DDoS Mitigation: A Measurement-Based Approach

Mattijs Jonker, Anna Sperotto, and Aiko Pras 트벤테 대학교, 엔스헤데, 네덜란드

요약 - 사회는 글로벌 커뮤니케이션을 위해 인터넷에 크게 의존합니다. 동시에 인터넷 안정성과 신뢰성은 지속적으로 고의적인 위협의 대상이 됩니다. 이러한 위협에는 잠재적으로 치명적일 수 있는 (분산) DDoS(서비스 거부) 공격이 포함됩니다. DDoS로 인해 기업은 매년 수억 달러의 손실을 입습니다. 더욱이 중요한 인프라의 경우 국가 안전과 심지어 생명까지 위험에 처할 수 있습니다. 따라서 효과적인 방어가 절대적으로 필요합니다. 쉽게 사용할 수 있는 완화 솔루션의 잠재 사용자는 선택할 수 있는 다양한 모양과 크기가 있다는 것을 알게 되지만, 그 모양과 크기가 항상 명확하지는 않을 수 있습니다. 또한 완화 솔루션의 배포 및 운영에는 더 잘 이해해야 하는 숨겨진 위험이 있을 수 있습니다. 정책 입안자와 정부는 또한 국가 차원에서 사이버 안전을 증진하기 위해 무엇을 해야 하는지에 대한 질문에 직면해 있습니다. 따라서 DDoS에 대처하기 위한 최적의 행동 방침을 개발하는 것은 사회적 문제를 야기하기도 합니다. DDoS 문제가 새로운 것은 아니지만 문제의 규모는 여전히 불분명합니다. 우리는 우리가 방어하고 있는 것이 무엇인지 정확히 알지 못하며 공격에 대해 더 잘 이해하는 것은 문제를 정면으로 해결하는 데 필수적입니다. 상황 인식을 발전시키기 위해서는 여전히 많은 기술적, 사회적 과제를 해결해야 합니다. 전반적인 인터넷 보안을 개선하기 위해 DDoS 문제를 더 잘 이해하는 것이 매우 중요하다는 점을 감안할 때, 이 백서에서 요약하는 논문에는 세 가지 주요 기여가 있습니다. 첫째, 공격과 공격 대상을 대규모로 엄격하게 특성화합니다. 둘째, 다양한 완화 솔루션의 인터넷 전반적 채택, 배포 및 운영 사용에 대한 지식을 발전시킵니다. 마지막으로, 완화 솔루션을 완전히 무력화시킬 수 있는 숨겨진 위험을 조사합니다.

색인 용어 - 서비스 거부, DDoS, 공격, 완화, 인터넷 측정

I. INTRODUCTION

우리의 주요 통신 체계는 포위 공격을 받고 있습니다. 인터넷의 진화는 현대 사회에 혁명적인 영향을 미쳤습니다. 교육 기관, 연구 센터 등을 상호 연결하는 기술로 시작된 것이 지난 30여 년 동안 글로벌 커뮤니케이션을 장악했습니다. 인터넷은 현대 사회의 필수적인 부분이 되었으며 무엇보다도 상거래, 기술 및 엔터테인먼트와 관련이 있습니다. 우리는 커뮤니케이션을 위해 인터넷에 의존하고 있기 때문에 많은 사람들이 당연하게 여기는 인터넷의 가용성이 매우 중요합니다. 인터넷의 중요한 구성 요소는 원래 복원력을 염두에 두고 설계되었지만, 오늘날 인터넷의 안정성과 신뢰성은 파괴적인 DDoS 공격을 비롯한 고의적인 위협에 지속적으로 노출되어 있습니다. DDoS 현상에 대한 엄격한 특성과 관련 위험을 완화하기 위한 대책이 누락되어 있으며 많은 분석 과제에 직면해 있습니다. 이 논문은 공격 및 완화 솔루션을 특성화하기 위해 측정 기반 접근 방식을 취함으로써 이 미해결 문제를 정확하게 해결합니다. 우리의 업무는 상황 인식을 발전시키고 인터넷 연구, 네트워크 운영 및 정책 입안자에게 증가하는 DDoS 위협에 대해 알릴 수 있는 능력을 보여줍니다.

A. DDoS Attacks

지난 수십 년 동안 DDoS 공격은 발생률과 강도 면에서 급격히 증가하여 인터넷의 안정성과 신뢰성에 대한 가장 큰 위협 중 하나가 되었습니다. 이름에서 알 수 있듯이 서비스 거부 공격은 공격자가 서비스 거부를 달성하는 데 사용됩니다. 본질적으로, 이것은 가능한 모든 수단을 동원하여 네트워크, 즉 인터넷에서 네트워크 서비스를 차단하는 것을 수반합니다. 공격자의 동기는 매우 다양할 수 있으며, 여기에는 다른 악의적인 활동(예: 데이터 도난 마스킹[1], [2]), 핵티비즘(예: 정치적 동기의 공격)[3], [4] 또는 사이버 갈취(예: 몸값을 지불하지 않으면 은행이 전자 뱅킹 애플리케이션을 중단하도록 위협하는 것)[5]가 포함되지만 이에 국한되지 않습니다. 공격이 성공하면 파급 효과가 발생하고, 연쇄적인 오류가 발생하며, 잠재적으로 인터넷에 막대한 영향을 미칠 수 있습니다[6]. DDoS 위협에 직면했을 때 효과적인 방어는 절대적으로 필요합니다.

