Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

	Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

D’après les informations de FireEye, le malware Irongate, qui vise les systèmes de contrôle des procédés industriels ressemble en certains points au terrible ver Stuxnet. Cette découverte est une nouvelle source d’inquiétude pour les membres de la communauté de la sécurité de l’information et elle vient confirmer la nécessité du perfectionnement des systèmes de détection des malwares qui attaquent les infrastructures critiques.

Les chercheurs ont également signalé qu’Irongate ne constituait pas une menace sérieuse pour l’instant car il fonctionne uniquement dans des environnements simulés. Ceci étant dit, FireEye indique que ce malware est passé inaperçu pendant des années alors qu’il figurait pendant tout ce temps dans la base VirusTotal. « La compétence du secteur dans le domaine de l’identification et de la détection des menaces s’améliore, mais elle n’a pas encore atteint un niveau satisfaisant comme le montrent ces exemples » constate Rob Caldwell, directeur du groupe d’analyse FireEye Labs Advanced Reverse Engineering (FLARE). Il poursuit en expliquant qu’il faut absolument mieux comprendre ce que représentent les menaces pour les systèmes de contrôle des procédés industriels, comment les détecter et comment améliorer la protection contre celles-ci. »

D’après FireEye, le malware qu’elle a identifié se distingue par sa capacité à mener une attaque de type homme du milieu contre l’entrée et la sortie des procédés et à attaquer l’application qui exécute des opérations sur les processus dans les environnements simulés. Un système compromis par Irongate permet aux attaquants de substituer les contrôles industriels à l’insu de l’opérateur du système. Des techniques semblables ont déjà été utilisées par le passé pour mettre hors service des infrastructures critiques diverses, depuis des réseaux de distribution d’électricité jusqu’aux contrôleurs logiques de centrifugeuses dans le secteur nucléaire.

Les chercheurs ont découvert une exemplaire d’Irongate vers la fin de l’année 2015 sur VirusTotal alors qu’ils recherchaient des droppers compilés à l’aide PyInstaller. L’échantillon trouvé ressemblait très fort aux malwares qui visaient les systèmes d’automatisation industrielle et autres systèmes de contrôle des procédés industriels. Il se fait que ce modèle avait été chargé pour analyse en 2012, mais aucun logiciel antivirus ne l’avait reconnu.

L’analyse a démontré que le malware utilise une technique de l’homme du milieu qui permet de réaliser des attaques contre une application personnalisée de l’utilisateur qui fonctionne dans un milieu de modélisation des contrôleurs logiques programmables Step 7 de Simens Les experts ont découvert également une bibliothèque dynamique capable de masquer le comportement malveillant du code exécutable. Cette DLL est capable d’enregistrer cinq secondes du trafic « normal » provenant du contrôleur logique programmable modélisé ; l’attaquant peut reproduire ce fragment afin de masquer le transfert des données codées en dur vers l’équipement d’imitation.

Les chercheurs ont été surpris de voir que pour rendre l’analyse plus difficile, ce malware spécialisé se comporte comme un malware traditionnel : lorsqu’il est exécuté sur une machine virtuelle ou dans un bac à sable (Cuckoo), il passe en mode de veille et refuse de s’exécuter.

« Bien que Stuxnet soit plus complexe sur le plan technique, Irongate possède quelques traits similaires » a déclaré Sean McBride, analyste antivirus principal chez FireEye. Pour être plus précis, il a noté que ces deux malwares sont destinés à attaquer un système particulier de gestion et ils utilisent des outils de protection contre la détection : Stuxnet est capable de détecter la présence d’un logiciel antivirus et Irongate, celle d’une machine virtuelle. Toutefois, à la différence de ses rares confrères commeBlackEnergy, Havex, et même Stuxnet, Irongate n’est pas très répandu dans la pratique : il fonctionne seulement dans les environnements simulés orientés sur les systèmes Siemens.

Qui est donc à l’origine de ce malware et quel est son objectif ? FireEye avance trois hypothèses en réponse. Tout d’abord, les experts supposent que son auteur peut avoir nourri l’espoir que quelqu’un transfèrerait ce code depuis l’environnement simulé et commencerait à l’utiliser dans son environnement de travail. Il est également possible qu’Irongate soit un modèle expérimental et que son créateur a décidé de vérifier à quel point il était facile de le détecter via les services VirusTotal. La troisième hypothèse est celle considérée comme la plus probable par FireEye : un expert en sécurité de l’information a oublié qu’il avait soumis ce code à une vérification il y a un certain temps.

« Il convient de fournir de plus gros efforts dans le secteur pour détecter les menaces qui visent les systèmes de contrôle des procédés industriels » conclut Dan Scali, conseiller principal de la division conseil de FireEye sur les questions de sécurité des systèmes d’automatisation industrielle. « Globalement, il n’y a pas eu de gros progrès dans la résolution des problèmes posés par Irongate depuis Stuxnet. Dans la mesure où l’accès à de tels attaques se démocratise, le thème de l’adéquation des mesures de protection est source de préoccupation.

Réagissez à cet article

Original de l’article mis en page : Un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet – Securelist