지도환 - DDoS Mitigation: A Measurement-Based Approach

Abstract

- DDoS 공격으로 인해 기업은 매년 수억 달러의 손실을 입고, 중요한 인프라의 경우 국가의 안전과 생명까지 위태로울 수 있다.
- 따라서 효과적인 DDoS 방어가 필요하다.
- 쉽게 사용할 수 있는 방어 솔루션의 선택은 명확하지 않을 수 있고, 사용에 있어 숨겨진 위험이 있을 수 있음.
- DDoS 문제를 더 잘 이해하는 것이 중요함.

기여하는 것

1. 공격과 공격 대상을 대규모로 엄격하게 특성화.
2. 다양한 완화 솔루션의 인터넷 전반의 채택, 배포 및 운영 사용에 대한 지식을 발전.
3. 방어 솔루션의 효과를 완전히 무력화시킬 수 있는 숨겨진 위험 요소 조사.

I. INTRODUCTION

A. DDoS Attacks

DoS : 공격자가 서비스 거부를 달성하기 위해 가능한 모든 수단을 동원하여 인터넷에서 네트워크 서비스를 차단하는 것.

목적

- 악의적인 활동으로부터 주의를 분산.
- 핵티비즘
- 사이버 갈취

공격이 성공하면 파급 효과가 발생, 잠재적으로 인터넷에 막대한 영향을 미칠 수 있음.
방어는 절대적으로 필요.

B. Mitigation Solutions

공격에 대한 방어 - 소스 가까이에서 수행하는 것이 더 효과적.

탐지 - 피해가 발생하는 표적에 더 가까운 곳에서 더 잘 수행.

따라서 두 영역 간에 정보가 서로 공유됨.

인터넷에서 방어 솔루션 도입에 대한 정보가 적음.

또한 운영자들도 이것에 대해 이해가 부족함.

C. Hidden Hazards

완화 솔루션은 쉽게 구할 수 있고, 사용할 수 있어, 전문가가 아니어도 사용 가능.

비전문가가 겪을 수 있는 잠재적 위험, 솔루션을 비효율적으로 만들 수 있는 것은 무언인가?

D. Challenges

1. 방어 대상을 정확히 파악하는 데 따르는 어려움.
2. 방어 솔루션의 도입 및 운영과 관련된 어려움.

모두 데이터에 관한 것임.

DDoS 문제를 연구하기 위한 데이터 소스를 확보 및 개발 그 자체가 어려운 과제.