B. Mitigation Solutions

DDoS 문제가 급증하면서 다양한 완화 솔루션이 개발되었으며 상용 제품 시장이 호황을 누리고 있습니다. 일반적으로 말하자면, 공격 트래픽이 수렴되어 피해를 입히기 시작하기 전에 공격에 대한 방어가 소스에 더 가깝게 수행되는 것이 좋습니다. 반면에 탐지는 일반적으로 해를 끼치는 대상에 더 가깝게 수행하는 것이 좋습니다. 이 때문에 입증된 다양한 솔루션은 도메인 간에 이루어지며, 이는 탐지를 위한 원격 분석 정보와 완화를 위한 사후 제어 조치가 조직 경계를 넘어 교환된다는 것을 의미합니다. 인터넷에서 완화 솔루션의 채택에 대한 정량적 지식은 제한적입니다. 또한 운영자가 공격에 직면했을 때 어떻게 배포되고 운영되는지에 대한 이해가 부족합니다.

C. Hidden Hazards

완화 솔루션을 쉽게 사용할 수 있지만 설정의 용이성과 사용자의 전문 지식 사이에는 잠재적인 단절이 있습니다. 솔루션 제공업체는 낮은 채택 장벽을 제공함으로써 이점을 얻을 수 있습니다. 종종 그들은 신속한 제품(또는 서비스) 배포를 활용하려고 하는데, 이는 위기 상황(즉, 공격을 받았을 때)에 필요한 것이기 때문입니다. 그러나 노련한 네트워크 운영자 및 보안 엔지니어가 아닌 사용자가 특정 완화 기술을 사용할 때 직면할 수 있는 잠재적인 함정은 무엇입니까? 솔루션을 비효율적으로 만들 수 있는 숨겨진 위험이 있습니까?

D. Challenges

DDoS 완화와 관련하여 다음을 포함하되 이에 국한되지 않는 많은 과제가 있습니다: (i) 우리가 방어하고 있는 것이 무엇인지 정확히 아는 데 어려움이 있습니다. (ii) 완화 솔루션의 채택 및 운영과 관련된 문제. 이 논문은 처음부터 우리가 직면한 기본적인 과제가 데이터와 관련이 있음을 보여줍니다. DDoS 문제를 방법론적으로 연구하기 위해 다양한(원시) 데이터 소스를 수집하고 개발하는 것은 그 자체로 어려운 일입니다. 우리는 이러한 문제를 극복하는 데 크게 기여합니다.

E. Approach

우리가 취하는 접근 방식은 측정 기반입니다. 우리는 다양한 독립 데이터 유형을 수집하기 위해 전 세계의 다양한 유리한 지점에서 대규모 수동 및 능동 측정을 사용합니다. 이러한 데이터 처리의 어려움을 감안할 때 Big Data Analytics를 적용하여 데이터 세트를 융합, 도출 및 분석합니다. 이 과정에서 해당되는 경우 기존 측정 방법론을 식별 및 검증하고 필요한 경우 새로운 측정 방법론을 고안합니다.

F. Contributions

데이터를 성공적으로 융합함으로써 (i) 글로벌 공격 활동에 대한 놀라운 통계를 공개합니다. (ii) 인터넷 전반의 완화 솔루션 채택 및 사용자의 운영 관행에 대한 통찰력을 얻습니다. (iii) 배치 및 운영 실수의 바람직하지 않은 부작용을 드러내고 조사합니다. 또한, 기존 방법론을 추가로 검증하고(즉, 이전 검증 노력을 보완하는 작업) 일부 데이터를 연구 커뮤니티에서 사용할 수 있도록 합니다. 우리가 무엇에 대해 방어하고 있는지 아는 측면에서 우리는 공격의 대규모 특성을 제시합니다. DDoS 문제의 거대한 규모를 공개합니다. 당사의 특성화에 따르면 약 2,100만 건의 공격이 발생했으며, 특히 인터넷에서 활동하는 것으로 추정되는 모든 /24 네트워크의 1/3이 최근 2년 간의 관찰 기간 동안 최소 한 번의 공격을 받은 것으로 나타났습니다. 또한 완화 솔루션의 채택 및 운영에 대한 이해를 증진합니다. 특히 클라우드 기반 보호 서비스와 BGP 블랙홀링이라는 두 가지 도메인 간 솔루션에 중점을 두고 채택 및 운영 관행에 대한 글로벌 동향을 밝힙니다. 마지막으로, 우리의 작업은 배포 및 운영에서 실수가 발생하여 일부 운영자와 사용자에게 잘못된 보안 인식을 남긴다는 것을 뒷받침합니다. 우리의 연구는 또한 공격자가 이러한 실수를 방어를 우회할 수 있는 기회로 삼을 수 있다는 개념을 뒷받침합니다.

G. Organization

이 문서의 나머지 부분은 다음과 같이 구성되어 있습니다. § II에서는 식별, 개발 및 사용한 기본 데이터 원본을 간략하게 설명합니다. § II-A에서 공격의 특성을 제시합니다. § IV에서는 완화 솔루션으로 관심을 옮깁니다. 다음으로 § V에서는 이러한 솔루션과 관련된 숨겨진 위험에 대한 분석을 제시합니다. 마지막으로, § VI에서 우리의 작업을 요약합니다.

