Akamai

보고서

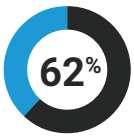
중소기업은 큰 위협에 직면해 있습니다

서론

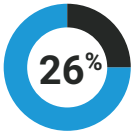
대기업에 대한 사이버 공격이 주요 뉴스로 부각되고 있지만, 중소 기업(SMB)은 대기업과 동일한 사이버 보안 리스크에 직면하고 있습니다. 공격자들이 금전적 이득에만 관심이 있기 때문에, 오늘날의 많은 공격은 대상을 구분하지 않습니다. 돈을 벌 수만 있다면 기업 규모에는 신경 쓰지 않습니다. 범죄자들은 다양한 방법을 사용하여 직원과 직원이 의지하는 디바이스, 심지어 널리 사용되는 지능형 연결 디바이스를 표적으로 삼습니다. 인터넷 서비스 사업자는 SMB가 스스로를 방어할 수 있도록 지원할 수 있는 유리한 입지에 있습니다.

이 간략한 문서에서는 SMB가 노출되는 가장 일반적인 위협과 그 영향에 대해 설명하겠습니다.

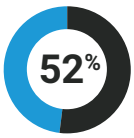
전국 중소기업 협회에서 발간한 기술 및 중소기업 설문조사에서 다음과 같은 흥미로운 통계 자료를 볼 수 있습니다.



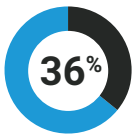
중소기업 경영자의 62%는 사이버 보안이 매우 중요한 우려 사항이라고 응답했고, 33%는 약간 중요하다고 응답했으며, 5%만이 전혀 중요하지 않다고 응답했습니다



기업 경영자의 26%만이 사이버 보안 문제를 처리하는 방법을 알고 있다고 응답했습니다



52%는 자기 기업이 사이버 공격의 영향을 받을 수 있다고 매우 우려하고 있으며 44%는 약간 우려했습니다. 반면 35%는 사이버 공격의 피해가 발생했다고 보고했습니다



36%는 정보가 도메인 또는 이메일 주소에서 잘못 전송되었다고 응답했고, 5%는 민감한 정보가 도난당했다고 말했으며, 4%는 은행 계좌에 접속했다고 했으며, 52%는 공격이 발생하여 서비스가 중단되었다고 보고했습니다

오늘날의 웹 기반 위협은 크게 멀웨어와 피싱이라는 두 가지 주요 영역으로 분류할 수 있습니다. 봇넷은 특별한 주의가 필요한 멀웨어의 중요한 하위 집합입니다.

멀웨어는 디바이스에 몰래 설치되는 악성 소프트웨어입니다. 감염된 웹 사이트는 디바이스의 소프트웨어 결함을 이용하여 멀웨어를 로드할 수 있습니다. 사용자가 악성 웹 사이트를 탐색한 후 클릭하여 악성 파일을 로드할 수도 있습니다. 일부 멀웨어는 디바이스에서 활성화된 다음 자체 네트워크를 통해 전파될 수 있습니다. 기업을 대상으로 하는 다양한 종류의 멀웨어가 있습니다.

암호화폐 채굴자는 피해자의 동의 없이 디바이스의 처리 능력을 사용하는 프로그램입니다. SMB 리소스가 손상되며, 랜섬웨어와 달리 디바이스 소유자에게 돈을 지불하라는 메시지가 표시되지 않기 때문에 이러한 공격을 탐지하기 어려울 수 있습니다.

POS(point-of-sale) 장치에 로드된 **특수 멀웨어**는 카드 데이터를 캡처하여 적에게 업로드해서 기업 경영자가 위험에 노출될 수 있습니다.

APT(Advanced Persistent Threats)는 네트워크에 액세스해서 중요한 데이터를 수집 및 추출합니다. APT는 매우 은밀한 상태로 설계되어 오랫동안 활성 상태를 유지할 수 있습니다. SMB는 소중한 데이터를 잃거나, 더 중요한 고객의 신뢰를 잃을 수도 있습니다. 또한 개인 데이터가 노출되는 경우 규제 조치를 받을 수도 있습니다.

랜섬웨어는 디바이스 또는 서버의 모든 것을 암호화하여 파일에 대한 액세스를 차단합니다. 공격자는 상당한 돈을 받고 암호 해독 키를 제공하지만 일부 경우에는 돈을 받고 키는 보내지 않습니다. 몸값으로 돈을 지불하는 건 SMB에게 그나마 나은 경우에 해당합니다. 최악의 경우 자금 및 업무상 중요한 데이터를 잃게 됩니다.

