STUXNET : une cyberattaque spectaculaire

Rose-Milca CENAT
M1 (AMSD), Université Paris Cité - UFR des Sciences Fondamentales et Biomédicales

Université Paris Cité

C'est quoi Stuxnet ?

Stuxnet est un logiciel malveillant (ou malware) qui a été conçu pour attaquer les systèmes de contrôle industriel SCADA utilisant les logiciels Siemens SIMATIC® WinCC ou Siemens STEP 7 pour la visualisation des processus et le contrôle du système. Il vérifie si l'ordinateur est connecté à des modèles spécifiques de contrôleurs logiques programmables (PLC) fabriqués par Siemens. Si aucun PLC n'est détecté, il ne fait rien.

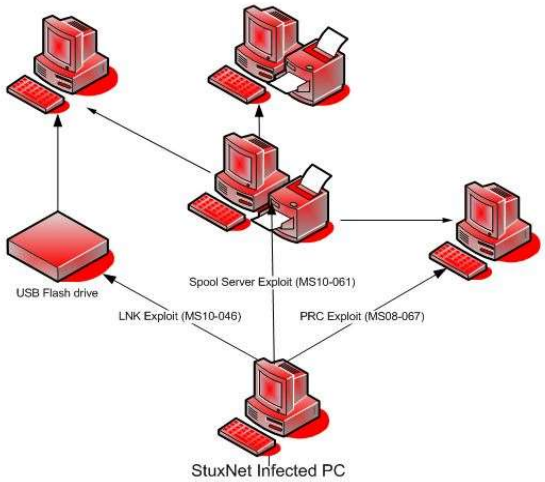

Figure 1: Stuxnet

Découverte de Stuxnet

En janvier 2010, en Iran, des inspecteurs de l'Agence internationale de l'énergie atomique ont fait une inspection, les centrifugeuses de l'usine iranienne d'enrichissement d'uranium explosaient sans raison apparente. En juin 2010, le malware a été découvert par une entreprise de sécurité informatique biélorusse appelée VirusBlokAda. Les experts en sécurité ont rapidement compris que Stuxnet était un malware très sophistiqué et inhabituel. Plus tard, vinrent des théories qui le relièrent au programme nucléaire Iranien.

Fonctionnement

Stuxnet est principalement propagé via des clés USB infectées, qui sont ensuite utilisées pour infecter les ordinateurs du réseau. Une fois qu'un ordinateur est infecté, le malware cherche à se propager à d'autres ordinateurs sur le même réseau. Il utilise les vulnérabilités dans les logiciels pour pénétrer dans le système SCADA. Il utilise également des méthodes d'ingénierie sociale pour tromper les utilisateurs et les amener à exécuter le malware. Une fois qu'il est installé sur l'ordinateur cible, Stuxnet injecte du code malveillant dans le logiciel de contrôle des centrifugeuses en faisant varier leur vitesse de rotation de manière subtile mais dangereuse. Ce qui peut provoquer des pannes et des dommages aux centrifugeuses. Il est conçu pour se cacher et pour ne pas être détecté par les logiciels de sécurité.

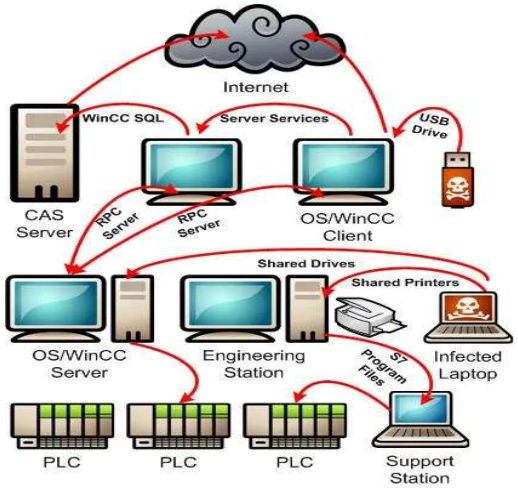

Figure 2: Stuxnet hitting Siemens PCS 7 objects.

Conséquences

Selon Symantec, il y avait environ 100 000 hôtes infectés par Stuxnet. Près de 58 % de ces hôtes infectés se trouvaient en Iran. Les dommages causés aux centrifugeuses iraniennes ont été estimés à plusieurs centaines de millions de dollars.

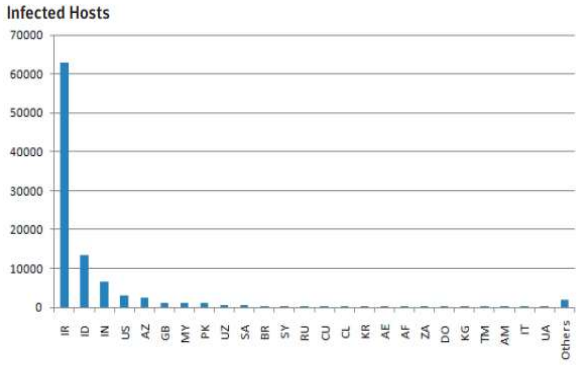

Figure 3: The number of unique infected hosts by country

Dispositions à prendre

Stuxnet a été l'une des plus grandes cyberattaques, et d'autres s'ensuivirent. Des mesures ont été prises, des recherches ont été faites, cependant, nous aurons toujours à faire face à des attaques de cyber. Il serait important de garder les bons principes et de rénover à chaque fois.

– Utiliser un réseau avec pare-feu afin de protéger votre réseau.
– Mettre en place des politiques strictes pour les périphériques.
– Utiliser des mots de passe complexes.
– Surveiller de façon optimale les systèmes.
– Mettre à jour régulièrement les systèmes d'exploitation et les logiciels.
– Installer un logiciel antivirus et le maintenir à jour.

Références

1 'Stuxnet' Worm Far More Sophisticated Than Previously Thought, 14 septembre 2010.
2 Stuxnet Report II: A Worm's Life, 2 mars 2011, ISSSource.
3 W32.Stuxnet Dossier, version 1.4 (February 2011), Nicolas Falliere, Liam O Murchu, and Eric Chie.