E. Approach

- 측정 기반 접근 방식
- 빅 데이터 분석 적용

F. Contributions

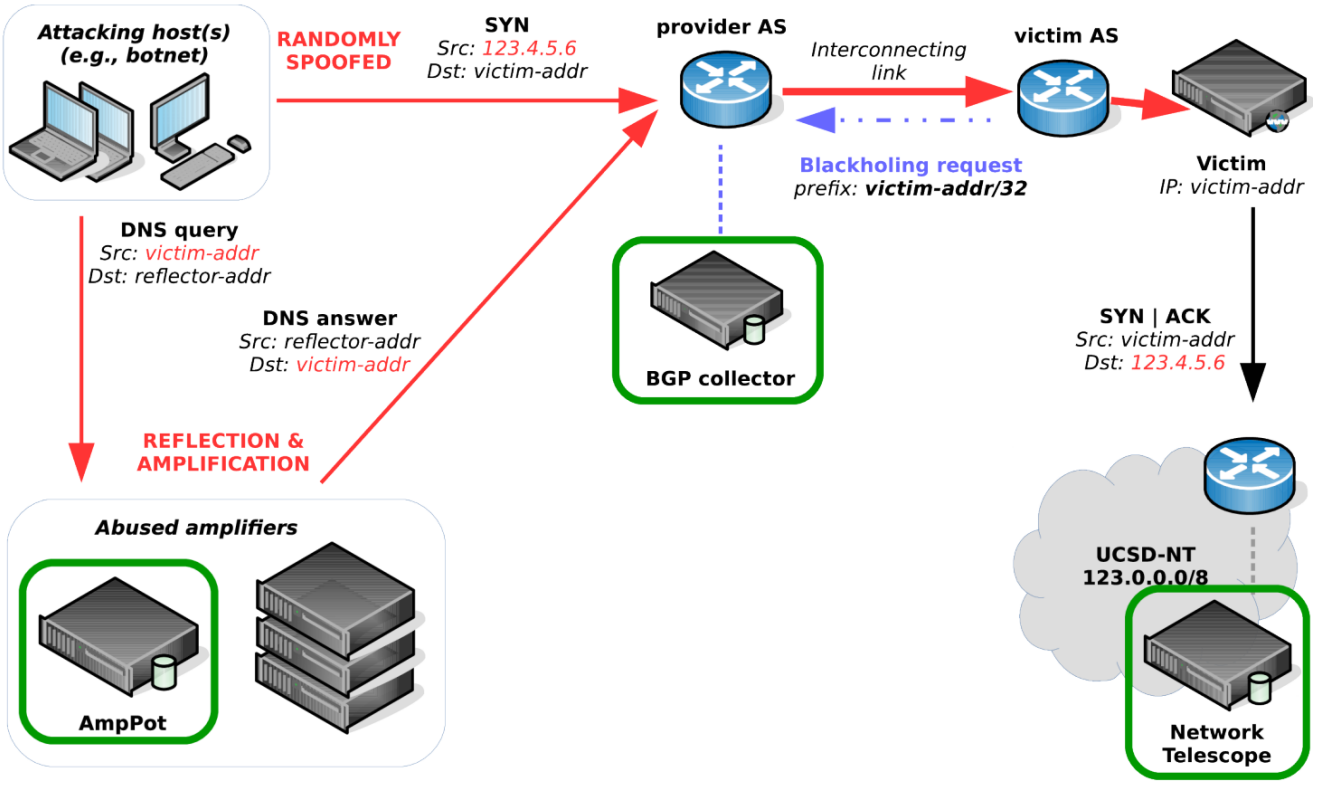
1. 전 세계 공격 활동에 대한 놀라운 통계 공개.
2. 인터넷 전반의 완화 솔루션 도입과 사용자들의 운영 관행에 대한 인사이트를 확보.
3. 배포 및 운영상의 실수로 인한 바람직하지 않은 부작용을 드러내고 조사할 수 있음.
4. 기존의 방법론을 더욱 검증하고, 일부 데이터를 연구 커뮤니티에 공개.

G. Organization

II. 식별 개발 및 사용한 기본 데이터 원본 설명
II-A. 공격의 특성
IV. 완화 솔루션
V. 완화 솔루션에 관련된 숨겨진 위험에 대한 분석
VI. 요약

II. DATA SOURCES

A. Data on (D)DoS Activity



DDoS 활동의 글로벌 지표

1. 무작위로 균일하게 스푸핑된 IP 주소를 사용하는 DoS 공격의 증거를 포착하는 UCSD-NT의 Network Telescope
2. 특별히 스푸핑된 IP 주소를 포함하는 공격 유형인 반사 및 증폭 DoS 공격을 캡처하는 AmpPot 허니팟

Randomly Spoofed Attacks

TCP SYN Flood 공격
Src : 무작위로 균등하게 Spoofing한 IP 주소

만약, Src가 UCSD-NT의 주소 공간 내에 있으면, Network Telescope가 해당 패킷 수집 및 분석 가능.

- UCSD-NT는 IPv4의 1/256을 차지함.
- 같은 방식의 공격은 이 다크넷에서 탐지될 가능성 높음.

Reflection and Amplification Attacks

AmpPot : Reflection Attacks을 할 수 있는 여러 protocol들을 emulate해 놓음.
공격자들은 AmpPot을 악용할 것이고, 이 공격들이 logging 됨.

위 두 공격에서 얻은 IP 주소와 아래 데이터를 종합하여, 특성 연구 진행.

