Le piratage des voitures modernes et bateaux

Avoir une voiture connecté, ou un bateau utilisant du WIFI, 4G, 3G ou 2G c'est bien en soit, même une belle avancée technologique, mais les piratages vont être important et ultra-dangereux !

Voiture qui accélère toute seule, voiture qui ne freine pas, voiture qui n'est plus contrôler par l'ordinateur de bord.. Bateau qui va en pleine puissance, direction bloquée... C'est ce qui commence a arriver...

Il faut les protéger, alors pour cela que KASPERSKY propose et continue de développer une application pour limiter ce genre de problème.

Grâce aux technologies de l'information qui sont devenues partie intégrante de domaines qui n'étaient pas spécialement liés à l'informatique, l'importance de la cybersécurité a pris de l'ampleur. De nos jours, dans plusieurs cas, la sécurité d'objets physiques (et même de vies humaines) dépend d'une forte cybersécurité. C'est comme ça que les choses fonctionnent dans l'industrie automobile (ou comment elles seront dans un avenir très proche). Selon les prévisions de Gartner, 250 millions de voitures connectées seront sur les routes d'ici 2020. C'est la raison pour laquelle il est primordial de mettre en place l'idée de la sécurité informatique dès le tout début, au stade de la conception de ces voitures connectées.

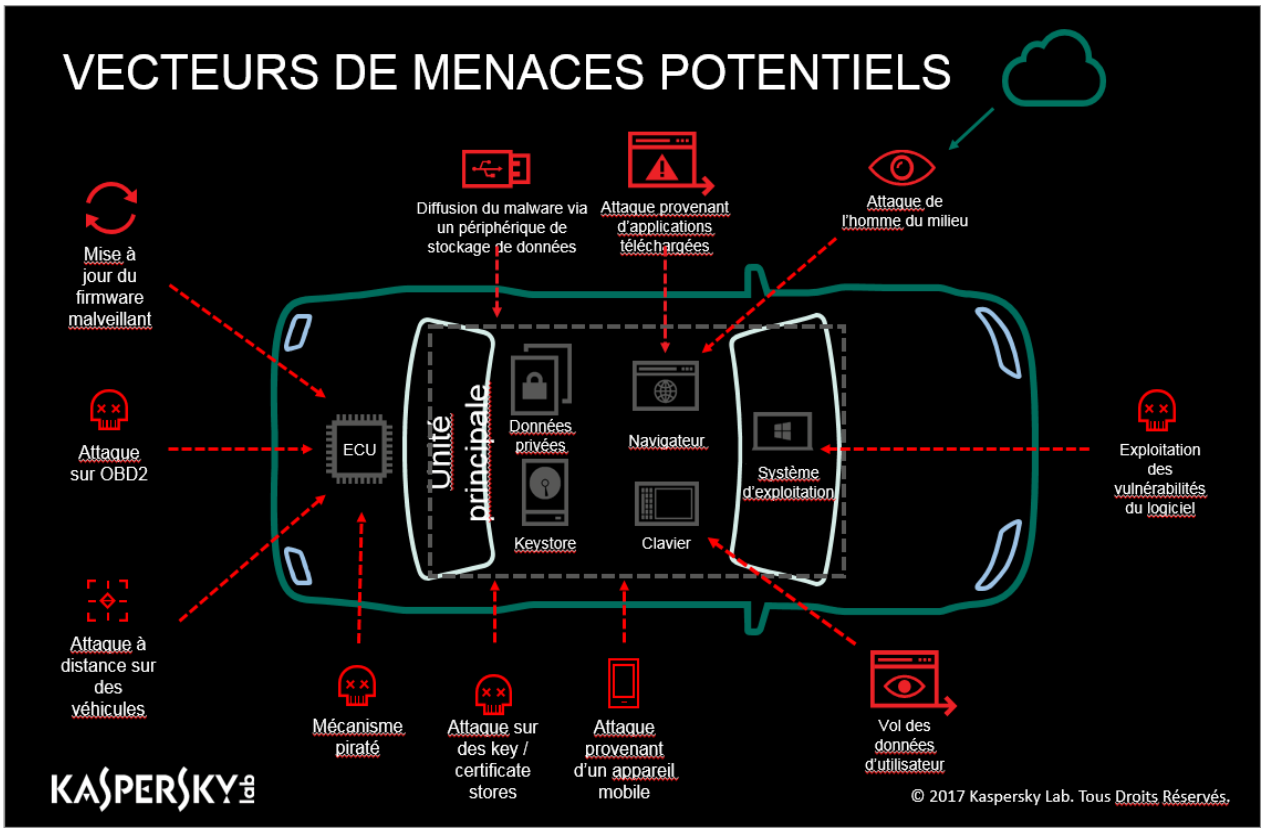
Heureusement, plusieurs constructeurs automobiles et fabricants de systèmes embarqués comprennent la signification de la sécurité informatique et sont déjà en train de réfléchir aux moyens de protéger les systèmes informatiques des voitures connectées, qui ne sont pas encore répandus. Chez Kaspersky Lab, nous sommes prêts à aider ces fabricants de quelque manière que ce soit. Nous avons l'expérience et les connaissances nécessaires pour concevoir des systèmes informatiques qui soient protégés dès la conception des véhicules.

