IBM Security
리더십 사고의 백서

모바일은 보안 업계의 새로운 놀이터입니다

모바일 악성 프로그램에 대한 보호 방법

IBM

모바일이 성장하는 만큼 위협도 커집니다

서론

이동성은 지속적인 스마트 장치의 증식, 폭발적으로 개발되는 모바일 앱, 그리고 작업 파일에 대한 접근성의 증가와 함께 전례 없는 속도로 기업을 빠르게 변화시키고 있습니다. 직원들은 BYOD（회사 업무에 직원 개인의 통신기기를 사용할 수 있게 하는 방침）를 위한 정책 채택과 심지어 업무 관련 활동에 개인 앱을 이용할 수 있도록 허가받음으로써 조직으로부터 사실상 언제 어디서든 더 큰 생산성을 부여받게 되었습니다.

그러나 조직은 민감 정보를 보호하는 데 필요한 기업 등급의 보안성을 배치하여 급증하는 이동성을 따라 잡는 데는 실패하고 있습니다. 해커, 절도범들은 모바일 엔드포인트에서 네트워크에 침투하여 민감한 업무 데이터를 손에 넣을 기회만 포착하고 있습니다. IT와 보안 업계 리더에게는 이러한 모바일 위협을 사전에 감지, 분석 및 개선하기 위한 최신의 강력한 보안 솔루션이 필요합니다.

약 1,600만 개의 장치가 언제든 악성 프로그램에 감염된 것으로 추산됩니다.

기업 내 모바일 급증

이동성의 성장과 관련된 수치는 계속해서 누적되고 있습니다. 2014년에는 휴대폰의 수（73억）가 지구상의 인구 수（70억）를 능가할 것이라고 예측되기도 했습니다.[1]

Arxan Technologies에 따르면 2014년에는 1,380억 개의 모바일 앱이 다운로드되었으며, 이 수치는 2017년까지 약 두 배로 증가하여 2,680억 개에 달할 것으로 예상됩니다.[2]

소비자는 스마트 장치와 앱을 개인적으로 사용함으로써 모바일 이동의 최초 촉매제 역할을 하였으나, 기업이야말로 이러한 가속적 추세로부터 확실한 이득을 취해 왔습니다. 직장 내 BYOD 경향은 계속해서 확산되고 있으며, 이에 따라 조직에서는 각자의 전체 노동력을 동원하도록 지원하여 조달 및 지원 비용을 절감하고 있습니다. 실제로 Gartner는 2017년에 고용주들의 절반이 BYOD를 요구할 것이라고 예측하고 있습니다.[3]

모바일 앱은 직원들을 위해 새롭고 효율적인 작업 흐름을 만들어 가고 있습니다. 또한 작업 데이터, 이메일 및 컨텐츠에 대한 막힘 없는 접근성이 증대되고 있으며, 이에 따라 생산성 증진 효과도 강화되고 있습니다. 조직에서는 모든 업무 과정에서 모바일을 최우선으로 고려하기 시작했으며, 더 나아가 기업 내 이동성 발달을 추진하기 시작했습니다.

모바일 앱이 공격할 때

그러나 해커와 절도범들은 기업의 변화에서 나타나는 이러한 중요 이점을 탈선시키는 위협 요소로 작용하고 있습니다. 모바일 장치 감염은 2013년에 20%였던 것에 비해 2014년에 25%로 증가하는 추세를 보이며 지속적으로 가속화되고 있습니다. 약 1,600만 개의 장치가 언제든 악성 프로그램에 감염된 것으로 추산됩니다.[4]

모바일 악성 프로그램은 특정 운영 체제를 이용하여 모바일 장치를 공격하도록 특수 설계된 악성 소프트웨어입니다.

데이터 위반의 영향은 회사 브랜드에 대한 손상뿐 아니라 잠재적 재정적 손실을 동반하여 상당한 비용을 유발합니다. Ponemon Institute에서 추정한 바에 따르면 2014년 단일 위반 비용은 $350만이며, 이는 매년 15%씩 증가할 것으로 예상됩니다.[5]

그림 1: 해킹 당한 최다 구매 Android 및 iOS 앱

악성 모바일 앱으로 인해 손상된 장치는 모든 기업에 실질적으로 막대한 위험원으로 작용합니다. 사용자를 보호하지 않는 네트워크에 연결하거나 믿을 수 없는 출처로부터 위험한 앱을 설치할 때 모바일 장치는 악성 프로그램에 취약해진다고 Arxan Technologies는 설명합니다. 최다 구매율을 기록한 Android 및 iOS 앱 가운데 각각 97%와 87%는 해킹 당한 후 타사 앱 스토어에 게시되었습니다.[6]

