해킹된 차의 몸값을 지불해야 한다면

WannaDrive? 총체적인 IT 보안으로 차량 랜섬웨어에 대비해야 합니다.

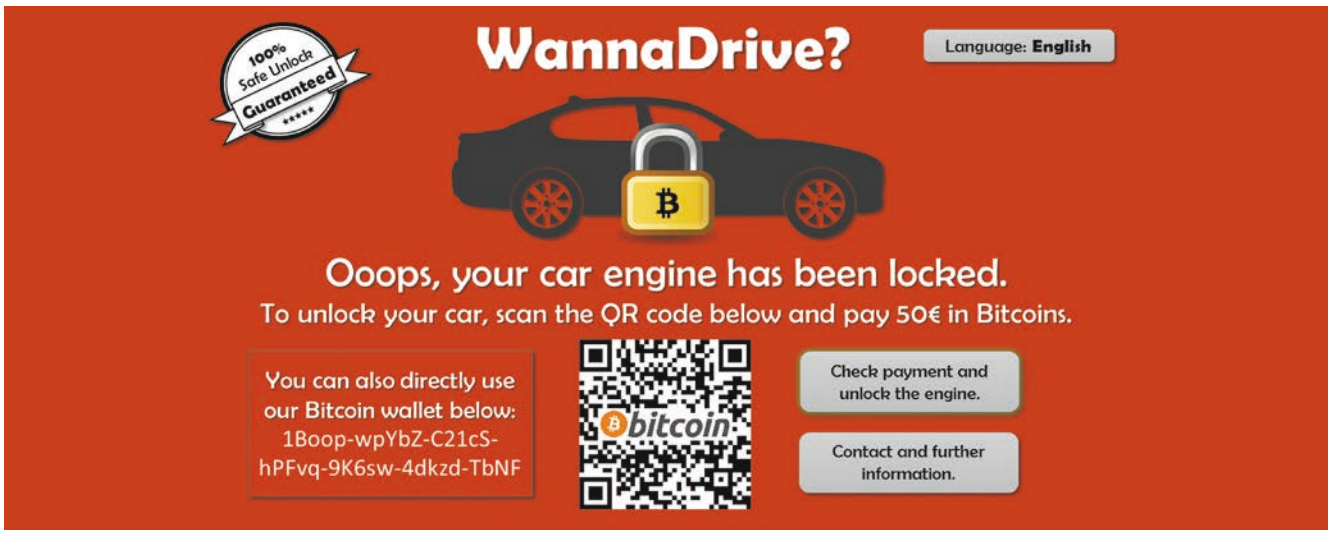
2017년 5월 랜섬웨어 WannaCry 사건으로, 자동차 산업 관계자들은 크립토-랜섬웨어의 현실적 위협에 대해 뼈저리게 인지하게 되었습니다. 그리고 인터넷과 연결된 차를 일컫는 커넥티비티(Smart mobility)와 자동차 기능의 소프트웨어화를 일컫는 디지털라이제이션(functional digitalization)으로 차량도 사이버 범죄자들이 활동하는 새로운 무대가 되었습니다.

커넥티비티를 갖춘 모든 차들이 사이버 해커들의 우선적인 타겟이 되고 있습니다. 상하는 상품을 운반하는 트럭, 버스, 렌터카, 공유차, 값비싼 건설용 차, 그리고 각종 특수목적 차량들처럼 빡빡한 일정으로 움직이는 차들이 잠정적 피해자가 될 수 있습니다. 만약 해커들이 이러한 차량들을 랜섬웨어를 이용해서 디지털 인질로 잡아 놓는다면, 돈을 받을 확률이 매우 높습니다.

랜섬웨어 공격은 큰 노력을 필요로 하지 않습니다.

차량에 대한 랜섬웨어 공격 사례는 아직까지 알려져 있지 않습니다. 하지만 지금까지 다른 분야의 실제 사례를 살펴보면 가능성 있는 공격 시나리오를 생각해낼 수 있습니다. 일반적으로 사이버 범죄자들은 랜섬웨어 키트나 봇 마스터 및 비트코인 지불 시스템으로 구성된 랜섬웨어 서비스로 랜섬웨어 공격을 시행할 수 있습니다. 그러므로 랜섬웨어 키트는 지금까지 주로 데스크톱 PC와 서버를 대상으로 했습니다. 그러나 공격에 무방비한 커넥티드카들이 점차 증가함에 따라, 자동차 리눅스나 오토사(AUTOSAR)용 랜섬웨어 변종들이 필연적으로 나타날 것입니다. 이미 수많은 사람들이 잠재적인 랜섬웨어 공격에 내몰려 있습니다.

