Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTERE DE L'INTERIEUR,

GROUPEMENT DE GENDARMERIE DU TARN
PÔLE SÉCURITÉ ECONOMIQUE TERRITORIALE
12 PLACE DE VERDUN 81000 ALBI

DATE : 06/ 02/ 2015
N° DOSSIER : 09/ 2015/ SET/ GGD81

FICHE D'ANALYSE PRÉVENTIVE ET SITUATIONNELLE

à l'attention de nos partenaires pour l'alerte de leurs réseaux.

OBJET : **Complément d'alerte sur les attaques de type RANSOMWARE par cryptage des fichiers.**

Le groupement de gendarmerie départementale du Tarn à mis en place une veille des menaces, ou atteintes informatiques, en vue d'alerter le réseau de ses partenaires, selon la thématique décelée.

Dés réception, vous il vous est demandé de diffuser cette alerte à votre propre réseau et à vos collaborateurs, afin qu'ils sécurisent, eux-aussi, leurs actions liées à l'informatique.

Comme d'habitude, vous pourrez également prendre attache avec le site prevention-partenariat-gendarmerie81.blogspot.fr afin d'entrer en contact ou de signaler des faits suspects, au N'Tech.

Action préalable : voir informations sur le site :

http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-003/CERTFR-2015-ALE-003.html

1- Le constat :

- **1 – Risque(s)**
  Atteinte à la disponibilité des fichiers après chiffrement.

- **2 - Systèmes affectés**
  Tous les systèmes d'exploitations Windows peuvent être victimes de ce rançongiciel.

– **3 – Résumé**

Depuis le début du mois de février 2015, le CERT-FR constate à nouveau une vague importante de compromissions de type rançongiciel, qui utilise cette fois principalement le programme malveillant appelé CTB-Locker.

Un rançongiciel est un code malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles en écriture à l'utilisateur dont la session est compromise. À travers une boîtede dialogue, la victime est ensuite invitée à verser de l'argent afin de récupérer la clé qui permettra de déchiffrer les documents ciblés (Bitcoin, Paypal, carte bleue). Il n'existe pas de moyens fiables pour récupérer la clé utilisée par le code malveillant.

Attention, le CERT-FR tient à souligner que le recouvrement des données après paiement n'est en aucun cas garanti. Au-delà du fait que cela encourage ce type d'attaque, le recours à un moyen de paiement par carte bleue expose la victime à des utilisations frauduleuses de celle-ci.

2- L'analyse :

– **Méthode d'attaque:**

Dans le cas présent, la propagation constatée repose sur une campagne d'hameçonnage. Les messages malveillants reçus prétendent être accompagné d'un fax en pièce jointe, qui en réalité est un programme malveillant.

– **Ce code s'installe localement sur le poste par différents moyens :**
* fichier avec l'extension SCR ;
* fichier avec l'extension SCR compressé dans un fichier au format zip (parfois il s'agit de compressions imbriquées) ;
* fichier avec l'extension CAB.

– Le fichier avec l'extension SCR est un fichier exécutable : ce dernier télécharge ensuite le code malveillant réalisant le chiffrement des fichiers.

3- Les conclusions et préconisations :

PRÉCONISATIONS :

– 1. **Toujours être vigilant** dans les pièces jointes du mail,

– 2. **Ne pas retransférer** mail suspect sur une autre messagerie,

– 3. **En cas d'infection**, isoler la machine du réseau. Voir si dépôt de plainte ou pas.

Faire intervenir un service compétent pour restaurer / réparer les dommages.

– 4. Selon la version du cryptage, essayer de décrypter le cryptage des fichiers compromis risque de prendre trop de temps à la société.

Il sera souhaitable de réinstaller une sauvegarde en cas de nécessité.

– 5. Ces Ransomware, cryptant essentiellement des fichiers Word / Excel et PDF, vous pouvez également mettre le répertoire de sauvegarde dans lesquels ils se trouvent en « lecture seule ». Aucune information ne nous est remontée sur la capacité de ces fichiers malveillants à modifier les droits d'écriture sur un répertoire.

RAPPEL : En cas d'attaque ou de suspicion, la scène de l'infraction devient alors une scène de crime.

Toute attaque doit faire l'objet d'un isolement de la machine suspecte du réseau internet.

Par ordre,
le Major Michel BOUCHER
RÉFÉRENT SÛRETÉ, AUDITEUR EN PRÉVENTION TECHNIQUE DE LA MALVEILLANCE ET VIDÉO-PROTECTION

L' ADJUDANT - CHEF PASCAL AZNAR
Enquêteur / Technicien en Nouvelles Technologies Numériques (N'TECH)

SOUS COUVERT DU LIEUTENANT-COLONEL DIDIER LAURENS
OFFICIER ADJOINT COMMANDEMENT ET OFFICIER PRÉVENTION PARTENARIAT
DU GROUPEMENT DE GENDARMERIE DÉPARTEMENTALE DU TARN

SIGNÉ