AKAMAI
솔루션 설명서

표적 공격을 방어하는 클라우드 기반의 솔루션!

표적 공격으로부터 비즈니스를 사전에 방어

대부분의 전문가들은 기업이 언젠가는 멀웨어, 랜섬웨어, 피싱 등의 표적 공격을 받게 된다는 생각에 동의합니다. 지난 한 해에만 비즈니스에 악영향을 끼친 보안 사고를 경험한 기업은 70%나 되며,[1] 매일 39만 개가 넘는 악성 프로그램이 등록되고 있습니다.[2] 커넥티드 디바이스가 급격히 증가함에 따라 사이버 범죄를 통해 취할 수 있는 금전적 이득도 높아지고 있으며, 동시에 표적 공격의 범위·규모·정밀성도 증가하고 있습니다.

범죄자들이 증가하고 기업이 이에 대한 대응책을 고심하면서 엔터프라이즈 위협 환경도 급격히 변화하고 있습니다. 공격자들은 표적 공격 기법을 날로 발전시키며 기업들의 보안 방어 체계에서 취약점을 찾아내고 있습니다. 최근 들어 사이버 범죄자들은 DNS(도메인 네임 시스템)에 크게 관심을 가지고 있습니다. DNS, 그중에서도 리커시브 DNS는 어디에나 사용할 수 있고 개방성이 높으며 보안이 취약한 경우가 많아 사이버 공격을 가하기가 아주 쉬운 표적이 됩니다. 이에 따라 DNS를 악용한 공격 기법을 사용하는 표적 공격이 급증하고 있습니다.

DNS가 악용되는 이유

인터넷에서 이루어지는 거의 모든 활동은 도메인 네임을 IP 주소로 변환해 달라는 DNS 요청으로 시작됩니다. DNS는 인터넷을 빠르고 효율적이며 탐색하기 쉽게 만들어 준다는 장점이 있지만, 어디에서나 사용할 수 있고 개방성이 높다는 특성 때문에 악용하기에도 쉽습니다. DNS 자체에는 인텔리전스가 없기 때문에 정상 도메인은 물론 악성 도메인에 대한 요청도 구분하지 않고 변환합니다. 사이버 범죄자들은 기업을 겨냥한 피싱 공격, 멀웨어·랜섬웨어 공격 캠페인, 데이터 유출과 같은 표적 공격을 수행하기 위해 이러한 DNS의 취약점을 악용합니다.

DNS 악용이 시급한 문제인 이유

리커시브 DNS를 모니터링하지 않은 채 그대로 둔다면 매일 기업 네트워크에서 전송되는 수십만 건의 인터넷 요청이 언제든지 악성 다운로드로 변환될 수 있습니다. 실제 업무 환경에서 이는 (1) 직원이 피싱 이메일에 들어있는 링크를 클릭하고 멀웨어가 포함된 광고를 선택하는 경우, (2) SNS 게시물에서 감염된 URL을 열어 타이포스쿼터(typosquatter) 사이트로 이동하는 경우, (3) 이름이 유사한 도메인에 액세스하는 경우, (4) 감염된 컴퓨터 스토리지 미디어를 공유하거나 소셜 엔지니어링에 속는 경우 등 다양한 방식으로 발생할 수 있습니다.

감염된 디바이스는 순식간에 기업 전체를 감염시키는 게이트웨이가 됩니다. 감염된 디바이스로 인해 네트워크가 느려지거나 마비되고, 비즈니스 활동이 감시되고, 정보를 도난당하거나 데이터와 파일이 삭제될 수 있습니다. 감염된 디바이스는 불법 콘텐츠를 호스팅하거나 DDoS 공격에 참여하는 '좀비 컴퓨터'로 악용되기도 합니다.

