# Sandworm : l'ombre de NotPetya et d'Industroyer a plané sur la France

*Mise à jour du 16 février 2020 à 16 h 18 : Centreon affirme que l'attaque n'a pas pu toucher les versions commerciales de son logiciel. L'éditeur dénonce une « modification sauvage » de la version* open source*, à travers un « module additionnel développé par un opérateur tiers ». La ligne de code sur laquelle vient agir ce module est absente des solutions Centreon depuis 2015, nous précise-t-on.*

Vous souvenez-vous des black-out qui avaient eu lieu fin 2015 et fin 2016 sur le réseau électrique en Ukraine ? C'est potentiellement là que mène le fil « Sandworm » tendu dans le dernier rapport du CERT-FR. Sujet : une campagne malveillante qui a touché, au moins entre 2017 et 2020, plusieurs entités françaises. Essentiellement des prestataires de services informatiques ; notamment d'hébergement web.

Cible de cette campagne : des serveurs exécutant Centreon, logiciel de supervision informatique signé de l'entreprise du même nom. On y a découvert deux charges utiles : un *webshell* PHP et une *backdoor*, respectivement dénommés P.A.S. et *Exaramel*.

L'ANSSI dit ne pas avoir connaissance du mécanisme qui a permis d'introduire P.A.S. sur les serveurs concernés. Tous avaient cependant la particularité d'exécuter une version de Centreon non mise à jour… et d'être exposés au réseau internet, à travers l'UI du logiciel, servie par défaut en HTTP sur Apache.
C'est cette interface que le *webshell* met à profit. On y accède *via* un formulaire dans lequel on spécifie un mot de passe qui sert à en déchiffrer le contenu.
Dans les grandes lignes, P.A.S. permet de :

- Réaliser des opérations sur les fichiers du serveur (listage, copie, déplacement, suppression, renommage, téléchargement/téléversement, modification y compris des permissions, etc.)
- Naviguer dans des bases SQL et en extraire des éléments
- Analyser le réseau et créer des *shells* supplémentaires
- Utiliser la force brute sur FTP, MySQL, MSSQL, POP3, PostgreSQL et SSH
- Exécuter des commandes ou évaluer des expressions PHP

La CISA, homologue américaine de l'ANSSI, avait mentionné, dans un rapport publié fin 2016, un *webshell* qui correspond à P.A.S. Il aurait été impliqué dans diverses cyberattaques ayant précédé l'élection présidentielle. En particulier celles qui ont mené à l'exfiltration d'e-mails du Parti démocrate.

## La piste Sandworm…

Qu'en est-il d'Exaramel ? ESET a donné ce nom à cet implant qu'il avait découvert en 2018. Il s'agit d'un outil d'administration à distance. Ses deux principales fonctions : copier des fichiers et exécuter des commandes *shell*. Son exécution se divise en deux phases :

- L'initialisation
  – Création d'un socket Unix pour empêcher d'éventuelles exécutions parallèles
  – Mise en place d'un *handler* qui stoppe l'exécution en présence de certains signaux (SIGINT, SIGTERM, SIGQUIT, SIGKILL)
  – Lecture de la configuration (stockée dans un fichier chiffré avec RC4)
  – Mise en œuvre d'un mécanisme de persistance s'il n'y en a pas déjà un en place. La technique varie en fonction des privilèges et du système de démarrage.
- L'exécution à proprement parler
  – Recherche d'un serveur de commande actif à partir d'une liste
  – Obtention de commandes et exécution
  – Obtention de l'intervalle de temps avant le prochain contact avec le serveur