- NetAcuity Edge Premium Edition data : 지리적 위치 정보(Whois)
- Routeviews Prefix-to-AS mappings data : BGP Routing metadata

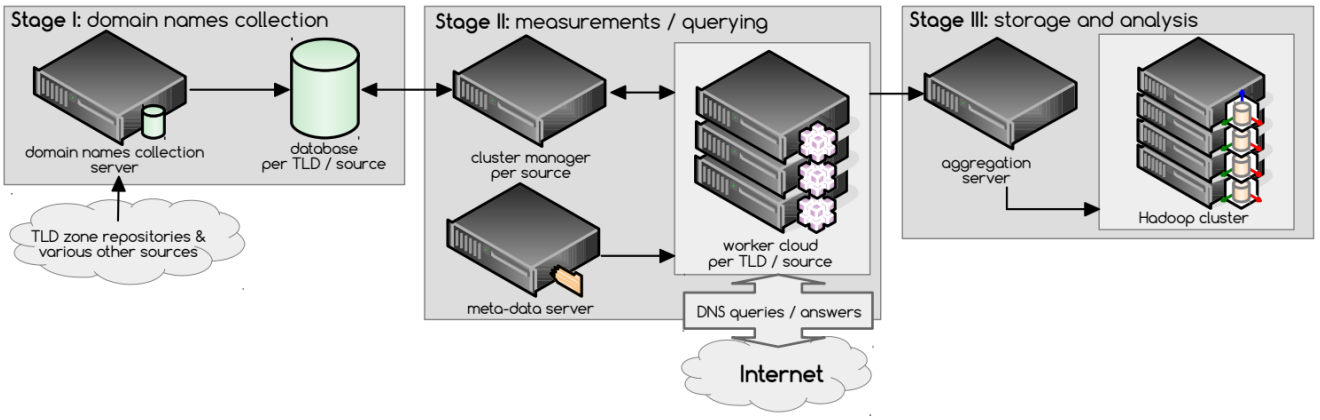


사진 - The OpenINTEL measurement and analysis architecture.

DNS Measurement Data

OpenINTEL : DNS 스냅샷 수집 플랫폼. 도메인 이름과 IP 주소등의 정보가 포함.

Inferring the Use of Protection Services

DPS는 네트워크 트래픽을 우회하기 위해서 DNS 또는 BGP를 사용함.

- DNS 기반 우회
  OpenINTEL가 수집한 DNS 레코드들(A, CNAME, NS)를 활용해, DPS를 사용했는지 유추.
- BGP 기반 우회
  IP 주소에 AS번호를 매핑하여, DPS를 사용했는지 유추.

Inferred Use of BGP Blackholing

BGP Blackholing : DDoS 공격 트래픽을 null 경로로 보내, 네트워크에 영향을 미치지 못하도록 함.
BGP 데이터에서 Blackholing 요청을 나타내는 이벤트를 분석하여 유추.
이벤트 내용

- Blackhol prefix
- 활성화 시간
- (선택적) 비활성화 시간

III. CHARACTERIZATION OF ATTACKS

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 ATTACK EVENTS DATA. WE CONSIDER TWO YEARS OF DATA FROM UCSD-NT AND AMPPOT.

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

ACTIVE DNS DATA SET. WE USE TWO YEARS OF DNS DATA COLLECTED BY THE OPENINTEL PLATFORM TO INFER WEB SITES AND ASSOCIATED IP ADDRESSES FOR THE .COM, .NET, AND .ORG GTLDS.

2년간 634만개의 IP주소를 대상으로 2100건의 공격 발생.
/24 네트워크 330만개 중 219만개가 적어도 한번 공격 당함. (전체의 1/3)
해당 IP의 웹사이트 관련성은 9% -> 같은 IP에서 1개 이상의 웹서비스 제공 중.
분석 기간 동안 웹의 64%가 공격 받은 IP 주소에서 운영 중.
-> 하나의 IP 공격만 하더라도, 다수의 웹에 영향을 미칠 수 있음.

