

Les caméras de surveillance de Washington paralysées par le Ransomware again



Selon le Washington Post, un ransomware aurait paralysé pendant plusieurs jours le réseau de caméras de surveillance municipale de Washington DC. Une réinitialisation générale a permis de se débarrasser du malware.

Quelques jours avant l'investiture de Donald Trump, la ville de Washington a fait face à une mauvaise surprise : selon le Washington Post, les caméras de la ville ont été victimes d'un malware de type ransomware qui les a rendus inutilisables, empêchant l'enregistrement d'image pendant plusieurs jours.



L'attaque a été détectée lorsque la police a réalisé que quatre caméras municipales ne fonctionnaient pas correctement et a contacté son prestataire informatique afin de résoudre le problème. La société a immédiatement détecté la présence de deux types de ransomware au sein des caméras, ce qui les a poussés à lancer une évaluation globale portant sur l'ensemble des appareils connectés au réseau de la ville. Au total, 123 caméras sur les 187 connectées au réseau présentaient des signes d'infection.

Les services municipaux n'ont néanmoins pas eu besoin de sortir leur porte-monnaie bitcoin pour remettre le système en route : une simple réinitialisation des caméras utilisées a permis de se débarrasser du malware et de relancer le fonctionnement. Le CTO de la ville a précisé qu'aucune rançon n'avait été payée par la ville et que le malware n'avait pas cherché à accéder au reste du réseau interne de la ville de Washington DC.

Washington s'en sort donc plutôt bien, contrairement à cet hôtel de luxe qui s'est vu contraint de payer les opérateurs d'un ransomware qui avaient bloqué l'ensemble du système de clef magnétique utilisé pour accéder aux chambres. Mais peu d'informations ont été diffusées par la ville sur la nature exacte de l'attaque, du ransomware ou même de la demande de rançon.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé 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, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Original de l'article mis en page : Ransomware again : les
caméras de surveillance de Washington paralysées – ZDNet