또 다른 Ponemon Institute 연구에서 밝혀진 바와 같이[7], 일반 앱 스토어에서 사용 가능한 믿을 수 있는 조직의 앱조차도 상당한 위험을 동반할 수 있습니다. 응답자 중 82%는 직장 내 모바일 앱이 보안 위험 정도를 매우 많이 (50%) 또는 많이 (32%) 증가시킨다고 답했습니다. 대부분의 직원들은 "앱 헤비 유저" (66%) 였으며, 절반 이상 (55%) 은 본인의 조직에서 직장 내 모바일 앱의 허용 가능한 사용을 정의하는 정책이 없다고 답했습니다.

응답자 중 단 30%만이 조직 내 기업 앱 스토어를 배치하고 있다고 답했습니다. 다만, 대다수 응답자 (67%) 는 앱 스토어가 있어도 직원들이 다른 출처를 통해 검열되지 않은 모바일 앱을 이용할 수 있다고 인정했습니다. 또한 조직 중 55%는 직원들이 각자 개인 장치에 기업 앱 스토어로부터 업무용 앱을 다운로드 및 사용하도록 허용하고 있다고 답했습니다.

현재 모바일 악성 프로그램 상태

모바일 악성 프로그램이란 무엇입니까?

모바일 악성 프로그램은 특정 운영 체제를 이용하여 모바일 장치를 공격하도록 특수 설계된 악성 소프트웨어입니다. 악성 프로그램 종류로는 일반적으로 세 가지가 있습니다.

- 스파이웨어 – 특정 유형의 데이터를 확보하여 해커에게 전달함으로써 이득을 취하는 장치 데이터 절도범 및 스파이
- 트로이목마 – 사용자가 알지 못하는 사이에 장치 또는 앱 기능에 영향을 주거나, 자동 트랜잭션을 수행하거나, 통신을 시작하는 악성 프로그램
- 탈옥 또는 루팅 악성 프로그램 – 해커에게 특정 장치 관리 권한 및 파일 액세스를 제공

이를 이해하고 이러한 위협이 모바일 엔드포인트에 집중되어 있는 이유를 이해하기 위해, 사이버 범죄자의 사고 과정을 살펴보도록 합시다. 모바일 장치는 민감 데이터에 접근할 수 있는 가장 쉬운 경로 중 하나입니다. 기업 백엔드 시스템은 방화벽, 침입 예방 시스템 및 바이러스 차단 게이트웨이로 적절히 보호를 받고 있지만, 기업과 개인 장치 모두에 동일한 수준의 보호 기능을 활용하지는 않습니다. 개인 장치 (BYOD) 는 특히 경계 범위 외 대상이며 조직의 통제 범위를 벗어나는 경우가 많아 특히 취약합니다.

해커가 엔드포인트를 공격할 수 있게 되면 사용자를 사회공학화하는 악성 프로그램을 이용할 수 있으며, 이를 통해 개인 신상 정보 (PII) 와 인증서를 취득할 수 있습니다. 이후 해커는 사용자의 계정을 탈취하고 인증된 세션을 이용함으로써 개인 데이터를 수집하고 사기 트랜잭션을 수행할 수 있습니다.

Android의 끝없는 걱정거리

IDC에 따르면 Android는 2014년에 81.2%의 점유율과 배송된 장치 수가 십억 개를 넘으며 모바일 장치 시장을 지배했습니다.[8] Android는 현재 소비자 시장을 장악하고 있지만 기업 내 사용률은 아무리 낙관해도 점차 낮아지는 추세를 보여 왔습니다.

Android의 플랫폼 및 앱 성장 시스템이 갖는 근본적인 설계와 개방성을 살펴보면 Android가 오늘날 모바일 업계에서 왜 가장 악성 프로그램에 취약한 대상 중 하나인지 그 이유를 알 수 있습니다.

