IBM MaaS360 Mobile Threat Management

iOS 및 Android 장치에서 모바일 악성 프로그램 중단

주요 장점

- BYOD 및 기업 소유 장치 모두 안전하게 지원
- 거의 실시간으로 모바일 위협을 사전 대처식으로 관리
- 기업 및 개인 정보의 민감한 데이터 누출 위험 감소
- 모바일 보안 위험을 개선하기 위한 자동 조치 실행

모바일 악성 프로그램 - 차세대 큰 보안 위협

조직들은 이동성으로 인해 유례 없는 속도로 변화하고 있습니다. 언제 어디서나 자신만의 장치를 가지고 다닌다(BYOD)라는 동향은 계속해서 기업 전반에 퍼지고 있습니다. 모바일 앱들은 직원들을 위해 새롭고 효율적인 작업 흐름을 만들어 가고 있습니다. 데이터, 이메일 및 컨텐츠 작업에 대한 원활한 접근 역시 이에 따라 성장하고 있으며, 이러한 동향으로부터 생산성을 강화하고 있습니다.

모바일 장치가 기업의 중심이 되게 한 인기와 속도 덕분에, 해커와 도둑들은 악성 프로그램으로 모바일 장치를 노리고 있으며, 차세대 큰 보안 위협을 만들어내고 있습니다. 기업 데이터는 특히 악성 앱과 악성 프로그램 웹사이트에 취약합니다.

- 2014년에 1,380억 개의 앱이 다운로드되었습니다.[1]
- 모바일 악성 프로그램이 늘어나고 있습니다. 악성 프로그램 코드가 언제든지 1,160만 개 이상의 모바일 장치로 감염됩니다.[2]
- 최근 WireLurker 및 Masque 공격이 iOS 장치를 위협했습니다.[3,4]
- 회사 브랜드 손실과 재정상 손실이 복합되면서, 1회의 침투로 인한 예상 손실액이 1,100만 달러를 넘습니다.[5]

IT와 보안 업계의 리더들은 모바일 악성 프로그램을 사전에 감지, 분석 및 개선하기 위한 최신의 강력한 보안 솔루션이 필요합니다.

기업에서 모바일 위협 중단

IBM® MaaS360® Mobile Threat Management는 iOS와 Android 장치에서 악성 프로그램으로부터 보호하는 최신 시스템을 제공합니다. 기업 데이터를 손상시키기 전에 위험을 감지하고 위협을 관리할 수 있습니다.

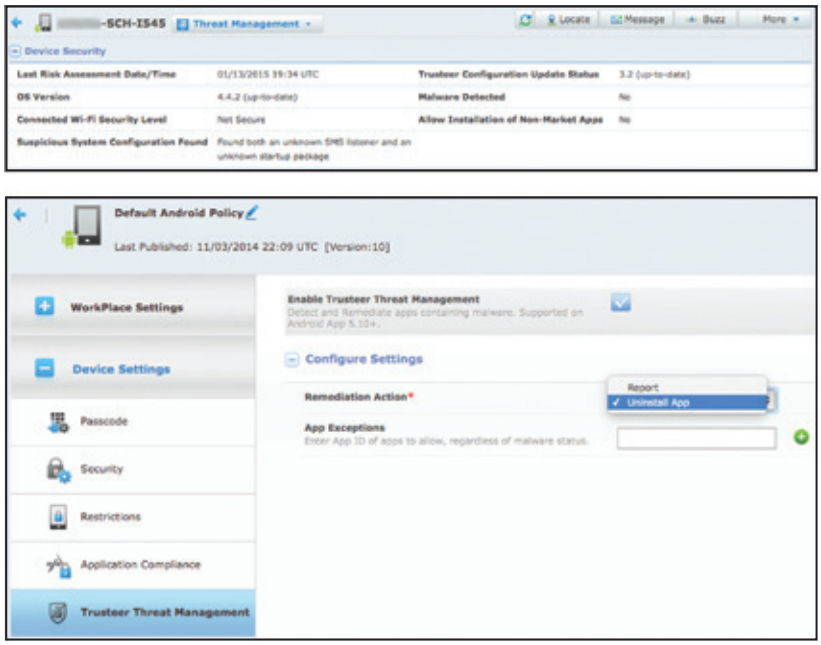

그림 1: MaaS360 Mobile Threat Management에서의 보호된 장치 및 정책 설정에 관한 보고 데이터 예시

IBM Trusteer®와의 전체적인 통합을 통해 사기와 데이터 침투로부터 조직을 보호하기 위해 수억 명의 사용자가 사용하고 있는 MaaS360은 EMM(Enterprise Mobility Management)으로 새로운 보안 계층을 제공합니다.

악성 프로그램이 조직의 모바일 변화를 늦추게 하지 마십시오. MaaS360으로 제공되는 보안과 기업 생산성 이니셔티브의 균형을 맞추십시오.