Nous avons travaillé activement en collaboration avec des constructeurs automobiles et composants associés du cybersystème sur la création de mécanismes de défense qui sont capables de sécuriser des ordinateurs de bord face à des cybermenaces existantes et prévisibles. Plus précisément, nous avons récemment conclu un accord de partenariat stratégique avec l'entreprise AVL. Dans le cadre de cet accord, nous développerons une passerelle sécurisée alimentée par notre propre système d'exploitation, KasperskyOS, qui activera un échange de données sécurisées entres les composants d'une voiture connectée et entre le système informatique embarqué et une infrastructure informatique externe.

Utiliser une plateforme qui est protégée dès sa conception et basée sur notre système d'exploitation rendra possible la création d'une passerelle qui ne sera pas seulement sécurisée mais aussi personnalisable. Après tout, le principal problème avec la mise en place de mécanismes de sécurité sur les voitures contemporaines est que le marché automobile possède un très grand horizon de planification. Les voitures qui apparaîtront sur le marché l'année prochaine ont été conçues il y a cinq ans, et il est trop tard pour faire des changements de conception. Nous avons pris cet élément en considération et conçu notre passerelle de façon à ce qu'il soit possible de l'intégrer sur une voiture même aux derniers stades du développement. La seule chose dont la voiture ait besoin est d'un support pour l'installation de la passerelle de sécurité. Cela permet à un constructeur d'installer notre produit sur pratiquement n'importe quel hardware moderne. Nous prévoyons d'avoir un prototype de passerelle en septembre.

Notre vision d'une voiture connectée sécurisée

Les constructeurs automobiles ne se reposent pas sur leurs lauriers, plusieurs d'entre eux essaient de créer leur propre solution de sécurité Nous sommes prêts à leur donner un coup de main également, ce n'est pas la première année que nos experts analysent les menaces potentielles des systèmes informatiques automobiles. Plus précisément, nous observons les vecteurs de menaces potentiels suivants :



Ces menaces comprennent essentiellement cinq couches qui nécessitent une protection :

- Unité de contrôle du moteur ;
- Réseau automobile ;
- Accès réseau mondial ;
- Services du Cloud automobile ;

Les quatre premières couches peuvent être protégées à l'aide d'une passerelle de sécurité alimentée par notre KasperskyOS et son principal sous-système, Kaspersky Security System. KasperskyOS contrôle toutes les interactions entre les composants du hardware à l'intérieur d'un système informatique et empêche toutes les déviations causées par les erreurs internes et les tentatives d'accès non autorisées. Beaucoup d'autres solutions de Kaspersky Lab pourraient également s'avérer utiles pour l'industrie automobile, sans parler de nos services d'experts, tels que le test d'intrusion et l'analyse de la sécurité des applications, que nous considérons comme particulièrement applicables aux constructeurs automobiles et aux fabricants de composants (des systèmes V2X en particulier). Le service de protection des attaques par déni de service peut s'avérer utile si les malfaiteurs tentaient de » déconnecter » une voiture connectée en organisant une attaque par déni de service sur le Cloud.

En d'autres termes, nous avons hâte de coopérer avec l'industrie automobile et sommes disposés à aider les constructeurs automobiles et leurs composants électroniques afin de résoudre n'importe quel problème de sécurité sur une voiture connectée.