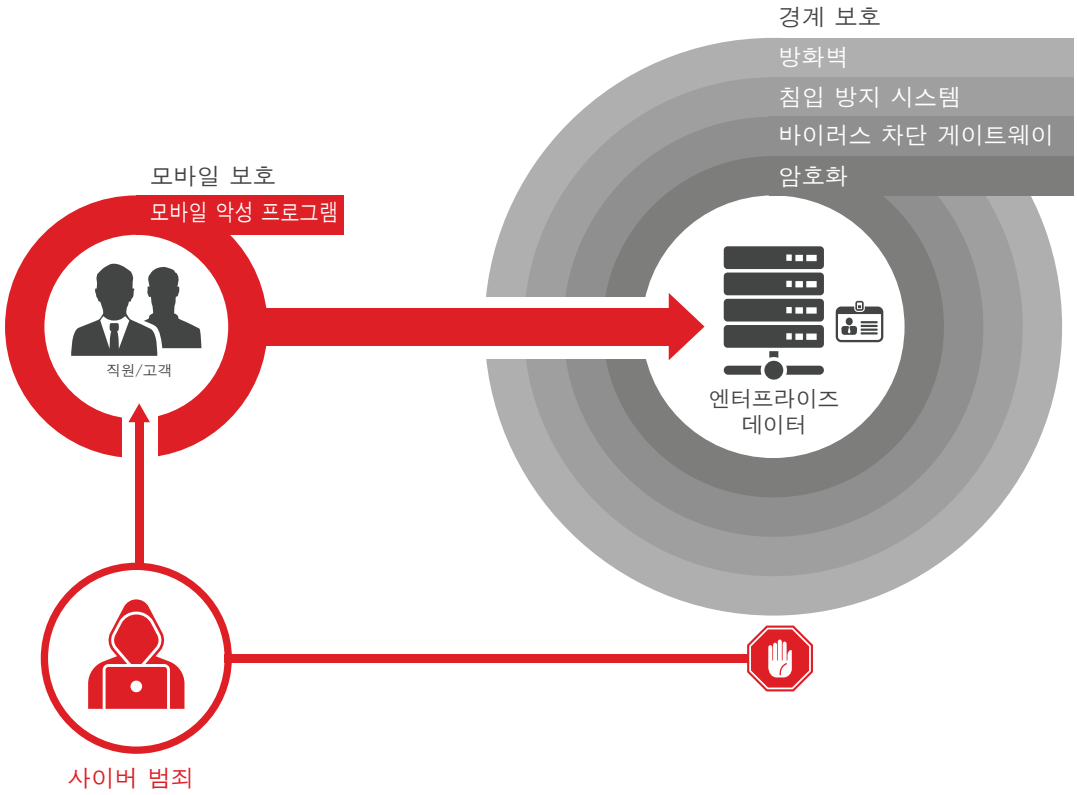

그림 2: 민감 데이터에 액세스하기 위해 가장 취약한 링크를 공격하는 범죄자들

Android의 플랫폼 및 앱 성장 시스템이 갖는 근본적인 설계와 개방성을 살펴보면 Android가 오늘날 모바일 업계에서 왜 가장 악성 프로그램에 취약한 대상 중 하나인지 그 이유를 알 수 있습니다. Android가 해커 및 절도범에게 가장 쉬운 표적이 되는 특징은 다음과 같습니다.

- Android 앱은 타사 앱 스토어 및 웹사이트에서 다운로드 및 설치가 가능합니다.
- Google Play Store는 Apple이 iOS 앱을 iTunes에 게시하기 전에 검열 및 승인하는 것처럼 각 앱을 강력하게 검열하고 승인하지 않습니다.
- Android 앱에 서명하는 디지털 인증서도 통제되지 않습니다. 이러한 앱은 보통 자체 서명되어 있으며 앱 개발자를 추적할 수 없습니다. 이러한 점들이 Android 앱을 해킹하고, 악성 프로그램을 주입하여 재서명하는 방법을 간단하게 합니다.

사이버 범죄자는 지속적으로 PC와 다른 모바일 OS 플랫폼의 취약성을 공격하는 새롭고 창의적인 방법을 찾아 내고 있습니다.

Google은 Google Play Store에서 악성 프로그램 앱을 근절하기 위한 보안 기준을 이행했습니다. 이 기준에 따라, 스토어에 올라오는 앱에 대해 스캔이 이루어지고, 각 앱을 실행해 악성 프로그램, 스파이웨어 및 트로이목마를 감지하고 제거합니다. Google은 새로운 종류의 악성 프로그램을 발견할 경우에 시스템에서 모든 Google Play 내역을 전체적으로 재검토하고 의심스러운 파일을 스토어에서 제거합니다. 또한 Google은 회사 약관 및 컨텐츠 정책을 위반하는 개발자 앱 및 계정을 비활성화하고 있습니다.

