Thomas Houdy, Lexsi : « Après Dragonfly, réagir sur la sécurité des Scada »

Si l'affaire Dragonfly, dévoilée par Symantec, est passée relativement inaperçue dans les médias, elle n'a pas manqué d'attirer l'attention des spécialistes. D'abord parce qu'il s'agit tout simplement de la **seconde attaque connue ciblant des systèmes de contrôle industriel**, les fameux Scada. Rappelons que la première, Stuxnet, probablement fomentée par les Etats-Unis et Israël, avait détruit une partie des capacités de l'Iran en matière d'enrichissement de l'uranium. Ciblant des industriels de l'énergie, Dragonfly est pris très au sérieux par le centre de réponse américain aux incidents ICS-CERT (US Industrial Control Systems Computer Emergency Response Team). Ce dernier a émis une alerte enjoignant les entreprises du secteur à analyser leurs réseaux pour y détecter des traces d'intrusion. En France, l'Anssi (Agence nationale de la sécurité des systèmes d'information) et le CERT-FR sont restés sans réaction.

Si Dragonfly a attiré l'attention, c'est aussi en raison d'une astuce utilisée par les assaillants. Plutôt que de cibler directement les systèmes Scada des industriels de l'énergie, ceux-ci ont **infecté les sites Web des fournisseurs**, de petites sociétés peu habituées à faire face à ce type d'intrusion, espérant que leurs clients viendraient télécharger les mises à jour dument vérolées. En recoupant diverses informations, le site Digital Bond a identifié au moins deux des trois fournisseurs concernés. Il s'agit de l'Allemand MB Connect Line (contrôles pour éolienne et usines de biogaz) et du Belge eWon (accès VPN).

Autant d'éléments qui doivent servir de signaux d'alerte pour **Thomas Houdy**, associé au cabinet Lexsi et spécialiste de la cybersécurité des systèmes industriels (Scada). Dans cette interview, le consultant met en exergue le retard des équipes de production industrielle en matière de prise de conscience des risques.

***Silicon.fr* : Est-ce que le modus operandi de Dragonfly vous a surpris ?**

Thomas Houdy : En tant que tel, ce n'est pas une surprise : le malware employé – un RAT (Remote Access Tool) – est d'ailleurs connu. Par contre, le fait que ce malware s'attaque directement aux systèmes industriels de contrôle commande est très significatif. Par ailleurs, parmi les méthodes utilisées pour s'introduire sur ces systèmes, il faut relever que les assaillants ont identifié et ciblé des fournisseurs dont le métier n'est pas la sécurité et dont les sites ne sont pas bien protégés en espérant que les industriels visés téléchargeraient les mises à jour des logiciels utilisés par les systèmes de contrôle et commande. Ces dernières étant évidemment infectées.

L'autre élément très significatif réside dans le fait que le RAT utilisé scanne et va rechercher des machines OPC, un protocole de communication spécifiquement utilisé par les systèmes industriels. Ce qui montre que les assaillants cherchent à exploiter les points d'adhérence de plus en plus nombreux entre les systèmes d'information de gestion et les systèmes industriels. Ces ponts servent notamment à remonter des informations issues de la production directement dans les systèmes de pilotage de l'entreprise.

Enfin, il faut noter le double objectif des assaillants. Le malware semble avoir été conçu pour voler de l'information mais portait en germes la capacité à saboter les systèmes de contrôle. Ce qui est évidemment préoccupant.

A votre connaissance, s'agit-il de la seconde attaque réussie contre les systèmes Scada ?

