Cyber menaces sur l'industrie automobile européenne : les campagnes de cyber espionnage

Par essence, l'industrie automobile est constamment innovante. Les véhicules sont mis à jour quotidiennement. De nombreuses technologies entrant en jeu - informatique, sécurité des informations, communication, réseau et chiffrement des données - l'importance de la cybersécurité continuera de s'intensifier au même rythme que la mondialisation et les communications. Les véhicules devenant toujours plus complexes et connectés à Internet, ils deviennent également plus exposés aux cyber attaques.

Les cyber risques auxquels sont confrontés les constructeurs automobiles peuvent comprendre :

Des atteintes à la réputation et à l'image de marque
Des problèmes potentiels de contrefaçon de brevets ou de licences
Une perte de confiance de la part des fournisseurs et des clients existants
Des sanctions financières
La perte ou la corruption de fichiers clients ou fournisseurs
Des frais juridiques
La rupture du supply chain et des liens avec les fournisseurs
Le non-respect d'accords de niveau de service
Des pertes potentielles de revenus
Des opportunités perdues en raison de la réduction de la valeur de l'entreprise
La perte de clients potentiels
La dépréciation du cours de bourse
Des coûts supplémentaires associés à la réparation des dommages

Le cyber espionnage est une menace sérieuse qui peut affecter le développement, la production et la livraison de véhicules. L'industrie automobile étant le siège d'une féroce concurrence, non seulement entre différents constructeurs, mais aussi entre différents pays, l'utilisation des nouvelles technologies et l'innovation y sont d'une importance cruciale. FireEye a le plus souvent observé des activités de cyber espionnage ciblant l'industrie automobile émanant de groupes liés à la Chine, mais a également identifié des activités en provenance de groupes liés à la Corée du Nord et au Vietnam. L'objectif de ces acteurs étatiques est de dérober des informations aux constructeurs automobiles -assurément liées à tout type de recherche liée à l'innovation, mais aussi au développement des véhicules et à de la propriété intellectuelle dont ils pourraient tirer avantage.

Des groupes APTs peuvent également cibler l'industrie automobile afin d'obtenir des informations sur de nouvelles technologies développées à des fins militaires. Le vol de propriété intellectuelle n'est pas nouveau. Mais cibler les constructeurs automobiles (y compris les écuries de F1) pourrait fournir à des nations adverses un éventail d'informations développées pour des entités gouvernementales ou des forces armées, notamment des systèmes de véhicules autonomes, de l'intelligence artificielle, des détails sur des capteurs et même le déploiement de ces systèmes.

Par le passé, l'activité de cyber-espionnage dans le secteur automobile était principalement centrée sur les activités de recherche et développement des constructeurs, les groupes de pirates informatiques étant particulièrement actifs dans l'espionnage des avancées techniques des constructeurs occidentaux et leur utilisation pour leur propre développement économique. Plus récemment, des données et des processus opérationnels ont également été ciblés. En raison des avancées en matière de transformation digitale, des données d'intelligence artificielle pour la conduite autonome et le développement de puissantes batteries ont également été visées par les pirates. Dans tous ces cas de figure, les informations dérobées peuvent causer des dommages importants à l'entreprise victime.

L'ensemble de l'industrie est d'une grande richesse pour les criminels à la recherche de gains financiers, économiques, de potentielles cyber attaques, de perturbations économiques et d'avantages concurrentiels. Ces dernières années, les analystes ont enregistré des intrusions dans l'industrie automobile dans divers pays d'Europe, principalement de la part d'acteurs chinois. Des activités ont également été constatées provenant de la Corée du Nord et du Viêt Nam.

Le groupe vietnamien APT32, sponsorisé par le gouvernement de ce pays, cible des entreprises automobiles étrangères dans des activités qui semblent destinées à soutenir les objectifs nationaux en matière de fabrication de véhicules. FireEye a vu l'activité d'APT32 s'accélérer depuis février 2019 ; ces opérations ne semblent pas avoir pour objectif d'acquérir de la propriété intellectuelle ; elles semblent plutôt rechercher des informations opérationnelles sur les entreprises.

Le groupe a ciblé des entreprises spécialisées dans la sécurité, l''infrastructure informatique et le conseil, ainsi que des militants politiques. Même si les groupes APTs basés en Chine, en Iran, en Russie et en Corée du Nord restent les plus actifs en matière de cyber-espionnage suivis par FireEye, des groupes tels que APT32 illustrent le nombre croissant de nouveaux pays impliqués dans de telles activités.

Les fournisseurs et autres membres de la chaine de sous traitance sont également ciblés par des acteurs malveillants à la recherche d'informations sur le secteur automobile. Parfois de manière illogique, ils peuvent sembler peu intéressants pour le pirate, et ne sont attaqués que pour accéder à d'autres systèmes situés plus haut dans la supply chain et ainsi pénétrer sur le réseau du constructeur. Que l'intrusion soit réalisée via des fournisseurs soit par voie directe, un constructeur automobile peut être la cible d'une série d'actions malveillantes, qui bien sûr peuvent inclure l'espionnage, le vol de données, la perturbation de ses opérations ou la prise de contrôle des systèmes dans les véhicules.

La sécurité du réseau est d'une importance critique et il est donc impératif de disposer de technologies avancées pour la garantir. L'absence d'authentification peut représenter une faille importante dans la sécurité. Les opérationnels doivent être capables d'authentifier l'ensemble des identités circulant sur le réseau. Alors que les menaces de sécurité continuent d'évoluer, la plupart des organisations restent tributaires de solutions de sécurité réactives pour protéger leurs actifs les plus précieux. La technologie seule n'offre pas une protection totale contre un attaquant déterminé, et il est difficile et coûteux de trouver, d'embaucher, de former et de retenir des experts en cyber sécurité, en particulier ceux qui sont spécialisés dans la recherche de menaces avançées.

Il est fortement conseillé de surveiller les réseaux 24H/24H avec une approche proactive, pilotée par des analystes qui s'appuient sur les renseignements les plus récents sur les menaces, enrichis par leur expérience. Les entreprises peuvent aujourd'hui s'appuyer sur des services managés de détection et réponse qui combinent une expertise reconnue sur la cyber sécurité, des technologies de protection et une connaissance unique des stratégies des attaquants afin d'aider à minimiser l'impact d'une intrusion. Des professionnels spécialisés peuvent contrôler en continu l'environnement de cyber menaces au niveau mondial et exploiter les plus récentes informations sur toutes les cyber

attaques majeures et leurs victimes obtenues sur le terrain.