그러나 앞서 이야기한 바와 같이, 최다 구매율을 기록한 Android 앱 가운데 97%는 이미 해킹을 당했으며, 타사 앱 스토어에 찾을 수 있게 되었습니다. 따라서 만약 여러분의 직원 또는 그들의 자녀가 기업 또는 개인용 Android 장치상에서 이런 비공식 출처를 통해 최신 프리미엄 게임 앱을 무료로 설치한다면 그 장치는 악성 프로그램에 감염될 수도 있습니다. 여러분의 조직은 이러한 관행을 예방하는 데 도움을 줄 수 있는 정책 및 사용자 교육을 도입할 수 있으나, Android 장치는 자동 보호 계층이 없어 취약할 수 있습니다.

Android 악성 프로그램의 예로는 SVPENG라고 불리는 은행 해킹 트로이목마가 있는데, 이 악성 프로그램은 러시아와 유럽의 금융 기관을 표적으로 삼는 것으로 알려졌습니다. SVPENG는 모바일 악성 프로그램이 상당 수준 진보되었음을 대표적으로 보여 주는 예입니다. 이러한 공격은 오버레이 어택이라는 일반 PC 악성 프로그램 기법을 이용하여 피해자가 본인의 인증서를 제공하도록 속임으로써 모바일 뱅킹 앱 사용자를 직접적으로 겨냥하고 있습니다.

감염된 장치상의 악성 프로그램은 이러한 공격 과정에서 사용자가 은행의 모바일 앱을 열 때까지 기다립니다. 악성 프로그램이 모바일 뱅킹 앱 세션의 시작을 확인하면, 앱 위에 은행 앱의 외양과 분위기를 모방한 화면을 띄우는데 (“오버레이”) , 실제로 이 화면은 가짜 페이지입니다. 사용자는 이 사실을 알지 못하고 악성 프로그램이 생성한 페이지를 실제 은행 페이지로 착각하여 상호작용하면서 은행 인증서를 제공하게 됩니다.

이와 유사한 오버레이 공격은 민감한 기업 데이터를 위협할 수 있습니다. 직원이 의도치 않게 본인의 업무용 인증서를 입력하면, 절도범에게 필요한 기업 시스템 인증을 제공하고 결국 데이터는 엉망이 됩니다.

최근 IBM X-Force® Application Security Research Team 에서는 Android용 Dropbox SDK의 취약성으로 인해 공격자가 모바일 장치상의 앱을 이용하여 피해자가 모르는 사이에 또는 무단으로 제어 가능한 Dropbox 계정에 접속한다는 사실을 발견했습니다.[9] DroppedIn이라고 불리는 이 취약성은 두 가지 방법으로 악용될 수 있는데, 하나는 사용자 장치에 설치된 악성 앱을 이용하는 것이고 다른 하나는 웹사이트에서 원격으로 반자동 제어 기법을 이용하는 것입니다.

이것은 Dropbox SDK 버전 1.5.4부터 1.6.1까지 이용하는 Android 앱의 인증 메커니즘에서 심각한 결점으로 작용했습니다. 그러나 IBM Security Team이 Dropbox 측에 문제를 제기한 후 단 4일 만에 Android v1.6.2용 Dropbox SDK가 해결되었습니다. DroppedIn 악용 방식의 개요는 SecurityIntelligence.com의 블로그 포스트 (각주 9 참조)에서 확인할 수 있습니다.

해커가 DroppedIn 악용법을 활용할 수 있었던 이유는 Android 장치상에 악성 앱을 설치하는 것이 쉬웠기 때문입니다. 사이버 범죄자는 지속적으로 PC와 다른 모바일 OS 플랫폼의 취약성을 공격하는 새롭고 창의적인 방법을 찾아 내고 있습니다.

Android는 계속해서 기업 사용과 관련하여 여러 가지 문제를 직면할 수 있겠지만, Google과 장치 제조업체들의 최신 보안 강화 및 선도적인 엔터프라이즈 이동성 관리 (EMM) 솔루션 제공업체들의 지지에 기반하여 기업 및 정부 기관에서 그 입지를 확장하고자 노력 중입니다. 소비자, 즉 여러분의 직원들이 Android 장치를 사용하기로 선택하는 경우에는 여러분의 조직에서 모바일 악성 프로그램을 방지하는 데 필요한 보안 및 보호 기능을 구현해야 합니다.

iOS는 취약하지 않습니다

iOS 장치는 여러 가지 주요 이유로 인해 기업 시장에서 강력한 지배력을 과시해 왔습니다. 2007년에 처음 iPhone이 출시되었을 때 전문가들은 기업에서 배포해 준 오래된 스마트폰 대신 iPhone을 업무에 이용하기 시작했습니다. iOS 앱의 샌드박스형 아키텍처와 동작 방식은 플랫폼 내 설계를 통해 보안을 확보하기 때문에, 사용자가 이러한 보안 시스템을 의도적으로 우회하지 않는 한 해커는 전체 장치와 모든 앱을 감염시키기 어려웠습니다.

