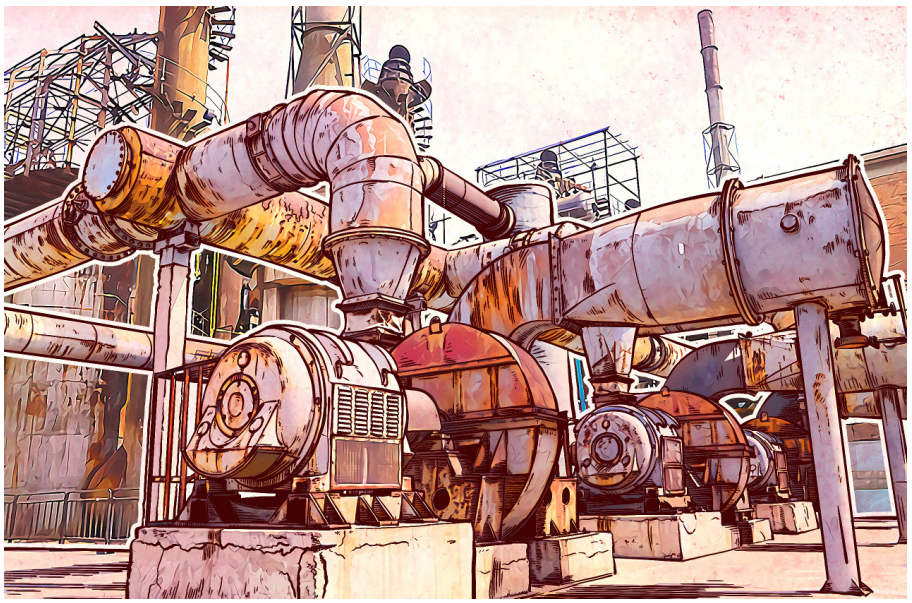
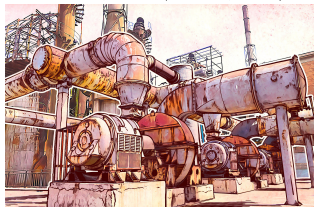
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie ?



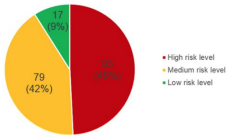
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie ?

On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.
Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).
View image on Twitter



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

Follow
Kaspersky Lab
✔@kaspersky
Industrial #cybersecurity threat landscape https://kas.pr/MY6j #klreport
8:29 PM – 11 Jul 2016
•
•
2020 Retweets
•
99 likes

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.
View image on Twitter

Follow
Kaspersky Lab
✔@kaspersky
Maritime industry is easy meat for cyber criminals – http://ow.ly/Nio2a
12:25 AM – 23 May 2015
•
•
3232 Retweets
•
1313 likes

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?
Les possibles effets et conclusions dépendent des entreprises que les cybercriminels visent, et quel SCI elles utilisent.
Nous avons connaissance de quelques exemples de piratages industriels. En décembre 2015, la moitié des maisons de la ville ukrainienne Ivano-Frankivsk s'étaient retrouvées sans électricité à cause du piratage d'un générateur électrique. La même année avait également eu lieu une attaque de l'entreprise Kemuri Water.
Comme si cela ne suffisait pas, l'**aéroport Frédéric Chopin de Varsovie** avait aussi été la cible d'une attaque. Et un an plus tôt, des hackers avaient perturbé l'opération d'un haut-fourneau dans une aciérie en Allemagne.
Follow
Kaspersky Lab
✔@kaspersky
Black Hat and DEF CON: Hacking a chemical plant –https://kas.pr/RT61
9:35 PM – 19 Aug 2015

Black Hat and DEF CON: Hacking a chemical plant
Since there's nothing unhackable in this world, why should chemical plants should be the exception?
blog.kaspersky.com
•
•
1313 Retweets
•
1010 likes

Globalement, la sécurité des systèmes de contrôle industriel laisse encore à désirer. Kaspersky Lab a émis à plusieurs reprises des mises en garde concernant ces risques, mais d'éternels insatisfaits trouvent en général la parade : informez-nous de cas *réels* où ces vulnérabilités ont*vraiment* été exploitées. Malheureusement, on peut désormais le faire.

Bien évidemment, une personne seule ne peut pas faire grand-chose pour résoudre un problème systémique. Un équipement industriel ne peut pas être changé du jour au lendemain ou même en l'espace d'une année. Toutefois, et comme nous l'avons déjà dit, la défense la plus importante en matière de cybersécurité est de rester informés. Plus de personnes sont au courant du problème, et plus il y a de chances pour que les infrastructures industrielles soient à l'abri d'attaques néfastes.
Article original de John Snow

Denis JACOPINE est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.