용자는 방어 솔루션의 어떤 위험에 주의해야 할까요? 이러한 질문은 당연히 많은 사람들이 궁금해하는 질문 중 하나입니다. 논문을 시작할 때 우리는 이러한 질문과 관련된 다양한 문제를 확인했으며, 그 중 일부는 *기술적인* 성격이 강하고 일부는 *사회적인* 성격이 더 강합니다. 저희는 주로 기술적 문제에 초점을 맞추기 시작했고, DDoS 공격에 대한 대규모의 과학적 보고가 없다는 점이 이 논문의 원동력이 되었습니다.

이 백서에서는 논문의 일부 결과를 강조합니다. 특히 공격과 공격 대상에 대한 엄격한 특성 분석, 다양한 방어 솔루션의 도입과 운영에 대한 연구, 방어 솔루션의 효과를 완전히 무력화시킬 수 있는 운영 및 배포상의 실수에 대한 조사를 통해 얻은 일부 결과를 요약합니다.

이 백서에 요약되어 있는 다양한 기존 데이터 소스가 없었다면 이러한 작업은 불가능했을 것입니다. 전 세계 인터넷 측정 인프라의 다양한 데이터를 보유하고 있더라도 이를 융합하고 추가 처리하여 대규모 공격 및 방어 체계를 연구하는 것은 간단한 문제가 아닙니다. 하지만 이 작업을 성공적으로 수행함으로써 새로운 인사이트를 얻었고 더 많은 기여를 할 수 있는 기반을 마련했습니다.

이 논문에서는 기술적 한계를 극복하면 사회적 공헌을 실현할 수 있음을 보여줍니다. 특히, 연구 커뮤니티와 네트워크 운영자뿐만 아니라 사회적 문제를 다루는 정책 입안자와 규제 당국에도 정보를 제공할 수 있었습니다. 이를 통해 저희의 연구를 더욱 검증하고 과학적 기여 이상의 의미를 부여할 수 있다고 생각합니다.

참조

[1] A. Garg, J. Curtis, H. Halper, "IT 보안 침해의 재정적 영향 정량화", *정보 관리 및 컴퓨터 보안*, 11권 2호, 74-83페이지, 2003.

[2] B. 크렙스, "은행에 대한 DDoS 공격으로 90만 달러의 사이버 범죄자가 숨어들다" , https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000- cyberheist/, 2013년 2월.

[3] T. 조던과 P. 테일러, *핵티비즘과 사이버 전쟁: 대의명분을 가진 반란군?* Routledge, 2004.

[4] D. E. 데닝, "행동주의, 핵티비즘, 사이버 테러리즘: 외교 정책에 영향을 미치는 도구로서의 인터넷", *네트워크와 네트워크 전쟁: 테러, 범죄, 무력의 미래*, 239권, 288쪽, 2001.

[5] R. A. Paulson과 J. E. Weber, "사이버 왜곡: 온라인 게임 회사에 대한 분산 서비스 거부 공격 개요", *정보 시스템 이슈*, 7권 2호, 52-56페이지, 2006.

[6] S. Hilton, "10월 21일 금요일의 Dyn 분석 요약", http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, 2016년 10월.

[7] "UCSD 네트워크 망원경 (UCSD-NT)", http://www.caida.org/projects/network telescope/, 2010.

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, S. Savage, "인터넷 서비스 거부 활동 추론", *ACM Transactions on Computer Systems*, 24권 2호, 115-139페이지, 2006.

[9] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, A. Dainotti, "수백만 개의 표적이 공격받고 있습니다: DoS 생태계의 거시적 특성 분석," *2017 인터넷 측정 컨퍼런스 논문집*, 2017, 100-113쪽.

[10] L. 크라우머, J. 크루프, D. 마키타, T. 니시조에, T. 코이데, K. 요시오카, 그리고
C. Rossow, "AmpPot: 증폭 디도스 공격 모니터링 및 방어", *침입 탐지의 최근 발전에 관한 국제 워크숍*, 2015, 615-636쪽.

[11] D. Element, "Netacuity 엣지 프리미엄 에디션" , http://www.digitalelement.com/solutions/netacuity-edge-premium.

[12] "라우트뷰 접두사를 IPv4 및 IPv6용 AS 매핑 데이터세트(pfx2as)로 전환", http://www.caida.org/data/routing/routeviews-prefix2as.xml.

[13] R. van Rijswijk-Deij, M. Jonker, A. Sperotto 및 A. Pras, "대규모 액티브 DNS 관리를 위한 고성능 확장형 인프라," *IEEE Journal on Selected Areas in Communications*, 34권 6호, 1877-1888페이지, 2016.

[14] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, A. Pras, "DDoS 보호 서비스 도입 측정", *2016 ACM 인터넷 측정 컨퍼런스 논문집*, 2016, 279-285쪽.

[15] V. Giotsas, P. Richter, G. Smaragdakis, A. Feldmann, C. Dietzel, 및 A. Berger, "인터넷에서 BGP 블랙홀링 활동 추론", 2017 *인터넷 측정 컨퍼런스 논 문 집* , 2017, 1-14쪽.

[16] M. Jonker, A. Pras, A. Dainotti, A. Sperotto, "DoS 공격과 BGP 블랙홀링에 대한 최초의 공동 연구", *2018 인터넷 측정 컨퍼런스*, 2018, 457-463쪽.

[17] S. Zander, L. L. Andrew, G. Armitage, "Capturing Ghosts: 관찰되지 않은 주소를 유추하여 사용된 IPv4 공간 미리 파악하기," 2014 *ACM 인터넷 측정 컨퍼런스 논문집*, 2014.

[18] P. Richter, G. Smaragdakis, D. Plonka 및 A. Berger, "Beyond Counting: 활성 IPv4 주소 공간에 대한 새로운 관점", *2016 ACM 인터넷 측정 컨퍼런스 진행 자료*, 2016.

[19] M. Jonker, "DDoS 완화: 측정 기반 접근 방식," 박사 학위 논문, 트벤테 대학교, 2019, https://doi.org/10.3990/1.9789036548687.

[20] R. Holland and E. Ferrara, "The Forrester $^{\text{WaveTM}}$: DDoS 서비스 제공업체(2015년 3분기)", Forrester Research, Inc. Rep., July 2015.

[21] M. Jonker와 A. Sperotto, "DDoS 보호 서비스의 노출 측정", *제13회 네트워크 및 서비스 관리 국제 컨퍼런스(CNSM'17)*, 2017, 1-9페이지.