처음에 소비자 시장에만 초점을 맞추었던 Apple은 이후 기업 시장의 잠재성을 빠르게 포착했습니다. 그리고 모바일 장치 관리 (MDM) 솔루션 제공업체의 도움을 통해 IT 리더들이 장치, 앱 및 데이터를 보호하고 관리하는 방식을 개선할 수 있도록 제어 기능을 통합하기 시작했습니다.

Apple은 Android의 개방형 앱 아키텍처 및 성장 시스템과 달리 더욱 폐쇄적인 장치 및 앱 환경을 제시하는 편입니다. 공식 iOS 앱은 iOS 장치가 탈옥하지 않은 한 iTunes App Store에서만 다운로드 및 설치가 가능합니다. iTunes에 업로드되는 앱은 공식적으로 앱을 게시하기 전에 Apple에서 엄격한 검열 과정을 진행합니다. 또한 iOS 앱에 서명하려면 디지털 인증서가 필요하기 때문에 앱 개발자를 추적할 수 있습니다.

iPhone과 iPad는 이러한 모든 이유 덕분에 수년간 기업, 정부 및 교육 기관으로부터 대중적으로 수용될 수 있었습니다. 그러나 이처럼 충분한 보안 조치 조차도 사이버 범죄자들이 iOS 장치의 해킹을 시도하는 것을 막을 수는 없었습니다. 실제로 WireLurker 및 Masque 공격이라고 불리는 신종 악성 프로그램을 포함하여 해커들이 iPhone과 iPad를 새롭게 감염시키는 사례가 있었습니다.

WireLurker는 Mac OS 및 iOS 장치를 모두 겨냥한 새로운 등급의 악성 프로그램입니다.[10] WireLurker만의 고유한 특징은 탈옥하지 않은 iOS 장치도 감염된 Mac OS 장치에 USB 케이블로 연결하면 감염시킬 수 있다는 점입니다.

WireLurker가 장치를 공격하는 일반적인 원리는 다음과 같습니다.

- 사용자가 흔히 비공식 타사 앱 스토어에서 악성 프로그램에 감염된 OS X 앱을 본인의 Mac OS 장치에 다운로드 및 설치합니다.
- 그 후 사용자가 감염된 앱을 열고 루트 권한을 부여합니다. 이 때 Mac OS 장치의 관리자 비밀번호가 필요합니다.
- 악성 프로그램에 감염된 OS X 앱이 실행되면 이 앱이 여러 iOS 앱을 다운로드하고, 해당 컴퓨터를 신뢰하는 iOS 장치가 USB 케이블을 통해 연결될 때까지 기다립니다.
- 감염된 Mac OS 장치를 신뢰하는 iOS 장치가 연결되면 악성 프로그램 앱이 악성 iOS 앱을 iPhone 또는 iPad에 로드합니다.
- iOS 앱은 그 자체적으로 기업 서명 앱이므로, 사이버 범죄자들이 조직의 계정을 훼손하거나 Apple로부터 본인의 iOS 앱을 승인하도록 할 수 있습니다. 이러한 앱은 프로비저닝 프로파일도 함께 제공하기 때문에 iOS 장치는 해당 앱을 신뢰하게 됩니다.

의심스럽지 않은 사용자의 비탈옥화 iOS 장치에 악성 iOS 앱이 업로드되면, 이 앱들이 정보를 훔친 뒤 공격자 서버에 규칙적으로 전송할 수 있습니다.

그런데 이 WireLurker보다 더 극악한 것은 아마도 최근 발견된 Masque 공격이라는 악성 프로그램일 것입니다.[11] 이 악성 프로그램은 감염된 Mac OS 장치에 연결하지 않고도 비탈옥한 iOS 장치를 감염시킬 수 있습니다. 이 공격이 시작되면 기업/임시 프로비저닝으로 설치된 iOS 앱이 iTunes App Store에서 승인된 앱을 대체할 수 있습니다. 단, 두 앱 모두 동일한 번들 식별자를 사용해야 합니다.

