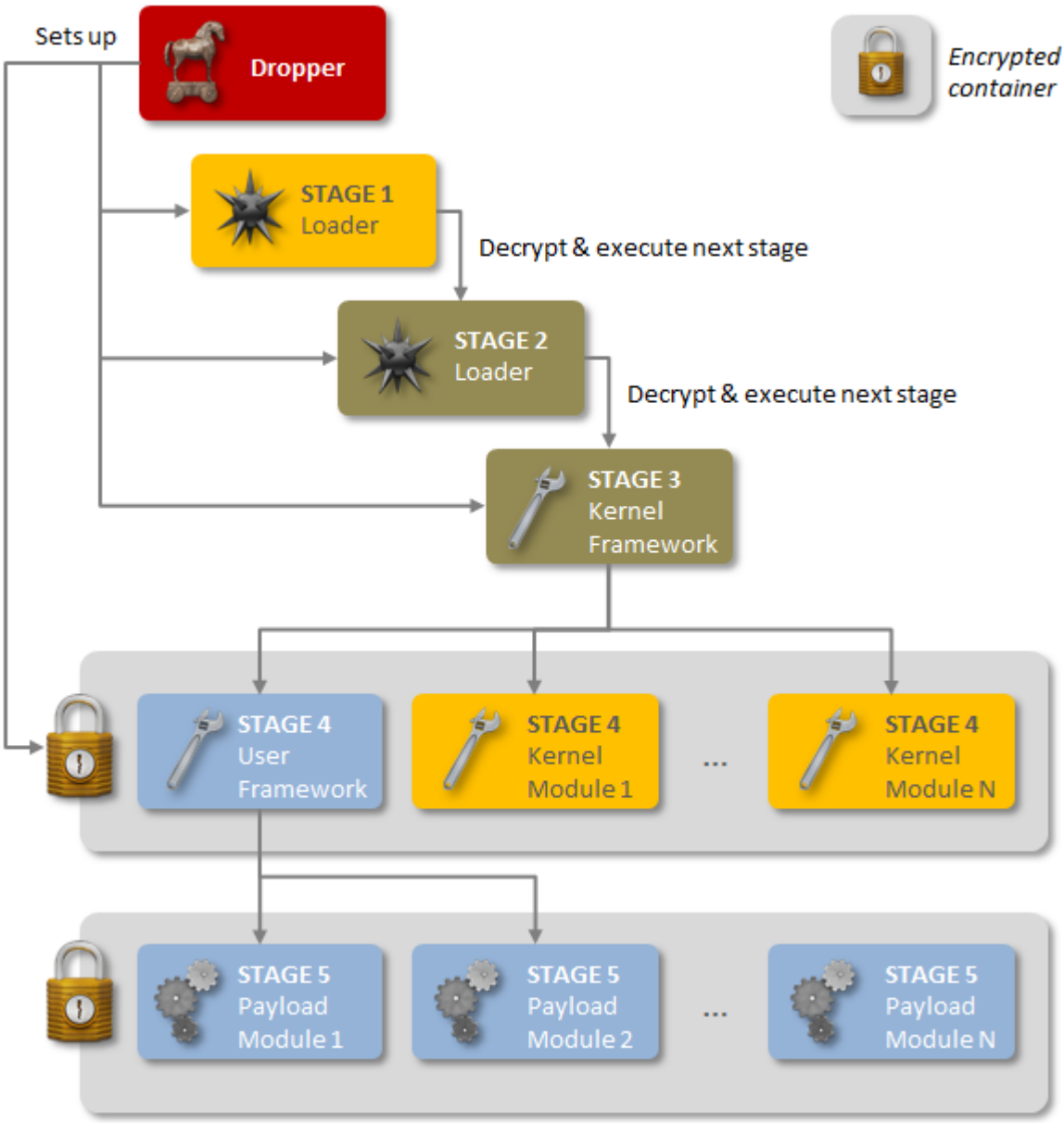
Regin : le malware d'un Etat à l'espionnite aigüe

La liste des malwares soupçonnés d'avoir été créés par des Etats s'allonge. On connaissait Stuxnet qui avait pour objectif le sabotage d'une centrifugeuse en Iran. Par la suite, d'autres chevaux de Troie chargés d'espionner des cibles ont été trouvés comme Duqu ou Flame. Aujourd'hui, les chercheurs de Symantec annoncent avoir découvert un autre malware entrant dans cette catégorie. **Surnommé Regin**, il présente des ressemblances avec ses prédécesseurs de par son élaboration qui a probablement nécessitait des mois ou des années de mise au point. Il comprend **une dizaine de modules** qui ont permis aux concepteurs d'adapter le malware aux cibles visées.

Dans sa découverte, Symantec explique dans un rapport que pour rester furtif le malware s'organise en **6 étapes** dont chacune est chiffrée sauf la première. Ces étapes entraîne une série d'actions de type domino où le module déchiffre son code et l'exécute avant de passer à l'étape suivante (cf schéma ci-dessous). Pour comprendre Regin, les chercheurs ont dû retracer l'ensemble du processus du malware. Il intègre **un catalogue d'attaques** qui va de la capture d'écran, la prise de contrôle de la souris, le vol de mots de passe, la surveillance du trafic ou la récupération de fichiers supprimés. Pour l'éditeur de sécurité, d'autres modules ont semble-t-il été adaptées pour des cibles particulières, comme la surveillance du trafic d'un serveur IIS de Microsoft ou le trafic des stations de base de téléphonie mobile.



PME-PMI, particuliers, opérateurs, Russie et Arabie Saoudite visés

Les entreprises visées par Regin sont variées, mais avec une prédilection (**48%) sur des PME-PMI ou des particuliers**. Vient ensuite le **backbone des opérateurs télécoms** (28%). L'hôtellerie, le transport aérien, l'énergie et la recherche ferment la marche. Sur les pays touchés par les attaques, la Russie et l'Arabie Saoudite représentent la majorité avec 52%. On trouve ensuite avec 9% chacun, l'Irlande et l'Inde. Les chercheurs de Symantec ont aussi tenté de donner une date de début des attaques avec deux échantillons, une V1 et une V2 de Regin. Le premier aurait été actif en 2008 avec un arrêt brutal et non expliqué en 2011. La V2 (en version 64 bits) a elle été utilisée à partir de 2013, mais a pu être active avant.

Il reste cependant beaucoup de zones d'ombre pour les chercheurs de Symantec sur Regin. Ils ont recensé une centaine de PC compromis, ce qui est relativement faible pour un malware avec ce

type de propriétés. De plus, le système de commandes et contrôle n'a pas été découvert. L'équipe n'a pas non plus d'idée sur le pays qui serait derrière Regin.

A lire aussi :

600 millions d'iPhone affectés par des backdoors ?
La NSA injecte des backdoors dans les matériels IT à l'export