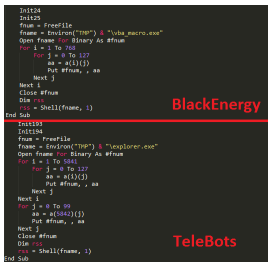
Découverte d’une activité de cybersabotage imitant les techniques de BlackEnergy

Découverte d’une activité de cybersabotage imitant les techniques de BlackEnergy

Les chercheurs ESET ont identifié un ensemble d'outils malveillants utilisés contre des personnes influentes venant du secteur financier ukrainien. Selon les experts ESET, ces attaques ont pour principal objectif le cybersabotage.

Le gang qu'ESET nomme TeleBots présente beaucoup de similitudes avec le groupe BlackEnergy qui a mené des attaques contre l'industrie énergétique en Ukraine en décembre 2015 et janvier 2016. ESET va jusqu'à dire que le groupe TeleBots n'est autre qu'une mutation du groupe BlackEnergy.



Comme pour les campagnes attribuées au groupe BlackEnergy, les cyberattaquants utilisent la méthode du spearphishing en envoyant par e-mails des documents Microsoft Excel contenant des macros malveillantes comme vecteur initial d'infection. Cependant, à la différence des attaques menées par le groupe BlackEnergy, les documents malveillants n'ont aucun lien avec les techniques d'ingénierie sociale, incitant les victimes potentielles à cliquer sur le bouton pour activer le contenu. Il semblerait que le choix reviendrait à la victime en décidant par elle-même de cliquer ou non sur le bouton.
Une fois que la victime clique sur le bouton "Activer le contenu", Excel exécute la macro malveillante. L'analyse d'ESET montre que le code de la macro diffusé dans les documents créés par TeleBots correspond au code de la macro utilisé par le groupe BlackEnergy en 2015.
Les cybercriminels démontrent une intention sérieuse de mener des attaques de cybersabotage. Pour être en mesure de les réaliser, les attaquants inventent constamment de nouveaux logiciels malveillants et de nouvelles techniques, comme l'utilisation de l'interface de programmation applicative (API) Bot Telegram au lieu d'un serveur C&C plus classique par exemple…

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article