Masque 공격이 사용자의 인증 앱을 대체하고 정보를 탈취하는 원리는 다음과 같습니다.

- 사용자가 아무 웹사이트에서든 악성 앱을 다운로드 및 설치하는 링크를 클릭합니다. 이 앱은 기업 인증으로 서명되어 있으며 "New Angry Bird"와 같은 라벨이 표시되어 있습니다.
- 악성 앱이 뱅킹 앱 또는 이메일 앱과 같이 동일한 번들 식별자를 갖는 합법적인 앱을 대체합니다.
- 공격자는 기존 앱의 로그인 인터페이스를 모방하여 사용자의 인증서를 탈취할 수 있습니다.
- 또한 이 앱은 로컬 데이터 캐시를 사용하여 이메일 앱의 최신 이메일 등과 같은 대체된 기능을 모방할 수 있습니다.

사이버 범죄자가 로그인 증명서를 획득하고 데이터를 로컬 방식으로 캐싱하면 사용자의 증명서 데이터와 금융 정보가 공격 및 데이터 손실에 취약해집니다.

엔터프라이즈 이동성 관리를 충족하는 악성 프로그램 보호

IBM® MaaS360® Mobile Threat Management

IBM은 모바일 악성 프로그램과 탈옥 또는 루팅된 스마트폰 및 태블릿과 같이 손상된 장치로부터의 보호를 위해 IBM Security Trusteer® 통합을 통한 새로운 EMM 보안 계층을 제공하고 있습니다.

이 독보적인 통합 및 시너지 방식은 범죄적 이득을 목적으로 기업 및 개인 정보를 얻으려는 해커 및 절도범을 강력하게 방어합니다.

지속적으로 업데이트되는 데이터베이스를 활용하여 악성 프로그램 서명이 있는 iOS 및 Android 앱을 감지하고 분석하십시오.

수천만 사용자가 사기 및 데이터 위반으로부터 조직을 보호하기 위해 이용하고 있는 Trusteer는 MaaS360에 위험 인식 및 보안 인텔리전스를 제공합니다.

모바일 악성 프로그램 감지 및 개선:

- 지속적으로 업데이트되는 데이터베이스를 활용하여 악성 프로그램 서명이 있는 iOS 및 Android 앱을 감지하고 분석
- 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
- 다음 사항과 같은 장치 위협 속성 수집 및 확인:
  - 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

그림 3: MaaS360과 Trusteer로 모바일 악성 프로그램 및 손상된 장치 감지, 분석 및 개선

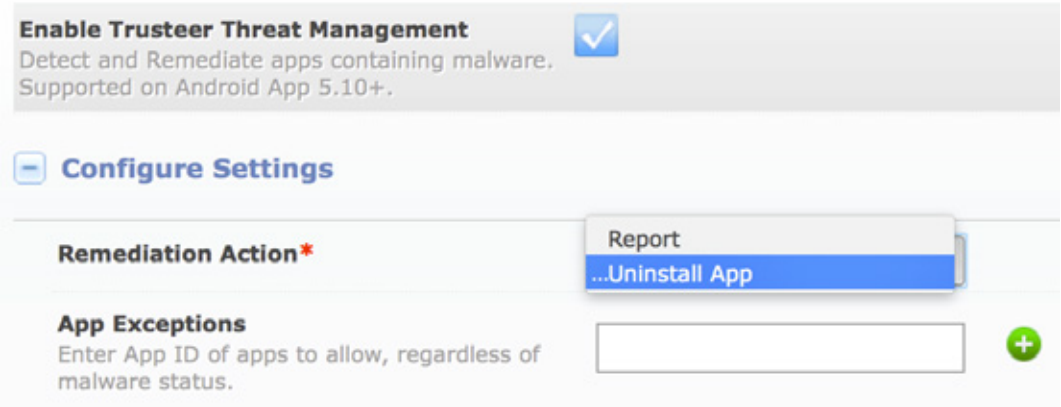

그림 4: MaaS360 구성 설정 중 일부

추가 탈옥 및 루팅 감지:

- 손상되거나 취약한 모바일 장치 감지
- 운영 체제에서 공격자에게 추가 권한을 제공하여 다양한 공격을 돕는 탈옥한 iOS 및 루팅된 Android 장치로부터 보호
- 탈옥 및 루팅 장치 감지를 숨기는 은폐자 및 활성 은폐 기술 모색
- 빠르게 움직이는 해커를 대상으로 보다 잘 대처하기 위해 앱 업데이트 없이 무선 업데이트되는 감지 로직 적용
- 보안 정책 및 규정 준수 규칙 설정으로 개선 자동화
- 액세스 차단, 장치에 대한 선택적 또는 완전 삭제, 또는 장치제어 삭제

이 보안 계층은 소비자가 즉시 사용할 수 있는 용도가 아님에도 사용자의 장치와 정보를 보호할 수 있습니다.

