ODIN, UN RANSOMWARE DE TYPE LOCKY QUI EN VEUT A VOS DONNÉES

Édité le 04/10/2016

CAS CONCRET

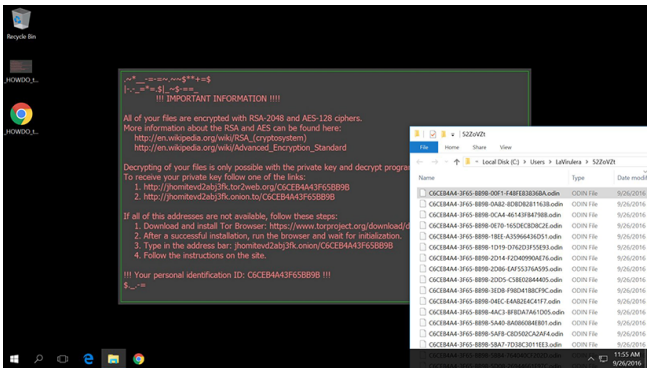
Dans l'après-midi du 03/10/2016, un salarié d'une PME rhônalpine reçoit un mail provenant d'une entreprise lui demandant de procéder au règlement d'une facture. Celui-ci contient une pièce jointe au format « *.xls* » nommée « *facture acompte 8720* ».

Une fois le document ouvert, de très nombreux fichiers sont immédiatement cryptés et modifiés pour apparaître en « *.odin* ». Très virulent, ce maliciel a également réussi à s'infiltrer sur le serveur et a pu impacter le système de sauvegarde.

DE QUOI PARLE-T'ON ?

ODIN serait apparu pour la première fois le **29 septembre 2016**. Il s'agit de la dernière déclinaison du ransomware ***LOCKY***. Il utilise un système de cryptographie identique aux versions précédentes (*Locky, Zepto, ...*) mais chiffre les fichiers en leur ajoutant désormais une extension en « ***.odin*** ».

La clé ayant été modifiée, le déchiffreur « ***Autolocky*** », qui permettait depuis quelques temps de décrypter les fichiers en « ***.locky*** » est inefficace.



A l'instar de ses prédécesseurs, ce nouveau ransomware change l'image de fonds d'écran et laisse apparaître une fenêtre contenant les instructions de paiement, lequel sera effectué via le réseau TOR.

Alors que pour Locky, les cybercriminels exigeaient la somme de ***360 euros*** (*soit environ un bitcoin*), la rançon désormais demandée s'élève à ***2000 euros*** (*toujours payable en bitcoins*).

COMMENT S'EN PRÉMUNIR ?

Bien que classique, cette nouvelle campagne de ransomware mise encore et toujours sur la méconnaissance des utilisateurs et leur manque de vigilance. Il est toutefois possible d'éviter de se faire piéger en appliquant les quelques mesures de bon sens suivantes :

En amont :

Sensibiliser régulièrement les salariés et ce quel que soit le niveau de responsabilité exercé (*Tout personnel connecté au réseau de l'entreprise peut recevoir un mail piégé pouvant infecter au mieux son ordinateur et au pire la totalité du système d'information*). **Règle d'or : « *Réfléchir avant de cliquer et non pas l'inverse* ».**

Installer et mettre régulièrement à jour des solutions de sécurité (*antivirus, antimalware, firewall, …*).

Effectuer des sauvegardes régulières et ***s'assurer régulièrement de leur viabilité*** (*notamment en effectuant des essais de restauration même partiels*).

Désactiver les macros exécutables automatiquement dans Microsoft ***Word*** et ***Excel***. Pour vous aider, consulter le ticket Microsoft suivant :
https://support.office.com/fr-be/article/Activer-ou-désactiver-les-macros-dans-les-documents-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12?ui=fr-FR&rs=fr-BE&ad=BE

Mettre en place une veille pour anticiper et s'adapter aux nouvelles menaces.
(***exemples*** : http://www.ssi.gouv.fr/, http://www.cert.ssi.gouv.fr/, http://www.malekal.com/ https://stopransomware.fr/)

En cas d'attaque :

Dans le cas où une pièce jointe suspecte aurait été ouverte, ***isoler IMMÉDIATEMENT la machine compromise*** en la déconnectant du réseau afin de limiter les dégâts.

Prendre en photo les écrans ou ***réaliser des copies d'écran*** (*mail frauduleux et pièces jointes*) et noter l'ensemble des opérations réalisées.

Sauvegarder les fichiers cryptés sur un support amovible externe pour un éventuel déchiffrement ultérieur.

Contacter rapidement le responsable informatique ou la société de maintenance.

Communiquer immédiatement sur l'attaque auprès de l'ensemble des utilisateurs.

Déposer rapidement plainte auprès du service de police ou de gendarmerie territorialement compétent.

Prévenir votre assurance pour éventuellement mettre en route la procédure d'indemnisation.