Ваиет impliqué dans la campagne Banacry!

Ce document est marqué TLP RED. Pour plus d'informations, consulter le site https://www.us-cert.gov/tlp

Résumé :
Le groupe d'attaquant Ваиет fait encore parler de lui. Depuis le 15 mars 2018, plusieurs fuites massives de données ont été attribuées à ce groupe que les chercheurs estiment implanté en Russie.
La première attaque attribuée à ce groupe date de 2015, lorsque plusieurs institutions gouvernementales situées aux USA avaient été attaquées par une campagne de *spearphishing* visant à installer un ver nommé à l'époque Lombrix.

Les secteurs ciblés pour cette nouvelle campagne baptisée Banacry sont ceux des télécommunications, de l'aéronautique et de la défense notamment de pays situés en zone Europe et membres de l'OTAN.

Les techniques utilisées n'ont pas été formellement identifiées mais des connexions à des serveurs C&C ont été repérées par les experts de McTersky.
Les url et les adresses IP de ces C&C apparaissent ci dessous ainsi que les condensés (hash) des fichiers infectés.

Pour plus d'informations, contacter intel-lab@mctersky.com

Indicateurs de compromissions (IOC) :

C2

```
jsaxsd.jelas.lunaclouds[.]com
info.akademy.rhclouds[.]com
46.252.242.1
46.252.242.2
46.252.242.7
46.252.242.8
46.252.242.9
46.252.242.10
81.94.32.10
81.94.32.11
81.94.32.17
81.94.32.18
81.94.32.19
212.24.32.56
212.24.32.57
212.24.32.62
212.24.32.63
212.24.32.64
212.24.32.65
```

Hashes

```
53555938742c97ff01f9a7f8b6f15587
bb911912db1295abf8d7613852624b50
b6469dcaffd168b7d0afc414b89685b5
f15443b088f7dfaa289af9e192c9cfc8
bfe3e1817c0c87d23980d87a8c0abbad
```