II. DATA SOURCES

A. Data on (D)DoS Activity

우리는 (D)DoS 활동의 글로벌 지표를 제공하는 두 개의 고유한 데이터 소스를 식별했습니다. 첫째, UCSD Network Telescope(UCSD-NT)는 무작위로 균일하게 스푸핑된 IP 주소와 관련된 DoS 공격의 증거를 캡처합니다. 둘째, AmpPot 허니팟은 반사 및 증폭 DoS 공격(특히 스푸핑된 IP 주소와 관련된 공격 유형)을 캡처합니다.

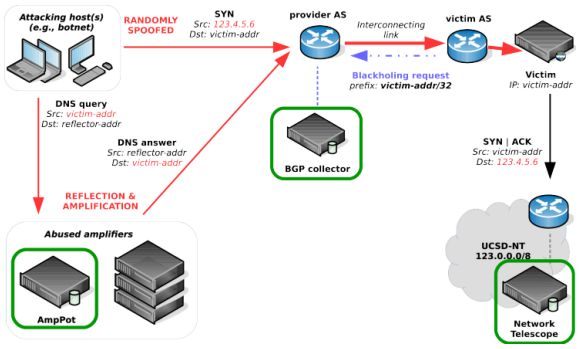

그림 1. 3개의 데이터 소스에 대한 측정 시스템의 배치에 대한 조감도. 특히 데이터 및 블랙홀링 관찰을 공격합니다.

무작위 스푸핑 공격 UCSD-NT는 샌디에이고 캘리포니아 대학교에서 운영하는 대규모 사용되지 않지만 라우팅된 /8 네트워크입니다. [7] 네트워크 망원경, 즉 다크넷은 서비스 거부 공격 등으로 인한 스캔, 구성 오류, 버그 및 백스캐터로 인해 발생하는 원치 않는 트래픽을 호스트가 포함되지 않은 주소 공간의 라우팅된 영역으로 보내는 트래픽을 수동적으로 수집합니다. 그림 1은 네트워크 망원경이 (D)DoS 후방 산란을 포착하는 방법을 보여줍니다(상단의 빨간색 선을 따라). 표시된 공격 예는 3방향 TCP 핸드셰이크의 첫 번째 패킷 유형을 포함하는 TCP SYN 플러드 공격입니다. 이러한 패킷의 소스 IP 주소는 공격자가 임의로 스푸핑한 IP 주소로 설정됩니다. 피해자는 링크가 공격에 의해 (아직) 포화되지 않은 경우 SYN 패킷을 수신하면 핸드셰이크 응답, 즉 SYN|ACK로 응답할 수 있습니다. 스푸핑된 주소가 네트워크 망원경의 주소 공간 내에 있는 경우 응답 패킷은 패킷을 수집하고 분석할 수 있는 망원경(공격 패킷의 실제 소스가 아닌)으로 전송됩니다. Moore 등[8]이 설명한 탐지 및 분류 방법론을 구현하여 UCSD-NT 데이터에서 무작위로 스푸핑된 공격을 식별했습니다. 이 프로세스와 데이터 소스에 대해서는 IMC 2017 백서[9]에서 자세히 설명합니다. UCSD-NT는 IPv4 주소 공간의 약 1/256을 커버합니다. 즉, 임의의 균일하게 스푸핑된 IP 주소를 가진 많은 패킷과 관련된 대규모 공격이 이 다크넷에서 볼 수 있습니다.

반사 및 증폭 공격 공격에 대한 두 번째 데이터 소스는 AmpPot 프로젝트에서 제공합니다. 이 새로운 오픈 소스 허니팟은 반사경을 모방하여 반사 및 증폭 공격을 추적하는 것을 목표로 합니다. 공격자에게 어필하기 위해 AmpPot은 반사 공격에서 악용되는 것으로 알려진 여러 프로토콜을 에뮬레이트합니다. 이러한 방식으로 AmpPot은 리플렉터를 스캔하는 공격자에 의해 발견될 수 있으며 후속 공격에서 "남용"될 수 있으며, 이를 추론하고 기록할 수 있습니다. 그림 1은 또한 AmpPot이 반사 시도를 기록하기 위해 어떻게 배치되는지를 보여줍니다(빨간색 선을 따라 아래로). 이 특정 예제에서는 위조된 DNS 쿼리가 허니팟으로 전송되어 반사 공격을 추론할 수 있습니다. AmpPot에 대한 자세한 내용은 Kramer et al.의 논문을 참조하십시오[10]. ¨ 두 공격 데이터 소스 모두 대상 특성을 연구하기 위해 메타데이터로 보강할 수 있는 대상 IP 주소를 제공합니다. NetAcuity Edge Premium Edition 데이터[11]를 사용하여 지리적 위치 정보를 추가합니다. 또한 Routeviews Prefix-to-AS 매핑 데이터[12]를 사용하여 BPG 라우팅 메타데이터를 추가합니다.

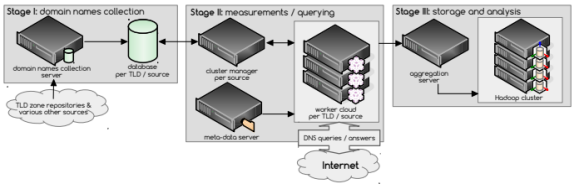

그림 2. OpenINTEL 측정 및 분석 아키텍처.

