Opération Cleaver : la riposte des Iraniens à Stuxnet ?

Selon un rapport de la **firme de sécurité américaine Cylance**, des hackers iraniens ont infiltré des entreprises majeures ou des organisations gouvernementales de l'énergie, de la défense, des infrastructures et des transports. Mais aussi des universités, où les hackers recherchaient des informations relatives à l'identité des personnes fréquentant ces institutions. Cette vague d'attaques, qui court **au moins depuis 2012**, a permis d'exfiltrer des « *informations très sensibles* » – dixit Cylance -, sans attirer l'attention des outils de détection jusqu'alors.

Affectant 16 pays, dont la France, l'opération, baptisée Operation Cleaver, était susceptible de provoquer des dommages dans le monde physique, selon le rapport de Cylance. Dans l'Hexagone, les opérations des hackers iraniens n'ont ciblé qu'**une entreprise du secteur pétrolier ou gazier, dont le siège est à Paris**.

Selon le journal américain Re/Code, parmi les sociétés victimes figurent la firme américaine **Calpine Corp**, les compagnies pétrolières d'Etat **Saudi Aramco** et **Petroleos Mexicanos** ainsi que les compagnies aériennes **Qatar Airlines** et **Korean Air**.

Cylance, de son côté, ne cite aucun nom de compagnie touchée par cette campagne. Mais affirme avoir identifié plus de **50 victimes** du groupe de hackers relié à une organisation baptisée Tarh Andishan (soit 'invention' ou 'innovation' en Persan, Cylance signale que plusieurs sociétés portent ce nom à Téhéran). Ces victimes sont situées au Canada, en Chine, en Grande-Bretagne, en France, en Allemagne, en Inde, en Israël, au Koweit, au Mexique, au Pakistan, au Qatar, en Arabie Saoudite, en Corée-du-Sud, en Turquie, aux Emirats arabes unis ou aux Etats-Unis. « *Cette équipe déploie des compétences évoluées et utilise une infrastructure complexe pour réaliser des attaques dont l'objectif est l'espionnage, le vol ainsi que la destruction potentielle de systèmes de contrôle et de réseaux* », assure Stuart McClure, le Pdg de Cylance.

Attaques basiques… mais ça marche !

« *Nous sommes ici face à une équipe de hackers de niveau intermédiaire. Ils utilisent des techniques peu complexes, basées sur des méthodes et outils existant, ainsi que des méthodes d'exfiltration de données assez basiques. On est loin de la complexité d'un malware comme Regin, qui multipliait les techniques permettant de masquer ses activités* », explique Gérôme Billois, senior manager en gestion des risques et sécurité chez Solucom. « *Mais les entreprises peinent toujours à détecter ces attaques et, quand elles y parviennent, c'est seulement longtemps après avoir été infiltrées. Par ailleurs, elles se limitent alors souvent à traiter l'infection sans tenter d'analyser la source ou de partager l'information* », déplore-t-il.

Les systèmes compromis incluraient des **serveurs Web Windows sous IIS ou ColdFusion**, des **serveurs Apache avec PHP**, de nombreuses variantes de **Windows pour desktop et serveurs**, des **serveurs Linux**, des **VPN Cisco** ainsi que des routeurs et switches de la même marque. « *Au cours de notre enquête, nous n'avons trouvé aucune preuve directe de la compromission d'un système de*

contrôle industriel ou d'un système Scada, tempère Cylance dans son rapport. *Mais Cleaver a exfiltré des informations extrêmement sensibles provenant de nombreuses entreprises gérant des infrastructures critiques permettant d'affecter le fonctionnement des systèmes que font tourner ces organisations.* » Autrement dit, les hackers auraient en mains de quoi cibler des Scada. Donc agir sur le monde physique.

« *Opération Cleaver est dans une logique d'exfiltration de données. Aucun code spécifique à un système industriel ne figure dans le rapport de Cylance*, note Gérôme Billois. *Mais ses auteurs ont l'impression que l'opération comportait une seconde phase ciblant ces systèmes industriels. C'est probable : en effet, une fois un SI classique compromis, il est possible de rebondir sur d'autres parties du réseau ; or systèmes industriels et système d'information partagent de plus en plus des pans d'infrastructures ou de réseau, facilitant ces rebonds. On voit même des systèmes de sûreté (gérant les alertes sur les processus industriels donc compensant les éventuelles défaillances des systèmes de contrôle, NDLR) fonctionner sur des réseaux mutualisés ; une aberration !* »

Les Iraniens mis en cause

Le groupe de hackers serait principalement **basé à Téhéran**, mais bénéficierait d'appuis aux Pays-Bas, en Grande-Bretagne et au Canada. Il utiliserait à la fois des techniques connues et des outils fabriqués sur mesure pour infiltrer ses cibles. « *Au cours de la collecte des éléments durant les 24 derniers mois de notre enquête, nous avons observé que les capacités techniques de l'équipe derrière l'opération Cleaver ont évolué plus rapidement que n'importe quel effort de l'Iran précédemment.* » Dans son rapport, Cylance semble persuadé que cette opération est directement sponsorisée par le gouvernement iranien.

« *Même s'il faut rester circonspect quand il s'agit d'attribuer une attaque à tel ou tel pays, Cylance met en évidence un faisceau de présomptions assez convaincant : IP, chaînes de caractères, noms des développeurs, noms de domaines*, note Gérôme Billois. *Cette attribution est facilitée par les erreurs commises par les hackers, des erreurs qu'on ne retrouvait pas dans Stuxnet ou Regin. On a ici affaire à une équipe qui attaque large et de façon brutale, mais qui commet des erreurs de sécurité opérationnelle, comme d'utiliser des IP ou des noms de domaine attribuables et de laisser des chaînes de caractères dans son code.* »

Rappelons que le **programme nucléaire iranien** a été **victime du virus Stuxnet**, qui aurait été conçu par les Etats-Unis et Israël. Ce malware ciblait les centrifugeuses enrichissant l'uranium. Téhéran aurait depuis investi massivement dans son arsenal cyber. En 2012, la compagnie pétrolière Saudi Aramco a vu environ 30 000 ordinateurs infectés par un virus destructeur de données nommé **Shamoon**. Attaque attribuée à l'Iran par les Etats-Unis. Le pays perse est soupçonné d'avoir également **infiltré l'intranet du corps des Marines en 2013**. En mai, la société iSight Partners expliquait encore avoir découvert une campagne très évoluée et courant sur 3 ans au cours de laquelle des hackers iraniens avaient développé des faux profils sur les réseaux sociaux et un faux site d'information pour espionner des dirigeants notamment américains et israéliens.

Interrogé par Re/code, un diplomate iranien a rejeté toute implication de son pays dans l'opération Cleaver parlant « *d'une allégation infondée fabriquée pour ternir l'image du gouvernement iranien et dont l'objectif est en particulier de ralentir les discussions en cours sur le nucléaire* ».

A lire aussi :
Dragonfly : après Stuxnet, nouvelle attaque réussie contre les systèmes Scada