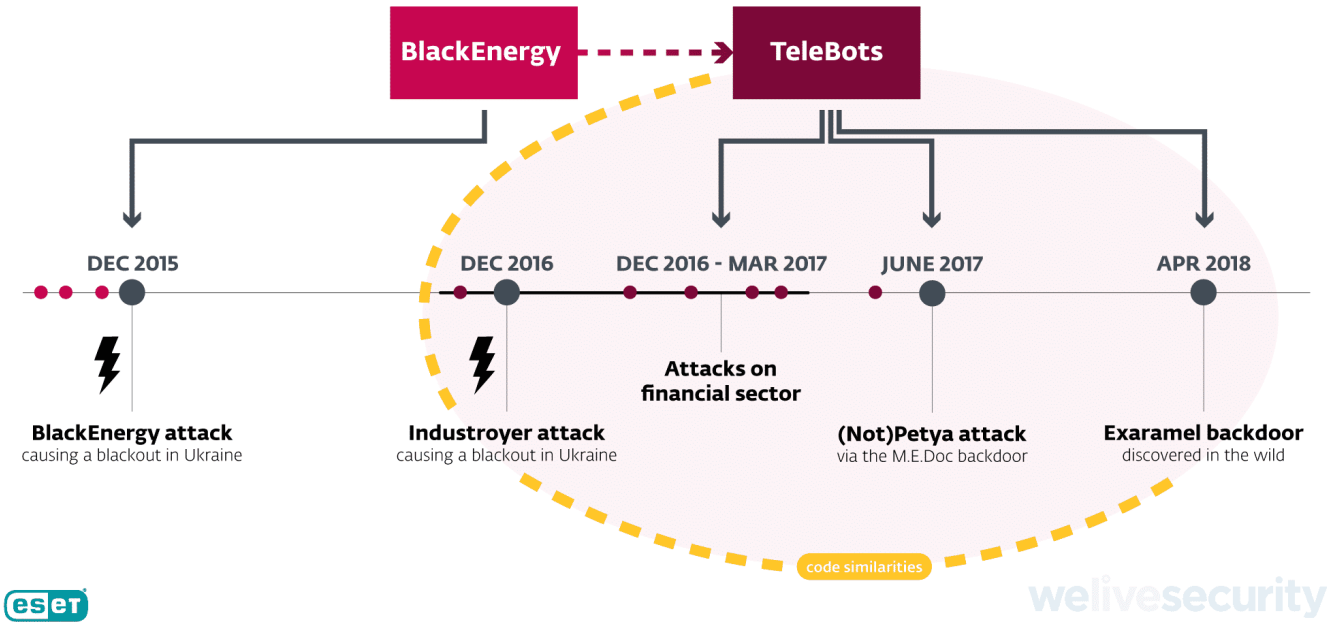
Cette campagne associant P.A.S. et Exaramel présente, affirme l'ANSSI, « de nombreuses similarités avec des campagnes antérieures du mode opératoire Sandworm ». De « mode opératoire », l'agence donne la définition suivante.

# … mène à Industroyer et à NotPetya

Sandworm est un alias de TeleBots, qu'ESET ne qualifie pas de « mode opératoire », mais tout bonnement de groupe cybercriminel. Il y perçoit l'évolution du groupe dit à l'origine du *trojan* BlackEnergy. Celui-ci avait ciblé des entreprises américaines et européennes en 2014. Mais il avait aussi été le bourreau des lignes électriques ukrainiennes lors du fameux *black-out* de fin 2015 (estimation : 250 000 foyers touchés).

TeleBots s'était d'abord distingué, en 2016, pour des attaques contre le secteur financier, là aussi en Ukraine. La même année, un autre black-out avait frappé le pays. On l'avait attribué à Industroyer, *malware* industriel codé précisément pour perturber les équipements déployés dans les stations de distribution (relais et coupe-circuits).

D'après ESET, Exaramel présente une certaine proximité vis-à-vis de la *backdoor* d'Industroyer. C'en serait en fait une version améliorée. L'éditeur tchèque fait aussi un lien avec le *ransomware* NotPetya, qui avait frappé en 2017. Sa propagation avait démarré depuis des entreprises ukrainiennes que TeleBots avait compromises, à travers le logiciel financier M.E.Doc, populaire sur place.




L'ANSSI propose diverses méthodes de détection de P.A.S. et d'Exaramel, sous la forme de règles Snort et YARA. Elle rappelle l'importance de garder à jour ses applications. Mais aussi de limiter l'exposition des outils de supervision sur le réseau Internet. Ou alors mettre en œuvre des mécanismes de sécurité non applicatifs. Par exemple, un certificat client TLS. Ou une authentification basique par le serveur web.

*Illustration principale © psdesign1 – Fotolia*