Norton™
by Symantec

좋은 앱, 나쁜 앱, 이상한 앱: 앱이 어떤 일을 하는지 알고 계십니까?

앱은 즐겁고 생산적이며 게다가 무료로 제공됩니다. 하지만 숨겨진 비용과 악의적인 행동으로 피해를 입힐 수도 있습니다. 위험에 대한 사후 대처에 머무르지 말고 새로운 사전 예방적 접근으로 모바일을 보호하십시오.

목차

오늘날에는 스마트 모바일 디바이스가 전 세계적으로 사용됩니다. 전 세계적으로 약 18억 명, 즉 세계 인구의 1/4이 스마트폰을 보유하고 있습니다.[1] 모바일 디바이스 사용이 증가하면서 앱 사용도 늘고 있습니다.

전 세계의 스마트폰 사용자들은 앱을 사용하는 데 86%의 시간을 보내며, 웹에서 사용하는 시간은 14%에 불과합니다.[2] 전 세계적으로 전화기당 평균 26개의 앱이 설치되어 있으며, 상위 10개국의 경우 35개가 넘습니다.[3]

사물 인터넷(Internet of Things) 시대가 열리면서 앱은 PC에서 수행한 것과 동일한 작업을 모바일 디바이스에서 새롭고 다양한 방식으로 할 수 있게 해줍니다. 예를 들어, 이미 앱을 사용하여 거실 온도를 조절하고 집에 도착하기 전에 조명을 켜며 주거 침입을 방지할 수도 있습니다.

이렇듯 앱은 놀라운 일을 해냅니다. 전화기가 자동차라면 앱은 운전대, 가속 페달, 방향 지시등과 같습니다. 또한 모바일 디바이스가 저장하는 모든 정보 및 사용자가 클라우드에 저장할 모든 정보로 연결되는 문을 여는 열쇠이기도 합니다.

사이버 범죄자도 이 사실을 잘 알고 있습니다. 사용자의 개인 정보는 경제적 가치를 지니며, 해커들은 검증된 전술(가짜 앱, 랜섬웨어 등)을 구사하면서 모바일 디바이스를 공략하기 시작했습니다. 그뿐만이 아닙니다. 돈벌이에 급급한 앱 개발자들도 사용자의 개인 정보를 노립니다. 그렇다고 이들의 목적이 항상 불법적인 것은 아닙니다. 단지 사용자의 알림 표시줄에 타겟 광고를 넣으려는 것일 수도 있습니다. 하지만 그 방식이 위험할 수 있습니다.

이토록 많은 이들이 개인 정보에 눈독을 들이고 있는 만큼 앱이 어떤 일을 하는지 알아보고 모바일 디바이스의 안전을 지키기 위한 노력을 하는 것이 그 어느 때보다 중요합니다.

이제는 분실했거나 도난당한 전화기의 위치를 추적하고 잠그는 것만으로는 충분하지 않습니다. 물론 그러한 사후 대처는 중요한 안전 장치입니다. 하지만 사전 예방적 보안이 새로운 과제로 대두했습니다. 재산과 개인 정보를 노리는 노골적인 악성 앱을 차단할 뿐 아니라 사용자가 다운로드하는 앱의 잠재적 위험성, 그리고 무료 앱이 최종적인 비용을 부담할 가치가 있는지 여부를 현명하게 판단할 수 있게 해주는 보호가 필요합니다.

이제 모바일 보호는 새로운 선제적 접근을 필요로 합니다. 그러면 사용자는 안심하고 앱의 모든 혜택을 마음껏 누릴 수 있습니다.

[1] "Worldwide Smartphone Usage to Grow 25 Percent in 2014", eMarketer(2014년 6월 11일), www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920.

[2] "Apps Solidify Leadership Six Years into the Mobile Revolution", Flurry(2014년 4월 1일), www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU.

[3] Our Mobile Planet, www.think.withgoogle.com/mobileplanet/en/.

