Attaque informatique contre les fournisseurs d’énergie – Dragonfly lance la cyberguerre froide…

Attaque informatique contre les fournisseurs d’énergie – Dragonfly lance la cyberguerre froide…

Le scénario du pire. Ou presque. Un groupe de hackers, baptisé Dragonfly, est parvenu à corrompre certains systèmes de contrôle des opérateurs d'énergie. Notamment en France. Les pirates avaient alors la possibilité de saboter la distribution d'énergie de certains pays.

Selon Symantec, un groupe de pirates, probablement de l'Est, est parvenu à pénétrer les systèmes d'entreprises travaillant dans le secteur de l'énergie, à des fins d'espionnage. Pire : pour l'éditeur, les assaillants, baptisés Dragonfly, avaient les moyens « d'endommager ou d'interrompre la fourniture d'énergie dans les pays affectés » via la corruption de systèmes Scada (système de contrôle et d'acquisition de données). La France figure au troisième rang des pays touchés par l'infection derrière l'Espagne et les Etats-Unis. Interrogés par l'AFP, GDF Suez et EDF ont affirmé ne pas être au courant de ces attaques. Symantec assure avoir contacté les sociétés victimes des attaques ainsi que les autorités des pays concernés, notamment leurs CERT (Computer Emergency Response Centers). Avant de publier hier son alerte sur le Web.

Parmi les cibles de Dragonfly figuraient des opérateurs de réseau, des entreprises impliquées dans la génération d'électricité, des opérateurs de pipeline ou des fournisseurs d'équipements industriels pour le secteur. Selon Symantec, Dragonfly est un groupe de hackers bien financé, employant tout un arsenal de malwares. Pour sa campagne ciblant les spécialistes de l'énergie, Dragonfly a notamment employé des virus compromettant la sécurité de systèmes de contrôle industriels de trois constructeurs différents.

L'infection de l'ordinateur se fait par la technique du *watering hole* : au lieu de pratiquer le*phishing* (le « hameçonnage » via des mails qui imitent des mails officiels) ou l'envoi d'un mail accompagné d'une pièce jointe infectée, le*watering hole* consiste à pirater un site dûment fréquenté par le propriétaire légitime du PC. Quand le visiteur passe sur le site, ou quand il télécharge un des éléments du site, il y installe sans le savoir un virus. Le *watering hole* peut prendre des formes très sophistiquées : il y a eu des cas dans lesquels les pirates ont réussi à pirater les mises à jour de logiciels très répandus. En clair, quand le système va chercher la mise à jour, il télécharge un virus. Twitter, Microsoft, Facebook ou Apple par exemple, ont déjà été contaminées.

« *Dragon Fly est plus qu'un virus*, martèle Laurent Heslault, directeur des stratégies de sécurité chez Symantec France. *D'abord, c'est un programme très sophistiqué. Il a fallu plusieurs équipes très organisées sur une longue période pour le mettre au point et le diffuser. Cela dépasse les capacités d'un hacker solitaire et semble indiquer qu'un Etat se trouve derrière. Nous avons pu déterminer que les logiciels malveillants étaient compilés sur des horaires de travail, du lundi au vendredi avec un horaire de GMT – 4, ce qui correspond aux pays de l'Est.* » La piste russe, si elle n'est pas nommée de façon explicite, est la plus souvent citée chez les spécialistes de la sécurité. « *Qui peut avoir intérêt à lancer ce genre d'attaques,*s'interroge Loïc Guezo, directeur stratégie Europe du Sud de Trend Micro,*qui peut vouloir plonger la France dans le noir ? Nous sommes dans des problèmes géopolitiques avec en l'espèce une empreinte russe. C'est un des éléments de géopolitique d'une cyberguerre froide.* »

Fausses traces volontaires

« Nous devons être très prudents, rectifie Laurent Heslault, *il y a des cas où on laisse de fausses traces exprès pour faire croire que l'attaque vient d'un pays alors qu'elle vient d'un autre. Tout ce qu'on peut affirmer c'est que l'attaque vient de services de renseignement, privés ou publics. »* Un tel virus pourrait avoir été fabriqué et vendu par des sociétés privées spécialisées dans le renseignement. Un Etat qui ne dispose pas forcément des compétences informatiques nécessaires à la mise au point d'un tel virus, a donc pu tout simplement l'acheter, comme il peut acheter des chars d'assaut ou des fusils de précision. Il existe des groupes comme Hidden Lynx ou des sociétés privées qui proposent ce type de services.

