قرصنة السيارات والتحكم بها عن بعد.. حقيقة أم زوبعة إعلامية!



بعد أن أظهر الباحثون في المجال الأمني تشارلي ميلر وكريس فالاسك **Charlie Miller and Chris Valasek** قبل ثلاث سنوات قدرتهما على قرصنة سيارة جيب أثناء السير على الطريق والتحكم بها عن بعد فقد أكد كل من صانعي السيارات والمصانع الخاصة بالأمن السيبراني إن السيارات المتصلة بالإنترنت معرضة للقرصنة كأي شيء متصل بالإنترنت.

وقد نشرت شركة الأمن تريند مايكرو **Trend Micro** تدوينة تسلط الضوء على موضوع كيفية اختراق السيارات الذي قدمته الشركة في مؤتمر **DIVMA** في مدينة بون في ألمانيا إلى جانب باحثين في مختبرات لنك لاير **Link Layer Labs** وجامعة ميلان للتقنيات المتعددة **the Polytechnic University of Milan** حيث يركز عملهم على مسألة أمنية أساسية في بروتوكول (كان) **CAN protocol** أو بروتوكول شبكة نقاط التحكم الذي يستخدم للتواصل بين مكونات السيارة الحديثة. وهذا من شأنه أن يسمح للهاكر بالدخول إلى مداخل

السيارة وبالتالي إغلاق وإيقاف مكونات السيارة الإلكترونية بما في ذلك أجهزة الأمان والسلامة. يقول فيديريكو ماغي **Federico Maggi** أحد الباحثين في شركة ترينـد مايكرو والذي أعد التقرير: "بإمكانك تعطيل عمل الأكياس الهوائية ونظام عدم إغلاق المكابح **ABS** إضافة إلى أقفال أبواب السيارة ومن ثم سرقتها، مضيفاً: "إن هذه الطريقة هي أكثر احترافية وخفاءً من سابقاتها ومن المستحيل اكتشافها باستخدام التكنولوجيا الحالية".

على الجانب العملي هناك بعض التجارب التي قام بها باحثون في المجال الأمني تمكنوا فيها من فتح سيارات من ماركات مختلفة وتشغيلها، المفاجأة إن شركة **BMW** كشفت عن بعض البيانات الخاصة بسياراتها إضافة إلى جهاز تحكم عن بعد بالسيارة قادر على التحكم بها من خلال مدخل لشبكة الويب وهذا ما يعزز إمكانية سرقتها أو التحكم بها عن طريق الإنترنت. إضافة إلى ذلك هناك العديد من الأمثلة التي تبين مقدرة بعض الأشخاص على التحايل على أجهزة الاستشعار المسؤولة عن قيادة وتوجيه السيارات ذاتية القيادة وكذلك التلاعب بمالك السيارة لحظة التحويل من نظام شبه القيادة الآلي إلى النظام اليدوي.

يقول ستيفن سافج **Stefan Savage** الأستاذ في جامعة كاليفورنيا في سان دييغو والمتخصص في مجال قرصنة السيارات (**Hacking**): "إن صانعي السيارات قد تأخروا في الاعتراف بأهمية أساسيات الأمن الحاسوبي وتباطؤوا كذلك في تطوير سبل الحماية لأنهم حاليا غير قادرين على امتلاك شفرة البرنامج التي تدير سياراتهم. أما الباحث في المجال الأمني في جامعة واشنطن كارل كوشر **Karl Koscher** الذي عمل إلى جانب سافج في بحوث القرصنة في شركة جنرال موتورز **GM** بأن المكونات المادية والبرمجيات الموجودة في السيارات الحديثة معقدة جداً وحتى المصنعون أنفسهم غير ملمين بكل شيء فيها.

