La cybersécurité, nouvelle obsession de la Formule 1

Face à la menace d'attaques, les écuries s'entourent de géants de la protection de données.

GILLES FESTOR gfestor@lefigaro.fr

La McLaren de Lando Norris, lors du Grand Prix de Hongrie, le 19 juillet. Ultraconnectée et paramétrable à distance, chaque monoplace est équipée de 200 capteurs qui collectent en permanence des données télémétriques lorsqu'elle roule. JOE KLAMAR/AFP

FORMULE 1 Imaginez un instant. Dimanche après-midi, Lewis Hamilton caracole en tête du Grand Prix de Grande-Bretagne au volant de sa Mercedes quand, à dix tours du drapeau à damier, son écurie le rappelle soudainement au stand. Alerte sur la pression des pneumatiques avant. Le champion du monde signe un arrêt express. Après vérification, ses mécaniciens ne relèvent aucune anomalie. Le Britannique repart en trombe mais entretemps, son poursuivant l'a dépassé. Les champions du monde viennent d'être victimes d'une cyberattaque foudroyante qui leur a coûté la victoire.

Posé en quelques lignes sur le papier, ce scénario catastrophe semble tout droit sorti d'un film de science-fiction. Et pourtant, la cybersécurité et la protection des données constituent aujourd'hui des enjeux majeurs pour toutes les écuries du plateau. Une véritable obsession même, car une défaillance dans leur système pourrait avoir des répercussions catastrophiques. *« C'est l'une des hantises de toutes les écuries »*, confie au *Figaro* Éric Boullier, ancien patron de l'équipe Renault (2010-2014) puis de McLaren (2014-2018). *« Quand je suis arrivé chez Renault, sur 450 personnes, 80 pouvaient être amenées à travailler sur ces problématiques dans le département informatique. Cela montre à quel point le sujet était pris au sérieux »*, ajoute l'actuel directeur général du Grand Prix de France.

Les enjeux sont devenus colossaux pour toute une discipline lancée dans une course effrénée à l'innovation. Pour traiter le plus rapidement possible les effets des nouvelles configurations et tenter de devancer la concurrence, les équipes se livrent depuis de longues années à une surenchère du traitement des données en s'appuyant sur des supercalculateurs dont la puissance est désormais limitée par la Fédération internationale automobile (FIA). Aujourd'hui, l'informatique est partout dans le paddock. Ultraconnectée et paramétrable à distance, chaque monoplace est équipée de 200 capteurs qui collectent en permanence des données télémétriques lorsqu'elle roule. Celles-ci sont envoyées via des canaux sécurisés à des serveurs (clouds) et analysé en temps réel dans les stands et parfois même aussi à l'autre bout de la planète. À Enstone (Angleterre), siège de l'écurie Renault, des ingénieurs réunis dans un « centre des opérations », analysent la data récupérée et travaillent sur différents schémas et configurations des voitures en renvoyant leurs résultats alors que le pilote met la gomme sur le tracé. Pour une réactivité quasi immédiate.

Un sujet sensible

Pendant les essais et les courses, ce flux continu d'informations doit impérativement être protégé pour ne pas tomber entre les mains d'individus malveillants. Chaque écurie fait désormais appel à des mastodontes de la cybersécurité (Thalès, Microsoft, Kaspersky...) pour se prémunir de ces hackers organisés. *« Des attaques, il y en a tout le temps »*, assure Emmanuel Mériot, directeur France et Espagne de Darktrace, société associée à l'écurie McLaren depuis quelques mois. Cette entreprise spécialisée dans la cyberdéfense et valorisée 2 milliards d'euros fait la guerre aux pirates et à leurs très redoutés *ransomwares*, ces logiciels malveillants qui exigent un paiement en échange de rendre les données prises en otages.