IV. ADOPTION AND OPERATION OF MITIGATION

Cloud-based protection services

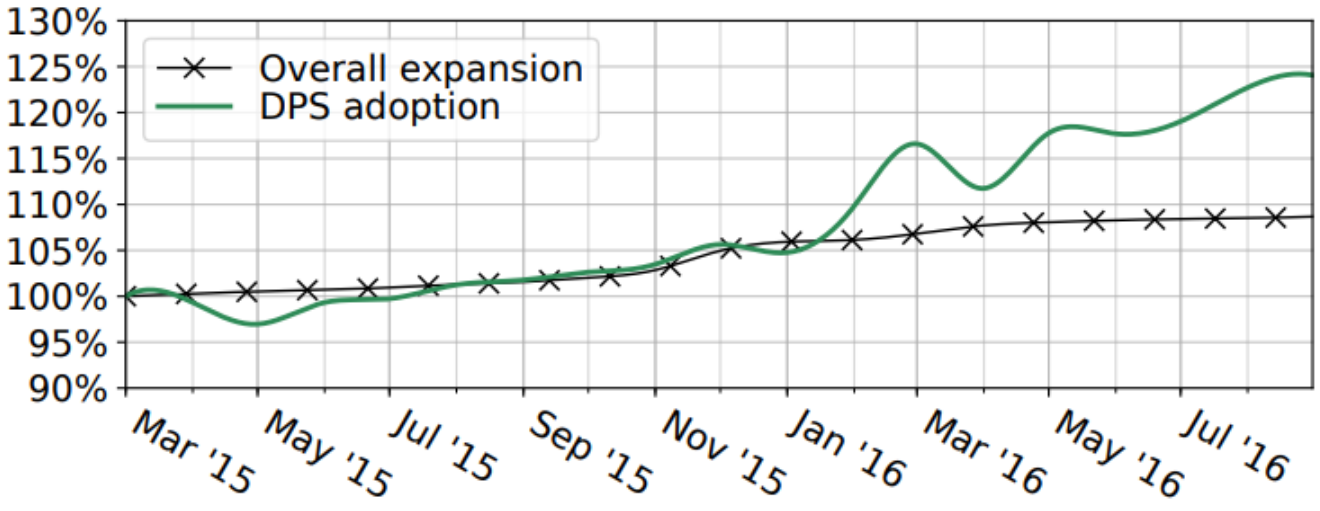
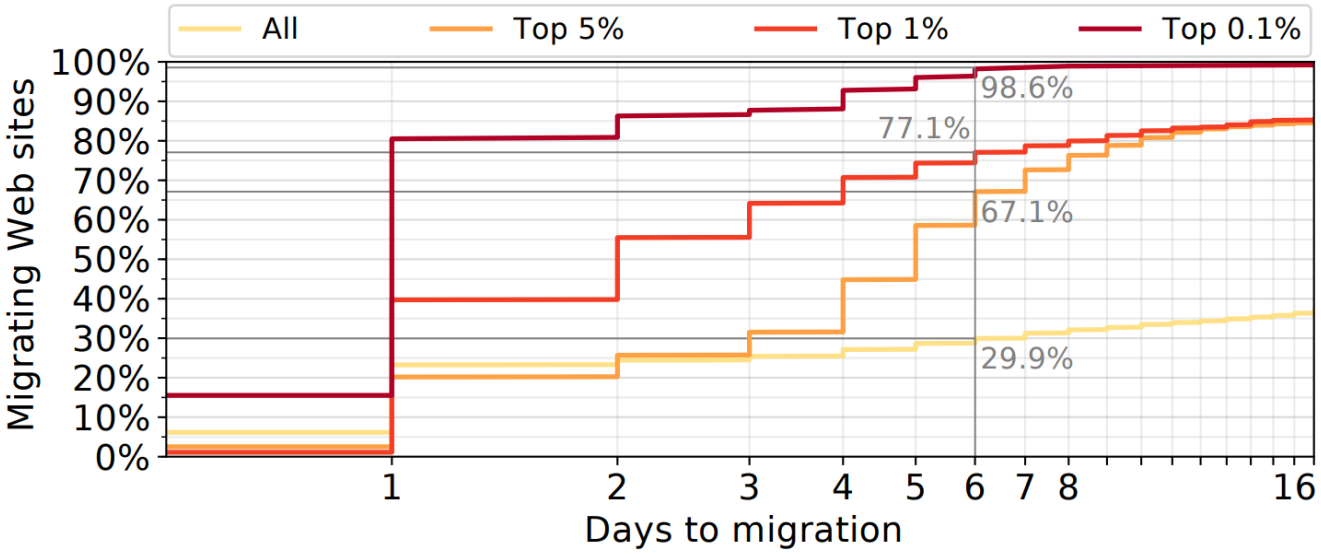


Fig. 3. Growth of DPS use in 50% of the DNS (com, net, and org)

주요 DDoS 보호 서비스 제공 업체 대상, 18개월 동안 주요 도메인(.com, .net, .org)대상 분석.

