Les ransomwares s'attaquent aux serveurs Linux

Chiffrer les données de ses victimes et n'y restaurer l'accès qu'en échange d'une rançon : c'est le mode de fonctionnement de **Linux.Encoder.1**. Ajouté le 5 novembre dans la base antivirus de Dr.Web, ce *malware* basé sur la bibliothèque de chiffrement PolarSSL vise, comme son nom l'indique, les systèmes Linux. Et plus particulièrement les serveurs Web.

Si les experts en sécurité informatique tentent encore de cerner ses vecteurs de propagation, la situation est plus claire concernant le reste du processus d'infection. Une fois exécuté avec des droits de niveau administrateur, Linux.Encoder.1 télécharge trois fichiers. Deux d'entre eux (*./readme.crypto* et *./index.crypto*) contiennent des instructions à l'intention des utilisateurs qui souhaiteraient déverrouiller leurs fichiers.

Pour obtenir la clé privée et le script PHP adéquats, il leur est demandé de payer 1 bitcoin – soit un peu moins de 340 euros au cours actuel (on notera que le message est rédigé dans un anglais approximatif ; il manque certains mots, selon ITespresso).

Le troisième fichier pointe vers une clé de chiffrement publique (RSA). Celle-ci est utilisée en association avec les clés privées (AES) que le *ransomware* exploite pour verrouiller les fichiers sur la machine infectée. Le mode opératoire est précis : les premiers fichiers chiffrés sont ceux situés dans les dossiers */home* et */root*, ainsi que ceux associés à l'administration de site(s) Web : */var/lib/mysql*, */var/www*, */etc/nginx*, */etc/apache2*, */var/log*).

Chiffrement étendu

Le chiffrement s'étend ensuite à l'ensemble du système de fichiers. Il est toutefois restreint sur certains points. D'une part à une cinquantaine d'extensions (dont .html, .css et .js) ; de l'autre, aux dossiers dont le nom contient des chaînes de caractères bien précises (public_html, www, webapp, backup, .git, .svn).

À tous les fichiers chiffrés s'ajoute l'extension .encrypted. Un guide de déchiffrement (README_FOR_DECRYPT.txt) est placé dans chacun des dossiers concernés. Lorsque la rançon est versée, le déchiffrement s'amorce et les fichiers sont restaurés dans l'ordre dans lequel ils avaient été verrouillés. En l'état actuel, la seule solution officielle en cas d'infection est de réaliser une copie de sauvegarde et de l'isoler du réseau.

A lire aussi :

Un ransomware change le code PIN des terminaux Android

Les publicités piégées au ransomware se multiplient

Code Linux Crédit Photo@isaak55-Shutterstock