모바일 악성 프로그램 감지 및 개선

- 지속적으로 업데이트되는 데이터베이스에서 악성 프로그램 서명과 악성 동작으로 iOS 및 Android 앱을 감지하고 분석하십시오.
- 앱 예외 추가로 허용 가능 앱 사용량 조정
- 세밀한 정책 제어로 적합한 조치 실행
- 거의 실시간에 가까운 규정 준수 규칙 엔진으로 개선 자동화
- 악성 프로그램이 감지되었을 때 사용자 및 담당자에게 알림
- My Alert Center에서 손상된 장치 보기 및 My Activity Feed 대시보드에서 감지 이벤트 보기
- 자동으로 악성 프로그램이 있는 앱 제거(일부 Android 장치의 경우, 예: Samsung SAFE™)
- 액세스 차단, 장치에 대한 선택적 또는 완전 삭제
- MaaS360 컨테이너 솔루션 사용 제한
- 다음 사항과 같은 장치 위협 속성 수집 및 보기:
  - 악성 프로그램 감지
  - 미확인 SMS 리스너 또는 시작 패키지 등 의심스러운 시스템 구성 발견
  - 비보안 Wi-Fi 핫스팟 연결
  - 비마켓 앱 설치 허용
  - 운영 체제 버전
- 악성 프로그램 감지 이벤트의 감사 기록 검토

추가 탈옥 및 루팅 감지

- 손상되거나 취약한 모바일 장치 감지
- 운영 체제에서 공격자에게 추가 권한을 제공할 수 있는 탈옥한 iOS 및 루팅된 Android 장치로부터 보호
- 탈옥 및 루팅 장치 감지를 숨기는 은폐자 및 활성 은폐 기술 발견
- 빠르게 움직이는 해커들에게 보다 잘 대처하기 위해 앱 업데이트 없이 무선 업데이트되는 감지 로직 사용
- 보안 정책 및 규정 준수 규칙 설정으로 개선 자동화
- 액세스 차단, 장치에 대한 선택적 또는 완전 삭제

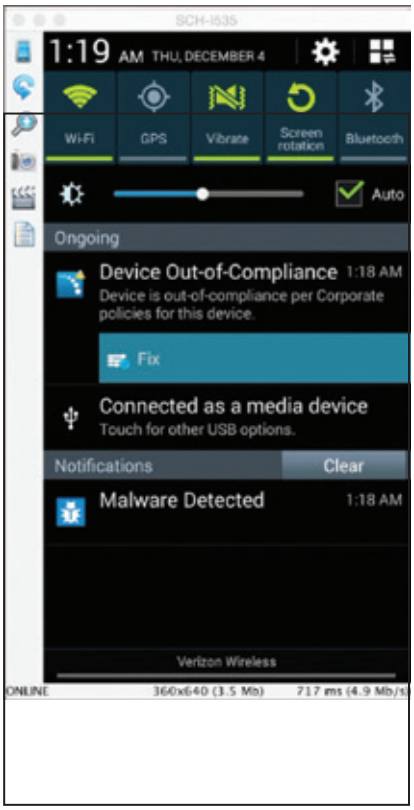

그림 2: 장치 상에서 악성 프로그램 알림 예시

IBM Security Trusteer Mobile Risk Engine

- 적응형 악성 프로그램 방지를 위한 보호 및 사이버 범죄 인텔리전스 계층 제공
- 최신 공격 행동에 대한 재빠른 감지 및 적응으로 악성 프로그램이 사실상 사기를 저지를 기회 상실
- 장치 및 앱위험 요소를 기반으로 거의 실시간으로 모바일 위험 평가 수행
- 최신 악성 프로그램, 탈옥 및 루팅 확인을 제공하기 위한 지속적인 업데이트

IBM 보안 사기 방지 솔루션에 관한 자세한 내용은 가까운 IBM 담당자 또는 IBM 비즈니스 파트너사에 문의하시거나 다음 웹사이트를 참조하십시오. **ibm.com**/security.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

제조: 미국
2016년 1월

재활용하세요

WGD03057-KRKO-01

1 Arxan의 연차 보고서: "*모바일 앱 보안 상태로 상위 100개의 모바일 앱에 대한 앱 해킹 증가 밝혀내*", 2014년 11월, Arxan Technologies, Inc., https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

2 Kindsight Security Labs 악성 프로그램 보고서 – 2013년 4분기, Alcatel-Lucent, http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf

3 Xiao, Claud, WireLurker: OS X 및 iOS 악성 프로그램의 새 시대, Palo Alto 네트워크 상의 블로그 포스트; 2014년 11월 5일, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

4 Zue, Hui, Wei, Tao 및 Zhang, Yulong; Masque 공격: 귀하의 모든 iOS 앱이 저희에게 속해 있습니다, 2014년 11월 10일, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

5 2013년 사이버 범죄 연구 비용: 미국, HP Enterprise Security, Ponemon Institute 후원, 2014년 10월, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf