Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 13 décembre 2013
N° CERTA-2013-ACT-050

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-050

1 - Codes malveillants de type RAT

Dans la plupart des scénarios d'attaques informatique, l'attaquant cherche en premier lieu à prendre le contrôle d'un poste utilisateur du réseau. Pour cela, il utilise par exemple l'exploitation d'une vulnérabilité en s'appuyant sur une pièce jointe piégée, attachée à un courriel en apparence légitime. Une fois cette attaque réussie, il va chercher à maintenir un accès à distance pour poursuivre son opération au sein du réseau compromis.

Pour arriver à ses fins, il est courant que l'attaquant utilise un logiciel malveillant de type RAT (Remote Administration Tool). Lors de son exécution sur la machine cible, le RAT effectue une connexion réseau vers un serveur de Commande et de Contrôle (dit serveur C&C), possédé par l'attaquant. C'est à travers cette porte dérobée que l'attaquant est en mesure de contrôler intégralement la machine infectée, et ainsi de l'utiliser afin d'exfiltrer des informations potentiellement sensibles. En effet, dans le cadre d'une intrusion ciblée, l'intérêt principal de l'utilisation d'un RAT est de fournir à l'attaquant un point d'entrée, qui lui permettra de rebondir sur d'autres machines de l'infrastructure, généralement plus critiques.

Les RAT fournissent en général de nombreuses fonctionnalités d'administration à distance permettant de :

- télécharger et exfiltrer des fichiers ;
- installer ou supprimer des applications ;
- modifier la base de registre ;
- terminer des processus ou des connexions réseau ;
- effectuer des captures d'écran ;
- effectuer des captures audio et vidéo (microphone / webcam) ;
- installer un enregistreur de frappes clavier (keylogger).

Par ailleurs, ces outils sont souvent utilisés pour la mise en place d'infrastructures illégitimes telles que des réseaux de machines zombies, offrant des ressources d'hébergement ou de calculs illicites et servant également de support à des attaques de grande ampleur, notamment de type déni de service distribué (DDoS).

Dans le cadre d'attaques non ciblées, il est fréquent de rencontrer des codes malveillants conçus à partir de RAT librement accessibles sur Internet. En revanche, dans le cadre d'attaques ciblées, les attaquants disposant de compétences techniques avancées peuvent être amenés à développer leur propre RAT, et ainsi disposer d'un outil performant et beaucoup plus difficilement détectable par les solutions de sécurité informatique.

Comme pour tout code malveillant, il est important de prendre des précautions pour limiter les risques d'infection et de mettre en oeuvre les moyens de détection adéquats. La détection de codes malveillants de type RAT peut assez souvent être réalisée par un antivirus, par l'analyse des journaux des serveurs mandataires (proxy) ou par des systèmes de détection d'intrusion réseau (NIDS).

Le CERTA recommande notamment :

- l'utilisation de systèmes d'exploitation et de logiciels maintenus ainsi que leur mise à jour régulière ;
- l'utilisation de logiciels antivirus régulièrement mis à jour (moteur de détection et bases de signatures) afin d'identifier la présence de RAT sur les postes ;

– la mise en oeuvre de la journalisation notamment sur des équipements tels que serveurs mandataires, serveurs DNS, parefeux ainsi que l'exploitation régulière des journaux ;
– l'utilisation de systèmes de détection d'intrusion réseau (NIDS) sur des points névralgiques des systèmes d'information (interconnexion du système d'information avec l'Internet, passerelles entre plusieurs systèmes d'information ...) qui peuvent avantageusement compléter l'exploitation régulière des journaux.

Documentation

– Recommandations de sécurité pour la mise en oeuvre d'un système de journalisation :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html
– Guide d'hygiène informatique :
http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

2 - Risques liés à l'informatique en nuage

L'informatique en nuage (cloud computing) permet d'externaliser des services informatiques chez des prestataires fournissant la plupart du temps des ressources mutualisées. Dès lors, les données de l'utilisateur qui étaient traditionnellement localisées sur le poste de l'utilisateur, sur son terminal ou sur des serveurs locaux, sont déplacées sur des serveurs distants gérés par un prestataire.