나쁜 앱

대부분의 개인 사용자는 10년 또는 15년 전에 데스크탑 애플리케이션 소프트웨어를 바라보던 것과 동일한 순진한 관점으로 모바일 앱을 대하고 있습니다. 모바일 앱의 잠재적 리스크에 대해 전혀 또는 거의 생각하지 않으면서 설치합니다. 그리고 간단하게 탭 한 번으로 다운로드할 수 있다는 이유로 설치하는 앱이 많습니다.

앱, 특히 무료 앱은 각종 혜택을 제공한다고 주장하지만 실제 "비용"에 대해서는 자세히 알려주지 않습니다. 이러한 비용은 숨겨진 위협 및 기타 잠재적 리스크의 형태를 띨 수 있습니다. Apple은 iOS 운영 체제를 샌드박스화하고 iTunes® 앱 스토어에 대해 엄격한 심사를 실시하면서 악성 코드가 쉽게 도달하지 못하게 합니다. 반면 Android™ 운영 체제는 개방적인 특성 때문에 더 쉽게 조작되어 보안 위협 및 잠재적 리스크의 온상이 될 수 있습니다.

시만텍 인터넷 보안 위협 보고서에 따르면, 2013년의 모바일 악성 코드는 Android OS만 겨냥한 것이 대부분이었으며 그중 32%가 사용자의 개인 정보를 훔쳐내는 앱이었습니다.[4]

전체 모바일 앱의 75% 이상이 다양한 위험 또는 악성 동작을 수행하면서 기본적인 보안 테스트에 걸립니다.[5]

시만텍은 2012년부터 2013년까지 모바일 악성 코드 사례가 69% 증가 했음을 확인했습니다.

[4] "2014 인터넷 보안 위협 보고서", 시만텍, www.symantec.com/security_response/publications/threatreport.jsp.

[5] "Gartner Says More Than 75 Percent of Mobile Applications Will Fail Basic Security Tests Through 2015", Gartner(2014년 9월 14일), www.gartner.com/newsroom/id/2846017.

모바일 앱이 해커들에게 각광받는 것도 당연합니다. 사용자 기반이 빠르게 확장되는 만큼 악성 앱이 성공적으로 자리잡는다면 엄청난 양의 정보를 차지할 수 있게 됩니다. 항상 그렇듯 해커들은 갈수록 발전하고 있습니다. 이들은 학습하고 공유하면서 더욱 정교한 공격 기술을 구사합니다. 사이버 범죄자들은 PC에서 검증받은 전술(피싱, 가짜 소프트웨어, 랜섬웨어 등)을 모바일 디바이스에 접목하기 시작했습니다.

한 가짜 앱 피싱 사기에서는 무료 통화 시간을 제공한다고 속였습니다. 사용자가 로그인 정보를 입력하고 이 무료 통화 혜택 정보를 10명의 친구에게 전달해야 한다는 조건이었습니다. 이 사기는 피해자 규모를 빠르게 늘리면서 인증 정보와 기타 개인 데이터도 훔쳐내는 데 목적이 있었습니다.

또 다른 가짜 앱은 이스라엘의 최대 은행 중 하나인 Mizrahi Bank의 실제 앱과 정확히 똑같은 형태였습니다. 해커는 Google Play™ 스토어에 업로드했고 의심하지 않은 은행 고객들이 다운로드했습니다. 고객이 앱을 열고 로그인 정보를 입력하자 앱에서 해당 사용자 ID를 수집했습니다. 그런 다음 가짜 오류 메시지를 보내 고객에게 은행의 진짜 앱을 다시 설치하도록 지시했습니다.

이 앱은 문제 없이 실행되었습니다. 대부분의 고객은 자신의 사용자 ID가 도용된 사실조차 몰랐습니다.

최근의 또 다른 사례인 Android. Simplocker는 가짜 앱을 통해 배포된 랜섬웨어 트로이 목마입니다. 디바이스에 설치되면 파일을 암호화하거나 잠그고 불법 포르노 컨텐트가 디바이스에서 발견되었다는 가짜 FBI 경고를 표시합니다. 그리고 파일의 잠금을 해제하려면 MoneyPak이라는 결제 서비스를 통해 300달러의 "벌금"을 내야 한다고 안내합니다.

