멀웨어를 선제적으로 방어하는 보안 체제가 필요한 3가지 이유

보안 스택에 존재하는 갭(gap)을 보호하는 방법 이해하기

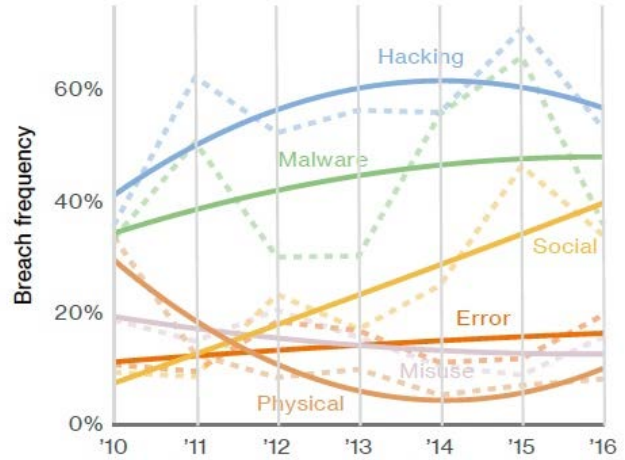
1 사이버 범죄의 증가

표적 공격의 지속적인 증가와 진화

멀웨어, 랜섬웨어, 데이터 유출, 피싱 등 표적 공격은 빈도, 규모, 정교함이 모두 증가하고 있습니다.

공격자들은 공격 기법을 끊임없이 발전시키고 기존의 보안 메커니즘을 우회하고 있습니다.

기업들은 폭증하는 위협을 효과적으로 막아내지 못해 어려움을 겪고 있습니다.



위협 유형별 데이터 유출 비율[1]

사이버 범죄의 현실

70%

지난 1년 동안 보안 사고가 비즈니스에 악영향을 끼쳤다고 응답한 기업의 비율[2]

390,000

매일 39만 개의 악성 프로그램이 새롭게 등록됨[3]

38%

38%의 글로벌 기업만이 정교한 사이버 공격에 대비했다고 응답.[4]

6조
달러

전세계적으로 사이버 범죄로 인해 발생하는 비용은 2021년 연 6조 달러에 이를 것으로 전망[5]

1800
만 달러

APT 데이터 유출로 발생하는 평균 비용은 1800만 달러이며, 이 중 50%가 브랜드 이미지 실추로 인해 발생[6]

2016년 기록적인 수의 데이터 레코드가 손실 또는 유출

3,046,456 매일[7]

126,936 매시간[7]

2,116 매분[7]

“Fortune 1000대 기업도 사이버 공격으로 인해 막대한 피해를 입을 것이다.”

출처: Forrester, *고객 중심 시대에 미래를 이끌어갈 역학 관계*

2

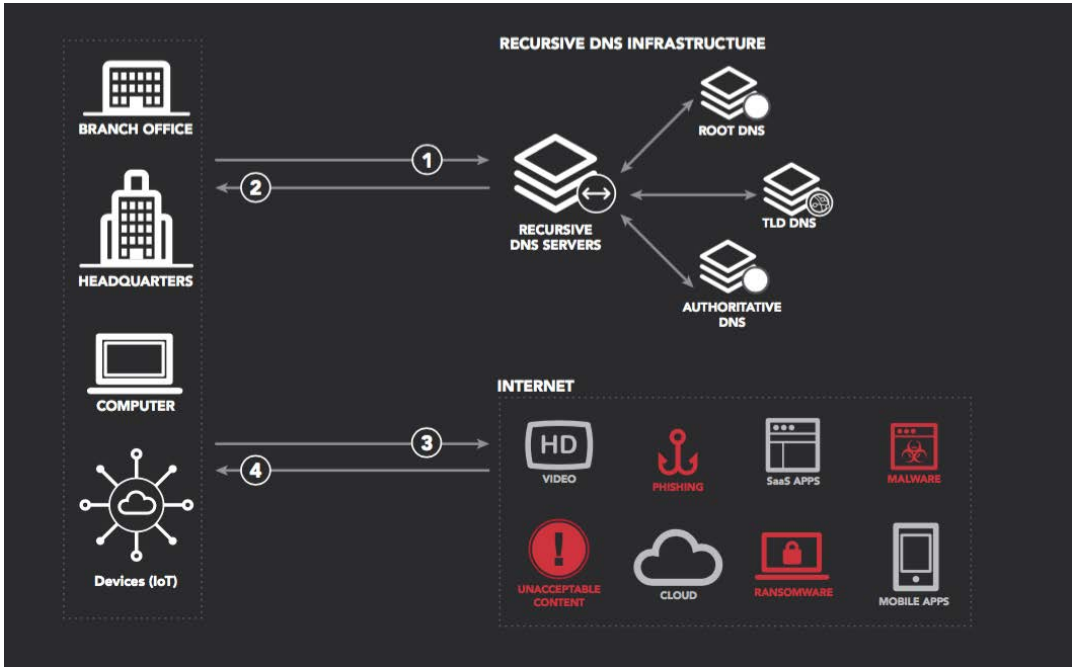
방어 체제를
우회하기 위해
DNS(도메인 네임
시스템)를 악용하는
사례 증가