DNS 측정 데이터 UCSD-NT 및 AmpPot 데이터 세트에는 대상 IP 주소가 포함되어 있습니다. 웹 사이트를 척도로 사용하여 공격의 잠재적 영향을 평가하려면 IP 주소와 웹 사이트 간의 기록 매핑이 필요합니다. 이 매핑을 얻기 위해 DNS 콘텐츠의 일일 스냅샷을 수집하는 대규모 활성 DNS 측정 플랫폼인 OpenINTEL 프로젝트의 활성 DNS 측정 데이터를 사용합니다[13]. RR(리소스 레코드) 집합에 대해 전체 영역, 즉 TLD(TopLevel Domain)의 모든 도메인 이름을 구조적으로 쿼리하여 스냅샷을 구축합니다. OpenINTEL은 많은 수의 TLD를 다룹니다. 결과 측정 데이터에는 특히 도메인 이름과 IP 주소 매핑(즉, A 레코드)이 포함됩니다. 우리는 OpenINTEL의 창립자 중 하나이며 처음부터 개발 및 운영에 적극적으로 참여해 왔습니다. 당연히 OpenINTEL 데이터는 다른 목적으로도 사용됩니다(나중에 자세히 설명). 또한 OpenINTEL 아키텍처를 사용하여 다양한 데이터를 융합하고 분석합니다. 그림 2는 아키텍처를 간략하게 보여 줍니다. 1단계는 영역(즉, TLD) 수집을 위한 것입니다. Stage II는 일일 측정과 관련이 있습니다. 그리고 3단계는 데이터 저장 및 분석과 관련이 있습니다.

보호 서비스 사용 유추 DPS(DDoS Protection Services)를 사용하려면 DNS 또는 BGP를 사용하여 네트워크 트래픽을 전환해야 합니다. OpenINTEL은 다양한 DNS 기반 전환 메커니즘이 의존하는 DNS 레코드를 측정합니다. 이를 통해 OpenINTEL 데이터에서 DNS 기반 전환을 추론하는 방법론을 고안할 수 있습니다. 특히 A, CNAME 및 NS 레코드에서 DPS 사용을 유추합니다. BGP 기반 네트워크 트래픽 전환을 유추하기 위해 BGP 라우팅 정보를 고려합니다. 이를 위해 OpenINTEL 데이터의 IP 주소 레코드를 자율 시스템 번호로 보완합니다. 이 작업은 UCSD-NT 및 AmpPot 공격 데이터에서 공격 대상 IP 주소를 보강하는 방법과 유사합니다. 방법론에 대한 자세한 내용은 IMC 2016 백서 [14]에 설명되어 있습니다. 보호 서비스는 상시 또는 온디맨드 방식으로 사용할 수 있습니다.

BGP 블랙홀링 사용 추론 Giotsas et al. [15]에서 설명한 방법론을 기반으로 구현된 확장 가능한 맞춤형 측정 시스템을 사용하여 공개적으로 사용 가능한 BGP 라우팅 데이터에서 BGP 블랙홀링 이벤트를 추론합니다. 우리는 두 가지 프로젝트의 데이터를 사용합니다: (i) 오레곤 대학교의 RouteViews 프로젝트(RV); (ii) RIPE NCC의 RIS(Routing Information Service)입니다. BGP 데이터 내에서 블랙홀링 요청을 알릴 가능성이 있는 커뮤니티로 태그가 지정된 BGP 알림을 찾습니다. 그림 1은 블랙홀링 활동(피해자의 AS에서 시작된 파란색 점선)이 BGP 경로 컬렉터의 데이터를 통해 유추될 수 있음을 보여줍니다. 데이터의 각 블랙홀링 이벤트에는 (i) 블랙홀 접두사; (ii) 활성화 시간; (iii) (선택 사항) 비활성화 시간. 자세한 내용은 관심 있는 독자를 대상으로 IMC 2018 논문 [16]을 참조하시기 바랍니다.

source	#events	#targets	#/24s	#/16s	#ASNs
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
Combined	20.90 M	6.34 M	2.19 M	43041	32580

TABLE I

DOS 공격 이벤트 데이터. UCSD-NT와 AMPPOT의 2년 치 데이터를 고려합니다.

start	#days	source	#Web sites	#data points	size
2015-03	731	.com	173.7 M	1045.9 G	23.5 TiB
		.net	21.6 M	121.0 G	2.8 TiB
		.org	14.7 M	90.7 G	2.1 TiB
		Combined	210.0 M	1257.6 G	28.4 TiB

TABLE II

활성 DNS 데이터 세트. OPENINTEL 플랫폼에서 수집한 2년간의 DNS 데이터를 사용하여 .COM, .NET, 및 .ORG GTLDs입니다.

III. CHARACTERIZATION OF ATTACKS

인터넷 전반의 공격 활동을 특성화하기 위해 DoS 활동에 대해 이전에 식별된 데이터 소스에서 구축된 두 개의 데이터 세트를 분석합니다. 두 데이터 세트 모두 2년(2015년 3월 1일 – 2017년 2월 28일)을 대상으로 하며 설명된 공격 유형 측면에서 서로를 보완합니다.

표 I에는 두 데이터 세트가 모두 요약되어 있습니다. 당사의 데이터 세트는 2년 동안 634만 개의 고유 IP 주소를 대상으로 하는 거의 2,100만 건의 공격을 차지합니다. 우리는 적어도 하나의 표적을 호스팅하는 총 2.19 M의 고유 한 / 24 네트워크 블록을 관찰했으며, 이는 최근 인터넷에서 활성화 된 것으로 추정되는 ~ 6.5 M / 24 블록의 약 1/3입니다 [17], [18]. Microsoft는 특정 공격 시 공격받은 IP 주소에 매핑된 www 레이블에서 A 레코드를 찾아 공격의 영향을 받을 수 있는 웹 사이트를 식별합니다.