악성 앱 방지 퀵 가이드

노턴 소프트웨어에서 지금까지 분석한 1,500만여 개 앱 중 20% 이상이 악성 앱입니다. 그 형태도 다양합니다.

추적 앱은 문자 메시지 및 통화 기록을 수집하고 GPS 좌표를 추적하며 통화를 녹음하고 디바이스에 저장된 사진과 동영상을 훔쳐냅니다. 2014년 노턴 보고서는 사용자 추적 보안 위협의 규모가 2013년의 15%에서 30%로 증가했다고 밝혔습니다.

도용 앱은 디바이스 관련 및 사용자 관련 데이터, 이를테면 디바이스 정보, 구성 데이터, 개인 컨텐트를 수집합니다.

감염 앱은 해커가 디바이스에 접근할 수 있게 하는 백도어 및 다운로더를 설치하는 등 일반적인 악성 코드 기능을 실행합니다.

재구성 앱은 운영 체제의 권한을 높이거나 설정을 수정하는데, 그로 인해 공격자가 침투할 수 있습니다.

금품 사취 앱은 단축 코드 할증 요금 문자 메시지 번호를 사용합니다. 그러면 해커가 감염된 디바이스에서 이 번호로 문자 메시지를 보내는 악성 코드를 만듭니다. 결국 사용자가 결제하는 통신 요금이 해커의 주머니로 들어가게 됩니다.

이중 도용 앱은 은행에서 보내는 일회용 인증 코드가 수록된 문자 메시지를 가로채 해커가 사용자의 은행 계정에 액세스할 수 있게 합니다.

그레이웨어도 위험할 수 있습니다.

합법적인 소프트웨어와 악성 코드의 경계가 모호해졌습니다. 소위 그레이웨어라는 웹 유형이 수상쩍은 중간 지대를 차지하고 있습니다. 이 중간 지대에서 활동하며 악의적 의도가 없는 수많은 개발자들은 "무료" 앱을 미끼로 내거는 경우 사용자들이 정보와 컨텐트를 노출시키는 잠재적 위험성이 있는 앱을 너무 쉽게 다운로드한다는 사실을 잘 알고 있습니다.

그레이웨어 앱이 악성 코드를 포함하지 않더라도 개인 정보를 유출하고 광고 및 각종 번거로운 동작으로 디바이스에 폐해를 줄 수 있습니다. 대표적인 그레이웨어 유형인 모바일 애드웨어, 일명 매드웨어 (madware) 중에는 전화기의 알림 표시줄에 광고를 게재하거나 발신음을 음성 광고로 바꾸거나 심한 경우 전화 번호, 사용자 계정 정보와 같은 개인 정보를 노출시키는 앱도 있습니다.

기술적 식견이 있고 Google Play 스토어에서 앱을 다운로드할 때 표시되는 무수히 많은 사용자 동의 목록을 꼼꼼하게 읽어보는 사용자라면 이러한 위험 중 상당수를 발견할 수도 있습니다. 하지만 대부분은 그렇지 않습니다. 사용자 동의 내용을 읽어보더라도 앱이 실제로 수행하는 모든 동작을 알 수는 없습니다.

노턴의 조사에 따르면

60%의

Android 앱이 애드웨어 또는 기타 그레이웨어를 포함하고 있습니다.

그레이웨어가 설치되면 사용자의 위치를 추적하거나 웹 탐색을 모니터링하고 그 정보를 마케터에게 팔 수도 있습니다. 앱에서 그러한 중요 데이터를 수집하는 합당한 이유를 내세우겠지만, 대개 사용자는 그러한 동작을 인식하지 못하며 아마도 특정 개인 정보를 그러한 앱과 공유하는 데 불쾌감을 느낄 것입니다. 예를 들어, 디바이스의 고유 ID로 전화 번호를 수집하고 암호화하지 않은 채로 네트워크를 통해 전송하는 앱이 있습니다. 어느새 각지각처의 마케터와 사기꾼이 내 전화 번호를 알고 있습니다.