Bien que l'accès aux données soit simplifié (une simple connexion Internet suffit), cet avantage peut aussi être un inconvénient au niveau de la gestion des données sensibles. En effet, la publication d'éléments sensibles, volontaire ou non, ou encore les récupérations de données privées en exploitant des vulnérabilités au niveau des applications reposant sur l'informatique en nuage montrent qu'il est nécessaire d'observer la plus grande vigilance.

De plus, les architectures de type informatique en nuage ne permettent pas systématiquement à l'utilisateur de connaître l'emplacement physique de ses données. Il peut donc s'avérer difficile de s'assurer que la réglementation du pays hébergeant les données de l'utilisateur soit compatible avec la réglementation du pays d'origine en matière de protection des données personnelles.

Le CERTA recommande donc de ne pas avoir recours aux services d'informatique en nuage, dans la mesure du possible, pour le stockage des données sensibles. Cependant si un stockage distant est indispensable, l'utilisation d'un processus de chiffrement robuste avant l'envoi des données peut permettre de limiter les risques liés aux atteintes à la confidentialité des données. Pour plus de détails, le guide d'externalisation de l'ANSSI traite en profondeur les risques liés à une migration des données vers des serveurs distants, tout en facilitant la détermination des objectifs de sécurité pour orienter l'entreprise dans le choix d'un prestataire adapté.

Documentation

– Recommandations de la CNIL :
http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_
– Guide d'externalisation de l'ANSSI :
http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html
– Tutoriel concernant la suppression de données sensibles dans le gestionnaire de version GitHub :
https://help.github.com/articles/remove-sensitive-data
– Publications involontaires d'éléments sensibles :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-006/
– Référentiel général de sécurité :
http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

3 - Les surprises ne sont pas toujours bonnes

Les périodes de fêtes de fin d'année sont propices aux tentatives de compromission des systèmes d'information par le biais de cartes de voeux numériques. Les versions virtuelles de la carte traditionnelle, si elles peuvent être animées, musicales ou interactives, ne sont pas pour autant exemptes du risque de véhiculer des codes malveillants.

La trève des confiseurs ne s'appliquant pas à la délinquance informatique, il convient de redoubler de vigilance en appliquant les bonnes pratiques en matière de sécurité des systèmes d'information (cf documentation).

Au-delà des bonnes pratiques, la période de fêtes de fin d'année peut aussi être mise à profit pour étendre cette vigilance aux efforts de maintien en condition de sécurité des systèmes d'information (application régulière des correctifs de sécurité, identification des systèmes ou versions de logiciels obsolètes dans les inventaires de parcs, mise à jour des cartographies des systèmes d'information...) afin d'aborder sereinement la nouvelle année qui s'annonce.

Documentation

- Guide d'hygiène informatique de l'ANSSI :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Mesures de prévention relatives à la messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

4 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié onze bulletins de sécurité. Les cinq bulletins suivants sont considérés comme critiques :

- MS13-096 qui concerne un composant graphique de Microsoft, cette mise à jour corrige une vulnérabilité ;
- MS13-097 qui concerne Internet Explorer, cette mise à jour corrige sept vulnérabilités ;
- MS13-098 qui concerne Windows, cette mise à jour corrige une vulnérabilité ;
- MS13-099 qui concerne Microsoft Scripting, cette mise à jour corrige une vulnérabilité ;
- MS13-105 qui concerne Exchange Server, cette mise à jour corrige trois vulnérabilités.

Les vulnérabilités corrigées dans les correctifs MS13-096 à MS13-099 ansi que MS13-105 pourraient, pour les plus dangereuses, permettre l'exécution de code à distance.

