Alertes en provenance du CERTA CERT-Renater

Alerte aux rançongiciels (Message du RSSI CNRS du 3 février 2015)

Il nous a été signalé plusieurs cas de machines infectées par un rançongiciel comme **CBT Locker**. L'infection arrive via une pièce jointe dans un message.

Parmi les messages suspects reçus certains ont une adresse d'expéditeur appartenant au CNRS.

La plus grande vigilance est demandée vis-à-vis des messages reçus et des fichiers qui peuvent y être attachés. Il ne faut jamais ouvrir une pièce jointe ou cliquer sur un lien dans un message si on n'est pas sûr de l'expéditeur. Dans le doute, Il ne faut surtout pas hésiter à demander une confirmation à l'expéditeur.

Lien sur un document traitant des rançongiciels :

https://extra.core-cloud.net/collaborations/RSSI-CNRS/Documentation/Documents/Rancongiciel.docx

Exemple de message reçu

From: "Marie-pierre Bernet" humanoid@pdcequestre.fr

Subject: Email de confirmation: No. Z9F9271211C768QI

Date: 3 Feb 2015 14:34:22 GMT+1

To: login@xxx.fr

Cher Monsieur / Chère Madame,

Merci de votre commande!

Voici les détails de votre commande:

Numéro de commande: Z9F9271211C768QI

Date de la commande: 03.01.2015 13:32:59

Option de livraison: Prioritaire

Ce message confirme que vous avez acheté les articles suivants :

---

1 x OUTIL D'INSERTION PRO TYPE 110/KRONE: EUR 9.81

3 x ASUS F1A55 R2.0 AMD A55,FM1,DDR3,PCI-E,ATX: 81.40*3 = EUR 244.2

1 x AU OPTRONICS B154EW04 V.1 - LCD 15.4 WXGA, 1280×800, mate, 30 Pin:

EUR 97.96

3 x RAPTOR GAMING M3 MOUSE 400/2400 DPI - 120/140GR.: 44.72*3 = EUR 134.16

1 x HP LASERJET M1536DNF, MULTI. LASER N/B A4, USB,ETH.,FAX.: EUR 283.2

1 x HEDEN - SACOCHE PC PORTABLE 15/16 POUCES: EUR 14.78

1 x EPSON C13S050040 - TONER MAGENTA 6 000 P: EUR 153.75

Total HT: EUR 937.86

TVA: EUR 178.19

Montant total pour cette commande : EUR 1116.05

Vous trouverez ci-joint une facture pro forma de même que les conditions

de paiement et de livraison en annexe de ce courrier électronique.

Si on regarde en détail la facture on s’aperçoit que le taux de TVA n’est pas le bon 19% au lieu de 20%.

Bonnes pratiques lors de l'installation d'un logiciel (Bulletin CERTA du 8 novembre 2013)

Il ressort des incidents traités par le CERTA que l'installation de logiciels sans vérifications préalables est régulièrement à l'origine de la compromission de postes de travail ou de serveurs.

Certaines précautions doivent être prises afin de garantir l'innocuité des logiciels installés sur un poste en production :

- le téléchargement d'un logiciel ou de son code source doit être réalisé, si possible, sur le site original de l'éditeur. En effet, de nombreux sites de téléchargement ajoutent à l'installation des programmes à vocation publicitaire ou des fonctionnalités non désirées (exemple : barres d'outils), qui peuvent faire l'objet de vulnérabilités ;
- les fichiers doivent être soumis à un ou plusieurs antivirus à jour;
- l'intégrité des fichiers téléchargés (sources ou binaires) doit être vérifiée en s'assurant que les condensats (MD5, SHA1, etc.) sont identiques à ceux publiés sur le site de l'éditeur. De même, la présence d'une signature numérique valide et d'origine sure garantira que le contenu n'a pas été modifié.
- la procédure d'installation doit être suivie avec attention afin de clairement identifier les composants installés et les options activées.

Ces précautions sont d'autant plus importantes lorsqu'il s'agit d'installer des composants de sécurité (exemple : OpenSSH) ou des services sensibles (exemple : Serveur Web).

Lors du déploiement dans un environnement critique, des précautions supplémentaires peuvent s'avérer utiles comme, par exemple, l'analyse du code source original, afin de s'assurer que le

programme ne contient aucune fonction malveillante, ou la compilation d'un binaire directement depuis le code source.

