



Forum: Trucs en vrac

Topic: Cyberattaques: des modes opératoires multiples

Subject: Re: Cyberattaques: des modes opératoires multiples

Publié par: Wullfk

Contribution le : 20/12/2016 21:35:52

Sans vouloir être désagréable, y a rien de nouveau dans cet article

Ceci dit ce n'est pas inutile de rappeler les façons dont on peut être infectée

J'ai regroupé les modes opératoires des Cyberattaques de l'article

- **mettre en place une campagne d'hameçonnage: le « phishing »** est l'une des méthodes les plus courantes, qui s'appuie sur l'action de l'utilisateur.
- **exploiter une faille «zéro-day»: les pirates cherchent à exploiter ces failles de sécurité** qui ne sont pas encore connues par les éditeurs de logiciel ou de système d'exploitation.
- **bénéficier d'une complicité interne:** «une personne va expliquer aux pirates comment le réseau est construit, quel type de logiciel de chiffrement est utilisé, quels certificats», etc... L'aide peut être volontaire ou contrainte: après un profilage, les pirates vont déterminer qui est susceptible d'accepter de participer à l'attaque ou d'être forcé à le faire.
- **transmettre une infection par un support externe:** les supports tels que les clés USB ou les disques durs externes peuvent être des vecteurs d'infection.

Pour ma part je trouve cette liste incomplète, il y aurait pu y avoir aussi l'utilisation du **P2P**, des **cracks**, des **keygens** qui sont aussi vecteurs d'infections