« La Formule 1 s'expose comme n'importe quelle entreprise à ce type d'attaques désormais courantes, à une différence près : les enjeux peuvent se jouer à la seconde alors que la monoplace est en piste. Nous devons donc être en mesure de pouvoir réagir immédiatement », explique le dirigeant. *« Si les hackers ne peuvent pas prendre le contrôle du volant, on peut tout à fait imaginer qu'ils s'emparent de certaines données transmises et les falsifient. Et s'ils parviennent à faire dire à la voiture qu'il n'y a plus de carburant, la monoplace rentrera au stand et la course sera perdue »*, ajoute le responsable. Le cauchemar de la prise de contrôle d'une Formule 1 en piste est donc pour le moment écarté. Heureusement, car un tel événement pourrait avoir un effet dévastateur pour la plus prestigieuse des compétitions automobiles. Par ricochet, toute l'industrie automobile, obnubilée aujourd'hui par la sécurisation absolue des systèmes informatiques à l'heure de la voiture autonome, pourrait être éclaboussée.

Le sujet des attaques est extrêmement sensible dans le paddock. Les écuries refusent de communiquer sur d'éventuelles failles de leurs systèmes informatiques. En 2008, la Red Bull de Mark Webber a pourtant été victime d'une défaillance de la boîte de vitesses causée ce jour-là, selon les responsables de l'écurie... par une interférence électronique avec une rame de métro à Singapour. Cette information avait été très vite démentie par le réseau de transport local. En 2014, l'écurie Marussia avait perdu une journée de test en raison d'un virus informatique. Un cheval de Troie avait été malencontreusement téléchargé par un employé, paralysant le système informatique et les monoplaces dans le stand.

Dans une discipline où l'espionnage est qualifié de *« sport national »* par un ancien responsable de la grille, la crainte de voir une écurie faire appel à un tiers pour que celui-ci s'empare des données d'une équipe rivale et opérer, pourquoi pas, un sabotage, est bien réelle. En 2007, le plateau a pris pleinement conscience de ces menaces d'un genre nouveau lorsque l'écurie McLaren fut convaincue par la FIA de tricherie et d'utilisation des données en provenance de chez Ferrari via des informations transmises par un ingénieur, Nigel Stepney. Ce scandale, baptisé « Stepneygate » avait abouti à l'exclusion de l'équipe du championnat du monde. Une véritable déflagration sur la grille. *« Si la Formule 1 est en avance dans le domaine de la cybersécurité, c'est à cause, ou grâce, plutôt, à ce scandale*, confesse Eric Boullier. *L'amende de 100 millions de dollars infligée à McLaren avait poussé toutes les écuries à investir massivement dans le secteur de la protection de leurs données. »* Une prise de conscience qui a permis aux écuries de conserver, pour le moment en tout cas, un coup d'avance sur la menace de la cybercriminalité. ■

1995 : Kevin Mitnick est enfin arrêté

Frustré d'être sans cesse interpellé, le cybercriminel le plus recherché des États-Unis avait décidé d'opérer dans l'ombre. Jusqu'à sa confrontation finale avec le FBI.

DIDIER SANZ @sanzdidier

CRIME Pendant presque vingt ans, il a joué au chat et à la souris avec les autorités, sur les réseaux et dans la vie réelle. De petits larcins en grandes opérations de piratage, Kevin Mitnick incarne toujours, en 2020, le prototype du hacker. Des livres ont été écrits sur lui, des films racontent ses exploits. Et il s'en est fallu de peu qu'il échappe à la police après une traque spectaculaire de plus de deux ans. Que lui reproche-t-on au juste ? Des activités de piratage, de vol de logiciels et de fichiers, de fraude informatique, d'intrusion illégale sur des réseaux gouvernementaux, d'utilisation de matériels électroniques non autorisés… La liste est longue.

Il faut dire que le personnage a sans cesse poussé le bouchon. Il commence à faire des bêtises à l'âge de 13 ans en trafiquant des tickets de bus pour voyager gratuitement. Mal dans sa peau, plutôt enveloppé, le gamin s'ennuie dans sa banlieue nord de Los Angeles, tiraillé entre des parents divorcés. Sa passion, ce sont les gadgets électroniques et l'informatique naissante. Il s'équipe d'une station de radioamateur et, comme beaucoup de lycéens de l'époque, bricole un boîtier de « phreaking » pour passer des appels téléphoniques sans payer.