멀웨어가 귀중한 데이터를 수집하는 여러 가지 방법이 있습니다. **스파이웨어**는 스파이웨어는 로그인 인증정보 및 금융 데이터와 같은 데이터를 찾고 보고서를 범죄자에게 부하 분산합니다. **데이터 유출** 멀웨어는 컴퓨터에서 중요한 데이터를 찾아 식별하고 추출할 수 있도록 개발되었습니다. 키로거는 키 입력을 기록하고 범죄자가 금융 계좌, 소셜 미디어 로그인 또는 기타 중요한 정보에 접속할 수 있도록 훈련 받을 수 있습니다. **은행 트로이 목마**는 사용자의 행동을 모니터링하여 로그인 자격 증명을 알아보거나 은행 웹사이트를 가장하여 돈을 훔칩니다.

봇넷은 일반 범죄자 또는 그룹이 중앙 채널(명령 및 제어[C2]라고 함)을 통해 제어하는 동일한 멀웨어에 감염된 디바이스 네트워크입니다. 봇넷은 주로 빌릴 수 있으며, 대부분의 봇넷은 위에서 설명한 것과 같은 다양한 기능을 수행하여 수익을 창출할 수 있습니다.

피싱은 사기, 특히 소셜 엔지니어링을 이용하여 피해자를 속여 공격자가 수익을 창출할 수 있는 정보를 노출하도록 유도합니다. 과거에는 피싱 공격을 통해 사용자가 원치 않는 스팸 이메일의 링크를 클릭하여 민감한 정보를 공개하도록 유도했습니다. 피싱 공격 개발자들은 다양한 노력을 기울이고 있습니다. 이제는 소셜 미디어 게시물이나 댓글에는 물론 문자 메시지, SMS, Skype, Messenger 또는 기타 서비스에 피싱 URL을 포함하기도 합니다.

모바일 디바이스는 주요 피싱 타겟입니다. 화면이 작고 멀티태스킹으로 사용할 수 있어 악성 링크를 식별할 수 있는 미묘한 신호를 놓치기 쉽기 때문입니다. 피싱 사기범들은 보다 교묘하게 속이기 위해 다른 문자 집합의 모양과 유사한 문자를 사용하여 합법적인 도메인 이름을 모방하고 있습니다.

다음은 사용된 문자열의 실제 예입니다.

