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 29 juin 2015
N° CERTFR-2015-ACT-026

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-026

1 - Maitrise des serveurs

Les serveurs de nom de domaine (DNS) sont des annuaires permettant d'obtenir des informations relatives à un nom de domaine. Il existe plusieurs types de requêtes offrant ainsi différentes informations. Par exemple, la traduction d'un nom de domaine (www.exemple.com) en adresse IP (1.2.3.4) se fait au travers des requêtes de type A (ou AAAA pour IPv6). L'adresse du serveur où envoyer des mails à destination du domaine est obtenue au travers de requêtes de type MX (Mail eXchanger), le serveur MX du domaine www.exemple.com pouvant être mx1.exemple.com.

Le CERT-FR a été amené à traiter divers incidents impliquant la compromission de serveurs DNS. Un attaquant ayant pris le contrôle de cet élément du système d'information est ainsi en mesure d'effectuer différentes actions parmi lesquelles :

- ajouter un enregistrement ;
- modifier l'adresse du serveur MX ;
- etc.

L'ajout d'un enregistrement dans la configuration du serveur DNS peut, au premier abord, sembler inutile, mais cette modification permet de réaliser différents types d'attaques dont par exemple:

- spear-phishing : un enregistrement ayant l'air légitime (par exemple production.exemple.com / web.exemple.com / etc.) mais pointant sur un serveur contrôlé par l'attaquant sera utilisé dans un mail de type spear-phishing. La victime travaillant pour exemple.com va probablement suivre le lien en toute confiance et sera redirigée sur le serveur de l'attaquant.
- masquer du trafic illégitime : un attaquant ayant déjà compromis un poste interne peut utiliser un nom à l'apparence légitime appartenant au même domaine que la victime (production.exemple.com par exemple) comme serveur de command & control ou d'exfiltration de données. Les administrateurs système et réseau de la victime ne verraient alors que des requêtes vers des noms de domaine "légitimes".

La modification de l'adresse des serveurs de mail (MX) induit quant à elle des conséquences plus importantes. En effet, un attaquant est en mesure, en modifiant uniquement un enregistrement MX, de recevoir tous les mails à destination du domaine de la victime. Il suffit ensuite à l'attaquant de les faire suivre sur le serveur de mail légitime de la victime. Ce type d'attaque peut potentiellement être rapidement détecté par la victime selon la configuration de son serveur de mail. Si le serveur de la victime vérifie la source émettrice du mail dans le but de filtrer les pourriels (en utilisant par exemple le Sender Policy Framework (SPF) qui permet d'obtenir la liste des adresses IP autorisées à émettre des mails pour un domaine donné), aucun mail ne sera accepté du fait que les mails de tous les domaines proviennent du serveur de l'attaquant. La victime ne recevant plus de mail investiguera donc le problème et découvrira l'incident.

Les conséquences en cas de compromission d'un serveur DNS étant importantes, une supervision adéquate et un contrôle des accès cohérent doivent être mis en place. De plus, la modification des informations publiées dans l'annuaire devraient être du seul ressort des équipes techniques.

Documentation

- http://fr.wikipedia.org/wiki/Domain_Name_System
- http://fr.wikipedia.org/wiki/Sender_Policy_Framework
- http://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms-de-domaine
- http://www.cert.ssi.gouv.fr/site/CERTA-2008-INF-002/

2 - Mise à jour de sécurité Adobe Flash Player

Le 23 juin 2015, Adobe a publié une mise à jour de sécurité (bulletin de sécurité APSB15-14) hors cycle habituel de mise à jour concernant la vulnérabilité suivante, pouvant conduire à une exécution de code arbitraire à distance :

- CVE-2015-3113 (critique) concernant un dépassement de tampon.

Cette vulnérabilité a été reportée comme activement exploitée dans la nature avant la diffusion du correctif de sécurité par le biais d'attaques ciblées visant des systèmes Microsoft Windows utilisant Internet Explorer ou Mozilla Firefox. Elle repose sur un dépassement de mémoire tampon sur le tas dû à une mauvaise analyse grammaticale de fichiers FLV embarqués pouvant conduire à une exécution de code arbitraire.

Les mises à jour de Microsoft et Google pour leurs navigateurs respectifs Internet Explorer (10 et 11) et Chrome afin de corriger les versions embarquées de Flash Player n'ont pour l'heure pas été mises à disposition des utilisateurs.

Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande ainsi leur application dès que possible.

Recommandations

Le CERT-FR recommande de désactiver l'exécution automatique de code Flash au sein des navigateurs jusqu'à installation du correctif.

Le CERT-FR conseille également d'installer des outils permettant de durcir les systèmes et de rendre l'exploitation de vulnérabilités plus difficile. En particulier, sous Windows, l'outil EMET proposé par Microsoft, permet de limiter les risques d'exploitation (voir Documentation).

Enfin le CERT-FR préconise d'activer les mises à jour automatiques pour l'ensemble des logiciels.

Documentation

- Avis du CERT-FR
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-262/CERTFR-2015-AVI-262.html
- Avis de l'éditeur
  https://helpx.adobe.com/security/products/flash-player/apsb15-14.html
- Élements techniques
  https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day
  html
- http://blog.trendmicro.com/trendlabs-security-intelligence/new-adobe-zero-day-shares-same-rootroot-cause-as-older-flaws/
- Microsoft EMET 5.1
  http://www.microsoft.com/emet

3 - Rappel des avis émis

Dans la période du 22 au 27 juin 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-261 : Multiples vulnérabilités dans le noyau Linux Debian
- CERTFR-2015-AVI-262 : Vulnérabilité dans Adobe Flash Player
- CERTFR-2015-AVI-263 : Multiples vulnérabilités dans le noyau Linux Red Hat
- CERTFR-2015-AVI-264 : Vulnérabilité dans GnuTLS

- CERTFR-2015-AVI-265 : Multiples vulnérabilités dans PHP
- CERTFR-2015-AVI-266 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-267 : Vulnérabilité dans le module de communication Siemens Climatix BACnet/IP

Gestion détaillée du document

29 juin 2015 version initiale.