

Des serveurs Linux attaqués par le ransomware Fairware



Des serveurs Linux attaqués
par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.

Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.

« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.

La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »

Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles. En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.

La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »

Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.

Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.

Article original de Securelist

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Réagissez à cet article

Original de l'article mis en page : Fairware attaque des serveurs Linux – Securelist