또는 앱의 용도로 미루어볼 때 합당하지 않은 정보를 수집하여 개인 정보 유출의 위험을 초래하는 앱도 있습니다. 이를테면 날씨 정보 앱에서 왜 사용자의 연락처 또는 일정 정보에 액세스할까요?

배터리를 소진시키고 디바이스 성능을 저하시키며 데이터 사용량을 증가시켜 요금 폭탄을 안겨주는 앱도 많습니다. 이러한 앱은 엄밀히 말하면 그레이웨어가 아니지만 불편을 끼치는 것은 분명합니다. 이러한 앱 중 상당수는 백그라운드에서 은밀하게 실행됩니다. 디바이스 사용 기간이 길어지면서 배터리 수명이 짧아지는 걸 느끼십니까? 앱이 그 원인일 수 있습니다. 데이터 요금이 갑자기 많아졌습니까? 역시 앱 때문일 수 있습니다. 열려 있지 않은 상태에서도 다운로드 작업이 빈번한 앱도 많습니다.

항상 깨어 있는 Norton™ Mobile Insight

Norton™ 기술은 PC에서 큰 신뢰를 받고 있습니다. 시만텍은 동일한 첨단 기술, 심층 분석 기능, 글로벌 인텔리전스 리소스를 모바일 디바이스 보안에도 적용합니다.

현재 모바일 보안 제품 대부분은 기본적인 보호 기능을 제공합니다. 시만텍은 여기서 한 걸음 더 나아가 악성 앱과 성가신 앱으로부터 사용자를 확실하게 보호하는 기술을 제공합니다. 30년간 축적한 보안 전문성 및 세계 최대 규모의 보안 위협 데이터베이스를 활용하여 Android 앱 보안 위협으로부터 지속적으로 보호합니다.

Norton Mobile Insight에서 200여 개의 앱 스토어를 끊임없이 탐색하고 Norton Community Watch 네트워크로부터 각종 앱 정보를 취합하면서 수집한 모든 Android 앱 데이터가 시만텍의 처리 파이프라인과 강력한 툴 모음을 거치고, 그 결과 문제가 있는 앱이 판별됩니다.

일차적으로 정적 분석을 실시하는데 여기에는 앱 제목, 개발자 서명, 권한 목록 등 일반적으로 앱을 다운로드할 때 제공되는 상당히 긴 기본 데이터를 추출하는 것이 포함됩니다.

그 다음에는 앱의 코드를 심층 분석하여 주의를 요하는 어떤 애플리케이션 프로그램 인터페이스(API)가 호출되는지 확인합니다. 이를테면 해당 앱이 전화 번호와 기타 개인 정보를 읽는 API를 호출한 다음 인터넷에 액세스하는지 살펴봅니다. 그뿐만이 아닙니다. 앱의 현지화 여부도 파악합니다. 시작 관리자에 아이콘을 추가하지 않고 설치됩니까? 이 정보는 앱의 안전성을 판단하는 데 중요한 단서가 됩니다.

그 다음에는 중요한 동적 분석을 실시하는데, 앱의 개인 정보 보호 및 정보 유출에 대한 전례 없는 관점을 제시합니다. 모든 앱을 계측형 Android 에뮬레이터에서 실행하며, 여기서 앱은 실제 환경에서 작동한다고 인식하게 됩니다. 예를 들어, 앱이 백그라운드에서 디바이스 정보나 개인 정보를 수집하여 디바이스 외부로 보낼 경우 허가받지 않은 제3자가 해당 정보를 수신할 수도 있습니다.

시만텍은 현실적인 사용 흐름과 기능을 재현하는 지능적이고 자동화된 방식으로 이러한 분석을 실시합니다. 상당수의 경쟁사가 실제 테스트 없이 모바일 앱 동작을 추론하고 앱 사용 권한에 근거하여 리스크를 보고하는 수준에 머무릅니다. 하지만 이 경우 사용자에게 부정확한 정보나 잘못된 경보가 전달될 수 있습니다.

