

Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière



Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière

Des chercheurs en sécurité ont créé LogicLocker, un logiciel malveillant capable de bloquer une station d'épuration d'eau dans le but d'extorquer des rançons. Ce type d'attaque serait la prochaine étape dans le domaine des ransomwares.

Les ransomwares cryptographiques, qui chiffrent les données des utilisateurs pour extorquer une rançon, vous font peur ? Alors attendez de voir les « ransomwares industriels », qui s'attaquent aux systèmes de contrôle des usines. Ils vous feront basculer en mode panique, car ils pourraient avoir des conséquences directes et néfastes sur notre environnement physique. Pour l'instant, ce type de malware ne fait pas encore partie de l'arsenal des pirates, mais des chercheurs de Georgia Institute of Technology pensent que ce n'est qu'une question de temps, étant donné la faible sécurité des systèmes industriels. Pour montrer l'étendue de la menace, ils ont développé un prototype d'un tel ransomware et l'ont testé sur une maquette industrielle qui représente une station d'épuration d'eau d'une ville. Ils ont présenté leur travail cette semaine à l'occasion de la conférence RSA 2017, qui s'est tenue à San Francisco.

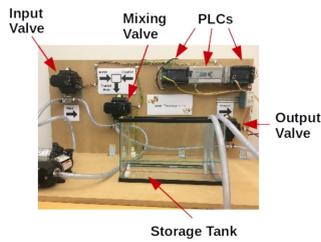


Fig. 2: Water Treatment Testbed

Baptisé LogicLocker, ce malware est capable d'infecter l'automate programmable industriel (programmable logic controller, PLC) qui régule la désinfection et le stockage de l'eau potable. L'attaque consiste à extraire le code exécutable de l'appareil et de le remplacer par un code malveillant, puis de changer le mot de passe d'accès. Ainsi, l'attaquant peut non seulement stopper le processus d'épuration, mais aussi empêcher les ingénieurs de réinstaller le code d'origine sur l'appareil. Le pirate peut alors envoyer aux responsables de la station d'épuration une demande de rançon doublée d'un ultimatum : s'ils ne payent pas au bout d'un certain temps, le code malveillant va surdoser le produit désinfectant et, du coup, rendre toute l'eau potable impropre à la consommation. Une fois la rançon payée, l'attaquant restitue le code volé.

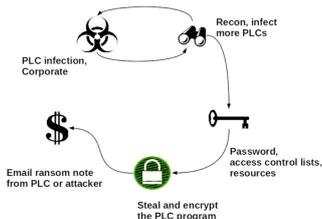


Fig. 3: General Flow of ICS Ransomware Attack

Un tel scénario est faisable dans n'importe quel domaine, à partir du moment où il y a des automates programmables connectés sur un réseau interne ou, carrément, sur Internet. Il suffit de se rendre sur le site Shodan.io pour constater qu'il existe d'ores et déjà des milliers de PLC accessibles par la Toile. Les chercheurs ont en trouvé d'emblée plus de 1400 de marque MicroLogix et 250 de marque Schneider Modicon.

Une question de profitabilité

Si les pirates n'ont pas encore exploité ce type d'attaque, ce n'est pas parce que ces automates sont bien sécurisés. Au contraire, leur manque de protection est notoire et connu depuis des années. « La seule explication est que les cybercriminels n'ont pas encore trouvé le business model qui leur permet d'opérer de manière profitable dans ce type d'environnement », estiment les chercheurs dans leur étude. En effet, le ransomware industriel nécessite plus de recherche et de connaissance. Par ailleurs, son mode opératoire est très pointu et ne peut donc faire qu'un faible nombre de victimes. C'est donc exactement l'inverse des cryptoransomwares, qui sont diffusés en masse auprès d'un large parc d'utilisateurs. [lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03841 84)
Plus d'informations sur : <https://www.Lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisée en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, conteneur, détournements de clientèle...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DCTEP n°1034 03841 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Ce malware pourrait empoisonner l'eau potable d'une ville entière*