리커시브 DNS가 악용되는 이유

인터넷에서 이루어지는 거의 모든 활동은 도메인 이름을 IP 주소로 변환해 달라는 DNS(도메인 네임 시스템) 요청으로 시작합니다.

DNS 프로토콜은 본질적으로 오픈되어 있고 필터링되지 않습니다.

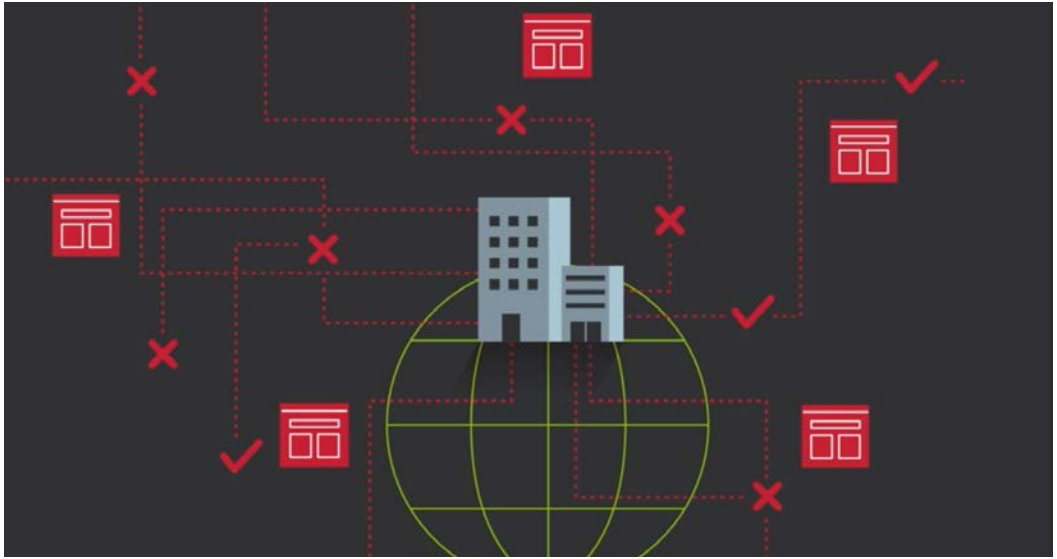
DNS 자체에 인텔리전스가 없기 때문에 정상 도메인은 물론 악성 도메인에 대한 요청도 구분하지 않고 처리합니다.



DNS 악용이 시급한 문제인 이유

사이버 범죄자들은 DNS의 보안상 허점을 악용해 쉽게 네트워크에 침입하고 민감한 데이터를 유출시킬 수 있다는 사실을 알게 되면서

DNS를 악용한 공격 건수가 급증하고 있습니다.



DNS 공격이 확산되고 있는 이유

DNS 인프라의 취약점이 알려지고 고객 데이터와 기밀 데이터를 보호해야 하는 압박이 증가하며 커넥티드 디바이스의 수가 급증하고 있는 현실에서도 DNS 인프라 방어를 최우선 과제로 생각하는 CIO와 IT 부서는 많지 않습니다.

3 방어하기 까다로운 공격 기법

멀웨어가 네트워크에 침입하는
다양한 방법을 생각해 보십시오.

한 명의 직원 혹은 방문자과 다음과 같은 행동을 한 경우 문제 발생

- 피싱 이메일에 포함된 링크에 접속
- 멀웨어가 포함된 광고 클릭
- 소셜 네트워크 게시물 중 감염된 URL 클릭
- 타이포스쿼터(typosquatter) 사이트 방문
- 이름이 유사한 도메인 접속
- 감염된 컴퓨터 스토리지 미디어 공유
- 소셜 엔지니어링에 속는 경우

멀웨어의 90% 이상이 DNS를 악용해 감염을 확산시키고 네트워크를 제어하고 데이터를 갈취합니다.[11]

트래픽 용량으로 인한 문제

네트워크에는 노트북, 휴대폰, 데스크톱, 태블릿, 프린터, 프로젝터, 게스트 Wi-Fi, '스마트' IoT 디바이스를 비롯한 수천 개의 디바이스가 있습니다.

