ataille de l'armée belge

attaque Décembre noir pour le réseau informatique de la Défense

JO.MA.

Novembre 2021, le 24. « Je veux rapporter une faille de sécurité. » Ce jour-là, Chen Zhaojun, spécialiste en sécurité d'Alibaba Cloud, avertit la fondation Apache, qui développe un serveur web très répandu dans le monde entier, qu'une brèche dans leur logiciel Log4j pourrait permettre à des pirates de prendre à distance le contrôle de serveurs informatiques. Le 8 décembre, Chen rapporte à Apache qu'il a été fait état de cette même brèche sur la plateforme de discussion WeChat, des correctifs doivent être mis à la disposition des utilisateurs aussi urgemment que possible.

9 décembre. La faille Log4j est publiquement révélée par Apache et une mise à jour est proposée mais encore faut-il recenser tous les services et applications web dans lesquels ce logiciel est intégré. Ce qui s'annonce long et fastidieux.

11 décembre. Matthew Prince, un des co-fondateurs de Cloudflare, entreprise californienne spécialisée dans les réseaux et la sécurité informatique, prévient sur Twitter que cette faille de sécurité dans Log4j a été exploitée par des tiers dès le 1er décembre au moins. Le même jour, l'Agence américaine de cybersécurité et de sécurité des infrastructures, qui dépend de la Sécurité intérieure, attire dans un communiqué l'attention sur les vulnérabilités de la bibliothèque logicielle log4j car elles « présentent un risque sévère ».

Tout le réseau de la Défense a dû être isolé d'internet. © PIERRE-YVES THIENPONT.

15 décembre. Un technicien de la Défense décèle une communication inappropriée entre deux serveurs, il s'en ouvre immédiatement à la direction Cyber du SGRS. Celle-ci dépêche des techniciens qui copient des données, procèdent aux premières analyses, déconnectent le serveur suspect et coupent d'autres accès.

16 décembre. En soirée, il apparaît que le compte administrateur d'un des utilisateurs du réseau de l'armée a été piraté, la menace est sérieuse même s'il est à ce moment encore impossible d'en mesurer l'exacte ampleur. « A 23 h, j'ai pris la décision d'isoler tout le réseau de la Défense d'internet », se souvient Sven, directeur technique du Centre de compétence du matériel volant et systèmes de communication et d'information de la défense (CC V&C). « Plus de 25.000 personnes ont ainsi été privées de tout accès à internet », enchaîne le colonel Pierre Ciparisse, directeur Cyber. « C'était un choix radical mais qui nous a permis de couper toute porte de sortie à l'adversaire et d'investiguer sans qu'il puisse interférer. »

17 décembre. « Les investigations se sont poursuivies, le réseau interne de la Défense continuait de fonctionner même si tout accès à l'extérieur était coupé. On savait que quelque chose avait été introduit dans le réseau mais on ne savait pas de quelle manière ni jusqu'où ça s'était propagé. C'était un puzzle à assembler sans savoir si la boîte était complète ni quelle était l'image à obtenir », reprend Pierre Ciparisse.

18 décembre. Une partie des malwares sont identifiés, il apparaît que l'intrusion a eu lieu dans la nuit du 9 au 10 décembre. Réunion de la direction Cyber avec le patron de la Défense, la Direction générale des ressources matérielles (DG MR) et le CC V&C. Une quarantaine de personnes sont alors mobilisées, 18 heures par jour. Un des buts est de rassembler les indicateurs de compromission (IOC), qui pourront à l'avenir être utilisés pour détecter de nouvelles tentatives d'attaques, et partager ces indicateurs avec les partenaires belges et étrangers.

20 décembre. Remise en route progressive du réseau, des équipes de Microsoft et quelques autres experts en cybersécurité sont appelés en renfort. « C'était une situation très complexe, il fallait lister les problèmes que connaissaient les différents clients de la Défense et tenter de trouver des solutions », explique Peter, de la DG MR. « Par exemple, le calcul des salaires se fait sur notre réseau interne mais pour qu'ils puissent être versés, il faut donner des ordres à la banque. Nous avons dû envoyer des coursiers dans les institutions bancaires, tous les militaires et employés ont ainsi pu être payés en décembre. » « Un renforcement de nos capacités de sécurité était prévu mais un peu plus tard dans l'agenda : nous avons profité de la réinstallation de tous les serveurs suspects pour l'anticiper », ajoute Benjamin, de la DG MR également.

24 décembre. « Tout le monde était sur le pont, c'était un travail d'équipe », conclut Pierre Ciparisse. « Toutes les informations que nous avons récoltées sur ce malware ont été partagées au moment de Noël avec nos partenaires, belges et étrangers. » La messagerie entrante et sortante refonctionnait depuis le 11 janvier, la remise en ordre complète du système s'est poursuivie jusqu'à cet été. Les hackers, souligne le colonel, n'ont pas eu le temps de dérober le moindre document : lorsque le système de la Défense a été débranché, ils étaient occupés à s'arroger des droits d'administrateurs de plus en plus élevés afin de pouvoir cartographier le réseau. Et ultérieurement sans doute, en exfiltrer des données.

18 juillet 2022. Dans un communiqué adressé à l'agence Belga, les Affaires étrangères attribuent les attaques de décembre à des pirates informatiques chinois : « La Belgique condamne fermement ces cyberactivités malveillantes, qui contredisent les normes de conduite responsable des Etats approuvées par tous les Etats membres des Nations unies. » Une déclaration que l'ambassade de Chine qualifie immédiatement de « peu sérieuse et irresponsable ».

Plainte a été déposée, le dossier est traité par le parquet fédéral.

Log4j

Log4j est un ensemble de routines informatiques programmées en Java et utilisées dans de nombreuses applications et services web afin de gérer l'historique des événements qui sont liés à un fichier ou une base de données. En décembre 2021, des hackers ont profité d'une vulnérabilité dans cet utilitaire pour exécuter du code sur des serveurs et ordinateurs distants. La fondation Apache a attribué à cette faille une note de 10 – la note maximale. JO.MA.