Alors qu'il vient de fêter ses 17 ans, il cambriole avec des copains le centre informatique de l'opérateur téléphonique Pacific Bell, emporte une liste de mots de passe des utilisateurs, des combinaisons de serrures de sécurité et des modes d'emploi. Mais la petite troupe manque d'expérience. Attrapé par la police, Kevin écope de trois mois de détention dans un centre de redressement.

1980 : le jeune homme s'inscrit à l'université de Californie du Sud, se perfectionne en informatique et cherche à mettre en pratique ses acquis en s'attaquant à des cibles emblématiques. En 1983, il s'aventure sur le réseau du Pentagone. Grave erreur. Immédiatement repéré, il est interpellé sur le campus et envoyé dans un pénitencier pendant six mois. Il en faut plus pour le désarmer. En 1987, il télécharge illégalement des logiciels et effectue des achats avec des numéros de cartes bancaires volées. Là encore, il sera arrêté et sanctionné de trois ans de mise à l'épreuve.

Menace pour la société

Rebelote quelques mois plus tard. Avec un complice, il s'introduit dans les ordinateurs de DEC (Digital Equipment Corporation), l'un des plus grands éditeurs informatiques de l'époque, pour s'emparer du code source du système d'exploitation VMS. Mais cette fois-ci, il prend ses précautions et brouille les pistes, ce qui empêche les enquêteurs de l'identifier. Le crime est presque parfait. Car à la suite d'une dispute, son complice décide de le dénoncer. Mitnick se fait arrêter. Une fois de plus. Les enquêteurs, qui lui reprochent également des intrusions dans les systèmes informatiques de Motorola, Nokia, NEC, Sun Microsystems et d'autres, le considèrent comme une menace pour la société. « *Ils ont réussi à convaincre un juge que j'avais la capacité de déclencher une guerre nucléaire en sifflant dans une cabine téléphonique* », racontera le pirate plus tard. Verdict : un an de prison assorti d'un programme destiné à lui faire passer son addiction aux ordinateurs.

Il a 26 ans quand il sort de prison. La détention semble lui avoir fait retrouver le bon chemin. Il se trouve un job de programmeur à Las Vegas, puis revient dans sa région de Los Angeles en 1992 pour travailler dans une agence de détectives. Le FBI, qui enquête alors sur une affaire de piratage, tombe mystérieusement sur le nom de Mitnick. Il risque gros : s'il est prouvé qu'il a utilisé du matériel informatique et qu'il a renoué avec ses anciens complices, il aura violé les termes de sa liberté conditionnelle. Quand les enquêteurs frappent à sa porte, Mitnick s'est envolé. Le FBI mettra deux ans à le retrouver.

Pour se protéger, il intercepte les communications du FBI, change d'identité et se déplace d'un État à l'autre. À Sacramento, fin 1993, il pirate les ordinateurs du Département des véhicules automobiles, l'organisme chargé d'enregistrer les permis de conduire, et réussit à disparaître au moment où la police est à deux doigts de le pincer. Encouragé par le retentissement médiatique de l'affaire, Mitnick prend confiance. Trop peut-être. Son erreur sera de s'attaquer à celui qu'il ne fallait pas défier, Tsutomu Shimomura. Fils du Prix Nobel de chimie Osamu Shimomura, cet ancien hacker devenu expert en sécurité informatique est aussi consultant pour le contre-espionnage américain. Une pointure.

Après plusieurs condamnations, Kevin Mitnick est allé jusqu'à intercepter les communications du FBI. Fort de ses succès, il va défier une autre pointure du hacking, consultant pour le contre-espionnage américain…

Kevin David Mitnick

Naissance : 6 août 1963
Nationalité : américaine
Profession : consultant en sécurité

Faits d'armes : fraude informatique, vol de documents et de logiciels, intrusion dans les ordinateurs du Pentagone, utilisation de matériel électronique illégal, violation de liberté conditionnelle