Certaines attaques rencontrées redirigent l'utilisateur vers un site malveillant, visuellement identique au site de l'éditeur. Il convient donc de s'assurer que l'adresse Internet de téléchargement correspond bien à celle de l'éditeur.

Cryptolocker : une rançon pour déchiffrer vos données (Avis de sécurité CNRS du 7 octobre 2013)

Il nous a été signalé qu'une machine avait été infectée par « Cryptolocker ». Ce logiciel malfaisant chiffre les différents fichiers de la machine et présente une demande de rançon pour les déchiffrer.

!cryptolocker.png!

L'implémentation de la cryptographie y est suffisamment robuste pour qu'à ce jour, il n'existe aucune méthode connue permettant de retrouver la clé de chiffrement et donc de déchiffrer les fichiers. Seul le pirate qui possède la clé peut le faire.

Il ne faut jamais payer la rançon. Il y a pour cela plusieurs raisons :

- On ne peut faire confiance à un criminel. Rien ne garantit qu'il fournisse la clé de déchiffrement. Les expériences relatées sur Internet montrent que, généralement, ce n'est pas le cas.
- Le pirate pourrait utiliser les éléments fournis lors du paiement pour détourner des sommes encore plus élevées que celle demandée.
- Céder montre que l'on est vulnérable et que l'on est une cible susceptible de céder à d'autres chantages encore plus importants. C'est d'autant plus grave que le pirate, outre le fait de chiffrer les fichiers, a bien évidemment espionné le contenu de la machine et possède donc des éléments pour cibler ses prochaines tentatives de chantage.

La seule parade est donc d'avoir une sauvegarde récente des fichiers. On ne répètera jamais assez l'absolue nécessité d'avoir des sauvegardes. Si une information n'est pas stockées en plusieurs endroits, c'est comme-ci elle n'existait pas. Attention ! Une vraie sauvegarde permet de récupérer les fichiers tels qu'ils étaient dans un état antérieur. La redondance des informations comme avec les RAID ne protège que d'une défaillance matérielle. La simple synchronisation de répertoires à la Dropbox protège contre la perte du support, à la suite d'une panne ou d'un vol par exemple, mais ne permet pas de rétablir les fichiers tels qu'ils étaient avant l'incident.

Comment est-ce arrivé ? L'utilisateur a reçu un message en provenance de auto-confirmnnn@amazon.com où nnnn est un nombre, dont le sujet est : <pre> Your Amazon.com order #R-7-8007143-1656114 </pre>

et le contenu :

!phishing_cryptolocker.png!

Le fichier joint était une archive ZIP qui contenait un exécutable Windows portant le nom de « Order details .exe ». L'utilisateur ne se méfiant pas a cliqué un certain nombre de fois pour récupérer la pièce jointe, en extraire le fichier de l'archive et exécuter le programme. Evidemment l'exécutable contenait un code malfaisant.

Le premier piège résidait dans le fait que l'adresse qui s'affichait auto-confirm@amazon.com n'était pas celle de l'expéditeur qui était en réalité xxxx@yahoo.com où xxxx est une suite de lettres et de chiffres relativement complexe et ne ressemblant pas à ce que choisirait un vrai humain. On peut donc présumer que cette adresse a été créée uniquement pour effectuer cette attaque. Comment le piège fonctionne-t-il ? Il faut savoir qu'une adresse complète de courrier électronique a le format suivant :

addresse_affichée<nom@domaine>

Ce qui est affiché dans l'outil de de messagerie est ce qui est extérieur à <> et ce qui est utilisé pour les échanges est ce qui est intérieur à <>. Evidemment dans le cas présent l'adresse affichée était une adresse du domaine amazon.com.

Envoi d'exécutables malveillants par courriel (Bulletin d'actualité CERTA du 23 août 2013)

De nombreux incidents traités par le CERTA ont pour origine des courriels malveillants. Souvent, de simples exécutables malveillants sont envoyés en pièce jointe et traversent pourtant l'ensemble des dispositifs de sécurité mis en place.

Si la malveillance de ces courriels est généralement assez facilement identifiable par leur contenu négligé (fautes d'orthographe, français approximatif, etc.), certains attaquants sont plus subtils. Récemment, le CERTA a eu affaire à une vague de messages où le nom et le prénom de l'utilisateur étaient inscrits dans le nom d'un exécutable malveillant en pièce jointe, faisant croire à ce dernier qu'il était directement concerné par le sujet pour l'inciter à l'ouvrir.

