07/10/2010

www.enisa.europa.eu

L'analyse du logiciel malveillant «Stuxnet» par l'agence Européenne: un changement de paradigme dans les menaces et la protection des infrastructures critiques de l'information

L'analyse du logiciel malveillant «Stuxnet» par l'agence Européenne: un changement de paradigme dans les menaces et la protection des infrastructures critiques de l'information.

L'agence Européenne de «cyber-sécurité» ENISA (Agence Européenne chargée de la sécurité des réseaux et de l'information) a proposé dans ses commentaire et résumé initiaux une analyse de haut niveau des récentes attaques de «Stuxnet» notamment concernant leur importance et leurs implications techniques pour l'Europe. L'agence considère que «Stuxnet» constitue un réel changement de paradigme et annonce que des attaques de nature similaire pourraient se produire à nouveau. Elle soutient en outre que l'Europe devrait reconsidérer ses mesures de défense en matière de Protection des infrastructures critiques de l'information (CIIP). L'ENISA a également livré une analyse d'impact de haut niveau du logiciel malveillant Stuxnet dont l'objectif était d'offrir aux décideurs de l'Union européenne les informations nécessaires pour interpréter au mieux le logiciel, son impact potentiel, les facteurs d'atténuation et ce que signifient ces nouveaux types d'attaques en général pour l'Europe.

Dr. Udo Helmbrecht, Directeur Exécutif de l'ENISA a déclaré:
«*Stuxnet constitue véritablement un changement de paradigme parce qu'il représente une nouvelle classe et une nouvelle dimension de logiciel malveillant et ce, pas uniquement pour sa complexité et sa sophistication : en combinant par exemple quatre exploitations de vulnérabilités différentes de Windows, et en utilisant deux certificats volés, il peut attaquer les systèmes complexes des logiciels SCADA de Siemens. Les auteurs de ce programme malveillant ont dû consacrer des quantités considérables de temps et d'argent pour élaborer des outils d'attaques d'une aussi grande complexité. Le fait qu'ils aient activé un tel outil d'attaque peut donc s'interpréter comme la «première frappe» du genre, c'est-à-dire, l'une des premières attaques organisées et bien préparées contre les ressources industrielles majeures. Cela devrait avoir un effet considérable sur la façon dont nous devrons désormais protéger nos infrastructures critiques de l'information (CIIP) nationales. Depuis Stuxnet, les théories actuellement les plus répandues en matière de CIIP doivent être intégralement reconsidérées. Elles doivent être développées pour résister à ces nouvelles méthodes d'attaque sophistiquées d'un type nouveau. Maintenant que Stuxnet et ses principes intégrés sont devenus publics, nous risquons de voir davantage d'attaques de la sorte. Tous les acteurs de la sécurité se doivent donc de collaborer plus étroitement et développer des stratégies meilleures et mieux coordonnées*», conclut Dr. Helmbrecht.
Pour accéder à une analyse technique plus approfondie et en ligne, ainsi qu'aux recommandations de l'Agence, veuillez cliquer sur:
<http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis>.

Comment l'ENISA soutient les États Membres pour qu'ils se préparent mieux contre les attaques visant les infrastructures critiques de l'information

Les attaques à grande échelle visant les infrastructures critiques de l'information nécessitent une réaction concertée impliquant les acteurs clés issus aussi bien des secteurs public que privé. En effet, aucun État Membre, distributeur de matériel/logiciel informatique, CERT ou organisme d'application de la loi ne serait capable seul de limiter avec succès des attaques aussi sophistiquées que celles de Stuxnet. C'est pourquoi l'ENISA, en tant que corps d'experts de l'Union Européenne en matière de Sécurité des réseaux et de l'information (NIS), **soutient le plan d'action de CIIP de la Commission**

<http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm>. Cela implique une collaboration étroite avec les États Membres et les parties prenantes des secteurs public et privé en vue de sécuriser efficacement les infrastructures critiques de l'information en Europe.

Le programme de résistance et de CIIP de l'ENISA <http://www.enisa.europa.eu/act/res> aide les États Membres et le secteur privé à mettre en place de bonnes pratiques dans plusieurs domaines liés à la protection des infrastructures critiques de l'information et notamment : la lutte contre les botnets, le renforcement de la sécurité des réseaux interconnectés et le signalement des incidents les plus sérieux liés à la sécurité. En 2011, l'ENISA interviendra dans la mise en place de bonnes pratiques concernant la sécurisation des systèmes SCADA et analysera les dépendances des secteurs critiques des technologies de l'information et des communications.

«CYBER EUROPE 2010», le premier exercice paneuropéen de cyber-sécurité

En outre, l'ENISA, conjointement avec l'ensemble des États Membres de l'Union Européenne ainsi que trois pays de l'Association Européenne de Libre-échange (EFTA), s'apprête à coordonner le premier exercice paneuropéen de cyber-sécurité en matière de CIIP <http://www.enisa.europa.eu/media/news-items/2018cyber-europe-20102019-the-1st-pan-european-ciip-exercise-phase-one>, «CYBER EUROPE 2010». Cet exercice testera les plans, les politiques et les procédures des États Membres en vue de répondre à une crise ou des incidents potentiels touchant à la CIIP, similaires à 'Stuxnet'».

Le renforcement des «pompiers numériques»; les CERT

L'ENISA mène également une initiative concernant le renforcement des «pompiers numériques» nationaux/gouvernementaux, aussi appelés Equipes de réponse aux urgence informatiques <http://www.enisa.europa.eu/act/cert> , ou CERT, en venant en aide aux États Membres pour mettre en place, former et entraîner des équipes capables de répondre aux incidents. Ensemble, nous définissons une série de capacités fondamentales dont toutes les équipes doivent pouvoir faire preuve. Nous travaillons aussi sur le développement des capacités en matière, par exemple, de coopération transfrontalière, de signes précurseurs, et de coopération dans l'application de la loi.

L'ENISA soutient activement le principe d'une réaction coordonnée aux attaques de grande échelle, et elle jouera volontiers son rôle (dans l'hypothèse où elle serait sollicitée) de coordinateur et de facilitateur pour la mise en place de contre-mesures appropriées.

Pour plus d'informations: Plusieurs **agences de NIS des États Membres de l'Union** Européenne ont fait paraître des informations concernant Stuxnet dans leurs langues respectives. Veuillez vous reporter aux rapports par pays de l'ENISA<http://www.enisa.europa.eu/act/sr/country-reports> pour une vue d'ensemble des activités de sécurité de chaque État Membre. Sur ces sites Internet, vous pourrez trouver par exemple, davantage d'informations sur le logiciel malveillant lui-même, sa détection et ses limitations, publiées par (les acteurs externes) Siemens et Symantec.

Outils et procédures de suppression Siemens <http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view> Analyse en cours de Stuxnet par Symantec <http://www.symantec.com/business/theme.jsp?themeid=stuxnet&inid=us_ghp_banner1_stuxnet>

Le livre blanc de Stuxnet (PDF) <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> Le blog en cours de réponse à Stuxnet <http://www.symantec.com/connect/blogs/w32stuxnet-dossier>

Pour les interviews: Ulf Bergstrom, Porte-parole, ENISA, press@enisa.europa.eu, Mobile : + 30-6948-460-143.

Traduction. La version anglaise est la seule version officielle.