웹서비스 1.09배 증가, DPS 사용량 1.24배 증가.
그래프가 출렁이는 것은 DPS를 on/off 할 수 있기 때문.

또한 DDoS 공격 받은 대상이 DPS를 도입한 것도 분석함.



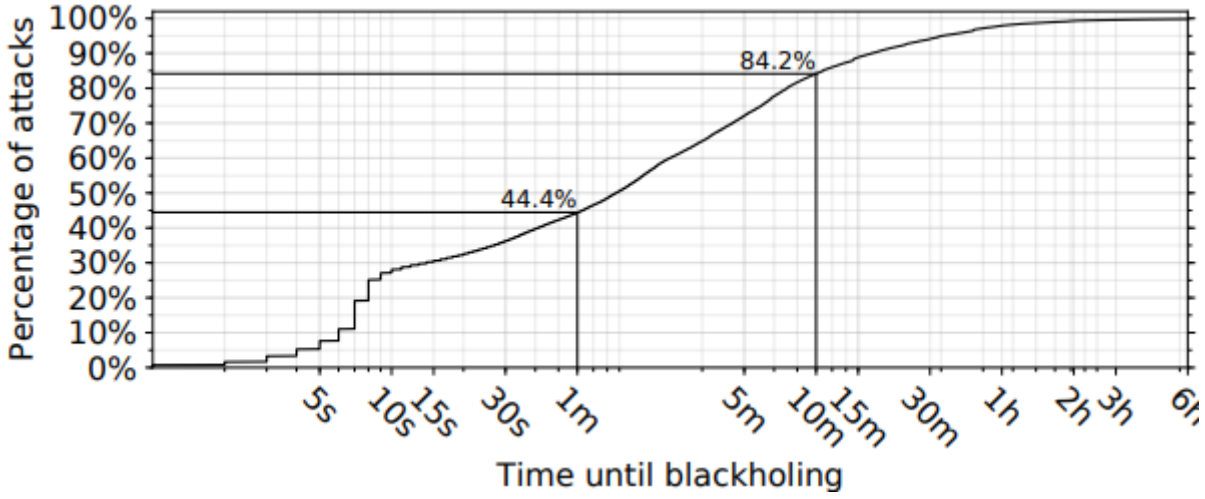
%는 공격 많이 받은 걸 줄 세웠을 때.

BGP blackholing

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

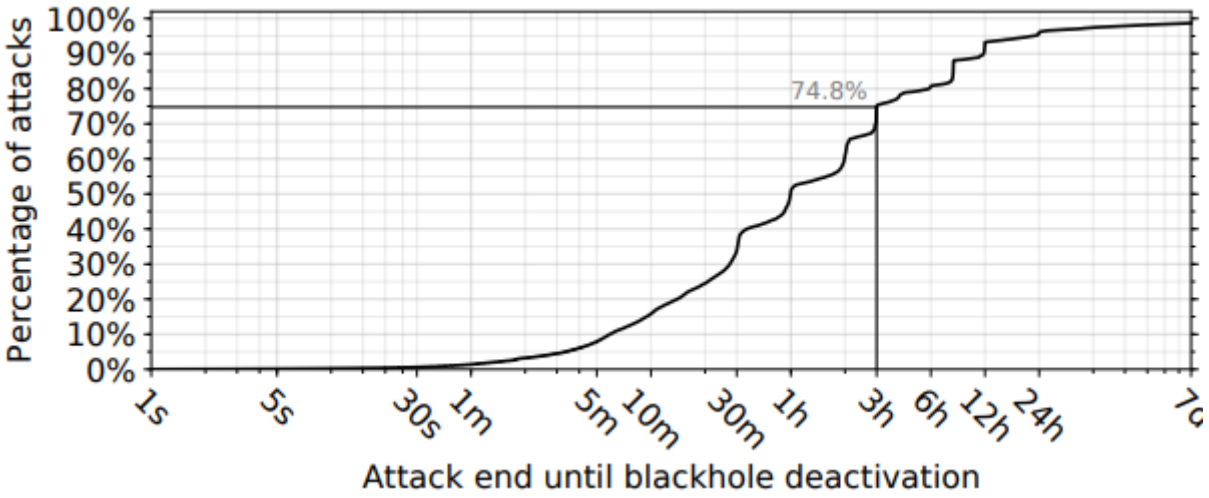
TABLE III
BLACKHOLING DATA SET INFERRED FROM PUBLIC BGP DATA.