가장 앞선 모바일 보호

Norton Mobile Insight는 Google Play를 포함한 200여 개의 앱 스토어에서 신규 또는 업데이트된 Android 앱을 계속 다운로드하고 분석하면서 현재 진행형의 고유한 앱 인텔리전스를 구축하는 역동적인 시스템입니다. 시만텍은 매일 3만 개 이상의 신규 앱을 분석하며 지금까지 분석한 앱의 수만 1,500만 개가 넘습니다.

Norton Community Watch는 수백만 명의 사용자가 활발하게 참여하는 네트워크로써 이들의 Android 디바이스에서 실행되는 앱으로부터 익명의 메타데이터 및 성능 데이터를 수집합니다. 여기에는 지금까지 발견된 적이 없는 앱 파일도 다수 포함되어 있습니다. Norton Mobile Insight는 이러한 커뮤니티 데이터를 활용하고 실시간 분석을 실시함으로써 설치된 앱의 동작뿐 아니라 디바이스에 앱을 유지할 경우 감수해야 할 리스크까지 파악할 수 있는 새로운 방법을 제시합니다. 실제로 Norton Mobile Insight에서 분석한 알려진 앱 중 25%가 Norton Community Watch에서만 수집된 것입니다. 즉 앱 스토어를 통해 배포되지 않는 다수의 앱도 분석하고 그에 관해 학습하고 있습니다.

보안 기술 연구소는 보안 엔지니어, 바이러스 추적자, 보안 위협 분석가, 연구원으로 구성된 글로벌 조직으로 모바일을 포함한 모든 시만텍 보안 제품의 근간이 되는 보안 기술, 컨텐트, 지원을 제공합니다. 이러한 전문가들이 시만텍의 눈과 귀가 되어 매일 쉬지 않고 보안 위협 환경을 감시하면서 고객의 안전을 지킵니다.

데이터: 더 많이 가질수록 더 많이 알게 됩니다.

Norton 솔루션은 Symantec™ Data Analytics Platform(SDAP)을 유리하게 활용합니다. 이 시만텍 솔루션은 엄청나게 증가하는 사이버, 모바일, 기타 보안 위협에 맞설 수 있는 기능과 민첩성을 갖춘 몇 안 되는 시스템 중 하나입니다.

SDAP는 시만텍의 모든 보안 데이터가 저장되면서 끊임없이 확장되는 거대한 데이터베이스입니다. 시만텍의 모바일 데이터에는 약 1조 6천억 건의 개별 데이터가 포함되어 있습니다. 실로 엄청난 양입니다. 하지만 모바일 보안 위협으로부터 사용자의 디바이스를 보호하려면 필요합니다.

애플리케이션 동작부터 애플리케이션 안정성, 성능 정보까지 시만텍이 수집하는 모든 앱 데이터가 SDAP에서 처리됩니다. 여기에는 앱이 실제 환경에서 어떻게 동작하는지, Norton Community Watch의 수많은 사람들이 어떻게 그 앱을 사용했는지, 어떤 앱 스토어에 있는지 그리고 몇 명이 다운로드했는지에 대한 정보도 포함됩니다.

시만텍은 이 모든 데이터를 분석하여 앱의 악성 여부를 판별합니다. Norton Mobile Insight는 지금까지 1,500만 개 이상의 앱을 처리했으며 매일 3만 개의 신규 앱을 처리하고 있습니다. 악성 코드의 특징적인 기능과 패턴을 탐지하고 앱에서 개인 정보 유출이 의심되거나 성가신 동작이 발생하는지 검사하며 배터리 및 데이터 사용량도 확인합니다.

게다가 보안 위협 환경의 변화에 발맞춰 더욱 지능적인 기술로 발전하고 있습니다. 수집한 새로운 데이터를 토대로 학습하고 진화합니다. 이를테면 악성 코드 앱이 정상적인 앱보다 더 작은 편이라는 것을 알고 있습니다. 대개 악성 코드 개발자는 더 세련된 앱으로 만드는 데 시간을 쓰지 않기 때문입니다.

