Lazarus Group

Histoire

#1

- Groupe de Corée du Nord
- Fondé en 2009
- APT38 et HIDDEN COBRA
- State-sponsored hacking organization
- Bureau de liaison 414

Recrutement

#2

Attaques

#3

Opération Troy (2009)

amazon

The Washington Post

DarkSeoul (2013)

Plusieurs TV et banques

Total de 750M $

Leak d’information
3M d’informations sont divulguées.

Sony Pictures Hack (2014)

Vol de 100T de données, allant de films à scripts ou encore d'information privées sur les employés.

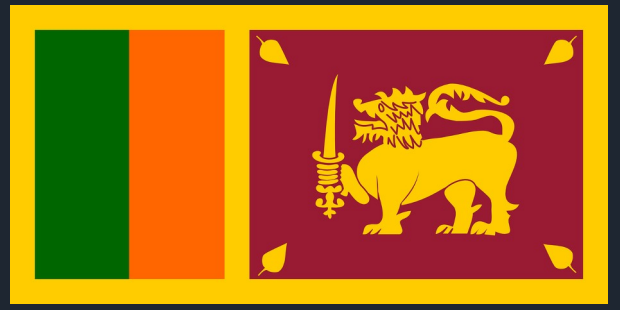
Sera accompagné d'une demande de suppression du film.

Protocole Server Message Block

Bangladesh Bank(2016)

850M $

81M $



WannaCry(2017)

300 000 PC dans 150 Pays visant les versions antérieurs a Windows 10

La faille EternalBlue exploitée par la NSA Servant a WannaCry d'être très efficace.

Attaque Crypto

Attaque avec du spread-phising et un malware pour récupérer les identifiants.

11M $ à des particuliers sud-coréen.

Conclusion

Merci!

Avez vous des questions?