5 ans et 8 mois
Durée totale
d'emprisonnement du pirate après son dernier procès

25
chefs d'accusation
ont été retenus contre Kevin Mitnick

2
ans et demi
de traque menée par le FBI avant l'arrestation de Kevin Mitnick

Piratage et fanfaronnade

Le soir de Noël 1994, Mitnick réussit à pirater l'ordinateur personnel de Shimomura pour s'introduire sur le réseau du San Diego Supercomputer Center où travaille le chercheur. Il met la main sur des messages électroniques, des logiciels de sécurité et divers programmes de communication. Mais l'ordinateur repère l'intrusion et alerte les techniciens du centre informatique. Informé, Shimomura rejoint son bureau de San Diego et découvre un message vocal délibérément provocateur : « *Sais-tu qui je suis ? Moi et mes amis, on va t'avoir. Mon style est le meilleur. Ta technique sera vaincue. Ta technique est nulle.* » Le forfait ne lui suffit plus, Mitnick veut aussi fanfaronner. Impardonnable. « *Il faut apprendre les bonnes manières à ce rigolo* », se dit alors le chercheur. Shimomura retrace l'opération menée par Mitnick grâce à un fichier caché qui a enregistré toutes les commandes saisies par le pirate. Il commence par en tirer parti pour sécuriser son ordinateur, puis continue ses investigations pour trouver l'origine de l'attaque. Sans grand succès jusqu'à un petit coup de pouce du destin quelques jours plus tard.

Le 27 janvier 1995, Bruce Koball, animateur d'une association de réflexion sur l'informatique, reçoit un message curieux : son compte sur le réseau culturel The WELL, qu'il n'utilise qu'épisodiquement, dépasse les capacités de stockage autorisées. Koball découvre alors que son espace est surchargé d'une quantité de fichiers de provenance inconnue. Et que l'un d'eux concerne Shimomura, dont il a suivi l'affaire de piratage dans la presse. Il alerte aussitôt le chercheur, qui est sûr de tenir une bonne piste.

L'objet d'un culte

Avec l'aide du FBI, Shimomura examine les ordinateurs de The WELL. Ils découvrent sur le compte de Koball des logiciels volés et une liste de 20 000 numéros de cartes de crédit de clients de Netcom, un opérateur internet. L'enquête s'accélère. Mitnick, qui a bricolé des relais téléphoniques pour passer inaperçu, est enfin localisé en Caroline du Nord, dans la ville de Raleigh. Le FBI décide de se rendre sur place, accompagné de Shimomura. Grâce à un détecteur de signal pour réseaux mobiles, le téléphone de Mitnick est repéré dans une résidence au nord de la ville. À l'issue d'une surveillance de 24 heures, le 15 février 1995, les agents encerclent le bâtiment, pénètrent dans l'appartement 202 et appréhendent le pirate le plus recherché des États-Unis.

Reconnu coupable d'usage illégal d'équipement téléphonique, il est condamné à 8 mois de prison auxquels s'ajoutent 14 mois pour violation de liberté surveillée. « *Il représente un danger pour la communauté*, estime le procureur adjoint Christopher Painter en charge de l'affaire. *Nous parlons de quelqu'un qui a constamment et compulsivement piraté des systèmes partout. C'est aussi un fugitif qui a utilisé de multiples identités* ». Pendant qu'il attend ses autres procès, Mitnick se morfond dans sa cellule, surtout qu'il lui est interdit d'utiliser un ordinateur. Des hackers se mobilisent pour protester contre son incarcération et la sévérité des peines qu'il encourt. Mitnick commence même à faire l'objet d'un culte de la part de supporteurs de tous horizons. Les plus motivés piratent les sites web du *New York Times* et de Yahoo! pour exiger sa libération. Et on commence à voir apparaître sur des voitures l'autocollant « Libérez Kevin ».

> « Mon style est le meilleur. Ta technique sera vaincue »

Il sera libéré le 21 janvier 2000, avec une période de probation de trois ans pendant laquelle il lui est interdit d'utiliser un ordinateur. Il en profite pour répondre à des interviews, animer une émission de radio et écrire son premier livre sur la sécurité informatique. Assagi, il semble avoir abandonné le côté obscur. Son expérience lui servira quand même. Il crée en 2003 une société de conseil en sécurité informatique, Mitnick Security Consulting, pour aider les entreprises à tester leur sécurité. Difficile de trouver mieux… ■

RETROUVEZ LUNDI
Les champions du style