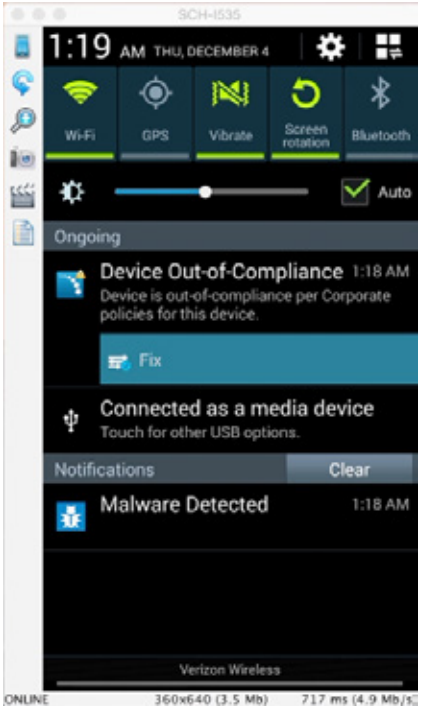

그림 5: 모바일 악성 프로그램 감지 상태 및 장치 비준수 상태를 보여 주는 스크린샷

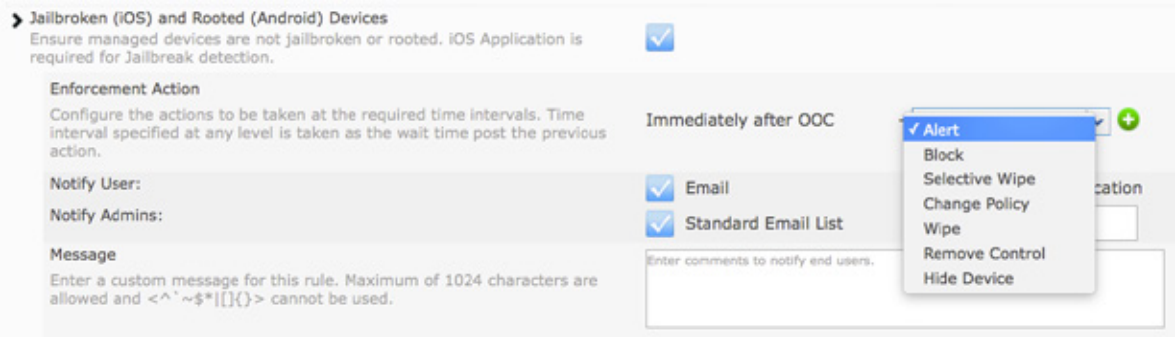

그림 6: 탈옥 또는 루팅된 장치에 대한 준수 집행 조치 구성

Trusteer Mobile Risk Engine은 적응형 악성 프로그램 방지를 통해 최신 공격 행동을 더욱 빠르게 감지하고 이에 대응할 수 있는 보안 계층과 사이버 범죄 인텔리전스를 구현함으로써 악성 프로그램이 실질적으로 사기 행위를 범행할 수 있는 가능성을 제로로 만듭니다. 이 엔진은 지속적인 업데이트를 통해 최신 악성 프로그램, 탈옥 및 루팅 점검을 실시함으로써 장치 및 앱 위험 요인에 기반하여 거의 실시간에 가까운 모바일 위험 평가를 수행합니다.

주요 장점

MaaS360 Mobile Threat Management 솔루션의 장점은 기업 장치와 데이터를 보호하는 것 이상의 기능을 제공한다는 것입니다. 이 보안 계층은 소비자가 즉시 사용할 수 있는 용도가 아님에도 사용자의 장치와 정보를 보호할 수 있습니다.

조직은 조직 내 사용자를 교육하고 이들의 데이터를 보호하는 데 더 큰 도움을 줄 수 있습니다.

