Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 26 janvier 2015
N° CERTFR-2015-ACT-004

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-004

1 - Vague de rançongiciels

Le CERT-FR est informé d'une recrudescence de messages électroniques malveillants incitant l'utilisateur à installer un rançongiciel sur son poste. Cet article s'inscrit dans la continuité de notre article précédent sur ce sujet (Bulletin d'actualité CERTFR-2014-ACT-048).

Un rançongiciel (ou ransomware) est un programme qui rend inaccessibles les fichiers de l'utilisateur, en général les documents bureautiques présents sur le profil de l'utilisateur (« Mes documents », « Mes Images », « Mes vidéos ») mais aussi (et surtout) dans tous les partages réseau ouverts en écriture à l'utilisateur compromis. Alors que les fichiers sont chiffrés par le rançongiciel, les fichiers originaux sont eux supprimés. A l'issue, un message de chantage est placé sur le bureau de l'utilisateur afin d'exiger le paiement d'une somme d'argent ou de bitcoins en échange de la clé de déchiffrement.

Les messages d'hameçonnage connus utilisent des techniques d'ingénierie sociale classiques indiquant par exemple « Votre fichier scanné est dans ce mail » pour inciter la victime à ouvrir l'archive en pièce jointe et à exécuter le maliciel.

La technique observée dans cette campagne est un message copiant la réception d'un fax dont la pièce jointe est une archive ZIP. Celle-ci contient le maliciel connu sous le nom de *CTB-Locker*. Ce rançongiciel figure parmi les plus avancés notamment au niveau de son cryptosystème et de ses communications à travers le réseau Tor, dont il embarque la librairie.

Recommandations

Le CERT-FR recommande les actions de prévention suivantes :

- la sensibilisation des utilisateurs : la plupart de ces messages sont non sollicités, d'un émetteur inconnu et contiennent des fautes d'orthographe ;
- l'utilisation des restrictions logicielles notamment pour interdire l'exécution de code depuis les répertoires temporaires ;
- la sauvegarde régulière des fichiers des utilisateurs sur des supports hors ligne ;
- la mise à jour des bases de signatures d'anti-virus et de passerelles de messagerie ;
- la protection appropriée des partages de fichiers, notamment en positionnant les permissions en lecture seule lorsque c'est possible ;
- l'application des correctifs de sécurité (système d'exploitation et applications).

Si un utilisateur est victime de ce type de maliciel, le CERT-FR recommande la conduite suivante :

- isoler au plus vite le poste compromis du réseau ;
- identifier le message malveillant et rechercher d'éventuelles copies envoyées à d'autres destinataires afin de les supprimer ;
- bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant ;
- reformater le poste client et réinstaller un système sain ;

– restaurer les copies de sauvegarde des fichiers perdus.

Le versement de la rançon à l'attaquant ne garantit ni le déchiffrement des fichiers ni la sécurité des moyens de paiement utilisés. Il peut notamment entraîner l'installation de maliciels supplémentaires sur le poste utilisé.

Documentation

- Bulletin d'Actualités CERTFR-2014-ACT-048 :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-048/
- Recommandation pour la mise en oeuvre d'une politique de restrictions logicielles sous Windows :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf
- Informations techniques sur CTB-Locker :
  http://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/
  https://blogs.mcafee.com/mcafee-labs/rise-backdoor-fckq-ctb-locker
- Méthodologie de suppression de mails malveillants :
  http://blogs.technet.com/b/exchange/archive/2010/10/27/removing-specific-messages-from-your-exchange-server.aspx
- Site stop ransomware :
  http://stopransomware.fr

2 - Le « certificate pinning »

Cet article présente une solution permettant de pallier des problèmes inhérents à la gestion des certificats sur Internet pour la sécurisation des échanges via le protocole HTTPS.

Concepts préalables

Un certificat X.509 contient trois informations importantes :

- un nom identifiant une entité ;
- une clé publique ;
- une signature cryptographique.

Le but d'un certificat est de prouver que la clé publique appartient à l'entité grâce à une signature cryptographique. La signature cryptographique est délivrée par une autorité de certification (AC) après un ensemble de vérifications.

Lorsqu'un navigateur se connecte à un site Internet via le protocole HTTPS (HTTP encapsulé par le protocole TLS), le site présente son certificat. Le navigateur est alors en mesure de s'assurer qu'il communique directement avec le site authentique en vérifiant la validité du certificat. Cette étape comprend, entres autres, la vérification de la signature cryptographique inclue dans le certificat.

Afin de vérifier la signature cryptographique, un client doit utiliser la clé publique de l'AC ayant effectué la signature. Pour l'obtenir de façon fiable, il peut l'extraire du certificat de l'AC, en prenant soin de vérifier la validité de ce certificat également. L'opération doit être réitérée jusqu'à arriver à un certificat dit "racine", connu à l'avance et jugé de confiance implicitement. La chaîne de certificats partant du certificat de départ jusqu'au certificat racine est aussi appelée chemin de certification.

Risques associés

Les navigateurs Internet utilisent une liste prédéfinie de certificats racines dont la confiance est reconnue publiquement. Cependant, plus cette liste est grande, plus la surface d'attaque est grande. En effet, la mauvaise pratique, simple erreur ou compromission d'une seule AC parmi celles se rattachant à un certificat racine peut mettre en péril toute l'infrastructure de confiance.

À titre d'exemple, en décembre 2012, des certificats émis frauduleusement ont été détectés. Ils permettaient à leur détenteur de se faire passer pour des sites dont le nom de domaine se termine par google.com. Cet incident est dû à une erreur de la part de l'autorité de certification Turque TURKTRUST [2] qui aurait délivré des certificats de AC intermédiaires au lieu de certificats finaux à des organisations.

Une mesure de contournement, le *certificate pinning*

En reprenant l'incident impliquant TURKTRUST, il est intéressant de noter qu'une simple observation du chemin de certification permet de repérer un élément inhabituel : le chemin remonte à une autorité racine Turque, ce qui semble étrange pour un domaine google.com et dont le certificat se rattache habituellement à l'AC racine GeoTrust Global. De manière sommaire, c'est sur ce raisonnement que repose le *certificate pinning*. Il permet, pour un site donné, d'« épingler » un point de son chemin de certification et d'émettre une alerte si cette contrainte supplémentaire n'est pas respectée. C'est d'ailleurs grâce à cette méthode, utilisée dans son navigateur Chrome, que Google avait détecté les certificats frauduleux liés à TURKTRUST.

Le *certificate pinning* peut être appliqué à plusieurs niveaux. Du moins au plus restrictif, il est par exemple possible :

- d'exiger que le certificat d'une AC particulière se trouve sur le chemin de certification d'un site Internet ;
- d'exiger une clé publique précise pour le certificat d'un site Internet (plus justement appelé *public key pinning*) ;
- d'exiger un certificat précis pour un site Internet.

Les principaux navigateurs, Internet Explorer, Chrome [4] et Firefox [5], supportent le *certificate pinning* et incluent des règles pour quelques sites Internet très connus. Dans le cas d'Internet Explorer, le support n'est pas natif avant la version 11 mais peut être apporté grâce à l'outil Microsoft EMET [6]. Ce dernier permet également de rajouter ses propres règles pour les sites Internet de son choix. A partir de la version 11 d'Internet Explorer, la fonctionnalité *SmartScreen* a été étendue [7], permettant à Microsoft de détecter des anomalies grâce à une supervision proche du *certificate pinning*.

Pour conclure, bien que le *certificate pinning* ne soit pas une solution idéale, notamment à cause de la complexité induite par la création ou mise à jour des règles, il reste un moyen simple et efficace pour remédier à des faiblesses de l'infrastructure de gestions de certificats basée sur les autorités de certification. D'autres méthodes de gestion sont actuellement à l'étude. Nous pouvons notamment citer DANE (DNS-Based Authentication of Named Entities) reposant sur des informations enregistrées dans l'infrastructure DNS, protégées par DNSSEC, pour associer un certificat ou une clé publique à un nom de domaine. L'adoption d'une méthode alternative telle que DANE nécessiterait cependant des modifications plus importantes des programmes l'utilisant, notamment les navigateurs.

Documentation

1 Article de Google annonçant la détection de certificats pour ses domaines remontant à l'IGC/A :
http://googleonlinesecurity.blogspot.fr/2013/12/further-improving-digital-certificate.html

2 Article de Google annonçant la détection de certificats frauduleux remontant à l'autorité de certification TURKTRUST :
http://googleonlinesecurity.blogspot.fr/2013/01/enhancing-digital-certificate-security.html

3 Recommandations de sécurité concernant l'analyse des flux HTTPS :
http://www.ssi.gouv.fr/IMG/pdf/NP_TLS_NoteTech.pdf

4 Annonce du support du *public key pinning* dans Chrome :
https://www.imperialviolet.org/2011/05/04/pinning.html

5 Annonce du support du *public key pinning* dans Firefox :
https://blog.mozilla.org/security/2014/09/02/public-key-pinning/

6 Annonce du support du *certificate pinning* dans EMET permettant à Internet Explorer d'en bénéficier :
http://blogs.technet.com/b/srd/archive/2013/05/08/emet-4-0-s-certificate-trust-feature.aspx