يصف أندي غرينبيرغ الصحفي في مجلة **Wired** أحداث التجربة التي تطوع لإجرائها من داخل السيارة أثناء القرصنة قائلاً: "على الرغم من عدم لمسي لوحة القيادة فإن فتحات الهواء الموجودة في سيارة الجيب بدأت بدفع الهواء البارد على أقصى درجة بعدها تحولت وجهة المذياع إلى محطة الهب هوب ثم ارتفع الصوت إلى أقصى درجة فحاولت تدوير مقبض التردد إلى اليسار وضغطت على زر الإطفاء ولكن محاولتي ذهبت أدراج الرياح، بعد ذلك بدأت ماسحات الزجاج الأمامية بالعمل وانتشر سائل التنظيف على الزجاج الأمامي. وبينما كنت أحاول التعامل مع كل هذه الفوضى ظهرت لي صورة الشخصين اللذين قاما بقرصنة السيارة تشارلي وفالاسك على الشاشة الرقمية داخل السيارة.

السؤال الأهم هنا هو كيف من الممكن أن يكون نظام غير حيوي مثل نظام المعلومات والترفيه في السيارة مرتبطاً بشكل وثيق جداً مع الوظائف الحساسة الموجودة داخل لوحة القيادة والمسؤولة عن حياة الركاب؟ فهذه الأنظمة ليست مفصولة عن بعضها وبالتالي إمكانية الاستيلاء على أي شيء في السيارة بسهولة، فكل ما يحتاجه (الهاكر) بحسب مجلة **Wired** هو معرفة المعرف الرقمي الخاص بالسيارة **IP address** ليحصل على مبتغاه.

لقد استطاع الباحثان ميلر وفالاسك اللذان قاما بتجربة الجيب إدخالَ الرعب في قلب صناعة السيارات وتمكنا في الوقت نفس من إلهام المشرعين لتشريع قانون جديد يفرض على السيارات أن تخضع لمعايير معينة تحميها من الهجمات الرقمية والخصوصية المعمول بها في الولايات المتحدة الأمريكية ومن المؤمل أن تحذوا باقي الدول حذوها. إذاً الخيار حالياً متروك للمصنعين في تغيير النهج القديم في تصميم المعدات الحديثة ذات التقنية المتطورة حيث من المفترض أن يأتي الأمن في المستوى الأول عند تصميم السيارة وحالياً يبدو هذا الخيار الوحيد لتقليل مخاطر القرصنة.

على الجانب الآخر هناك رأي يفند كل أو اغلب ما أُثير عن هذا الموضوع ويعتبر إن خبر إمكانية قرصنة السيارات والتحكم بها عن بعد هو مجرد زوبعة في فنجان أخذ هالة إعلامية أكبر من حجمه. ففي تدوينة للكاتب الأمريكي في شؤون التكنولوجيا ومقدم البرامج العلمية ديفيد بوغ **David Pogue** على موقع ساينتفيك أميركان **scientific american** يتساءل فيها: "هل يستطيع الهاكر فعلاً الاستيلاء على

سياراتنا! وهل حياتنا فعلاً معرضة للخطر!"، ويستعرض بوغ في تدوينته كل التفاصيل التي من شأنها تفنيد قرصنة السيارات حيث يقول: "لقد كانت سيارة الجيب (موضوع التجربة) تعود للشخصين اللذين قاما بتجربة القرصنة، فقد عملا عليها لأكثر من سنة ليبينا لنا كيف يمكن قرصنتها والتحكم بها عن بعد، وهل من المفترض أن ينتابنا الرعب اذا علمنا إن هذا النوع من القرصنة يتطلب سيارة مزودة بخدمة إنترنت خلوية ويحتاج فريقاً من الباحثين سنوات لجعلها تعمل، عندها سيكون صانعوا السيارات قد طوروا برنامجاً يجعل قرصنة السيارات على الطرق والتحكم به عن بعد أمراً مستحيلاً".

