MAIRE info

Cyberattaques : comment les pirates attaquent les réseaux informatiques des collectivités

24/03/2020

Num&#65533;rique

En cette période de crise sanitaire, la pérennité des systèmes informatique des administrations est un élément crucial – quand souvent le site internet d'une commune est l'un des seuls moyens de communication directe des citoyens avec l'administration. Mais face à des attaques qui se multiplient, l'Agence nationale de la sécurité des systèmes d'information publie des recommandations qui doivent attirer toute l'attention des responsables.

Moins d'un mois après la paralysie informatique subie de plein fouet par la région Grand Est (lire *Maire info* du 20 février), une nouvelle attaque informatique de grande ampleur a mis en péril, samedi 14 mars, les systèmes d'information et les données liées aux élections municipales des villes de Marseille et Martigues ainsi que de la métropole Aix-Marseille-Provence (Bouches-du-Rhône). Principales conséquences concrètes : les sites internet de ces collectivités étaient inaccessibles plusieurs jours, tout comme les téléphones fixes et les ordinateurs des agents. Une enquête a été ouverte par le parquet de Paris.

Depuis, les infrastructures informatiques ont été progressivement restaurées dans la cité phocéenne et sa région mais certains votes par procuration ont bien été perturbés, dimanche 15 mars lors du premier tour du scrutin. La remontée des résultats, elle, a dû s'appuyer sur les dispositifs de secours. Comment ces attaques - la dernière en date, dimanche 22 mars, a touché deux des adresses Internet de l'Assistance publique des hôpitaux de Paris (AP-HP) sans atteindre ses infrastructures (attaque par déni de service) - sont-elles construites ? Quel est le mode opératoire des pirates et comment s'en prémunir ?

Le lexique : rançongiciel, Mespinoza, Pysa…

L'Agence nationale de la sécurité des systèmes d'information (Anssi) a apporté dans un rapport, publié le 18 mars, des éléments de réponses à toutes ces questions. Le constat, d'abord, est sans appel : « *Lors de ces attaques, des codes malveillants de type rançongiciel ont été utilisés, rendant certains fichiers inutilisables* », écrit l'Agence.

Il s'agit plus précisément d'une variante d'un rançongiciel « *connu en source ouverte sous le nom de Mespinoz*a ». Depuis octobre 2018, date supposée de son apparition, Mespinoza s'est déclinée en plusieurs versions. L'une d'elles pourrait être à l'origine de la cyberattaque dans les Bouches-du-Rhône : Pysa. Utilisée depuis décembre 2019, celle-ci tire simplement son nom de l'extension - « .pysa » - des fichiers chiffrés qu'elle produit.

Poupées russes

Mais à l'instar des poupées russes, les rançongiciels en cachent toujours un autre. Ainsi, deux versions différentes de Pysa ont été découvertes lors des investigations de l'Anssi : un fichier exécutable nommé « svchost.exe » et une archive « Python » (peut-être même une troisième : « .newversion »).

Sans être trop technique, retenons que ces deux codes malveillants sont à l'origine de la création d'un fichier de demande de rançon. « *Ces demandes de rançon sont écrites dans un anglais approximatif. Bien que différentes, elles contiennent des chaînes de caractères identiques comme* "To get all your data back contact us" », décrit l'Anssi (« *Pour récupérer vos données, contactez-nous* »). L'une des deux propose également à la victime le déchiffrement gratuit de deux fichiers, « *en guise de bonne foi* ».

Il est à noter, enfin, que « *les messages de demande de rançon contiennent deux adresses de courriel protonmail qui semblent générées à partir de noms propres choisis au hasard* ».

De façon un peu plus concrète, « *plusieurs événements survenus peu avant l'attaque pourraient être liés au mode opératoire et avoir permis l'accès initial ou la latéralisation* ». L'Anssi fait référence ici, par exemple, à « *des tentatives de connexion par force brute sur une console de supervision ainsi que sur plusieurs comptes ACTIVE DIRECTORY* », la compromission de « *certains comptes d'administrateurs de domaine* », « *l'exfiltration d'une base de données de mots de passe peu avant l'attaque* » ou encore à « *des connexions RDP illégitimes entre contrôleurs de domaine avec l'utilisation d'un nom d'hôte inconnu potentiellement lié au mode opératoire* ». Conclusion : « *Le mode opératoire observé dans cette attaque semble compatible avec un acteur opportuniste motivé par un but lucratif*.»

Recommandations

Pour « *empêcher la compromission complète du système d'information, les mesures d'hygiène et de sécurité classiques s'appliquent* ». Il s'agit, en premier lieu, « *d'assurer une sauvegarde des données critiques* » comme les bases de données métier ou le partage de fichiers réseaux. « *Ces sauvegardes doivent être périodiquement exportées vers un support inaccessible depuis le réseau et leur restauration doit être testée périodiquement afin de s'assurer qu'elles soient utilisables en cas d'urgence. Cette mesure est la seule garantie de protection des données face à un rançongiciel qui chiffrerait les données en ligne par propagation réseau* », avertit l'Anssi. Qui conseille, en outre, de « *mener des campagnes de mises à jour, en commençant par les vulnérabilités exploitables à distance (RCE)* », de « *restreindre, par filtrage réseau, l'accès à certains ports réseau les plus critiques sur les postes de travail* » ou encore « *d'utiliser les comptes d'administration de l'Active Directory seulement depuis des postes dédiés sans usage bureautique (navigation, messagerie, etc.) et sans accès à Internet* ».

Ludovic Galtier

Télécharger le rapport de l'Anssi.