멀웨어를 선제적으로 방어하기 위한
DNS 모범 사례 채택

390,000

매일 **39만 개 이상의 악성 프로그램**이 새롭게 등록됩니다.[1]

사이버 위협 환경은 급격히 변화하고 있습니다. 2017년에 전세계적으로 민간 및 공공 분야에 심각한 피해로 이어진 초대형 랜섬웨어 공격이 몇 차례 발생했습니다. 매일 등록되는 악성 프로그램 수는 39만 개가 넘습니다.[1] 또한 1월부터 지금까지 수백만 명에 달하는 고객의 민감한 개인 정보를 노출시킨 엄청난 데이터 유출 사고가 여러 번 보고되었습니다.[2] 사이버 범죄는 전세계 경제에 4500억 달러의 손해를 끼친 것으로 추산되며, 이 수치는 2021년까지 6조 달러로 급증할 것으로 전망됩니다.

사이버 범죄는 지속적으로 발생하는 문제입니다. 수법이 지속적으로 진화하고 경제적 이득이 커지면서 해커들은 보안 스택의 취약점을 파고드는 노하우와 이유가 생겼습니다. DNS(도메인 네임 시스템)는 많은 기업의 방어 체계에서 취약한 부분입니다. 따라서 리커시브 DNS 인프라를 악용해 기업을 대상으로 피싱 공격 및 데이터 유출을 시도하고 멀웨어 및 랜섬웨어 캠페인을 실행하는 악의적 공격자들이 지속적으로 증가하고 있습니다.

재정적 손실과 기업 이미지에 미치는 악영향을 감안하면 잘 알려진 보안 백도어인 DNS를 반드시 강화해야 합니다. Ponemon Institute에 따르면, 공격을 방어하는 데 들어가는 비용은 약 1800만 달러에 달하고[3] 이후 데이터 유출까지 발생하는 경우 400만 달러가 추가로 발생합니다.[4] 따라서 Fortune 1000대 기업이 사이버 공격으로 인해 2017년에 순위에서 사라질 것이라는 Forrester Research의 예측 결과는 긴박하고 엄중한 경고로 받아들여야만 합니다.[5]

1,800만

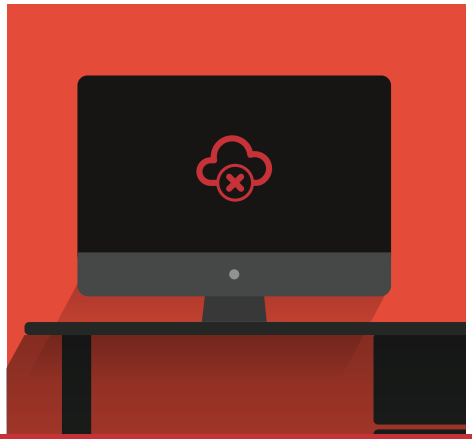
공격을 방어하는데 드는 비용은 **약 1800만 달러**입니다.[3]

사후 대응 및 대책 마련은 의미가 없습니다. 선제적으로 DNS 컨트롤포인트에서 멀웨어, 랜섬웨어, 피싱을 방어하는 일이 무엇보다 중요합니다. 간편한 설정 및 구축, 노출 시간을 제한하고 네트워크상의 모든 지사, 직원, 디바이스를 포함해 거의 즉각적으로 100% 컴플라이언스를 준수할 수 있는 클라우드 기반 솔루션이 가장 이상적인 해결 방안입니다.

그러나 기업 DNS 보안 솔루션을 방어 스택에 레이어로 배치할 때는 DNS 모범 사례를 동시에 적용해야 합니다. 다음은 DNS 악용을 방지하고, 기업 위협 보호 서비스와 함께 사용할 때 위협을 탐지, 차단, 방어할 뿐 아니라 제한적 사용 정책(AUP)을 기업 전반에 적용하도록 지원하는 업계 표준입니다.

1. 로컬 DNS 설정을 변경하지 못하도록 시스템을 차단합니다.

기업 위협 보호 시스템은 알려진 악성 사이트에 대한 요청을 차단합니다. 그러나 최종 사용자는 사진을 보거나 기사를 읽을 목적으로 이 기능을 피해서 사이트에 접속할 수 있습니다. 직원, 게스트 Wi-Fi 이용자, 네트워크상의 기타 사용자는 로컬 디바이스에서 DNS 설정을 우회하는 무료 리졸버(예: Google)를 통해 제한된 사이트에 쉽게 접속할 수 있습니다. 따라서 기업이 제공하는 모든 디바이스를 차단해 사용자가 로컬 DNS 설정을 변경하지 못하도록 차단해야 합니다. 이를 가장 쉽게 실행할 수 있는 방법은 Active Directory에서 그룹 정책을 생성하는 것입니다.



2. 써드파티 VPN을 설치하지 못하도록 시스템을 차단합니다.

인터넷 통신의 보안을 유지하기 위해 사용 가능한 VPN 터널은 2가지입니다.

- **분할 VPN 터널:** DNS 쿼리가 로컬 시스템에 도착하면 로컬 시스템이 관리자가 설정한 회사 정책을 준수하는 아웃바운드 쿼리를 생성합니다. 쿼리는 ISP로 전송되거나 회사의 로컬 DNS 서버로 전송될 수 있습니다.
- **비분할 VPN 터널:** DNS 쿼리가 터널을 통해 전송됩니다. 무료 또는 유료 써드파티 비분할 VPN 서비스를 다운로드하려고 하는 직원 또는 사용자는 회사에서 설치한 기업 위협 보호 필터를 우회할 수 있습니다.

