주요 국제 공항의 사이버 공격 저지 노력

IBM Security QRadar EDR을
사용하여 에어 갭 네트워크 내부의 멀웨어 찾기

세계에서 가장 큰 공항 중 한 곳은 에어 갭 네트워크를 활용하여 보안부터 물류까지 내부 운영을 관리합니다. 공항이라는 고립 환경 특성에도 불구하고, 정보를 캡처하고 로컬에 저장할 수 있는 멀웨어에 감염된 디바이스가 발견되었습니다.

보안 문제:

- 작동 중단 시간이 허용되지 않는 중요 인프라구조
- 네트워크 내 보안 조치 부족
- 낮은 보안 및 높은 보안의 디바이스를 함께 연결하는 에어 갭 네트워크
- 에어 갭 내 모든 디바이스의 비가시성

세계 최대의 교통 허브 중 하나인 이 주요 국제 공항은 하루 1,000건이 넘는 비행으로 매년 7,000만 명의 승객을 연결합니다. 공항은 전반적으로 매우 우수한 보안 프로토콜을 따랐습니다. 몇 가지 필수 서비스를 운영하고 인터넷 감염을 방지하기 위해 완전히 격리된 네트워크를 채택했습니다. 하지만, 에어 갭 네트워크는 잘못된 안도감을 심어주었습니다. 에어 갭 내의 모든 디바이스가 인터넷에 접속할 수는 없지만, 에어 갭 내 각 네트워크 세그먼트는 트래픽 제어 없이 서로 연결되어 있었습니다.

또한, 정보 키오스크와 같은 디바이스에 포함된 에어 갭 네트워크는 물리적으로 공용 접근이 가능했습니다. 이는 필수 서비스가 잠재적 공격에 노출된 상태였음을 뜻합니다. 게다가, 정보를 밖에서 안으로 가져올 수 있는 유일한 수단이 USB 드라이브를 사용하는 것이었습니다. 공항 직원이 멀웨어를 안으로 가지고 들어올 잠재적 위험이 있기 때문에 엔드포인트가 취약한 상태였습니다.

운영 중단 없는 탐지 및 문제 해결

솔루션 개요:

- 이 공항은 NanoOS 기술을 활용하여 엔드포인트와 인프라 전반에서 탁월한 가시성을 제공하는 IBM® Security QRadar EDR 소프트웨어를 구현했습니다.
- QRadar EDR의 행동 엔진은 격리된 네트워크상에서 성능 저하 없이 작동합니다.
- 이 공항은 강력한 위협 헌팅 기능을 활용하여 인시던트를 재구성하고 분석합니다.

이 공항은 일부 엔드포인트의 속도가 느려진 것처럼 보였기 때문에 IBM Security QRadar EDR 소프트웨어를 사용하여 에어 갭 네트워크에 대한 상태 점검을 실행했습니다. QRadar EDR이 첫 세그먼트에 배포되자 엔진이 소수의 디바이스에서 잠재적인 악의적 활동을 찾아냈습니다. 초기 분석에서는 공공 접근이 가능한 키오스크가 초기 엔트리 포인트로 표시되었고, 그 후의 분석에서는 체크인 구역의 기기가 두 번째 엔트리 포인트로 나타났습니다. 이 두 개의 악성 벡터가 제한된 수의 디바이스에 퍼져 다른 네트워크 세그먼트를 건드린 것입니다.

QRadar EDR 플랫폼이 제공한 가시성을 통해 인시던트를 처음부터 재구성할 수 있었고 공항의 비즈니스 연속성을 방해하지 않고 감염을 안전하게 치료할 수 있었습니다.

근본 원인 분석

초기 배포에서 몇 가지 행동 이상을 발견했습니다. 애플리케이션이 인메모리 키로거를 기본 브라우저의 숨겨진 인스턴스에 주입하면서 인메모리 키로거를 설치했습니다. 그런 다음, 또 다른 스레드가 디스크를 훑어 Microsoft Word 파일, PDF 파일, 쿠키, 브라우저 데이터베이스를 찾았습니다. 이러한 정보는 숨겨진 폴더 내에 수집되었으며 커맨드 및 컨트롤(C2) 서버로의 전송 시도가 일정한 간격으로 있었으나, 네트워크가 외부 세상으로부터 완전히 격리되어 있었기 때문에 성공하지는 못했습니다.

감염 벡터를 더 심층적으로 살펴보자 흥미로운 결과가 나왔습니다. 이 벡터는 비정상적으로 컸고, 로컬 안티바이러스 프로그램뿐만 아니라 샌드박스 분석도 우회하기 위한 일련의 메커니즘을 포함했습니다. 큰 사이즈는 안티바이러스 에뮬레이션 엔진을 회피하려는 시도의 일환일 가능성이 높았습니다. 이러한 시스템은 일반적으로 전체 바이너리의 작은 청크만을 대항하기 때문입니다.

결국, 서로 다른 두 벡터가 확인되었으며,

하나는 공용 키오스크에 설치되었고 다른 하나는 탑승 수속 관리 네트워크 센서의 일부를 구성하는 장치에 설치되었습니다. 두 벡터는 서로 다르게 생겼지만(주로 탐지 회피를 위해 사용되는 엄청난 양의 정크 인스트럭션으로 인해) 멀웨어는 동일하게 보였습니다. 두 가지 사례 모두에서 같은 C2 서버에 접속하려는 시도가 있었고 같은 방식의 움직임이 있었습니다.

공격 재구성

QRadar EDR이 유출 후에만 배포된 경우, 모든 정보를 이용할 수 있는 것이 아니며, 네이티브 인프라는 최소한의 운영 시스템 수준의 로깅만 사용합니다. 최소의 정보 양에도 불구하고, 추적 분석은 5개월 전에 발생한 감염과 서로 다른 두 개의 USB 드라이브로부터 며칠 간격으로 감염된 두 개의 엔드포인트를 보여주었습니다.

이 공항은 감염된 디바이스를 청소하고 데이터 유출을 피하기 위해 QRadar EDR의 문제 해결 모듈을 사용했습니다. 이 솔루션의 위협 헌팅 인터페이스는 전체 인프라에서 벡터가 없다는 것을 확인하는 데 도움이 되었습니다.

다른 엔드포인트는 이 벡터 중 하나에 의해 감염되었는데 이는 주로 취약한 패스워드가 원인이었으며, 멀웨어가 접속할 수 있는 모든 디바이스에서 패스워드를 맞추려는 시도가 무작위 간격으로 일어났습니다. 멀웨어가 정보를 끊임없이 수집했으며 어떤 보유 통제를 적용하거나 스스로의 스토리지에 제한을 적용하지 않은 것으로 보였습니다. C2로 연결하려는 시도가 8시간마다 있었지만 에어 갭 때문에 한 번도 성공하지 못했습니다.

멀웨어가 자가 복제 능력이 있고 자동으로 자신의 스토리지를 외부 USB 드라이브로 복사할 수 있다고 할지라도 이 기능이 활성화되지 않았다는 것을 최종 분석에서 확인했습니다. 아마도, 유출이 수동으로 개시되어야 했던 것 같습니다.

대응과 교정

이 공항은 감염된 디바이스를 청소하고 확인된 스토리지 폴더를 지워 데이터 유출을 방지하기 위해 QRadar EDR의 문제 해결 모듈을 사용했습니다. 이미 감염된 것으로 확인된 디바이스를 제외한 전체 인프라에서 같은 벡터의 부재를 확인하기 위해 이 솔루션의 위협 헌팅 인터페이스가 필수라는 것이 입증되었습니다. 또한 이 공항은 멀웨어의 인스턴스가 다른 디바이스에서 탐지되지 않은 채 실행되지 않도록 행동 검색을 수행했습니다. 해당 벡터와 그 변종이 인프라에 없다는 것을 확인할 수 있을 때까지 확인된 모든 행동, 지속적 위협 및 데이터 수집 방법을 찾았습니다.

마지막으로, 로컬 보안 팀이 내부 트래픽 제어를 위한 더 견고한 룰 세트를 수립했습니다. 네트워크의 공용 부분은 운영에서 격리되었고, 로컬 보안 팀은 지속적인 엔드포인트 모니터링과 정기적인 위협 헌팅 캠페인 실행을 시작했습니다.

결론: 공항 서비스에 대한 중대한 위험 제거

에어 갭은 강력한 수준의 보안을 제공할 수 있지만, 엄격한 방식으로 구현되지 않을 경우 잘못된 안도감을 생성할 수 있습니다. 데이터를 수집했지만 외부로 유출하지는 않았기 때문에 공격의 의도가 불분명하다 하더라도, 확실하게 추측할 수 있는 것은 공격자가 인프라 내에 오픈 도어를 갖고 있었던 이유가 단순히 정보를 유출하기 위해서가 아니라 공항의 운영을 적극적으로 방해하기 위해서였다는 것입니다. 탑승 수속 구역을 표적으로 하여 실행된 간단한 랜섬웨어는 불가피한 지연을 야기할 수도 있었으며, 보안 구역을 표적으로 하여 같은 공격이 실행되었다면 노골적으로 항공편을 차단하고 심각한 영향을 미칠 수도 있었습니다.

QRadar EDR 플랫폼이 제공한 가시성을 통해 인시던트를 처음부터 재구성할 수 있었고 공항의 비즈니스 연속성을 방해하지 않고 감염을 안전하게 치료할 수 있었습니다.

이 주요 국제 공항에 대한 정보

이 주요 국제 공항은 세계에서 가장 큰 운송 허브 중 하나입니다. 매일 1,000건 이상의 비행으로 매년 7,000만 명의 승객을 연결하는 이 시설은 중요한 인프라로 분류됩니다.

솔루션 컴포넌트

- IBM Security® QRadar® EDR