7 Mise à jour de la fonctionnalité *SmartScreen* pour Internet Explorer 11 :
http://blogs.technet.com/b/pki/archive/2014/02/22/a-novel-method-in-ie11-for-dealing-with-fraudulent-digital-certificates.aspx

3 - Bulletin de sécurité Oracle

Lors de la publication de son bulletin de sécurité du 19 janvier 2015, Oracle a annoncé des vulnérabilités concernant 13 de ses produits, notamment :

- Oracle Database ;
- Oracle Java SE ;
- la suite de produits Oracle Sun Systems ;

– Oracle Linux et les produits de virtualisation ;
– Oracle MySQL ;

Les vulnérabilités touchant Oracle Database sont considérées majoritairement par l'éditeur comme mineures ou importantes. La vulnérabilité CVE-2015-6567 sur le composant *Core RDBMS* est considérée comme critique. Celle-ci permet à un attaquant distant d'effectuer une exécution de code arbitraire distante.

Les vulnérabilités touchant Oracle Java SE sont considérées majoritairement par l'éditeur comme importantes ou critiques. Les vulnérabilités critiques affectent les composants *Hotspot*, *JAX-WS*, *RMI* et *Libraries*. Oracle signale notamment que les vulnérabilités très critiques (ayant un score de criticité de 10/10) CVE-2015-0408, CVE-2014-6601, CVE-2015-0412 et CVE-2014-6549 permettent toutes une exécution de code arbitraire distante relativement aisée.

Les vulnérabilités impactant les produits Oracle Sun Systems sont considérées majoritairement par l'éditeur comme mineures ou importantes. Cependant, deux vulnérabilités sur les composants *Solaris Cluster* et les serveurs Fujitsu *M10-1*, *M10-4* et *M10-4S* sont considérées respectivement comme critique et très critique. Cette dernière (CVE-2013-4784) permet une exécution de code arbitraire distante relativement aisée et ne nécessite pas d'authentification préalable à l'exploitation.

Les vulnérabilités concernant Oracle Linux et les produits de virtualisation sont considérées majoritairement par l'éditeur comme mineures ou importantes. Cinq vulnérabilités sur un total de dix permettent une atteinte à l'intégrité, à la confidentialité des données et/ou un déni de service, le tout de façon distante et majoritairement sans nécessiter d'authentification préalable. Les vulnérabilités les moins critiques sont exploitables localement et nécessitent donc très majoritairement une authentification afin de les exploiter.

Les vulnérabilités touchant Oracle MySQL sont considérées majoritairement par l'éditeur comme importantes. Elles induisent dans une grande majorité un déni de service partiel sur le service, à l'exception de :
– la vulnérabilité CVE-2015-0411 (importante), permettant une atteinte partielle à l'intégrité et à la confidentialité des données de façon distante et non authentifiée ;
– la vulnérabilité CVE-2015-0374 (mineure), permettant une atteinte à la confidentialité des données nécessitant une authentification. Selon l'éditeur cette dernière vulnérabilité serait complexe à exploiter.

Documentation

– Bulletin de sécurité Oracle CPUJan2015 du 20 janvier 2015 :
http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
– CERTFR-2015-AVI-030 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-030/index.html
– CERTFR-2015-AVI-031 : Multiples vulnérabilités dans Oracle Virtualization :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-031/index.html
– CERTFR-2015-AVI-032 : Multiples vulnérabilités dans Oracle MySQL :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-032/index.html
– CERTFR-2015-AVI-033 : Multiples vulnérabilités dans Oracle Database Server :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-033/index.html
– CERTFR-2015-AVI-034 : Multiples vulnérabilités dans Oracle Java SE :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-034/index.html

4 - Rappel des avis émis

Dans la période du 19 au 25 janvier 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-ALE-001 : Vulnérabilité dans Adobe Flash Player
– CERTFR-2015-AVI-028 : Multiples vulnérabilités dans Moodle
– CERTFR-2015-AVI-029 : Vulnérabilité dans PolarSSL
– CERTFR-2015-AVI-030 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
– CERTFR-2015-AVI-031 : Multiples vulnérabilités dans Oracle Virtualization
– CERTFR-2015-AVI-032 : Multiples vulnérabilités dans Oracle MySQL
– CERTFR-2015-AVI-033 : Multiples vulnérabilités dans Oracle Database Server
– CERTFR-2015-AVI-034 : Multiples vulnérabilités dans Oracle Java SE
– CERTFR-2015-AVI-035 : Vulnérabilité dans Huawei Quidway

– CERTFR-2015-AVI-036 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2015-AVI-037 : Vulnérabilité dans Adobe Flash Player

Gestion détaillée du document

26 janvier 2015 version initiale.