ويضيف عن استحالة حدوث مثل هذه القرصنة قائلاً: "حتى في حالة سيارة التيسلا التي تم التحكم بها عن بعد فقد قام الباحثان بربط حاسوبهما بكابل الشبكة المزودة به السيارة في لوحة القيادة، وذلك يؤكد على إن الهاكر لا يستطيع أن يتحكم بسيارة شخص غريب عن بعد إلا إذا قام بتوصيل حاسوبه بطريقة ما بلوحة القيادة الخاصة بتلك السيارة وهذا أمر من الصعب إنجازه لأنه يحتاج فرقاً بأكملها تعمل لوقت طويل لاكتشاف طريقة لفعل ذلك"، مؤكداً في الوقت ذاته على: "إن النظام الأمني في السيارة نظام مهم ومعقد جداً ولا تحتوي الكثير من السيارات على خدمة الإنترنت". ويختتم بوغ تدوينته بالقول: "نعم، التكنولوجيا الحديثة مخيفة إلى حد ما ولكن علينا أن لا نبالغ في خوفنا وأن نتحلى بقليل من التروي لننظر لموضوع التهديد الذي يواجهنا في قرصنة السيارات بكل هدوء. لأنه وببساطة شديدة موضوع السيارات القابلة للتحكم عن بعد مجرد تهديد افتراضي لا أساس له.

إضافة إلى رأي بوغ فإن التدوينة التي نشرت في مجلة **Wired** تفيد بأن الهجوم الذي تم تنفيذه على السيارات على الطريق يُعتقد أنه بعيد عن أن يكون تهديداً حقيقياً فهو مجرد محاولة لتعطيل مكونات السيارة فقط عن العمل حيث لم يستطع أي شخص السيطرة على وظائف القيادة الأساسية في السيارة كالتعجيل والتوقف والتوجيه، كما فعل الباحثون مع سيارة الجيب في عام 2015 أو اللصوص الصينيون مع سيارة تيسلا، وهو لا يعد تحكماً كاملاً عن بعد لأنه يتطلب من الهاكر وصولاً أولياً مسبقاً لشبكة السيارة عن طريق نقطة ضعف في الواي فاي أو الاتصال الخلوي الخاصين بنظام المعلومات والتسلية أو عن طريق منفذ تشخيص الأعطال **OBD** الموجود أسفل لوحة القيادة **dashboard**. ويقول ماغي: "رغم ذلك لا يزال موضوع قرصنة السيارات إلكترونياً شبيهة بلعبة القط والفأر بين اللصوص وصانعي السيارات، فالعملية لا تعتمد على نقاط ضعف معينة في البرمجيات بل هي بمثابة ثغرة أمنية في تصميم معايير بروتوكول (كان) نفسه. وبما إن السيارات أصبحت أكثر آلية وأكثر ارتباطاً بالإنترنت فقد أصبحت عملية قرصنتها تهديداً حقيقياً لمالكيها".

وبعد كل هذا الشد والجذب من المؤيدين والمعارضين على فكرة إمكانية قرصنة السيارات والتحكم بها عن بعد بقي أن نعرف رأياً واحداً من أهم الباحثين في مجال الأمن السيبراني للسيارات ذاتية القيادة ومدير برامج الحماية لنظم المعلومات في شركة بوينغ حيث يضع مسؤولية إمكانية تحقيق ذلك من عدمه على عاتق الشركات المصنعة قائلاً: "إن المشكلة تكمن بشكل أساسي في المال، فمصنعو السيارات هدفهم الأساسي هو التجارة والربح، فهم لن يدخروا جهداً في توفير بعض الدولارات وبذلك فهم يتجهون لصناعة ما هو رخيص أكثر مما هو آمن".

- التاريخ: 2018-02-28
- التصنيف: تكنولوجيا

#الإنترنت #قرصنة السيارات #السيارة الإلكترونية #BMW

المصادر

- WIRED
- ScientificAmerican
- TheParallax
- KasperSky

المساهمون

- إعداد
  - كرار زيني
- مُراجعة
  - فرح درويش
- تحرير
  - ليلاس قزيز
- تصميم
  - رنيم ديب
- نشر
  - روان زيدان