Campagne d'hameçonnage de type « rançongiciel »

Depuis le 25 novembre, le CERT-FR constate une très forte augmentation des infections de type rançongiciel.

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 boîte de 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.

Méthode d'attaque

La propagation actuellement constatée repose sur une campagne d'hameçonnage.
Les messages malveillants reçus ressemblent fortement à ceux d'une banque ou d'une compagnie d'assurance et contiennent un lien ou une pièce jointe délivrant un code malveillant.

Ce code s'installe localement sur le poste par différents moyens :

- exploitation d'une vulnérabilité sur Adobe Flash Reader ;
- fichier zip protégé par mot de passe ;
- exécutable masqué sous un autre format.

Afin de masquer l'exécutable sous un autre format dans le lecteur de messagerie électronique, le fichier malveillant est composé de la manière suivante :

- nom du fichier ;
- extension de document autorisé : PDF, etc. ;
- au moins 62 caractères ;
- extension .exe.

Sous cette forme, le client de messagerie présentera l'icône du format de document autorisé à la place de celle d'un exécutable.

Exemples de messages malveillants :

De: nicolettisales@meccanicanicoletti.it
Objet: Documentazione

Nous vous informons que vous avez un paiement en attente.
Nombre de paiement: 2438762495
Les raisons et les details peuvent etre trouves a l'adresse:
http :www.papercut-design.com/Details.zip/
RUnwKYtaG=XXXXX…..

Juste etre averti si ce ne effectuer le paiement, notre entreprise

sera obligee d'arreter la fourniture de produits.
Dans le cas de non-paiement, nous serons obliges de demander une indemnisation.
--
Sincerement
Lucianna
Tel./Fax.: 04-91-63-05-34.

Bonjour.
Nous vous informons que vous avez un paiement en attente.
Nombre de paiement: 47290341077
Les raisons et les details peuvent etre trouves a l'adresse:
http://www.mmelec.com/Details.zip?TtBjvFFZpw=XXXXX
Juste etre averti si ce ne effectuer le paiement, notre entreprise sera obligee d'arreter la fourniture de produits.
Dans le cas de non-paiement, nous serons obliges de demander une indemnisation.
2
Sincerement
Cara
Tel./Fax.: 04-91-84-52-35.

Mesures préventives

1. **Sensibiliser les utilisateurs**
   La seule mesure réelle de prévention est avant tout **d'informer et de sensibiliser les utilisateurs aux risques associés aux messages électroniques. Il convient en effet de ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes.** Les utilisateurs ne doivent pas ouvrir de messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse.[i]

2. **Surveiller tout signal faible sur une éventuelle propagation**
   Le code malveillant génère un fichier <mon document important>.encrypted. Une surveillance de l'apparition de ce type d'extension sur un ou plusieurs partages très exposés peut alerter très tôt la DSI d'une compromission.

3. **Installer les mises à jour de sécurité**
   Il convient de mettre à jour les postes utilisateur, notamment le système d'exploitation et les applications exposées sur Internet (lecteur PDF, lecteur messagerie, navigateur et greffons).

4. **Implémenter sur les postes les stratégies de restriction logicielle**
   Il convient de configurer sur les postes de travail les restrictions logicielles (SRP/AppLocker sous Windows) pour empêcher l'exécution de code à partir d'une liste noire de répertoires :
   <profil>\AppData\Local\Temp ;
   <profil>\AppData\Local\Temp* ;
   <profil>\AppData\Local\Temp** ;
   (cf la recommandation ANSSI sur ce sujet [ii])

5. **Mettre à jour les bases de signature anti-virus**
   Il convient de mettre à jour les logiciels anti-virus du parc informatique (postes utilisateurs, passerelle de messagerie, etc.). Le code malveillant étant polymorphe, les éditeurs anti-virus ont besoin de publier des signatures en constante évolution. Par ailleurs, il convient d'envoyer dès que possible un exemplaire du code malveillant à votre éditeur de logiciel antivirus.

6. **Réaliser des sauvegardes préventives**
   Il convient d'effectuer des sauvegardes régulières des systèmes et des données (postes de travail, serveurs) et de vérifier qu'elles se sont correctement déroulées. Les sauvegardes antérieures ne doivent pas être écrasées. Les sauvegardes doivent être réalisées en priorité sur les serveurs hébergeant des données critiques pour le fonctionnement de l'entité.

Mesures réactives

Si le code malveillant est découvert sur vos systèmes, il est préconisé d'adopter les principes suivants.

1. **Déconnecter immédiatement du réseau les machines identifiées comme compromises**

L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés**.**

2. **Alerter le RSSI, le service informatique au plus tôt**

3. **Protéger les partages de fichiers**

Le temps de revenir à une situation normale, il convient de positionner les permissions des dossiers partagés en LECTURE SEULE afin d'empêcher la destruction des fichiers sur les partages. Les personnels pourront continuer de travailler localement et mettre à jour ultérieurement le partage.

4. **Sauvegarder les fichiers importants**

Il convient de prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.

5. **Bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant**

L'objectif est de prévenir toute nouvelle compromission sur le même site. Une liste de noms de domaine connus du CERT-FR est fournie en pièce jointe, toutefois il est bien précisé qu'elle est incomplète.

6. **Rechercher et supprimer les messages malveillants similaires dans les boîtes de messagerie des utilisateurs**.

7. **Réinstaller les postes et réinitialiser les profils compromis**

Le CERT-FR recommande la réinstallation complète du poste et la restauration d'une sauvegarde réputée saine des données de l'utilisateur.

De plus, dans le cadre de l'utilisation de profils itinérants, il convient de supprimer la copie serveur du profil afin de prévenir la propagation des codes malveillants par ce biais.

---

[i] http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

[ii]http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-pour-la-mise-en-oeuvre-d-une-politique-de-restrictions.html

http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf