FireEye

FireEye SmartVision

엔터프라이즈 네트워크 내부의 의심스러운 이동 탐지

요약

- 이전에 탐지되지 않았던 의심스러운 내부 이동 탐지
- 네트워크 내부의 의심스러운 네트워크 트래픽에 대한 가시성 제공
- 고급 네트워크 이벤트 상관관계 및 분석 엔진, 머신 러닝 및 120여 가지 침입 탐지 규칙 활용
- FireEye Network Security의 일부로서 다양한 설치 방식 지원

변화하는 오늘날의 위협 환경

오늘날의 위협 환경은 끊임없이 변화하면서 지능화된 공격자를 저지하기 위한 예방 수단의 신뢰성이 갈수록 낮아지고 있습니다. "진열장을 깨고 물건을 탈취하는" 일차원적인 공격 방식의 시대는 이제 갔습니다. 오늘날의 공격자들은 일단 네트워크에 침입하면 침입한 환경에서 계속 활동하면서 은밀한 내부 조사를 통해 유용한 정보를 빼냅니다.

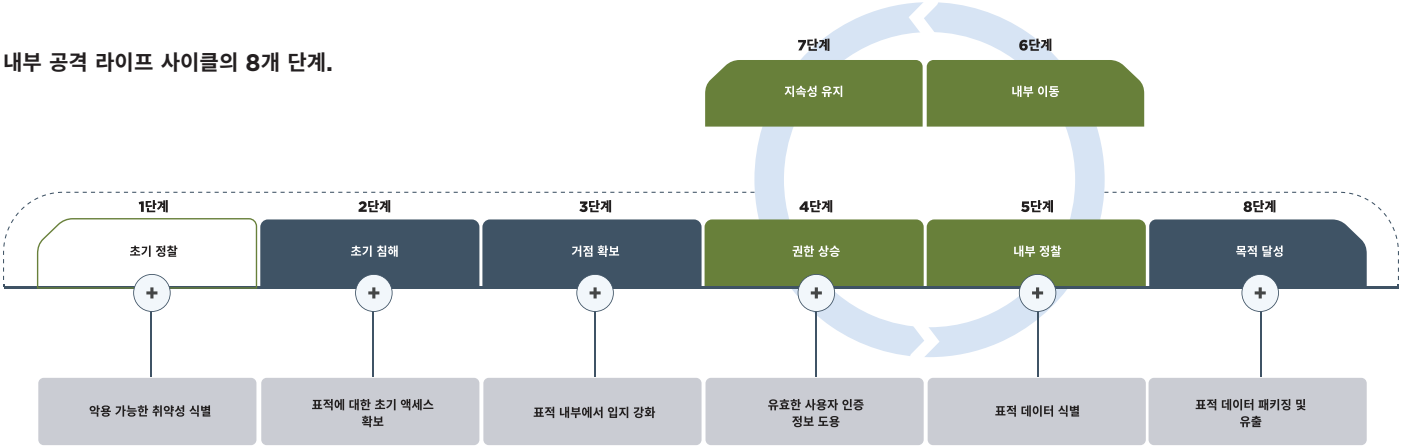
한편 공격자는 발전된 포렌식 무효화 기법을 이용해 내부적인 "East-West" 이동 행위를 감추고 전자적인 흔적을 숨깁니다. 이 같은 사이버 범죄자들은 향후에 계속 진입하고 네트워크에 액세스할 수 있도록, 침입한 각 시스템마다 고유한 구성의 맞춤형 백도어를 로드하는 경우가 많습니다.

침입 후 탐지와 관련한 문제

유감스럽게도, 오늘날 침입 후 내부 활동을 탐지하는 데 사용되는 툴은 한계가 있거나 그러한 활동을 전혀 탐지하지 못합니다. 일례로, 보안 정보 및 이벤트 관리 시스템(SIEM)은 번거로운 설정 과정과 복잡한 관리 방식으로 인해 내부 이동을 놓치거나 최악의 경우 수많은 오탐을 발생시켜 보안 팀의 업무 부담을 가중시킵니다.

공격자의 이동을 제한하고 한정된 네트워크 세그먼트로 피해를 억제하기 위해 여러 개의 방화벽을 설치하는 조직이 많습니다. 이 같은 방식은 비용이 높고 복잡할 뿐만 아니라, 공격자가 이미 일정 수준의 신뢰받고 인증된 액세스 권한을 확보한 상태이고 따라서 방화벽을 완전히 무력화할 수 있기 때문에 방화벽으로는 의심스러운 내부 이동을 탐지하고 차단하지 못하는 경우가 많습니다.

내부 공격 라이프 사이클의 8개 단계.



Fireeye SmartVision

FireEye는 데이터 도용을 위한 내부 활동의 징후가 되는 몇 가지 고유한 지표와 행동을 찾아냈습니다. 이 같은 인텔리전스를 바탕으로 FireEye는 이전에 탐지되지 않았던 내부 공격 이동을 탐지하는 새로운 기능인 FireEye SmartVision™을 개발했습니다.

SmartVision을 FireEye Network Security 플랫폼과 함께 사용하면 보안 관리자가 여러 가지 의심스러운 내부 이동을 탐지하여 환경의 경계 전반과 핵심 네트워크 및 서버 내의 의심스러운 네트워크 트래픽에 대한 새로운 가시성을 확보할 수 있습니다.

SmartVision의 핵심 구성 요소는 다음과 같습니다.

고급 상관관계 및 분석 엔진

데이터 유출 시도를 탐지하는 머신 러닝 모듈

사소한 침해 지표(IOC)를 식별하는 120여 가지 탐지 규칙

SmartVision이 탐지 불가능한 공격을 탐지하는 방법

SmartVision은 엔터프라이즈 네트워크 내에서 다양한 악의적인 활동을 탐지합니다. 내부 공격 라이프사이클 동안 공격자의 이동에서 나타나는 고유한 특성 덕분에 SmartVision은 특정 활동을 포착하여 경보를 트리거할 수 있습니다.

권한 상승 단계

이 단계에서 SmartVision은 다음을 식별합니다.

- **"Pass the hash":** 공격자가 사용자 암호의 기반 NTLM 또는 LanMan 해시를 사용하여 원격 서버 또는 서비스에 대해 인증을 받는 해킹 기법입니다.
- **파일 없는 악성코드:** SmartVision은 평문 패스워드, 해시, PIN 코드 및 Kerberos 티켓을 빼내기 위한 잘 알려진 툴인 "mimikatz"와 같은 파일 없는 악성코드를 탐지합니다.

내부 정찰 단계

이 단계에서 FireEye Network SmartVision은 다음을 식별합니다.

- **네트워크 매핑:** 공격자가 SNMP 기반 기법, 적극적인 탐색 또는 경로 분석 기법을 사용하여 네트워크에서 엔드포인트 및 서버 같은 장치를 찾고, 장치의 운영 체제 정보, 연결 상태 등을 알아낼 수 있습니다.
- **호스트 및 서비스 열거:** 공격자들은 검색 툴을 사용하여 사용자 이름, 작업 그룹, 공유 리소스, 개방 포트, 원격 호스트, 기타 네트워크 서비스 등에 대한 정보를 수집합니다.
- **사용자 검색:** 공격자들은 관리자 권한이 있는 사용자를 알아내기 위해 WinAPI 호출을 사용하는 툴을 활용합니다. WinAPI 호출은 서버, Active Directory, 도메인 컨트롤러 및 엔드포인트의 사용자 계정에 대한 정보를 제공합니다.

내부 이동 단계

이 단계에서 SmartVision은 공격자가 SMB and SMB2 프로토콜을 이용하여 악성코드, 파일, 특히 패스워드 덤프를 전송하는 SMB 프로토콜 트래픽을 식별합니다.

데이터 유출 단계

이 단계에서 SmartVision은 머신 러닝 데이터 유출 모듈을 통해 데이터 도용과 관련한 비정상적인 파일 전송을 탐지합니다.

SmartVision의 설치

SmartVision은 네트워크 설계와 요구 사항의 조합에 최적화된 다양한 방식으로 FireEye Network Security 환경의 일부로 설치할 수 있습니다. FireEye Network Security 센서는 일반적으로 서버에 연결된 트래픽상의 내부 방화벽 배후에 설치됩니다. 따라서 센서가 클라이언트와 서버 간 또는 피어 시스템 간의 트래픽을 캡처할 수 있습니다.

SmartVision은 인라인 및 대역외 설치를 지원하며 온프레미스 환경과 네트워크 패킷 브로커/TAP 환경에 사용할 수 있습니다.

요약

위협 환경은 끊임없이 변화하면서 지능화된 공격자를 저지하기 위한 예방 수단의 신뢰성이 갈수록 낮아지고 있습니다. 따라서 침입 탐지의 중요성이 점점 더 커지고 있습니다. 특히 네트워크를 통해 들키지 않고 손쉽게 이동하는 위협 범죄자의 능력이 향상되고 있다는 점을 감안할 때 그 중요성은 더욱 커집니다.

내부 공격 라이프사이클의 구조는 기존 보안 솔루션으로는 완벽하게 해결할 수 없는 수많은 문제를 야기합니다. 하지만 FireEye는 데이터 도용을 위한 내부 활동의 징후가 되는 고유한 지표와 행동을 찾아냈습니다.

이 같은 인텔리전스를 바탕으로 FireEye는 이전에 탐지되지 않았던 내부 공격 이동을 탐지하는 혁신적인 솔루션으로서 SmartVision을 개발했습니다. 이제 기업이 FireEye Network Security 플랫폼의 일부로 다양한 네트워크 아키텍처에 SmartVision을 설치하여 내부 위협 행위에 대한 가시성을 확보하고, 내부에서 이동하는 위협에 대한 보안 상태를 유지할 수 있습니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

SB.FSV.KO-KR-032018

FireEye