OpenINTEL이 측정하는 TLD의 하위 집합을 사용합니다. 특히, 세 가지 일반 TLD(gTLD) com, net 및 org에 대한 데이터를 사용하며, 이 두 가지를 합치면 전역 도메인 네임스페이스의 약 50%를 차지합니다. 표 II는 데이터 세트의 세부 정보를 보여줍니다. 총 210M개의 웹 사이트를 추론합니다.

공격 데이터에서 6.34M 고유 대상 IP 주소 중 572k에서 웹 사이트 연결 연결을 찾습니다. 즉, 고유하게 타겟팅된 IP 주소 중 9% 이상이 하나 이상의 웹 사이트를 호스팅합니다.

여러 웹 사이트가 공격받은 IP 주소를 공유하는 것을 자주 관찰합니다. 결과적으로 단일 IP에 대한 공격은 수백만 개의 웹 사이트에 동시에 영향을 미칠 수 있습니다. 추가 분석 결과, 많은 대상 IP 주소가 각각 최대 수백만 개의 웹 사이트에 매핑되는 대규모 호스팅 업체에 속한다는 것을 알 수 있습니다. 극단적인 경우 단일 공격에 최대 3.6M 웹 사이트가 포함될 수 있습니다. 그리고 2년 동안 210M으로 추정되는 웹 사이트 중 거의 3분의 2(64%)가 공격의 대상이 된 IP 주소에서 호스팅되었습니다. 공격 및 공격 대상의 특성화에 대한 자세한 내용은 호기심 많은 독자에게 이 섹션의 기반이 되는 논문(또는 논문)[9], [19]을 참조하도록 합니다.

IV. ADOPTION AND OPERATION OF MITIGATION

이 논문에서는 클라우드 기반 보호 서비스와 BGP 블랙홀링이라

는 두 가지 AS 간 완화 솔루션을 다룹니다.

클라우드 기반 보호 서비스 2015년 Forrester Wave 보고서[20]에 나열된 9가지 보호 서비스를 모두 중점적으로 클라우드 기반 완화 분야의 주요 제공업체를 연구합니다.1 특히 Akamai, CenturyLink, Cloudflare, DOSarrest, F5 Networks, Incapsula, Level 3, Neustar, Verisign이 있습니다. 당사는 1.5년 동안의 사용 증가를 연구하고 com, net 및 org의 세 가지 gTLD에 따라 사용자(즉, 웹 사이트)를 고려합니다.

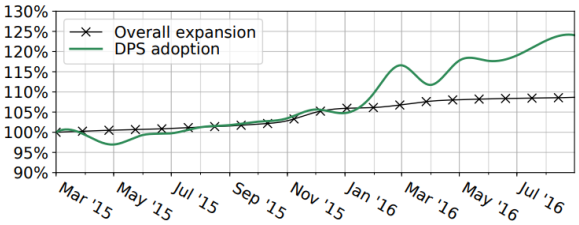

그림 3. DNS(com, net 및 org)의 50%에서 DPS 사용 증가

그림 3은 데이터 집합의 시작과 비교하여 9개 공급자의 성장을 합산한 것을 보여줍니다. 관련된 영역의 전반적인 확장도 표시됩니다. DPS 채택 추세가 뚜렷해집니다. DPS 사용은 1.5년 동안 1.24× 증가했으며, 이는 고려된 네임스페이스의 전체 확장(1.09×)을 초과합니다. 이 분석을 위해 몇 주 동안 합산 고객 수의 중앙값을 취하여 사용량의 최고점과 최저점을 평활화했습니다.

또한 사용자 기반과 DPS 공급자의 채택에 큰 기여를 하는 것은 타사에 의해 이루어지며, 그 예로는 웹 호스팅 서비스 공급자와 도메인 사용자가 있습니다. 이러한 대규모 플레이어 중 일부는 하루에서 다음 날까지 수백만 개의 도메인에 대한 보호를 활성화하거나 비활성화합니다. 또한 예를 들어 선택적 권한 있는 네임서버 보호의 사용과 관련하여 보호 서비스가 어떻게 사용되는지도 배웁니다. 분석에 대한 자세한 내용은 논문 [14]에서 확인할 수 있습니다.

또한 공격을 받은 것이 DPS 채택에 어느 정도 영향을 미치는지도 조사했습니다. DoS 공격의 표적이 된 후 운영자는 DPS에 보호 아웃소싱을 시작할 수 있습니다. DPS 사용에 대한 데이터를 통해 웹 사이트에서 DPS를 채택했는지 여부와 시기를 분석할 수 있습니다. § III에서 우리는 이미 공격과 웹 사이트를 연결했습니다. 이러한 데이터 세트를 융합하면 어떤 공격이 채택으로 이어지는지 확인할 수 있습니다. 이 프로세스를 마이그레이션이라고 합니다. 공격 특성이 마이그레이션에 미치는 영향을 조사했습니다. 그림 4는 정규화된 공격 강도 분포의 95번째, 99번째, 99번째 백분위수 강도에 따라 공격받은 웹 사이트(가장 느린 CDF)에 대해 웹 사이트를 마이그레이션하는 데 걸린 일수의 누적 분포 함수를 보여 줍니다. 이러한 CDF를 비교하면 공격과 영향을 받는 사이트가 DPS로 마이그레이션되는 사이의 대기 시간이 크게 줄어든다는 것을 알 수 있습니다. 공격 이벤트의 강도는 특히 속도 측면에서 DPS로의 마이그레이션과 밀접한 상관관계가 있으며, 이는 DDoS 피해 및 위험을 완화하는 데 있어 긴박감을 직관적으로 시사합니다. 전체 조사를 위해 독자에게 [9]를 참조하도록 합니다.