네트워크에 침입한 대부분의 멀웨어는 네트워크 명령 및 제어(CnC) 센터로 요청을 전송하여 후속 명령을 받기 위해 대기합니다. DNS 트래픽은 필터링되지 않고 개방되어 있어야 하기 때문에 이와 같은 악성 커뮤니케이션은 네트워크 수준 보안을 우회하면서 탐지되지 않고 성공적으로 통과합니다. 공격자들은 이러한 DNS 터널링을 통해 금융 기록, 주민등록번호, 신용카드 정보, 지적 재산 및 기타 민감한 정보를 갈취합니다. 즉, 민감한 정보의 데이터 패킷을 암호화 및 압축하고 분할하여 네트워크 외부로 전송하는 것입니다.

기업에 미치는 영향

표적 공격은 기업에 상당히 큰 영향을 미칩니다. Ponemon Institute는 공격을 방어하고 문제를 해결하는 데 투입되는 비용을 4가지 범주(기술 지원, 생산성 손실, 매출 감소, 브랜드 이미지 실추)로 구분합니다. 공격 1회당 발생하는 비용은 평균 1800만 달러를 넘습니다.[3] 여기에서 흥미로운 부분은 브랜드 이미지·평판의 실추로 인한 비용이 950만 달러에 달해, 다른 3가지 범주 각각에 비해 세 배나 높다는 사실입니다.[4] Ponemon의 추산에 따르면 표적 공격을 받아 데이터 유출이 발생한 경우에는 공격에 대응하는 데 추가로 소요되는 비용이 4백만 달러에 달합니다.[5] 고객 및 위기 관리, 사고 대응, 조사, 보안 감사, 직원 교체, 신규 CISO 및 보안 담당자 채용을 위한 인력 확보, 법률 수수료와 합의금, 규정에 의한 벌금 등이 모두 이와 같은 비용에 포함됩니다.

현재 사이버 범죄가 세계 경제에 미치는 영향은 4500억 달러로 추산되며, 2021년이면 무려 6조 달러에 달할 것으로 전망됩니다.[6] 이러한 사실들을 고려하면, 기업에서 방어 체계를 강화하고 기존 보안 스택에 솔루션, 제품 및 툴을 추가하여 알려진 네트워크 취약점과 리커시브 DNS와 같은 공격 기법에 대비하는 것이 얼마나 중요한 일인지 알 수 있습니다.

당면 과제: 방어하기 까다로운 공격 기법

기존의 보안 솔루션에는 리커시브 DNS 인프라를 보호하기 위해 필요한 효율성과 일관성이 부족합니다. 네트워크 수준의 보안 수단으로는 기업의 경계 외부에서 이루어지는 리커시브 DNS를 악용한 데이터 유출이나 위협을 탐지할 수 없습니다. 방화벽, 보안 웹 게이트웨이, 바이러스 백신 프로그램, 위협 인텔리전스 서비스와 같은 제품은 블랙리스트, 수동 업데이트, 사후 조정, 그리고 사용자가 각종 규정을 100% 준수하는지의 여부에 좌우되며, 그나마도 보안 서비스 사업자의 데이터베이스에 존재하지 않는 위협은 탐지하지 못합니다.

게다가 대부분의 보안 서비스는 포트 80과 443을 통과하는 HTTP와 HTTPS 프로토콜만 조사합니다. 이를 모를 리 없는 공격자들은 다른 포트와 프로토콜을 사용합니다. 대부분의 방어 메커니즘에는 멀웨어는 물론 공격자들이 발각되지 않기 위해 사용하는 은폐 수단(슬로우 드립(slow drip, IP 스푸핑(spoofing), DGA(도메인 생성 알고리즘), Fast Flux 등)이 발전하는 속도를 따라잡을 만한 민첩성이 부족하며, 따라서 곧 무용지물로 전락하게 됩니다.