Outre la sensibilisation des utilisateurs à ce genre d'attaques, quelques mesures permettent de s'en prémunir :

- le blocage des fichiers de type exécutable, y compris lorsqu'ils sont compressés, au niveau du serveur de messagerie est la solution la plus simple à mettre en œuvre. Cette recommandation peut aussi s'appliquer aux serveurs mandataires HTTP ;
- la mise en place des stratégies de restriction logicielles (SRP), ou d'AppLocker à partir de Windows Vista, sur les postes de travail protège non seulement de ce type d'attaques, mais aussi de nombreux logiciels malveillants circulant sur Internet.

Documentation

```
Guide de configuration des stratégies de restriction logicielles :
http://technet.microsoft.com/library/cc163080.aspx
Guide de configuration de AppLocker :
http://technet.microsoft.com/library/dd723678.aspx
```

Clés USB, encore et toujours un risque pour le SI (Bulletin d'actualité CERTA du 2 août 2013)

Comme mentionné par le passé, l'utilisation de clés USB non maitrisées présente un risque important pour la sécurité du SI.

Cette menace est aujourd'hui d'autant plus importante que depuis quelques semaines, certains constructeurs commercialisent des clés piégées prêtes à l'emploi, utilisant un mécanisme d'émulation d'un périphérique clavier plutôt que l'utilisation des fonctionnalités dîtes d'exécution automatique (Autorun).

Cette technique, bien que déjà connue dans le milieu de la recherche en sécurité, n'en reste pas moins efficace et permet d'exécuter une charge malveillante lors de la connexion de la clé à un poste Windows.

De plus, même si les modèles actuels semblent limités au système de Microsoft, des clés utilisant des principes similaires pourraient voir le jour sur d'autres systèmes.

D'un point de vue extérieur, rien ne permet aujourd'hui de différencier ce type de clé piégée d'une clé saine. Il est cependant possible d'observer les activités malveillantes car elle fait apparaitre une invite de commandes lors de son insertion.

Le CERTA recommande, une nouvelle fois, de prendre garde à ce type de périphériques aujourd'hui largement accessibles. Il est notamment nécessaire de sensibiliser les utilisateurs à ce type d'attaque afin qu'ils puissent prévenir rapidement la chaîne SSI en cas de comportements suspects.
Documentation

```
Bulletin d'actualité CERTA-2013-ACT-029, périphériques USB promotionnels et
cadeaux électroniques :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-029/index.html
```

Protections dans les applications Adobe reader et Adobe Acrobat (Avis CERTA du 18 février 2013)

L’ANSSI a publié une alerte sur une faille activement exploitée des produits Adobe Reader et Adobe Acrobat. L’ANSSI recommande d’utiliser la version XI (11) de ces produits qui offrent des fonctionnalités supplémentaires de sécurité (sandbox) permettant de contrer nombre d’attaques. Il faut noter que cette version XI n’est pas disponible sur tous les systèmes. Pour ces systèmes (Vista, Linux) où il n’est pas possible d’installer la version XI, il est vivement conseillé d’utiliser la dernière version disponible (X pour Vista, 9 pour Linux) qui est plus sécurisée que les précédentes. Dans tous les cas il faut appliquer les derniers correctifs de sécurité. Le CERTA recommande aussi d’activer la « Vue protégée », cette fonctionnalité n’est disponible que pour la version XI :

(Edition à Préférences à Protection (renforcée) à cocher « Activer le mode protégée au démarrage » et sous « Vue protégée » « Tous les fichiers ».

Pour toutes les versions il est aussi recommandé d’activer la « Protection renforcée » ce qui en principe est la valeur par défaut à l’installation :

Edition à Préférences à Protection (renforcée) à cocher « Activer la protection renforcée ».

L’ANSSI recommande aussi de désactiver JavaScript :

Edition à Préférences à JavaScript à Ne pas cocher la case « Activer Acrobat JavaScript ».

L’ANSSI recommande aussi de désactiver (désinstaller) les logiciels Adobe Reader et Acrobat. Cette mesure, certes efficace, ne nous semble pas réaliste et nous préférons insister sur la vigilance

nécessaires vis-à-vis de fichiers PDF téléchargés et le durcissement des configurations évoqué précédemment.