7eleven.com

Adîdas.com

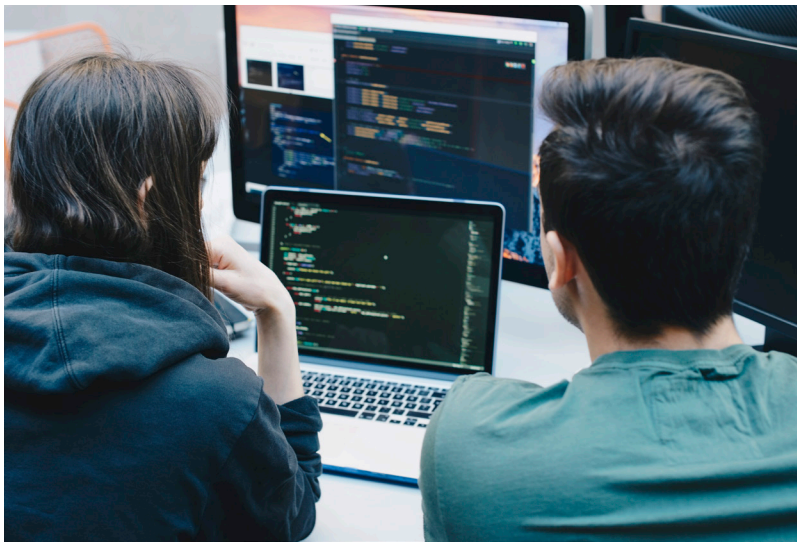
adidąs.com

philippineairlınes.com

rolęx.com

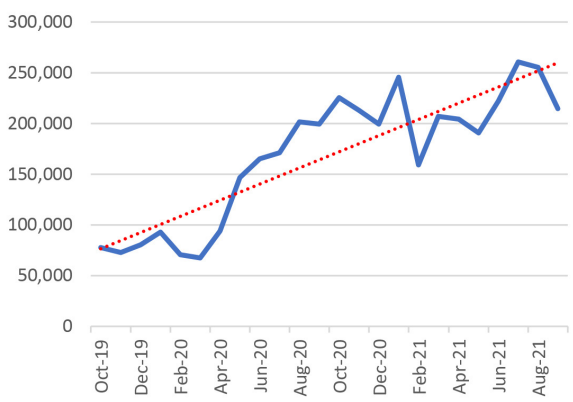
singaporeaır.com

thaiairways.com



피싱은 최근 성장세를 보이고 있습니다. Anti-Phishing Working Group에서 발표한 2021년 3분기 피싱 활동 동향 보고서: "피싱 공격은 3분기에 월간 신기록에 달하였으며 2019년 말에 비해 두 배로 증가했습니다." 보고서에서 가져온 아래 차트에서 트렌드를 볼 수 있습니다. 이는 소프트웨어 결함을 악용하는 것보다 사용자를 속여서 의도하지 않은 조치를 취하도록 하는 것이 더 쉬울 수 있기 때문입니다.

2019년 4분기 — 2021년 3분기 중 피싱 공격



Akamai의 통신 사업자 및 기업 보안 연구 팀이 수집한 데이터에 따르면 피싱에 사용되는 도메인 이름의 수명이 감소하는 것으로 나타났으며, 2019년 3월 기준 평균 수명은 약 1.5시간으로 줄었습니다. 이는 보안에 직접적인 영향을 미칩니다. 방어는 공격만큼 민첩해야 합니다.

결론

다음은 웹 위협의 일부분에 불과합니다. 공격자들은 공격의 실행 가능성을 지속적으로 평가하고 수익을 극대화하기 위해 혁신해서 작업의 모습과 기능을 변화시키고 있습니다. 또한 다른 종류의 멀웨어는 주로 주의를 산만하게 하거나 귀찮게 하여 원치 않는 광고나 콘텐츠를 보여줍니다.

SMB는 고유한 요구 사항과 제약 조건과 호환되는 솔루션을 통해 웹 기반 위협으로부터 보호받아야 합니다. Akamai는 SMB용으로 설계한 Secure Internet Access Service를 제공합니다. 이 보안 솔루션을 사용하면 관리 부담 없이 이 문서에서 설명한 공격으로부터 SMB를 보호할 수 있습니다. 직장의 모든 디바이스와 모든 사람(게스트 포함)을 자동으로 보호할 수 있습니다. 비즈니스 매니저는 간단한 그래픽 포털을 통해 네트워크에서 발생하는 상황 및 차단된 위협에 대해 즉시 확인할 수 있습니다.

Akamai Secure Internet Access Services는 ISP에 다음을 지원하도록 제작되었습니다.

- SMB용 엔터프라이즈급 보안 방어로 수익 창출
- 속도 및 가용성을 뛰어넘어 넘어 보안을 기반으로 SMB 서비스 차별화 추구
- 배포 장벽을 최소화, 비용 절감 및 서비스 제공 간소화

이 서비스는 브랜드에 맞는 모양과 느낌으로 완전히 사용자 정의할 수 있으며, 기능 세트와 위협 인텔리전스도 현지 시장의 요구 사항에 맞게 조정할 수 있습니다.

누구에게나. 모든 디바이스 대상으로. 언제든 가능합니다. Akamai가 도와드릴 수 있습니다.

자세한 내용을 알아보려면지금 Akamai에 문의하세요.

Akamai

Akamai는 온라인 라이프를 지원하고 보호합니다. 전 세계 대표적인 기업들은 매일 수십억 명의 사람들의 생활, 업무, 여가를 지원할 디지털 경험을 구축하고, 전송하고, 보호하기 위해 Akamai를 선택합니다. 클라우드에서 엣지까지 전 세계에서 가장 분산된 컴퓨팅 플랫폼을 구축한 Akamai는 고객의 애플리케이션 개발과 실행이 용이하도록 도우며, 사용자와 가까운 곳에서 경험을 제공하고 위협을 먼 곳에서 차단합니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 대한 자세한 정보는 akamai.com 및 akamai.com/blog를 방문하거나 Twitter 및 LinkedIn에서 Akamai Technologies를 팔로우하세요. 2022년 6월 발행.