CYBERSÉCURITÉ

Et si le matériel agricole était une cible pour les criminels ?

23/03/2018 | Sébastien Duquef • **TERRE-NET MÉDIA**

Alors que les engins agricoles sont de plus en plus connectés, avez-vous déjà imaginé ce qui arriverait si un cybercriminel pénétrait au cœur du système électronique de votre machine ? Lors de la 2e journée technique de l'Axema, Yannick Guyomarch, ingénieur projet chez Kereval, a alerté les constructeurs quant à la sécurité des logiciels et à l'importance du cryptage des données. Selon lui, les constructeurs négligent trop souvent cet aspect dans leur développement au profit des fonctionnalités.

Une application sur son smartphone peut parfois suffire pour prendre le contrôle d'une machine agricole. (©Montage Terre-net Média/Fotolia)

Vous êtes-vous déjà interrogé en montant dans la cabine de votre tracteur sur ce qu'il se passerait si un criminel prenait la main sur l'électronique de votre machine ? Vous sentez-vous à l'abri d'une cyberattaque ? Selon un sondage réalisé sur Terre-net la semaine du 13 au 20 mars 2018, la moitié des agriculteurs ayant répondu considèrent que les données de leur matériel ne sont pas en sécurité. Et ils n'ont probablement pas tort !

Le 2 mars dernier, à l'occasion du **2e rendez-vous technique de l'Axema**, **Yannick Guyomarch**, ingénieur projet chez **Kereval**, a profité de la présence des principaux **constructeurs de matériels agricoles** pour les sensibiliser aux risques que leurs machines encourent en cas d'**attaque cybercriminelle**. Tracteur, moissonneuse-batteuse, pulvérisateur, charrue, presse… les machines sont de plus en plus bardées de capteurs et de technologies. De quoi ouvrir l'appétit insatiable des cybercriminels !

Le matériel connecté : source alimentaire pour les délinquants

Kereval, une entreprise bretonne située à Thorigné-Fouillard (Ille-et-Villaine), veille depuis plus de 15 ans à l'amélioration de la qualité et de la sécurité des logiciels dans des secteurs variés tels que la santé, la banque, le multimédia, les télécommunications et l'automobile. Depuis deux ans, une cellule s'intéresse tout particulièrement aux systèmes embarqués dans les véhicules connectés, de plus en plus nombreux sur le marché. Pour le moment, le matériel agricole est épargné par cette délinquance. Mais le secteur, de plus en plus connecté, représente une source intéressante pour les cybercriminels.

Selon Yannick Guyomarch, ingénieur projet de la marque, « il suffit parfois d'une application sur son smartphone pour prendre les commandes d'une machine. Imaginez alors qu'une personne malveillante modifie la dose d'application de votre pulvérisateur. Et à distance en plus ! Prendre la main sur le système de guidage GPS pour rendre le tracteur fou ; modifier les paramètres moteur pour mettre l'engin en panne… les hackers ne manquent pas d'imagination pour gagner de l'argent. Et ce n'est pas très compliqué de se procurer les outils et composants nécessaires. Ils sont très accessibles sur Internet pour quelques euros.

Isobus, clés USB… portes d'entrée pour les hackers

Pour le moment, les attaques ciblent plutôt le secteur automobile et bancaire. Cependant, avec la vulgarisation de l'Isobus, des clés USB, de la 3G ou des connexions sans fil (Wi-Fi, Bluetooth) … les portes d'entrée sont nombreuses pour les hackers. Ils pénètrent dans le système et le détournent.

Selon l'architecture du réseau et des connexions entre les logiciels, les malfrats n'ont pas forcément accès au fonctionnement de la machine. Et là, on

trouve de tout chez les constructeurs. Par exemple dans l'automobile, certains ont développé des réseaux très complexes qui séparent bien ceux qui commandent la mécanique du véhicule (freins, moteur, essuie-glaces…) de ceux qui gèrent les loisirs (radio, navigateur Web…). Chez d'autres, les architectures sont beaucoup plus permissives. Les composants logiciels peuvent aussi être à l'origine de problèmes.

Pas de cryptage de données = victime facile

Pour Yannick Guyomarch, « la plupart des constructeurs négligent la sécurité de leurs logiciels et préfèrent se concentrer sur les fonctionnalités ». Cependant, les attaques se multiplient. Par exemple, en novembre 2016, des chercheurs chinois avaient pris le contrôle à distance d'une voiture Tesla. Résultat : les marques prennent conscience de la réalité du risque. « Chez Kereval, notre rôle est d'analyser leur système en se mettant dans la peau d'un hacker. La faille est souvent au niveau de l'échange de données avec l'extérieur. Quand un tracteur communique avec son constructeur via la télémétrie, le plus souvent les données ne sont même pas cryptées. Entrer dans le système devient alors un jeu d'enfant ! », insiste le spécialiste breton.