직원, Wi-Fi 이용자 및 기타 사용자가 기업 위협 보호 또는 네트워크 방화벽을 우회할 수 있는 써드파티 VPN을 설치하지 못하도록 시스템을 차단하는 것이 모범사례입니다. 이렇게 차단하면 비즈니스 요구사항에 부합하는 경우를 제외하고 모든 워크스테이션에서 원격 VPN 접속이 차단됩니다.

3. 로컬 DNS 시스템에서 전송되는 DNS 쿼리만을 허용하도록 방화벽을 차단합니다.

모범 사례는 방화벽을 통해 신뢰할 수 있는 소스(로컬 DNS 포워더)로부터 들어오고 신뢰할 수 있는 대상(기업 위협 보호 시스템이 사용자에게 할당하는 리졸버 가상 IP인 VIP)으로 나가는 트래픽을 제외하고, DNS 포트 53의 아웃바운드 트래픽을 차단하는 것입니다. 해당 로컬 DNS 포워더는 기업 위협 보호 시스템을 통해 기업의 모든 로컬 쿼리를 조사해 정상 주소로만 전송되도록 합니다.

4. DNS 로그에서 의심스러운 패턴을 찾습니다.

DNS 로그에 의심스러운 패턴이 발견되면 멀웨어가 있을 가능성이 높습니다. 악의적 패턴에는 다음이 포함될 수 있습니다.

- **업무 시간 외에 발생하는 쿼리:** 새벽 2시에 직원의 노트북에서 쿼리가 수신되는 경우, 해당 직원이 그 시간까지 야근하고 있을 가능성이 거의 없으므로 의심스러운 쿼리로 간주해야 합니다.
- **비표준 네이밍 규칙을 사용하는 쿼리:** 악의적 공격자는 비표준 네이밍 규칙을 따르는 도메인 네임을 사용합니다. 이러한 도메인 네임은 사용 또는 등록되지 않기 때문에 즉각적인 등록이 가능하기 때문입니다. 따라서 도메인의 네이밍 규칙을 조사하고 정상 여부를 판단해야 합니다.
- **롱테일 로그 쿼리:** 롱테일 로그에서 쿼리를 찾으려면 먼저 모든 도메인 네임을 알파벳 순으로 정렬하고 중복된 도메인 네임을 모두 삭제합니다. 그런 다음 각각의 도메인 네임에 대한 요청 건수를 계산합니다. 로그의 테일 부분을 보면 한 두 차례만 접속한 도메인 네임 수를 확인할 수 있습니다. 이러한 도메인은 주로 업무 시간 외에 접속되고 비표준 네이밍 규칙을 사용합니다. 이와 같이 의심스러운 도메인은 소유자가 누구이고 등록된 기간은 얼마나 되었는지 등을 자세히 조사해야 합니다. 예를 들어, 도메인이 10시간 전에 등록되었고 등록 후 30분만에 접속되었다면 정상 도메인이 아닐 가능성이 높습니다.

5. 사용자 트래픽을 데이터 센터 트래픽과 분리합니다.

아웃바운드 트래픽을 데이터 센터 트래픽과 분리한 후 네트워크의 다양한 지점에서 트래픽이 송신되게 합니다. 이렇게 하면 데이터 센터에서 나가는 트래픽을 더욱 철저히 관리할 수 있습니다. 또한 데이터센터에서 나가는 DNS 트래픽이 의심스러운 도메인에 접속하고 있는지 확인합니다.

6. Tor 네트워크를 철저히 경계합니다.

Tor 네트워크란 기업과 개인이 인터넷상 정보의 프라이버시와 보안을 강화하기 위해 자발적으로 운영되는 서버 그룹입니다. 상당 수의 Tor 네트워크 사용자들은 정상적인 사용자이지만 Tor를 기업 네트워크에서 사용할 이유는 없습니다. Tor 진입 노드로 들어가는 접속이 있다면 악성 접속일 가능성이 높습니다. 수많은 표적 공격이 Tor를 사용해 CnC 서버와 통신하므로 엣지 방화벽에서 Tor 진입 노드를 차단하는 것이 바람직합니다. Tor 진입 노드를 차단하려면 일반에게 공개된 진입 모드 목록을 기반으로 모든 Tor 진입 노드를 차단하거나 방화벽의 HTTPS 트래픽에서 심층 패킷 검사(DPI)를 진행하면 됩니다.

멀웨어와 기타 표적 공격으로부터 비즈니스를 선제적으로 방어하는 방법에 대해 자세히 알아보려면 ETP 알아보기(Spotlight on ETP) 동영상을 시청하거나 akamai.com/etp 페이지를 확인하시기 바랍니다.

출처

1. https://www.av-test.org/en/statistics/malware/
2. https://www.identityforce.com/blog/2017-data-breaches
3. Ponemon Institute: The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN
4. Ponemon Institute: 2016 Cost of a Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. Forrester's 2017 Predictions: Dynamics That Will Shape The Future In The Age Of The Customer, https://go.forrester.com/wp-content/uploads/Forrester-2017-Predictions.pdf