Internet : SystÃ¨mes industriels et APT filent-ils le parfait amour ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 15/2/2013 13:00:00

En 3 ans, la sÃ©curitÃ© est devenue lâ□□une des prÃ©occupations majeures lors de la mise en place de systÃ¨mes industriels. Nul doute que lâ□□Ã©moi gÃ©nÃ©ral provoquÃ© par le vers StuxNet en 2010 y soit pour quelque chose.

Et pour cause : alors que les attaques Â« classiques Â» de PC se terminent par des dÃ©gÃ¢ts immatÃ©riels, le public a ici pris conscience de la capacitÃ© destructrice bien rÃ©elle des vers et virus avancÃ©s. Comment ne pas imaginer le pire ? Dâ□□ailleurs, inutile dâ□□aller chercher lâ□□inspiration bien loin puisquâ□□Hollywood sâ□□en est dÃ©jÃ chargÃ© : avions tombant du ciel, fin de lâ□□approvisionnement en eau et Ã©nergie, effondrement des services publics et de lâ□□Ã©tatâ□¦

MÃªme si lâ□□exagÃ©ration y est de mise, ces scÃ©narios illustrent nÃ©anmoins lâ□□immense impact que pourrait avoir des cyber-attaques terroristes de grande ampleur, confirme **Ã□douard Viot**, Product Manager StormShield, groupe Arkoon

La mauvaise nouvelle ? Pour la plupart, les systÃ¨mes industriels ne prÃ©sentent pas de dÃ©fi particulier pour un pirate. En effet, nombre dâ□□entre eux utilisent des technologies standard qui les rendent assez semblables Ã des PC : systÃ¨mes dâ□□exploitations, antivirus, pare-feu, rÃ©seaux IP, connectiques USB, etc. Or, lâ□□histoire rÃ©cente a dÃ©montrÃ© la permÃ©abilitÃ© des PC aux attaques avancÃ©es. En effet, pour des hackers dâ□□un niveau correct, contourner les contre-mesures Â« classiques Â» mises en place sur ces machines sâ□□avÃ¨re Ãªtre un jeu dâ□□enfant. Pourquoi en serait-il diffÃ©rent sur les systÃ¨mes SCADA ? En lâ□□Ã©tat, il semble raisonnable de considÃ©rer que ces systÃ¨mes industriels prÃ©sentent le mÃªme niveau dâ□□insÃ©curitÃ© que des postes de travail traditionnels.

Compte tenu des enjeux engagÃ©s, on peut se demander pourquoi ces systÃ¨mes ne bÃ©nÃ©ficient pas de mesures de protection exceptionnelles. Le rapport de lâ□□ANSSI sur la protection des systÃ¨mes industriels pointe du doigt un mythe entretenu sur ces infrastructures : sÃ©curitÃ© et sÃ»retÃ© de fonctionnement y seraient antagonistes. De fait, beaucoup de systÃ¨mes industriels sont jugÃ©s tellement sensibles quâ□□on ne leur applique pas de correctif de

sÃ©curitÃ© : la peur de nuire Ã leur production, un risque court-terme bien tangible, est plus forte que la peur dâ□□attaques informatiques potentielles mais pour lâ□□instant peu observÃ©es.

Dans le meilleur des cas, le systÃ¨me sera dÃ©connectÃ© du rÃ©seau pour Ã©viter les attaques... une sÃ©curitÃ© trÃ¨s limitÃ©e, que le ver StuxNet a notamment mise Ã mal (on rappellera quâ□□il utilisait lâ□□USB comme vecteur de propagation).

Alors comment lutter contre ces menaces lorsque lâ□□on Ã un systÃ¨me industriel ?

Avant tout, comme recommandÃ© par lâ□□ANSSI dans son guide Â« MaÃ®triser la SSI pour les systÃ¨mes industriels Â», en prenant soin dâ□□adopter une dÃ©marche globale, avec une couche de sÃ©curitÃ© Ã tous les niveaux : intÃ©gration, test, requalification suite Ã des modifications, etc. On notera quâ□□il sâ□□agit lÃ dâ□□une bonne pratique de sÃ©curitÃ© qui peut (et doit) dâ□□ailleurs sâ□□Ã©tendre Ã tous les systÃ¨mes, industriels ou pas.

Reste cependant Ã se protÃ©ger de maniÃ¨re adaptÃ©e au contexte spÃ©cifique prÃ©sentÃ© par les SCADA. Typiquement, une approche antivirus par base virale est inadaptÃ©e :

-Les mises Ã jours quotidiennes sont un souci pour ces systÃ¨mes (souvent dÃ©connectÃ©s du rÃ©seau).

-Les bases de signature ont montrÃ© leur inefficacitÃ© face aux attaques Ã©voluÃ©es. Compte-tenu de lâ□□ampleur du risque encouru, faire de ces technologies la pierre angulaire de la sÃ©curitÃ© des SCADA est clairement inadaptÃ©.

Il convient plutÃ´t dâ□□utiliser des approches (vraiment) proactives, qui permettent de concilier les difficultÃ©s de mises Ã jour et le risque spÃ©cifique prÃ©sentÃ© par les SCADA. On considÃ©rera notamment les produits mettant en Å□uvre des analyses comportementales poussÃ©es. Malheureusement, la plupart des produits de sÃ©curitÃ©, antivirus en tÃªte, prÃ©tendent bÃ©nÃ©ficier de telles technologies, tout en restant obscurs sur le contenu rÃ©el de ces options. Alors comment choisir le bon produit ?

La rÃ©ponse est finalement assez simple : il suffit de choisir une attaque avancÃ©e aujourdâ□□hui bien connue, par exemple Conficker ou StuxNet, et de la confronter Ã une version suffisamment ancienne du logiciel de sÃ©curitÃ©. On simule ainsi Ã peu de frais une attaque inconnue. Nul doute quâ□□un Ã©diteur confiant dans sa technologie comportementale pourra fournir ce matÃ©riel de test... Sauf que curieusement, le nombre de fournisseurs acceptant de se prÃªter Ã ce genre dâ□□expÃ©rience lors de maquettes avant-vente est bien, bien faible. Un signe, sans aucun doute possible, que le chemin avant la sÃ©curisation effective des SCADA est encore bien long !