BGP Blackholing 이벤트 추출한 3년치 표.

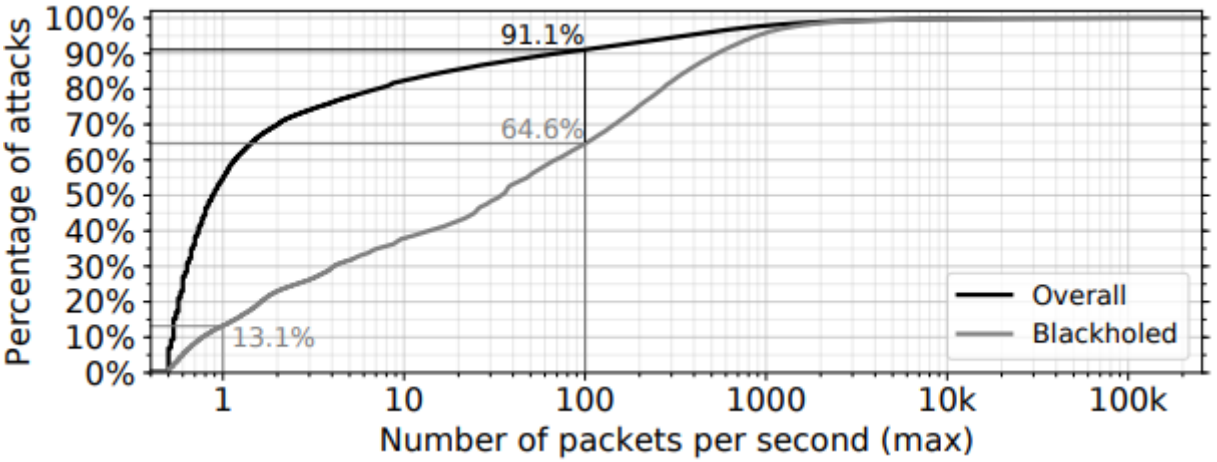


Blackhole이 활성화하는데 걸린 시간 그래프.

- 1분 안에 작동 44.4%
- 10분 안에 작동 84.2%
- 6시간 이상 소요 0.2%



Blackhole이 비활성화하는데 걸린 시간 그래프.
활성화에 비해 원 상태로 돌아오는데 많은 시간이 걸림을 확인할 수 있음.



DDoS 공격으로 인한 원치 않은 패킷(backscatter)의 초당 관측된 량, 처리한 패킷에 관한 그래프.
64.6%의 Blackholing된 공격은 최대 100ppsmax의 강도. (약 300Mbps) 이는 전체 공격 중 91.9%.
13.1%의 Blackholing된 공격은 최대 1ppsmax의 강도일 때도, 같은 방법으로 막음.

위 그래프를 모두 종합하여 해석하면, 적은 공격으로도 원 상태로 돌아오기까지 시간이 걸리므로, 관리자 스스로 DoS 공격을 해버린 꼴이 됨.