Un code malveillant utilise GoogleDocs (Alerte CERTA du 21 décembre 2012)

Les cas d'utilisation malveillante des réseaux sociaux ou de l'informatique dans le nuage, voire de webmails, se multiplient.

Cette année le CERTA a également été amené à traiter plusieurs incidents en relation avec ces services. Symantec a récemment publié un article à propos d'un code malveillant dont les connexions aux serveurs de commande et contrôle passaient par Google Docs. Un tel détournement a été rendu possible par une fonctionnalité de visualisation de fichier, à laquelle on peut soumettre une URL, sans vérification de sa malveillance. Ce phénomène rend difficile la détection des flux illégitimes :

- les serveurs destinataires ne sont, par essence, pas malveillants ;
- les flux entre le poste infecté et le serveur sont généralement chiffrés.

Ce comportement confirme également que les botnets évoluent vers des alternatives plus discrètes qu'IRC, historiquement utilisé comme protocole de communication, et donc plus difficile à bloquer.

Le CERTA recommande donc de faire preuve de vigilance, voire de réserve, à l'égard de l'utilisation des réseaux sociaux, des services de stockage dans le nuage ou de messagerie en ligne, quelle que soit la réputation de l'hébergeur.

Il est également préconisé de surveiller de tels flux à des heures qui ne correspondent pas une activité classique de bureau. Documentation

Symantec - Malware targeting Windows 8 Uses Google Docs

```
www.symantec.com/connect/blogs/malware-targeting-windows-8-uses-google-docs
```

Bulletin d'actualité CERTA-2009-ACT-045 :

```
http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-045/
```

Vigilance vis à vis des rançongiciels ou ransomwares (annonce CERT-RENATER du 22 août 2012)

De : rssi-request@ml.recherche.gouv.fr [mailto:rssi-request@ml.recherche.gouv.fr] De la part de Dominique Launay Envoyé : mercredi 22 août 2012 16:14 À : rssi@ml.recherche.gouv.fr Objet : [rssi] Vigilance vis à vis des rançongiciels ou ransomwares

Bonjour à toutes et à tous,

Nous attirons votre attention sur l’augmentation de l’activité d'un type de malware appelé « ransomware » ou « rançongiciel ». Il s’agit de malware infectant l’ordinateur cible par différents biais, notamment des pages web piégés (streaming ou autre).

Le malware bloque alors tout accès à l’ordinateur (chiffrement de vos données par exemple) et, se

faisant passer souvent pour un logiciel des autorités, demande le paiement d'une somme d'argent en échange du déblocage de la machine.

Cette somme est vue par l'utilisateur comme une amende car il croit avoir affaire aux autorités et, de plus, est souvent honteux du type de contenu qui l'a amené à cette situation (téléchargement illégal entre autre). Les sommes demandées vont parfois jusqu'à 500€.

Le paiement de cette somme passe généralement par des systèmes type ukash (http://www.ukash.com/fr/fr/home.aspx) ou paysafecard (http://www.paysafecard.com/fr/fr-paysafecard/) et on perd alors toute trace des commanditaires.

Le CERT polonais propose une page afin d'aider les personnes bloquées par ce type de logiciels : http://www.cert.pl/news/5707/langswitch_lang/en

Nous avons peu de cas pour le moment sur RENATER mais suffisamment pour se dire que la rentrée risque de compliquer les choses.

La sensibilisation des usagers est importante et un antivirus à jour est très efficace contre ces malware. Il est essentiel que les usagers ne paient pas.

Il ne faut pas hésiter à porter plainte pour escroquerie si un paiement a été effectué.

Quelques références sur le sujet : - Abuse.ch : https://www.abuse.ch/?p=3718 - ANSSI : http://www.ssi.gouv.fr/fr/menu/actualites/attention-arnaque-en-ligne-portant-le-logo-de-l-anssi.html - à propos du malware citadelle : http://www.ic3.gov/media/2012/120809.aspx - le virus « gendarmerie » : http://blog.crimenumerique.fr/2011/12/17/le-virus-gendarmerie-bilan-de-la-semaine/ - FBI (ransomware reveton): http://www.fbi.gov/news/stories/2012/august/new-internet-scam - Article de l'ANSSI sur le site sécurité informatique : http://www.securite-informatique.gouv.fr/gp_article781.html

Si des cas apparaissent dans votre établissement, n'hésitez pas à le signaler au CERT RENATER : certsvp@renater.fr

– Dominique Launay RENATER