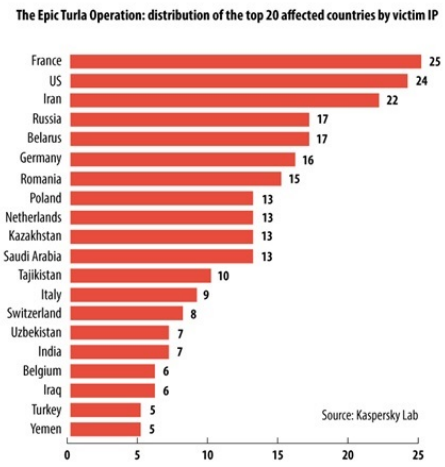
La France en première ligne de cyber-espionnage face à Epic Turla

La France en première ligne de cyber-espionnage face à Epic Turla

Selon le centre de recherche de Kasperky, notre pays est le plus touché par une attaque de cyber-espionnage connue sous le nom d'Epic Turla.
Selon Kaspersky Labs, la France est le pays le plus visé par une attaque de cyber-espionnage référencée sous le nom d'Epic Turla ou UroBuros, ou encore snake, pour d'autres éditeurs de logiciels de sécurité. La plupart des cibles sont des entités gouvernementales ou des ambassades sises en Europe ou au Moyen-Orient.

Une APT assez classique
Techniquement, l'attaque suit le schema classique d'une APT (Advanced Persistent Threat) avec hameçonnage par du spear phishing, l'utilisation d'exploits zero day, du social engineering et du waterholing par des sites infectés. Une fois dans la place, Epic se connecte au serveur de command and control et envoie les informations sur le système de l'utilisateur. Le système est ensuite compromis avec des outils spécifiques, des fichiers préconfigurés avec des commandes. L'attaque se déplace ensuite latéralement pour obtenir les bonnes accréditations et prendre la main pour soutirer les informations voulues. Selon le laboratoire, l'attaque est toujours en cours.
Tous les détails techniques ici :
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/



Les statistiques d'infection par Epic Turla

par Bertrand Garé, le 22 août 2014 14:42

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.linformaticien.com/actualites/id/33931/cyber-espionnage-la-france-en-premiere-ligne-face-a-epic-turla.aspx