Le ransomware Cuba s’en prend aux serveurs Exchange

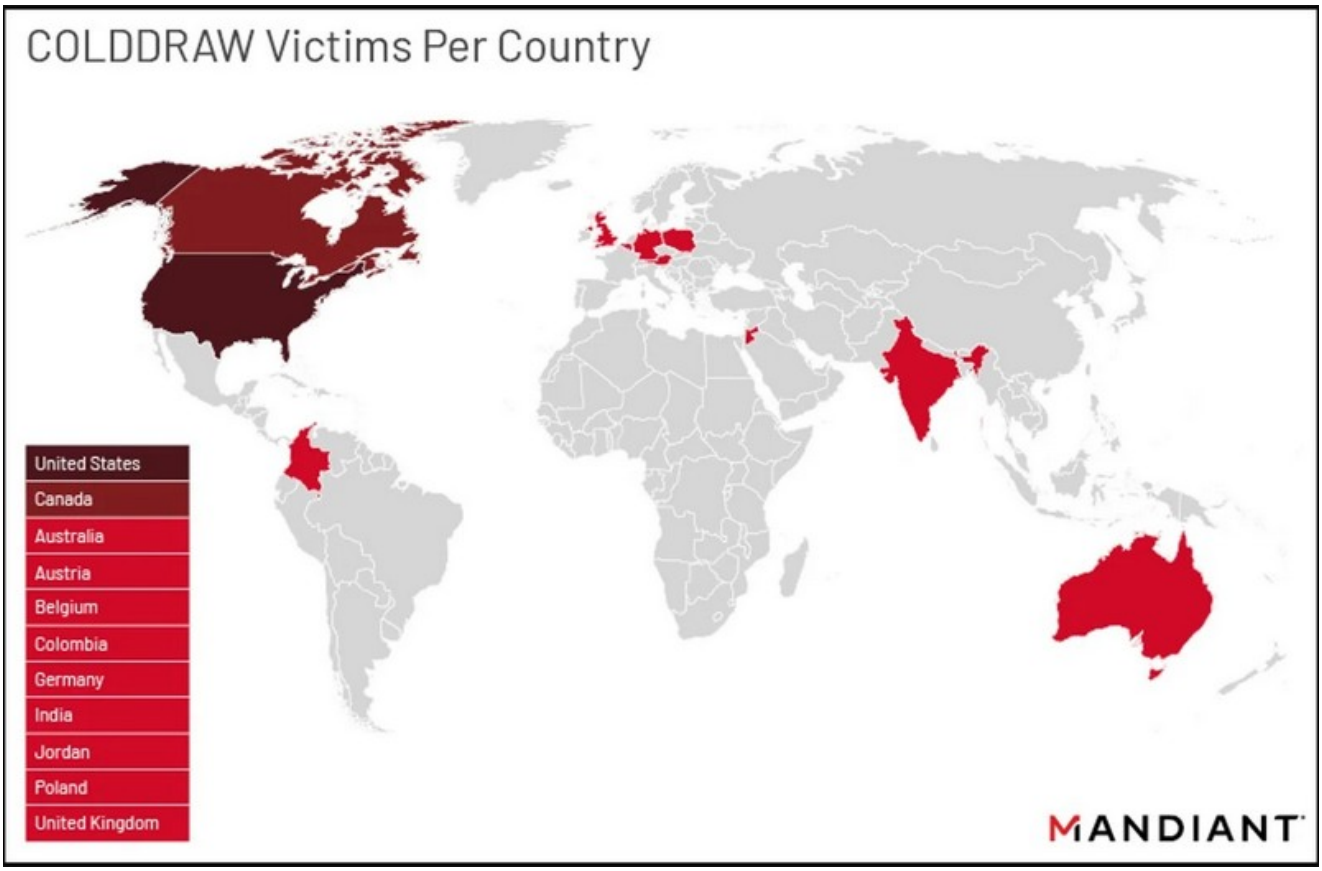
it-connect.fr/le-ransomware-cuba-sen-prend-aux-serveurs-exchange/

Florian Burnel 25/02/2022

Le ransomware Cuba exploite des vulnérabilités connues au sein de Microsoft Exchange pour obtenir un accès au réseau d'entreprises et chiffrer les machines une fois l'infrastructure compromise.

L'entreprise spécialisée en sécurité Mandiant, suit de près les activités du gang **UNC2596** et de leur ransomware nommé **COLDDRAW**, bien connu sous le nom de **Cuba**. Il n'est pas nouveau puisqu'il est en activité depuis la fin 2019, et en 2021 il s'est montré particulièrement actif. À tel point que le FBI a émis un bulletin de sécurité au sujet du ransomware Cuba car ses auteurs ont **compromis 49 organisations critiques aux États-Unis**.

D'ailleurs, d'après le rapport de la société Mandiant, on peut voir qu'il agit surtout aux États-Unis et au Canada. Sa présence en Europe est relativement faible, mais il n'est pas à exclure que cela évolue.



Lorsque le serveur est compromis, une porte dérobée est installée sur le serveur, en s'appuyant sur deux outils : Cobalt Strike et NetSupport Manager, un logiciel de prise en main à distance. En complément, les pirates utilisent leurs propres outils :

- **Bughatch** : téléchargement de fichiers à partir du serveur Command & Control
- **Wedgecut** : énumération de l'Active Directory à partir de commandes PowerShell
- **Burntcigar** : un outil capable de terminer n'importe quel processus au niveau du noyau en exploitant une faille de sécurité

Pour effectuer des mouvements latéraux sur l'infrastructure de la victime, ils s'appuient sur différentes méthodes et outils : RDP, SMB, PsExec et Cobalt Strike. Enfin, des données peuvent être exfiltrées vers la propre infrastructure des pirates, et non pas vers des services Cloud, avant que les données soient chiffrées par le ransomware Cuba.

Quelles sont les vulnérabilités utilisées ?

Lorsque l'on évoque la compromission d'un serveur de messagerie Exchange, il y a deux noms qui ressortent à chaque fois depuis l'année dernière : **ProxyShell** et **ProxyLogon**. Bingo ! Ces deux ensembles de vulnérabilités sont exploités par le gang UNC2596 afin de compromettre les serveurs Exchange.

D'ailleurs, ces failles de sécurité font partie du **top 10 des vulnérabilités de 2021 selon l'ANSSI**, et cela se confirme une fois de plus qu'elles sont très appréciées par les pirates. Il y a fort à parier qu'il existe encore des serveurs Exchange vulnérables un peu partout dans le monde, alors c'est l'occasion de faire une piqure de rappel sur la nécessité d'installer les correctifs disponibles depuis plusieurs mois.

Source