Menace réelle

Loïc Guezo explique que Symantec *« a très bien su architecturer cette information, bien qu'elle soit ancienne. »* De fait, les sociétés de sécurité informatique peuvent avoir tendance à exploiter ce genre de cyber-attaques pour inciter les entreprises à acheter de fort coûteux systèmes de protection.

La menace est pourtant réelle. *« Nous avons simulé la mise en place virtuelle de l'implantation d'une station de traitement des eaux, raconte Loïc Guezo. Nous avons ainsi pu qualifier les attaques. Beaucoup venaient de Russie, en mode renseignement. Les attaques chinoises étaient plus intrusives et semblaient venir d'APT One, autrement dit des militaires chinois. »*

Les services américains ne sont pas en reste. *« Stuxnet, un virus développé par les Etats-Unis et Israël pour perturber les installations nucléaires iraniennes, a fait exploser plus d'une centaine de centrifugeuses reconnaît Laurent Heslault, mais Dragonfly va plus loin : il permet une prise de contrôle à distance. Une usine ou une centrale peuvent être contrôlés. Par exemple on peut contrôler une centrale nucléaire ou une usine d'embouteillage de jus de fruit ou la fabrication de médicaments. »*

En complément de cette technique hautement sophistiquée ouvrant la porte à des opérations de sabotage, qui pousse Symantec à soupçonner des liens entre Dragonfly et un Etat, les hackers ont infiltré les organisations ciblées via de classiques campagnes de phishing et des sites vérolés (via l'injection de iframe). C'est via cet ensemble de techniques que les assaillants ont pu se ménager un accès sur les réseaux de leurs cibles pour y récupérer des informations.

Des mises à jour vérolées !

C'est le second cas avéré de piratage de systèmes Scada, après le virus Stuxnet qui avait ciblé les centrifugeuses utilisées par l'Iran dans le cadre de son programme d'enrichissement d'uranium. Rappelons que les spécialistes attribuent la paternité de Stuxnet aux services secrets américains et israéliens. Le piratage des Scada apparaît comme la préoccupation numéro un des Etats en matière de cybersécurité (c'est le cas en France), tant le potentiel d'une attaque ciblant ces équipements apparaît dévastateur.

Dans le cas présent, selon Symantec, Dragonfly est parvenu à corrompre les sites de trois constructeurs de systèmes de contrôle, insérant un malware dans les mises à jour logicielles qu'ils publient sur leur site à destination de leurs clients. Le premier système compromis fournit un accès VPN à un contrôleur logique programmable. Si son fournisseur a découvert l'attaque rapidement, 250 téléchargements avaient déjà eu lieu. Dans le second cas, un driver pour un périphérique d'un autre contrôleur, la mise à jour infectée est restée disponible pendant six semaines. Le troisième fournisseur ciblé, un constructeur de systèmes gérant des turbines éoliennes, des usines de biogaz et d'autres infrastructures, aurait lui laissé le logiciel infecté sur son site pendant une dizaine de jours. Pour Symantec, cette technique consistant à infecter des fournisseurs plus petits – et moins bien protégés – que les cibles réelles de Dragonfly – des géants de l'énergie – montre l'intelligence tactique du groupe de pirates.

Pour l'éditeur américain, Dragonfly est actif depuis au moins 2011 et se serait d'abord intéressé au secteur de la défense et de l'aviation aux Etats-Unis et au Canada, avant de se focaliser sur le secteur de l'énergie début 2013. Détail amusant : en se basant sur une analyse des opérations de Dragonfly, Symantec note que le groupe travaille essentiellement entre le lundi et le vendredi, pendant les horaires de bureau…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.silicon.fr/apres-stuxnet-nouvelle-attaque-reussie-contre-les-systemes-scada-95359.html