이들은 매일 무수한 DNS 요청을 전송합니다.

이렇게 막대한 규모 때문에 비정상적인 활동을 파악하기가 어려운 데다가 거의 대부분이 정상 트래픽이고 악성 트래픽은 극히 일부이기 때문에 DNS 로그를 모니터링하기도 쉽지 않습니다.

글로벌 트렌드에 대한 가시성 확보가 중요한 이유

지속적으로 DNS 로그를 모니터링하고 분석하는 리소스를 할당했다 하더라도 실제로 피해를 입기 전에 미리 탐지하고 차단할 가능성은 매우 낮습니다.

글로벌 인터넷 트렌드와 위협을 가려내기에는 기업의 샘플 사이즈가 매우 작습니다.

기존의 보안 솔루션과
어플라이언스로는 역부족

효율성과 일관성이 떨어지는
사후 대응식 접근 방식의 한계

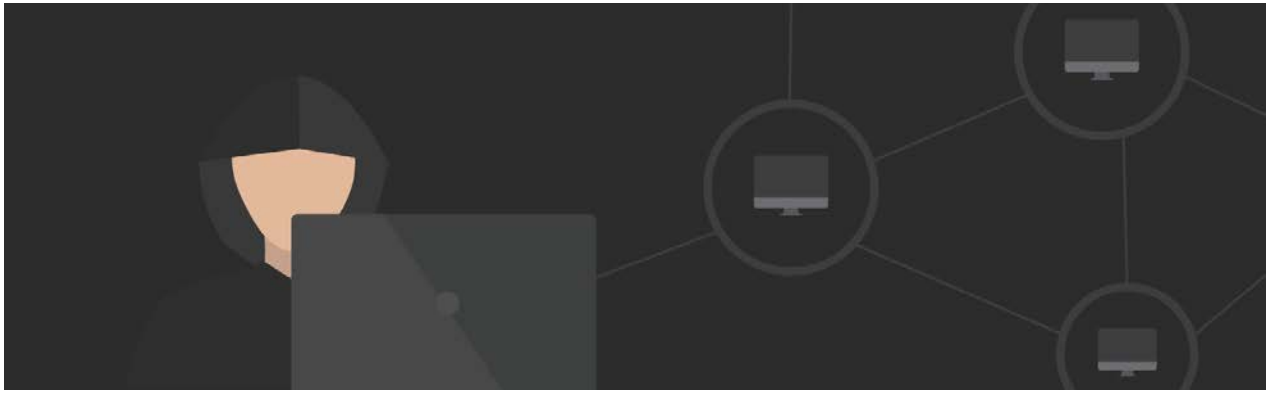
멀티레이어 방어의 중요성

방화벽, 보안 웹 게이트웨이, 엔드포인트 바이러스 백신 프로그램, 위협 인텔리전스 서비스와 같은 제품은 블랙리스트, 수동 업데이트, 사후 대응, 그리고 사용자가 각종 규정을 100% 준수하는지의 여부에 좌우됩니다.

서비스 공급업체의 위협 인텔리전스 데이터베이스에 존재하지 않는 위협은 탐지하지 못합니다.

필사적인 추격전

공격자들은 탐지를 피하기 위해 비표준 포트 및 프로토콜, DGA(도메인 생성 알고리즘), Fast Flux, DNS 유출 등의 방법을 사용하고 멀웨어는 끊임 없이 진화하고 있습니다. 대부분의 방어 메커니즘은 발전하는 위협에 능동적으로 대처하지 못하고 곧 무용지물로 전락합니다.



There is a better way

Akamai
Enterprise Threat Protector

Sources

1. Verizon 2017 데이터 유출 조사 보고서, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

2. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016

3. https://www.av-test.org/en/statistics/malware/

4. ISACA 2015 Global Cybersecurity Status Report, http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

5. Cybersecurity Ventures: 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

6. Ponemon Institute - The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN

7. www.cyberark.com/noteworthy-cyber-security-statistics/

8. MMC Cyber Handbook 2016, http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf

9: Arxan: 2017 Study on Mobile and Internet of Things Application Security, https://www.arxan.com/2017-Ponemon-Mobile-Iot-Study

10. www.securityweek.com/nearly-50-percent-organizations-hit-dns-attack-last-12-months-survey

11. Cisco 2016 Annual Security Report