리커시브 DNS 공격을 더욱 어렵게 만드는 요인은 바로 DNS 보안에 관한 의사결정이 근거 없이 이루어지는 경우가 많다는 사실입니다. 노트북, 휴대폰, 데스크톱, 태블릿, 프린터, 프로젝터, 게스트 Wi-Fi와 각종 '스마트' 커넥티드 디바이스에서 전송하는 DNS 요청의 양과 종류가 매우 많기 때문에 DNS 로그를 지속적으로 모니터링하고 분석하는 전담 리소스를 배치한다고 해도 정확히 무엇이 '정상'인지 제대로 파악하기가 어렵습니다. 비정상 DNS 트래픽을 효과적으로 가려내기에는 기업의 샘플 사이즈가 너무 작기 때문입니다. 위협을 일관되게 효율적으로 식별하기 위해서는 글로벌 패턴을 심도 있게 파악해야 합니다.

빠르고 간편하고 편리한 클라우드 기반 보안으로 위협으로부터 기업을 사전에 방어

Akamai의 새로운 Enterprise Threat Protector는 기업의 리커시브 DNS 설정을 수정함으로써 표적 공격으로부터 기업을 사전에 방어합니다. 기업의 모든 웹 요청은 DNS로 시작되기 때문에, DNS는 기업 전체의 웹 요청에 대한 가시성을 확보하고 보안 정책을 적용하기에 가장 적합한 지점입니다.

클라우드에서 실행되는 솔루션인 Enterprise Threat Protector는 간편하게 설정·확장·배치할 수 있습니다. 하드웨어나 소프트웨어를 설치할 필요가 없으며, 다운타임이 없습니다. 단 몇 분 만에 모든 지사와 전 직원, 모든 디바이스에 대해 보안 및 제한적 사용 정책(AUP) 규칙과 업데이트를 적용할 수 있습니다. 클라우드 포털을 통해 한 곳에서 관리를 수행할 수 있으며, 대시보드에서 DNS 트래픽, 위협 이벤트, AUP 활동을 상세하게 파악할 수 있습니다. 여타 보안 제품과 보고 툴과도 손쉽게 통합할 수 있어 기업의 심층적 방어 전략을 구성하는 모든 레이어에서 투자를 극대화할 수 있습니다.

Enterprise Threat Protector는 Akamai의 통신사급(carrier-grade) Intelligent Platform을 기반으로 설계되었으며, Akamai CSI(Cloud Security Intelligence)의 실시간 인텔리전스를 기반으로 실행됩니다. Akamai는 포괄적인 DNS 도메인 관련 전문 지식, 100% 가용성 SLA, 입증된 AnswerX 서비스와 매일 전 세계 웹 트래픽의 30%를 관리하고 매일 1500억 개의 DNS 쿼리를 처리하며 축적한 인사이트를 바탕으로 한 글로벌 트래픽과 위협에 대한 독자적인 가시성을 활용하여 기업과 기업 직원을 안전하게 보호합니다.

Enterprise Threat Protector에 대해 더 자세히 알아보시려면 akamai.com/etp에서 제품 설명서를 읽고 제품 데모를 살펴보십시오.

출처

1. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
2. https://www.av-test.org/en/statistics/malware/
3. Ponemon Institute: The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN
4. 상동
5. Ponemon Institute: 2016 Cost of a Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
6. Cybersecurity Ventures: 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Akamai는 신뢰도가 높은 세계 최대 규모의 클라우드 전송 플랫폼을 기반으로 고객이 사용하는 장소와 디바이스에 상관없이 안전하고 쾌적한 디지털 경험을 손쉽게 제공할 수 있도록 지원합니다. 전 세계적으로 촘촘하게 분산 배치된 Akamai의 플랫폼은 130개 국가에 위치한 20만 대의 서버로 구성되어 있으며 고객에게 우수한 성능을 제공하고 보안 위협을 방어합니다. 웹·모바일 성능 향상, 클라우드 보안, 기업 접속, 비디오 전송 솔루션으로 구성된 Akamai의 솔루션은 우수한 고객 서비스와 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 금융 기관, 이커머스 기업, 미디어·엔터테인먼트 사업자, 정부 기관이 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하십시오. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2017년 6월 발행.