TdG-18122020-Les e-barbouzes visent le cœur de la cybersécurité

SolarWinds et FireEye étaient piratées depuis des mois pour infiltrer des milliers de multinationales et d'agences étatiques. La frontière entre criminalité et espionnage n'a jamais été aussi floue.

Pierre-Alexandre Sallier
Publié: 17.12.2020, 15h29

L'intensification du piratage de serveurs stratégiques fait ressurgir la menace d'un «cyber Pearl Harbour» dans la presse anglo-saxonne.
KEYSTONE
Une cyberattaque d'ampleur contre des agences fédérales américaines a été confirmée dimanche par Washington, quarante-huit heures après une nouvelle infiltration de la recherche sur le vaccin contre le Covid-19 par des «hackers». Cette intensification du piratage de serveurs stratégiques fait ressurgir la menace d'un «cyber Pearl Harbour» dans la presse anglo-saxonne.

Sur le front des vaccins, le FBI avait inculpé cet été deux Chinois accusés de procéder, en coopération avec leur gouvernement, à des «reconnaissances» chez Moderna, laboratoire de Boston qui démarrait les essais de son sérum révolutionnaire. Début décembre, l'alerte était lancée sur une série d'attaques contre l'OMS, l'alliance Gavi et les sociétés assurant la chaîne du froid pour les sérums Pfizer-BioNTech et Moderna. Jeudi dernier, c'était au tour de l'Agence européenne des médicaments de reconnaître des infiltrations menaçant les secrets du vaccin de Pfizer-BioNTech, confiés en vue de son homologation.

SolarWinds et FireEye piégés

L'offensive révélée ce week-end est plus large et vise les outils de surveillance des réseaux de SolarWinds, utilisés par les plus grandes multinationales et agences gouvernementales. Sur leurs 300'000 clients, 18'000 auraient installé une mise à jour vérolée, capable de communiquer avec des «hackers». Responsable de Dreamlab Technologies, une société de cybersécurité bernoise, Nicolas Mayencourt se dit «convaincu» que cette mise à jour est présente «dans de nombreuses sociétés suisses».

«Les moyens mobilisés n'ont rien à voir [avec ceux de cybercriminels].»

Steven Meyer, ZENDATA
Aux yeux de Steven Meyer, responsable de ZENDATA à Genève, cette attaque tous azimuts pourrait en réalité se focaliser sur une douzaine d'institutions. C'est ce qui s'était passé il y a quelques années avec «les attaques sur C-Cleaner, un logiciel installé sur des millions de postes mais qui ne visaient que onze sociétés précises» ou avec «celles contre les ordinateurs Asus».

La dernière offensive sur les outils SolarWinds a notamment permis d'infiltrer FireEye, groupe californien chargé de protéger de grandes institutions contre… des cyberattaques. La menace ayant été découverte avec des mois de retard, «le nettoyage requis dans les entreprises va être considérable, un peu comme si de l'amiante avait été identifiée dans leurs plafonds», estime le responsable de cette société de cybersécurité genevoise.

Un travail trop bien organisé

On ne parlerait plus ici de groupes criminels tentant d'obtenir 50 ou 100 millions de dollars en faisant chanter les entreprises dans lesquelles ils ont fait irruption. «Les moyens mobilisés n'ont rien à voir, on fait face à une attaque touchant toute une chaîne d'approvisionnement [de services informatiques] pour descendre jusqu'aux entreprises», prévient Steven Meyer. Le «Washington Post» pointe du doigt la Russie et des groupes de «hackers» comme ATP 29, déjà accusés il y a quatre ans de viser la campagne électorale de Hillary Clinton.

Autre indice, le calendrier. Selon les premiers éléments de l'enquête, l'infiltration aurait eu lieu au plus tard en mars, avec des mises à jour pirates inactives durant des semaines. «Des criminels essaieraient de monétiser leur attaque en quelques heures», rappelle le responsable de ZENDATA.

Les barbouzes offrent leurs codes

«La Russie ne mène pas d'opérations offensives sur internet», a pourtant répliqué l'ambassade russe à Washington. Alors crime organisé ou espionnage? Nicolas Mayencourt souligne à quel point «la frontière est devenue floue».

«Lorsqu'un hacker plante un logiciel espion dans un groupe stratégique, il a tout intérêt à le mettre aux enchères.»

Nicolas Mayencourt, Dreamlab Technologies AG

La cybercriminalité est plus sophistiquée que jamais «ne serait-ce qu'en raison des retours sur investissements énormes qu'offrent ce type d'attaques». Mais ces raids s'avèrent plus juteux encore s'ils attirent l'attention de services de renseignements. «Lorsqu'un hacker plante un logiciel espion dans une entreprise stratégique – par exemple un labo pharma – il a tout intérêt à en mettre les codes aux enchères sur le Darkweb», souffle le patron de Dreamlab.

Ce brouillage des cartes entre renseignement industriel, racket et espionnage «a surgi au début de la dernière décennie», rappelle Nicolas Mayencourt, qui dit y avoir été confronté dès 2011, dans une affaire touchant plusieurs groupes de défense en Europe.

Les récentes attaques contre la logistique des vaccins procéderaient d'une telle logique. «Cela peut être une tentative d'accéder aux labos par ce biais», pointe Steven Meyer, le secteur pharmaceutique ayant toujours été marqué par une «forte activité» des «hackers». Mais des opérations d'espionnage sont également évoquées, Londres ayant ouvertement accusé la Russie. «Tous les gouvernements comparent les réponses déployées contre cette pandémie, tous redoutent de faire faux», observe le patron de ZENDATA.