Forum: Sécurité

Topic: Un malware qui piège les antivirus

Subject: Re: Un malware qui piège les antivirus

Publié par: tignothe

Contribution le : 12/01/2022 23:57:45

Bonjour,

—Typiquement le genre d'information balancée sans aucunes explications (comme d'habitude).

Tout d'abord cela concernerait spécifiquement les serveurs sous Linux avec un mode de contamination pas clair du tout ; Donc pas la peine de tenter d'affoler l'utilisateur lambda avec sa distribution Ubuntu, Manjaro ou Fedora… D'autant plus que les utilisateurs sous Linux vont chercher les logiciels et autres mises à jour dans les dépôts et non pas n'importe où et n'importe comment comme il se pratique allègrement dans le monde Windows avec des sessions ouvertes sous administrateur…

Bon, un peu de lecture ;

Le 12 octobre 2021 — FontOnLake, des malwares discrets pour les systèmes Linux
https://www.lemondeinformatique.fr/act ... esxi-de-vmware-85401.html

Le 12 octobre 2021 — FontOnLake : un virus discret et sophistiqué attaque les systèmes sous Linux
https://cybersecuritymag.africa/index. ... ue-attaque-systemes-linux

Le 31 octobre 2021 — FontOnLake : Un logiciel malveillant redoutable qui cible les ordinateurs sous Linux
https://www.20minutes.fr/high-tech/315 ... ux-ordinateurs-sous-linux

D'après ce qui est noté sur le monde informatique les premières manifestations sur certains serveurs ont eu lieu en mai 2020

par modification de certains utilitaires Linux ; je cite ; « cat » « kill » « sftp » « sshd » les deux premiers notés sont des commandes utilisées couramment dans un terminal, la troisième est un protocole de transfert

SSH File Transfer Protocol
https://fr.wikipedia.org/wiki/SSH_File_Transfer_Protocol

le quatrième terme est ce que l'on veut ;

SSHD
https://fr.wikipedia.org/wiki/SSHD

Bef, nous sommes loin d'avoir des explications très claires car je suis certain que le rédacteur de l'article n'a pas idée de l'utilisation de la commande « cat » ou « kill » dans un terminal (des trucs que j'utilise sans frémir sous mes machines linux).

Je n'ai pas pris la peine de faire des recherches plus approfondies concernant le monde Windows et encore moins Mac ; je suis persuadé que d'autres que moi vont s'y atteler.

Encore une fois Tof81, il aurait été plus sérieux de fournir un minimum d'info plutôt que de favoriser le scoop vite fait bien fait.

L'article de Futura Tech est tombé à 16 h 06, largement le temps d'une petite recherche non ?