BYOD 및 기업 소유 장치 모두 안전하게 지원

BYOD의 부가적인 직원 혜택으로 개인 데이터 보호

거의 실시간으로 모바일 위협을 사전 대처식으로 관리

기업 및 개인 정보의 민감한 데이터 누출 위험 감소

기업 내 Android 사용 시 특히 BYOD를 이용하는 경우 더욱 쾌적한 환경 제공

모바일 보안 위험 발생 시 이를 개선하기 위한 자동 조치 실행

사용자 교육 및 보호

조직은 이 MaaS360 Mobile Threat Management 솔루션 외에도 다른 방법으로 조직 내 사용자를 교육하고 이들의 데이터를 보호하는 데 더 큰 도움을 줄 수 있습니다.

조직은 다음과 같은 모바일 보안 활동을 고려해야 합니다.

- 애플리케이션 보안 관련 직원 교육: 직원들에게 제삼자 애플리케이션을 다운로드하는 것의 위험과 취약한 장치 허가로 인한 잠재적 위험에 대해 교육합니다.
- BYOD 장치 보호: 엔터프라이즈 이동성 관리 기능을 적용하여 직원들이 각자의 장치를 사용하는 동안 조직 보안을 유지할 수 있도록 합니다.
- 직원들이 허가된 앱 스토에서만 다운로드할 수 있도록 허용: 직원들이 Google Play, Apple App Store 및 여러분 조직의 앱 스토어 (해당하는 경우) 와 같이 허가된 애플리케이션 스토어에서만 애플리케이션을 다운로드할 수 있도록 허용합니다.
- 장치 손상 시 빠른 대처: 장치 손상 또는 악성 프로그램 앱 발견 시 자동 조치를 취할 수 있는 스마트폰 및 태블릿 관련 자동화 정책을 수립합니다. 이러한 접근법은 여러분 조직의 데이터를 보호하는 동시에 문제를 개선합니다.

왜 MaaS360인가?

IBM은 MaaS360을 이용하여 고급 악성 프로그램 보호 기능과 업계 선도적인 엔터프라이즈 이동성 관리 및 보안 기능을 하나로 통합하였습니다. 이 제품은 기업용과 개인용 모바일 장치 모두에서 빠르고 간편하게 설치 및 사용하여 민감한 데이터를 보호할 수 있습니다.

IBM MaaS360 정보

IBM MaaS360은 엔터프라이즈 이동성 관리 플랫폼으로서 사람들의 업무 방식과 관련된 생산성 및 데이터 보호 기능을 제공합니다. MaaS360은 수천여 개의 조직들로부터 이동성 이니셔티브의 기반으로 인정받고 있습니다. MaaS360은 어떤 모바일 배포 과정이든 지원할 수 있도록 사용자, 장치, 앱 및 컨텐츠 측면에서 모두 강력한 보안 제어를 가능케 함으로써 종합적인 관리를 도와줍니다. IBM MaaS360에 대한 자세한 정보를 보고, 무료 30일 시험판을 시작하려면, 다음 웹페이지를 방문하십시오. www.ibm.com/maas360

IBM Security 정보

IBM의 보안 플랫폼은 조직에서 직원, 데이터, 애플리케이션 및 인프라를 총체적으로 보호할 수 있도록 도와주는 보안 인텔리전스를 제공합니다. IBM은 ID 및 액세스 관리, 보안 정보 및 이벤트 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 차세대 침입 보호 등을 위한 솔루션을 제시합니다. IBM은 전 세계 가장 광범위한 보안 연구 개발 및 인도 성과를 자랑하는 조직 중 하나입니다. 자세한 정보는 다음 웹사이트를 참조하십시오. www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
2016년 3월

재활용하세요

1 World to have more cell phone accounts than people by 2014, January 2013 International Telecommunications Union, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2 State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 Bring Your Own Device: The Facts and the Future, May 2013, Gartner, http://www.gartner.com/newsroom/id/2466615

4 Motive Security Labs Malware Report, H2 2014, Motive Security Labs, http://www.gartner.com/newsroom/id/2466615

5 2014 Cost of Data Breach Study: Global Analysis, May 2014, Ponemon Institute, http://www-03.ibm.com/security/data-breach/

6 State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7 The State of Mobile Application Insecurity, February 2015, Ponemon Institute, https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 IDC Worldwide Quarterly Mobile Phone Tracker, February 2015, IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9 DroppedIn: Remotely Exploitable Vulnerability in the Dropbox SDK for Android, March 2015, IBM Security, http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10 Wirelurker: A new Era in OS X and iOS Malware; Blog, PaloAlto Networks, 11/5/14; http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue, H., Wie, T., Yulong, Z.; Masque: All Your iOS Apps Belong to Us; Fire Eye; 11/10/14; https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html