따라서 Norton Mobile Insight는 이 모든 정보를 수백 개의 다른 데이터 지점과 연계 참조하면서 앱의 악성 코드 여부를 판단하고 앱의 보안에 대한 신뢰 수준을 설정합니다. 공격자가 쉽게 바꾸지 않는 악성 코드의 내재된 요소, 즉 코드 패턴, 악성 동작의 기법, 커뮤니티에서 해당 개발자의 현재 평판 등을 파악합니다.

Norton Mobile Insight: 역동적인 '실시간' 인텔리전스 시스템

지금은 강력한 사전 예방적 보호가 필요한 앱 전성 시대

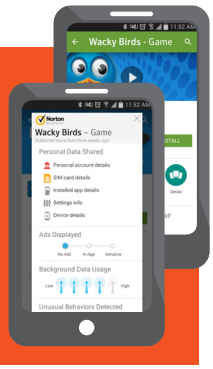
이제 웹 기반 제품 사용 기간 서비스 하나로 모든 디바이스를 편리하게 보호할 수 있습니다. Norton Mobile Insight 기술 기반의 Norton Mobile Security는 리스크가 들어 있는 앱을 정확한 데이터에 기초하여 더 신속하게 찾아내도록 설계되었습니다.

Norton Mobile Security의 핵심은 App Advisor라는 앱 검사 기능입니다. App Advisor는 Google Play 스토어의 앱을 다운로드하기 전에 자동으로 검사하여 사전 예방적으로 보호합니다(Android 4.0 이상, Samsung 디바이스는 Android 4.2 이상). 앱에 악성 코드가 있거나 개인 정보와 관련된 위험성이 있는지, 사용자를 성가시게 하거나 배터리 또는 데이터 사용량이 많은지 검사하여 알려줍니다. 또한 이전에 다운로드한 Android 앱이나 앱 스토어가 아닌 곳에서 설치한 앱도 자동으로 검사하여 그와 같은 리스크가 있는지 찾아낸 후 사용자의 선택에 따라 제거합니다.

간편한 하나의 단계에서 정보에 근거하여 Android 앱에 대한 결정을 내릴 수 있습니다. 따라서 어떤 앱이 "투자"할 만큼의 가치가 있는지 판단할 수 있습니다.

Norton Mobile Security는 개인 정보와 재산을 노리는 사기 웹 사이트를 차단하는 Web Protection을 포함하여 사용자와 기타 Android 디바이스를 위한 사전 예방적 보호 구성 요소도 제공합니다. 또한 원격 디바이스 복구 보호 기능을 제공하여 Android 디바이스, Apple® iPhone®, iPad® 디바이스를 신속하게 찾아낼 수 있습니다. 연락처 정보를 저장해 뒀다가 분실하거나 도난당했을 때 복원할 수도 있습니다.

Norton Mobile Security의 핵심은 App Advisor라는 앱 검사 기능입니다.



노턴 솔루션으로 자유를 만끽하세요.

바쁘게 움직이고 상시 연결된 우리의 삶에서 모바일은 필수 조건입니다. 하지만 이 소형 컴퓨터, 즉 모바일 디바이스에 대한 의존도가 증가하는 만큼 모바일 보안 리스크를 인식하고 스스로를 지키기 위한 노력이 필요합니다.

시만텍은 크로스플랫폼 Norton Security, Norton Security with Backup, Norton Small Business 제품 사용 기간에 노턴 모바일 보호 기술도 함께 제공합니다. 이 세 가지 제품은 언제 어디서나 사용하기 편리한 단일 통합 솔루션의 형태로 PC, Mac® 시스템, Android, iOS 디바이스를 위한 맞춤형 보호 기능을 제공하며 개인과 가족, 기업을 보호합니다.

Google Play 를 통해 Norton Mobile Security Premium의 모든 강력한 사전 예방적 보호 기능을 30일간 무료로 사용하실 수 있습니다. 신용 카드 정보를 제공할 필요 없이 노턴 계정만 만드시면 됩니다. 평가 기간이 끝나면 Premium으로 업그레이드하거나 무료 기능을 계속 사용하실 수 있습니다.