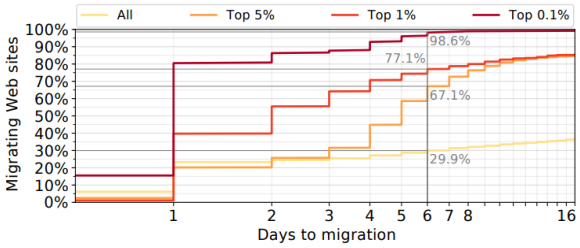

그림 4. 정규화된 공격 강도의 백분위수에 대한 마이그레이션 지연입니다.

BGP 블랙홀링 BGP 블랙홀링에 초점을 맞춥니다. § II에 설명된 대로 생성된 블랙홀링 데이터 세트는 2015년 3월부터 3년 동안 사용됩니다. 표 III은 요약을 제공합니다.

collectors	#events	#prefixes	#origins	#AS paths
34	1.30 M	146193	2682	31493

BLACKHOLING DATA SET INFERRED FROM PUBLIC BGP DATA.

우리는 "블랙홀 공격"을 찾기 위해 공격과 블랙홀링 데이터를 공동으로 분석합니다. 공격받은 대상 IP 주소를 블랙홀 접두사와 일치시키고 블랙홀 활성화보다 최대 24시간 앞선 공격 시작 시간을 요구합니다. 이를 통해 운영자가 공격에 직면했을 때 어떻게 행동하는지 연구할 수 있습니다. 이 섹션의 나머지 부분에서 논문의 일부 결과를 강조할 것입니다.

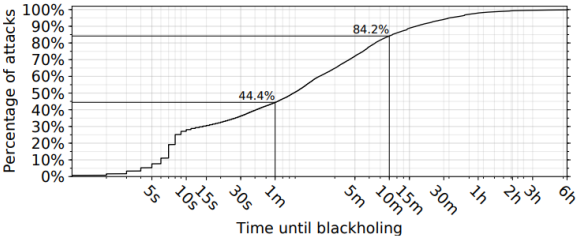

그림 5. UCSD-NT 및 AmpPot 데이터 세트의 블랙홀 공격에 대한 공격 시작과 블랙홀 사이의 시간 분포입니다.

그림 5는 블랙홀링이 활성화되는 데 걸리는 시간을 보여줍니다. 블랙홀 공격의 거의 절반(44.4%)은 1분 이내에 블랙홀이 활성화되는 것을 경험했으며, 84.2%는 10분 이내에 활성화되는 것을 경험했습니다. 이러한 시간에는 자동화된 검색 및 완화를 사용하는 것이 좋습니다. 블랙홀 공격의 0.02%에 대해서만 블랙홀이 활성화되는 데 6시간 이상 걸립니다.

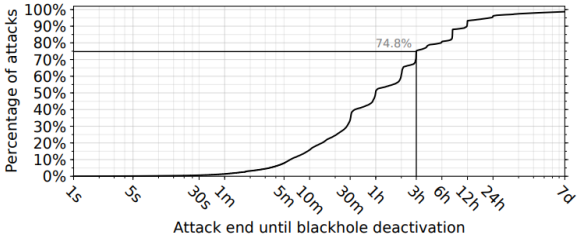

그림 6. AmpPot 데이터 세트의 공격 종료와 상관 블랙홀링 이벤트 종료 사이의 시간 분포입니다.

그림 6은 AmpPot 데이터 세트에서 블랙홀 공격이 종료된 시점과 관련 블랙홀 이벤트가 비활성화된 시점 사이의 시간을 보여줍니다.2 블랙홀 공격의 96.1%는 24시간 이내에 비활성화됩니다. 따라서 3.9%의 경우 며칠이 걸릴 수 있습니다. 이러한 결과는 블랙홀링 복구에 자동화가 부족함을 시사하며, 블랙홀 접두사로 향하

는 모든 트래픽을 완전히 차단하는 부작용이 공격 기간을 넘어 확장되어 자초한 DoS에 해당한다는 점을 강조합니다.

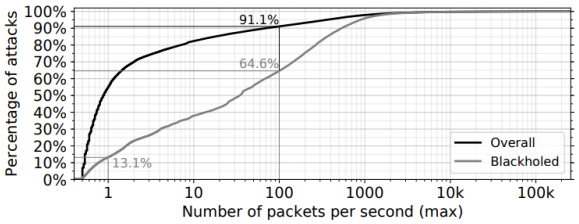

그림 7. UCSD-NT 데이터 세트의 모든 공격(검은색 곡선)과 블랙홀 처리된 공격(회색 곡선)에 대한 강도 분포입니다.