Le correctif MS13-096 corrige la vulnérabilité activement exploitée et évoquée dans l'alerte CERTA-2013-ALE-007. Cette mise à jour met donc fin à l'alerte de sécurité.

Les six bulletins suivants sont considérés comme importants :

- MS13-100 qui concerne SharePoint Server, cette mise à jour corrige plusieurs vulnérabilités ;
- MS13-101 qui concerne les pilotes en mode noyau de Windows, cette mise à jour corrige cinq vulnérabilités ;
- MS13-102 qui concerne le client LRPC de Windows, cette mise à jour corrige une vulnérabilité ;
- MS13-103 qui concerne ASP.NET SignalR, cette mise à jour corrige une vulnérabilité ;
- MS13-104 qui concerne Microsoft Office, cette mise à jour corrige une vulnérabilité qui pourrait permettre une divulgation d'information ;
- MS13-106 qui concerne un composant partagé de Microsoft Office, cette mise à jour corrige une vulnérabilité.

Les vulnérabilités corrigées dans les correctifs MS13-100 à MS13-103 pourraient, pour les plus dangereuses, permettre l'exéction de code à distance.

Le correctif MS13-106 permet de forcer le chargement à une adresse dynamique de la bibliothèque HXDS.DLL (voir l'article 3 du bulletin d'actualité CERTA-2013-ACT-042), ce qui met fin à une méthode de contournement de la protection ASLR fréquemment utilisée par des codes malveillants.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de décembre 2013 :
  https://technet.microsoft.com/fr-fr/security/bulletin/ms13-dec
- Bulletin d'alerte portant sur une vulnérabilité dans un composant graphique de Microsoft
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-007/
- Bulletin d'actualité CERTA-2013-ACT-042
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-042/

– Avis du CERTA portant sur les bulletins de sécurité de Microsoft
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-662/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-663/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-664/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-665/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-666/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-667/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-668/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-669/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-670/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-671/
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-672/

5 - Rappel des avis émis

Dans la période du 06 au 12 décembre 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-656 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
– CERTA-2013-AVI-657 : Multiples vulnérabilités dans VMware ESX
– CERTA-2013-AVI-658 : Multiples vulnérabilités dans Samba
– CERTA-2013-AVI-659 : Vulnérabilité dans Siemens COMOS
– CERTA-2013-AVI-660 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2013-AVI-661 : Multiples vulnérabilités dans Adobe Shockwave Player
– CERTA-2013-AVI-662 : Vulnérabilité dans un composant graphique de Microsoft
– CERTA-2013-AVI-663 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2013-AVI-664 : Vulnérabilité dans Microsoft Windows
– CERTA-2013-AVI-665 : Vulnérabilité dans Microsoft Bibliothèque d'objets de l'exécutable de Microsoft Scripting
– CERTA-2013-AVI-666 : Multiples vulnérabilités dans Microsoft SharePoint
– CERTA-2013-AVI-667 : Multiples vulnérabilités dans les pilotes en mode noyau de Microsoft Windows
– CERTA-2013-AVI-668 : Vulnérabilité dans le client LRPC de Microsoft
– CERTA-2013-AVI-669 : Vulnérabilité dans Microsoft ASP.NET SignalR
– CERTA-2013-AVI-670 : Vulnérabilité dans Microsoft Office
– CERTA-2013-AVI-671 : Multiples vulnérabilités dans Microsoft Exchange Server
– CERTA-2013-AVI-672 : Vulnérabilité dans un composant partagé de Microsoft Office
– CERTA-2013-AVI-673 : Vulnérabilité dans Xen
– CERTA-2013-AVI-674 : Multiples vulnérabilités dans les produits Juniper

Durant la même période, les publications suivantes ont été mises à jour :
– CERTA-2013-ALE-007-001 : Vulnérabilité dans un composant graphique de Microsoft (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur.)

Gestion détaillée du document

13 décembre 2013 version initiale.