Après Stuxnet, il s'agit bien là de la seconde affaire publique en la matière. Clairement, un palier est franchi avec Dragonfly. Il faut que cette affaire serve de prise de conscience. Notamment auprès de ce que j'appelle les OINV, les opérateurs d'importance NON vitale (par opposition aux OIV identifiés par l'Etat, NDLR). Des organisations peu suivies mais chez qui des problématiques peuvent exister. Au sein de Lexsi, nous sommes par exemple intervenus sur des automates de collectivités territoriales exposés sur Internet, et certaines des connexions à ces machines que nous avons identifiées dans les logs provenaient de Chine ou de Corée du Sud. La prise de conscience doit

également toucher les fournisseurs, pour lesquels la sécurité reste trop souvent mésestimée. Parmi ceux qui ont été touchés par l'attaque Dragonfly, nous connaissons ainsi un fournisseur chez qui les login et mots de passe par défaut sont triviaux.

De leur côté, les industriels utilisateurs des Scada sont-ils prêts ?

Clairement pas. Le rapport de force est totalement disproportionné. Déjà, dans les systèmes informatiques de gestion, on est face à un constat d'échec. Et, dans le contexte industriel, il faut comprendre qu'on a 10 à 15 ans de retard dans la prise de conscience par rapport à l'informatique de gestion. Nombre d'industriels ne comprennent tout simplement pas où se situe la problématique. 100 % des tests de perméabilité que nous avons menés depuis 3 ans et demi ont été concluants : depuis le SI de gestion ou un sous-réseau de l'entreprise, nous sommes parvenus à prendre le contrôle de l'usine. Sur des sites Seveso, nous avons identifié des problèmes d'architecture. Et si on se tourne vers le futur, avec les smart grid et l'Internet des objets, le problème ne va aller qu'en s'accentuant. Tous les systèmes industriels vont reposer sur des protocoles (Modbus, OPC…) faibles au plan sécuritaire. On est en train de construire des châteaux sur des sables mouvants.

L'objectif de Dragonfly était de récupérer de l'information mais aussi d'implanter des malwares dormants sur des Scada en vue d'éventuelles opérations de sabotage ultérieures. Pensez-vous que d'autres malwares dormants sont aujourd'hui présents sur des systèmes industriels ?

Non seulement j'en suis persuadé, mais je le sais. Des malwares aussi connus que Conficker se baladent allégrement sur les systèmes de contrôle commande. Ils sont souvent introduits par les PC ou les clefs USB des fournisseurs, lors de leurs interventions. Des industriels ont déjà connu des dégradations de performances à cause de virus datant de 2005. Tout simplement parce que les systèmes affectés ne sont pas conçus pour résister à des cyber-attaques. Partant de là, on peut très bien imaginer d'autres infections, plus ciblées et potentiellement destructrices.

Les concepteurs de systèmes industriels sont-ils en train d'évoluer pour mieux designer leurs solutions aux contraintes de sécurité ?

Les géants comme Schneider ou Siemens, placés sur le grill, ont réagi en mettant en place des équipes cyber-sécurité en interne. Mais 99 % des problèmes concernent le parc installé. Un parc qu'il est souvent impossible de ré-architecturer faute de budgets pour le faire.

Sur ce parc, ne pourrait-on pas améliorer la situation via une gestion de patch intelligente ?

Mais les industriels ne sont pas bons sur la gestion des patchs ! Qui plus est, une mise à jour peut parfois dégrader la production. Et les aspects de revalidation du serveur sont très lourds. Or, la priorité de l'usine est de produire, pas de consacrer ses ressources à la sécurité. Souvent la problématique est donc sous-traitée. Et on retrouve parfois des prestataires utilisant de simples box ADSL pour appliquer les patch… Entraînant une nouvelle faille de sécurité !

Que recommandez-vous ?

Tous les fournisseurs s'activent pour vendre leurs solutions de défense en profondeur. Mais je

pense qu'il faudrait avant tout mettre en place une capacité de détection des signatures de virus et des événements de sécurité au sein des environnements industriels. Une simple sonde Snort sur Linux pourrait suffire. La création d'une solution dédiée pourrait d'ailleurs faire l'objet d'un projet européen.

En complément :

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

IBM recense les cyberattaques à haut risque pour 2014