V. HIDDEN HAZARDS WITH MITIGATION SOLUTIONS

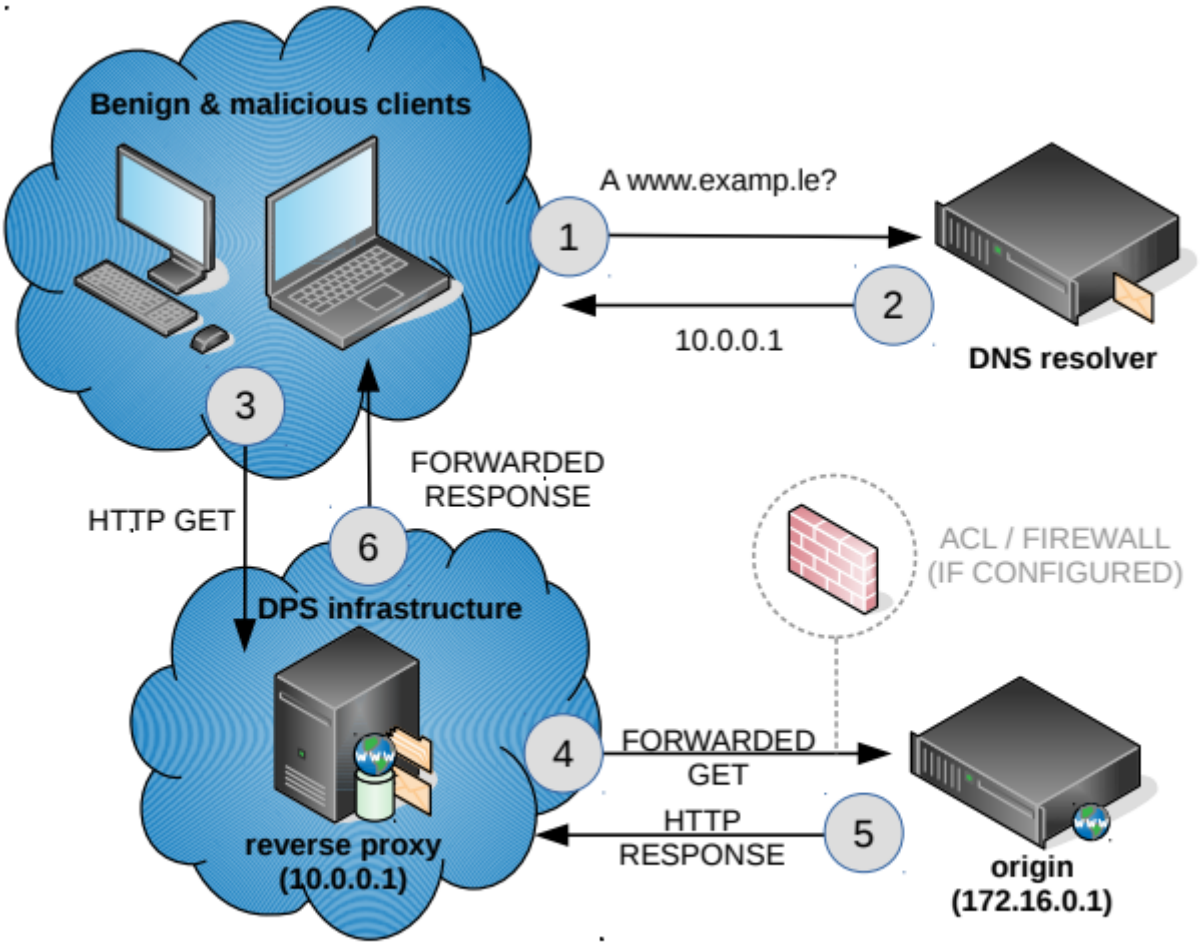


Fig. 8. Schematic of DNS-based network traffic diversion

웹서버 작동 방식

origin exposure : 웹서버의 실제 IP주소가 노출되어, 이 것으로 요청시 DPS를 우회하게 됨.

실제로 origin IP를 추적해서, 직접 요청 시, 40.5%가 DPS를 우회할 수 있었고, 843개 웹사이트는 실제로 공격도 당함.

노출되는 경우는 DNS 구성 및 운영 미숙.

VI. SUMMARY

공격과 공격 대상의 엄격한 특성화
다양한 방지 솔루션의 채택 및 운영에 대한 연구
운영 및 배포 과정에서 저지른 실수에 대한 조사를 요약