UCSD-NT 데이터 세트에는 관찰된 초당 최대 후방 산란 패킷 수로 표현되는 공격 강도(ppsmax) 측정값이 포함되어 있습니다. 그림 7은 모든 공격과 블랙홀 공격에 대한 이러한 강도의 분포를 보여줍니다. 블랙홀 공격(회색 곡선)의 64.6%는 최대 100ppsmax의 강도를 가지며, 이는 약 300M bps의 공격 트래픽 볼륨에 해당합니다. 이는 모든 공격의 91.1%에 적용됩니다(검은색 곡선). 블랙홀 공격의 무시할 수 없는 비율은 강도가 낮습니다. 특히, 13.1%는 최대 1ppsmax(3M bps)의 강도를 보입니다. 이 결과는 운영자가 블랙홀링과 같은 극단적인 조치를 통해 훨씬 덜 강력한 무작위 스푸핑 공격을 완화한다는 것을 보여줍니다. 이는 운영자가 DoS를 자초하도록 하기 위해 공격자가 해야 할 노력이 얼마나 적은지에 대한 질문을 제기합니다. AmpPot 데이터 세트에서 블랙홀 공격을 분석한 결과도 비슷한 결과를 얻을 수 있습니다. 우리는 독자에게 여기에서 다룰 수 없는 이러한 발견과 다른 발견에 대해 우리 논문을 참조하도록 합니다[16].

V. HIDDEN HAZARDS WITH MITIGATION SOLUTIONS

여기서는 클라우드 기반 보호 서비스 사용의 주요 단점, 즉 공격자가 소위 "출처 노출"의 결과로 필자의 방어를 우회하고 비효율적인 보호를 제공한다는 사실을 강조하고 정량화합니다.

§ II에서 처음 논의한 바와 같이 보호 서비스에는 트래픽 전환이 필요합니다. 즉, 트래픽은 보호 서비스의 보안 인프라를 통해 라우팅되어야 합니다. 그림 8은 DNS를 사용할 때 이 기능이 어떻게 작동하는지에 대한 개략도를 보여줍니다.

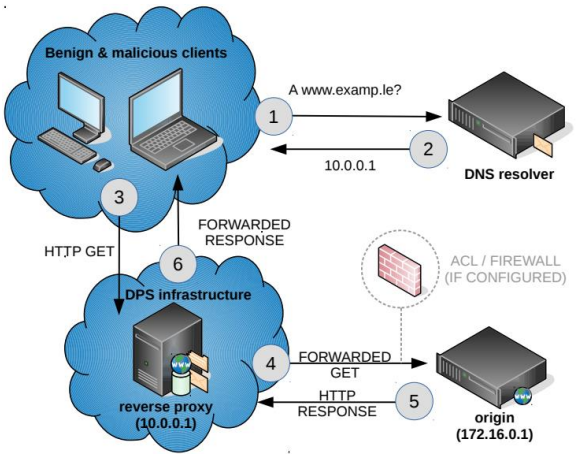

그림 8. DNS 기반 네트워크 트래픽 전환 개략도

보호가 아웃소싱되는 서비스의 출처(예: 웹 서버의 실제 IP 주소)는 보호 서비스에만 알려야 합니다. 이는 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 원본 흔적을 남기거나 과거 DNS 데이터(OpenINTEL에서 제공)를 통해 노출되도록 하는 것으로 요약됩니다. 다양한 DNS 기반 벡터를 조사하며, 이에 대한 자세한 설명은 CNSM 2017 논문[21]에서 확인할 수 있습니다. 당사는 이러한 벡터와 OpenINTEL 데이터를 사용하여 Alexa Top 1M 목록에 있는 웹 사이트의 출처에 대한 후보 IP 주소를 찾고 클라우드 기반 보호를 사용합니다. 당사는 웹 사이트가 § IV의 9개 보호 서비스 중 8개의 보호를 받는 것으로 간주합니다(CenturyLink는 DNS 기반 전환을 지원하지 않음). 후보 주소를 사용하면 HTTP 요청을 직접 전송하여 보호를 우회하려고 시도합니다. 그런 다음 결과 HTTP 콘텐츠를 일반 요청(즉, 역방향 프록시를 통해)을 통해 검색된 콘텐츠와 비교합니다. Zhang과 Shasha의 트리 편집 거리 알고리즘을 기반으로 하는 DOM 트리 비교 방법을 사용하여 한 트리에서 다른 트리로 이동하기 위한 편집 작업(삽입, 삭제 및 대체)의 수를 계산합니다. 전체 웹 사이트의 40.5%가 보호를 우회할 수 있는 것으로 간주합니다. 이는 10884개의 웹 사이트 중 4408개로 귀결됩니다.

또한 노출된 웹 사이트를 공격 데이터와 일치시킨 결과, 4,408개의 웹 사이트 중 843개의 출처가 DPS에 대한 소싱 보호를 시작한 후 공격을 받은 것으로 나타났습니다. 이는 노출된 모든 웹 사이트의 19%에 해당합니다. 이러한 결과는 보호 서비스를 효과적으로 사용하기 위해 올바른 관리 및 구성이 필요하다는 것을 뒷받침합니다.

