SAURON UN VIRUS POUR CONTRÔLER LES ÉTATS

Origine du Virus

- 1939 nouveau concept, le Core Warrior : deux programmes s'attaquent mutuellement jusqu'à ce que l'un deux échoue ou ne puisse plus se réparer.
- Le Core Warrior est une des bases des virus d'aujourd'hui. Sauron s'inspire de Remsec, cheval de Troie sous Windows. Grâce à ses capacités de dissimulation, il peut récupérer n'importe quelle donnée en toute discrétion, il est resté inaperçu pendant près de 5 ans sur des réseaux d'organisation gouvernementales.
- Actif depuis Octobre 2011, Sauron a été découvert seulement en septembre 2015.

Espionnage d'Etat ou Cyberguerre ?

Les failles informatiques peuvent mettre en danger un pays :

- Sur le plan économique, l'espionnage d'Etat permet de prendre de court les marchés, extorquer de l'argent, ou encore bloquer les banques…
- Sur le plan technologique, des recherches clés peuvent être dérobées et prendre un avantage stratégique.
- Au niveau politique, des élections peuvent être manipulées et favoriser un candidat jugé plus « intéressant » qu'un autre.

Dans quel but Sauron a-t-il été créé ?

- Dérober des informations sur des PC, et même sur les smartphones ou encore les tablettes non connectés à Internet via des clés USB infectées
- Obtenir des informations gouvernementales, économiques, militaires, scientifiques.

Quelles sont les cibles visées ?

- 36 infections depuis Octobre 2011 au travers de 7 organisations dans 4 pays : Belgique, Russie, Suède, Chine.
- 30 organisations infectées en Russie, Iran et Rwanda.
- Les organisations attaquées sont liées aux fonctions clés de l'Etat: gouvernement, centre de recherche scientifique, armée, télécommunication et finance.

Quelle est la structure du Virus?

- Programmes indépendants qui peuvent tourner isolément l'un de l'autre, les rendant difficile à identifier
- Capacité à changer de forme
- Malware modulaire
- Algorithme de cryptage fort (RC4, RC5…)
- Apparence d'un cheval de Troie (Remsec)

IUT Lyon 1 l'excellence technologique

Mathez Claire • Vauzelas Rémi
Henrionnet Antoine • Pertuiset Alex

Département Informatique
Veronique Deslandres