예를 들어, 온라인 콘텐츠를 재생하는 인포테인먼트 시스템(ex. 이메일, 문자, 디지털 라디오 등), 차량통신 시스템, 차에 연결되어 있는 스마트폰 또는 네비게이션 시스템, 무선 펌웨어 업데이트(FOTA, Firmware updates over-the-air)시스템, 클라우드 서



만약 랜섬웨어가 시스템을 성공적으로 장악한다면, 디지털 인질인 차량을 사이버 범죄자의 손에서 벗어나도록 하는 것은 매우 어려운 일입니다.

비스 또는 원격 진단 서비스 등이 랜섬웨어의 침투 경로가 될 수 있습니다.

이러한 예측 속에서, 에스크립트의 보안 엔지니어들은 테스트 모델을 사용하여 랜섬웨어 공격을 시뮬레이션 할 수 있었습니다. 시뮬레이션을 위해 리눅스 OS로 운영되는 라스베리 파이(Raspberry Pi)와 터치 스크린으로 자동차 인포테인먼트 시스템을 구성하였으며, 이들을 정품 속도계에 정품 게이트웨이를 연결하였습니다. 그들은 USB 포트를 통해 라스베리 파이, 즉, 호스트 ECU를, 파이썬으로 만든 랜섬웨어로 '감염'시켰습니다. 그 후 의도한대로, 랜섬웨어는 속도계가 항상 최고 속도를 표시하도록 잠갔습니다.

동시에, 익명의 비트코인 계정으로 몸값 지불 요구를 인포테인먼트 시스템의 터치 스크린에 나타나도록 했습니다(그림 참조). 에스크립트의 전문가들은 IT 보안이 지속적으로 업그레이드 되지 않으면, 증가하고 있는 커넥티드 차량에 대한 랜섬웨어 공격이 쉽게 현실화되고 진정한 위협이 될 우려가 있다고 결론지었습니다.

총체적인 보안 접근방식은 공격을 시작부터 방지할 수 있습니다.

공격에 취약함에도 불구하고, 오늘날 도로를 주행하는 차량은 중요한 데이터와 소프트웨어 백업에 대한 대응책을 제대로 갖추지 않고 있습니다. 또한 정기적인 보안 업데이트도 하지 않습니다. 더욱 심각한 것은, 오늘 날 차량의 대부분이 게이트웨이에 아주 기본적인 보호벽만 가지고 있으며, 적절한 보호에 필요한 자동 침입탐지 및 예방 시스템(IDPS)은 거의 가지고 있지 않다는 점입니다. 차량 업그레이드는 일반적으로 복잡하고, 많은 비용이 들기 때문입니다. 랜섬웨어 및 사이버 공격에 대항하여 차량의 IT 시스템을 보호하는 가장 효과적인 방법은 차량개발의 시작단계부터 포괄적이고 효과적인 정보보안대책을 차량 플랫폼에 적용시키는 것입니다. 보안은 차량의 전체 라이프사이클을 고려하여 차량이 폐기될 때까지, IT 인프라부터 차량 내 전체 시스템의 끝에서 끝까지를 포괄해야 합니다. 또한 보안 프로세스와 보안 운영과 같은 조직적 측면에서의 대비가 이뤄져야 합니다.

그러므로 차량의 총체적인 보호를 위해 일련의 상호 연결된 보안조치가 필요합니다. 차량에서 임베디드 보안 구성요소는 해커의 공격과 알려진 멀웨어에 대한 방어에 도움이 됩니다. 더 나아가, 침입탐지 및 방지 시스템 (IDPS, Intrusion Detection and Prevention System)은 랜섬웨어 공격을 포함하여 차량 내부 통신 네트워크의 치명적인 이상징후를 차단할 수 있습니다. 이는 차량에서 이뤄질 수 있습니다. 다른 방법으로, 사이버 보안 운영센터(SOC)는 백엔드에서 모든 차에 새로 발견된 해킹 방지를 위한 보안 업데이트를 배포할 수 있습니다. 그러나 랜섬웨어 공격이 성공한다면 어떻게 해야할까요? 이 경우, 피해자는 신속하고 효과적으로 대응해야 합니다. 사전에 정의된 사건 대응 절차가 도움이 되는데, 최악의 상황에서 최후수단으로 몸값을 지불하는 것을 미리 염두에 두는 것도 대책의 일부분이 됩니다.

한 가지는 확실합니다. 랜섬웨어의 잠재적 위협은 차량에 대한 전체범위의 보안을 필요로 합니다. 그리고 이는 '비용'이 아닌 성공의 핵심적 요건으로 고려되어야 합니다. 결과적으로 보안은 운영자와 차량 제조업체들을 온라인 협박자들로부터 보호하며, 리콜 및 손해배상을 방지하기 때문입니다. ■

저 자

마르코 울프(Marko Wolf) 박사, 에스크립트, 컨설팅 및 엔지니어링 책임자.