VI. SUMMARY

DDoS 공격이 급증하면서 개인 사업자부터 정부에 이르기까지 많은 사람들이 DDoS 문제를 가장 잘 해결할 수 있는 방법에 대해 의문을 제기하고 있습니다. 우리는 정확히 무엇에 대해 방어하고 있습니까? 완화 솔루션은 실제로 어떻게 작동하나요? 그리고 운영자, 즉 최종 사용자가 주의해야 할 완화 솔루션의 위험은 무엇입니까? 이러한 질문들은 당연히 물어볼 수 있는 많은 질문들 중 하나입니다. 논문을 시작할 때 우리는 이러한 질문을 둘러싼 다양한 문제를 확인했는데, 그 중 일부는 본질적으로 더 기술적이고 일부는 사회적 성격에 더 가깝습니다. 우리는 주로 기술적 과제에 초점을 맞추기 시작했으며, DDoS 공격에 대한 대규모 과학적 보고가 부족하다는 점이 논문의 원동력이었습니다. 이 논문은 우리 논문의 결과 중 일부를 강조합니다. 특히, 공격 및 공격 대상에 대한 엄격한 특성화, 다양한 완화 솔루션의 채택 및 운영에 대한 연구, 완화 솔루션을 완전히 무력화할 수 있는 운영 및 배포 실수에 대한 조사에서 선별된 결과를 요약합니다. 우리가 식별한 다양한 기존 데이터 소스가 없었다면 우리의 작업은 불가능했을 것이며, 그 중 일부는 이 문서에 요약되어 있습니다. 글로벌 인터넷 측정 인프라의 다양한 데이터를 보유하고 있더라도 이를 융합하고 추가로 처리하여 대규모로 공격 및 완화를 연구하는 것은 간단한 문제가 아닙니다. 그러나 이러한 성공은 새로운 통찰력으로 이어졌고 더 많은 기여를 위한 길을 열었습니다. 이 논문에서 우리는 또한 기술적 문제를 극복하는 것이 사회적 기여를 가능하게 한다는 것을 보여줍니다. 좀 더 구체적으로 말하자면, 우리의 연구 노력을 통해 연구 커뮤니티와 네트워크 운영자 외에도 사회적 문제를 다루는

정책 입안자와 규제 기관에게 정보를 제공할 수 있었습니다. 우리는 이것이 우리의 연구를 더욱 입증하고 과학적 기여를 넘어 의미를 부여한다고 생각합니다.

REFERENCES

[1] A. Garg, J. Curtis, and H. Halper, "Quantifying the financial impact of IT security breaches," Information Management & Computer Security, vol. 11, no. 2, pp. 74–83, 2003.

[2] B. Krebs, "DDoS Attack on Bank Hid $900,000 Cyberheist," https://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000- cyberheist/, February 2013.

[3] T. Jordan and P. Taylor, Hacktivism and cyberwars: Rebels with a cause? Routledge, 2004.

[4] D. E. Denning, "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy," Networks and netwars: The future of terror, crime, and militancy, vol. 239, p. 288, 2001.

[5] R. A. Paulson and J. E. Weber, "Cyberextortion: an overview of distributed denial of service attacks against online gaming companies," Issues in Information Systems, vol. 7, no. 2, pp. 52–56, 2006.

[6] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack," http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21- attack/, October 2016.

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

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-service Activity," ACM Transactions on Computer Systems, vol. 24, no. 2, pp. 115–139, 2006.

[9] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti, "Millions of Targets Under Attack: A Macroscopic Characterization of the DoS Ecosystem," in Proc. of the 2017 Internet Measurement Conference, 2017, pp. 100–113.

[10] L. Kramer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and ¨ C. Rossow, "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks," in International Workshop on Recent Advances in Intrusion Detection, 2015, pp. 615–636.

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

[12] "Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4 and IPv6," http://www.caida.org/data/routing/routeviews-prefix2as.xml.

[13] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, "A HighPerformance, Scalable Infrastructure for Large-Scale Active DNS Measurements," IEEE Journal on Selected Areas in Communications, vol. 34, no. 6, pp. 1877–1888, 2016.

[14] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, "Measuring the Adoption of DDoS Protection Services," in Proceedings of the 2016 ACM Internet Measurement Conference, 2016, pp. 279–285.

[15] V. Giotsas, P. Richter, G. Smaragdakis, A. Feldmann, C. Dietzel, and A. Berger, "Inferring BGP Blackholing Activity in the Internet," in Proc. of the 2017 Internet Measurement Conference, 2017, pp. 1–14.

[16] M. Jonker, A. Pras, A. Dainotti, and A. Sperotto, "A First Joint Look at DoS Attacks and BGP Blackholing in the Wild," in Proc. of the 2018 Internet Measurement Conference, 2018, pp. 457–463.

[17] S. Zander, L. L. Andrew, and G. Armitage, "Capturing Ghosts: Predicting the Used IPv4 Space by Inferring Unobserved Addresses," in Proceedings of the 2014 ACM Conference on Internet Measurement Conference, 2014.

[18] P. Richter, G. Smaragdakis, D. Plonka, and A. Berger, "Beyond Counting: New Perspectives on the Active IPv4 Address Space," in Proceedings of the 2016 ACM Internet Measurement Conference, 2016.

[19] M. Jonker, "DDoS Mitigation: A Measurement-Based Approach," Ph.D. dissertation, University of Twente, 2019, https://doi.org/10.3990/1.9789036548687.

[20] R. Holland and E. Ferrara, "The Forrester WaveTM: DDoS Services Providers (Q3 2015)," Forrester Research, Inc., Tech. Rep., July 2015.

[21] M. Jonker and A. Sperotto, "Measuring Exposure in DDoS Protection Services," in Proc. of the 13th International Conference on Network and Service Management (CNSM'17), 2017, pp. 1–9.