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 28 décembre 2015
N° CERTFR-2015-ACT-052

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-052

Pistage d'utilisateurs sur le Web

Introduction

Dans un précédent bulletin d'actualité [1], nous présentions comment les *cookies* HTTP (ou témoins de connexion), pouvaient être utilisés à des fins de profilage de l'utilisateur, dans le but notamment de pouvoir lui proposer du contenu ciblé. Après un bref rappel, cet article se propose de parcourir plus largement les mécanismes complémentaires existants à l'heure actuelle, à des fins de sensibilisation aux problématiques de vie privée sur l'Internet, et dans l'optique de permettre la prise des précautions d'usage adaptées à son utilisation au quotidien, dans un contexte professionnel comme personnel.

Techniques de pistage

Cookies et évolutions

La technique la plus utilisée en matière de pistage d'utilisateurs sur l'Internet repose sur l'exploitation des cookies. Nous rappelons que le terme *cookie* désigne une variable utilisée par un serveur HTTP pour sauvegarder des informations sur la session HTTP courante. Il est composé d'une paire obligatoire nom/valeur, et d'attributs optionnels, comme la date d'expiration, le domaine et le chemin. Ces informations sont créées et mises à jour lors des échanges entre un serveur et un client Web grâce à des en-têtes dédiés du protocole HTTP ("*Set-Cookie*", "*Cookie*") [2].

Le premier cas d'usage des *cookies* est tout à fait nécessaire à la navigation sur de nombreux sites Web, par exemple pour le maintien d'une session applicative ou la mémorisation d'un panier d'achats, on parle alors de "*cookies* de premier niveau". Il existe cependant d'autres cas d'utilisations controversés sur le plan du respect de la vie privée. En particulier, l'usage de "*cookies* tiers" (ou "tierce partie") [1], notamment dans l'optique d'établir des statistiques de consultation, peut permettre par exemple d'offrir des services de publicité ciblée. Ces *cookies* sont reconnaissables en particulier à leur domaine d'appartenance différent de celui de la page consultée, et peuvent parfois permettre d'identifier finement un utilisateur donné (par exemple *cookies* Google).

D'autres mécanismes permettent la conservation de données utilisateur, qui exploitent d'autres modes de création et de stockage que les cookies HTTP. On regroupe généralement ceux-ci sous le terme "*supercookie*". Ils s'appuient notamment sur l'utilisation :

- de mécanismes de stockage local dédiés à des applications Web au-dessus du protocole HTTP, comme Adobe Flash ("*Local Shared Objects*", également appelés "*cookies* Flash"), Microsoft Silverlight ("*Silverlight Isolated Storage*") ou encore HTML5 ("*HTML5 storage*") ;
- d'objets dans le contenu des pages Web, comme la propriété "*window.name*" en JavaScript, qui peut être détournée pour stocker temporairement des informations ;
- du cache du navigateur et de l'historique de navigation, pour stocker sous forme encodée des informations ;

– de HSTS ("*HTTP Strict Transport Security*") [3], mécanisme de politique de sécurité pour HTTP, permettant à un serveur de demander le passage vers HTTPS via un champ d'en-tête HTTP ("*Strict-Transport-Security*"), mais dont une utilisation détournée permet à tiers contrôlant plusieurs domaines d'identifier de façon unique un utilisateur [4].

Cette liste, non exhaustive, montre bien qu'il existe de nombreuses façons de stocker des données issues de la navigation Web, et qu'un simple nettoyage des *cookies* HTTP via le navigateur ne peut pas suffire à effacer proprement l'ensemble de celles-ci. D'ailleurs, on parle de "*cookie zombie*" pour désigner des *cookies* HTTP qui sont régénérés après leur suppression grâce à l'utilisation des *supercookies*. L'application *Evercookie* [5], par exemple, illustre cela, permettant la propagation des *cookies* HTTP dans autant que mécanisme de stockage que possible afin d'assurer la résilience de l'information.

Autres techniques

Si les *cookies* (et assimilés) permettent d'obtenir une masse d'informations très intéressante, ils ne sont pas pour autant la seule source considérée par les entités cherchant à pister l'utilisateur. Il existe en particulier de nombreuses autres méthodes permettant d'identifier de façon unique un utilisateur, parfois à la granularité du terminal utilisé (téléphone, ordinateur, téléviseur connecté, tablette, etc.).

Ces méthodes peuvent être classées en cinq catégories [6] :

– Identification générée par le client : certains terminaux ou applications clientes génèrent un identifiant unique pouvant être accessible par les services tiers à des fins publicitaires (*advertising identifiers*).
– Identification via des éléments réseau : certains équipements réseau situés entre le client et le serveur insèrent des éléments permettant, volontairement ou non, d'identifier l'utilisateur. Par exemple, l'utilisation du champ "*X-Forwarded-For*" dans l'en-tête HTTP précise l'adresse IP d'origine d'un client se connectant à travers un serveur mandataire.
– Identification par le serveur : certains serveurs ajoutent des pixels-espions [7], images de très petite taille généralement non repérables par l'utilisateur, qui permettent la génération de *cookies* tiers.
– Identification unique : certains services permettent à l'utilisateur de s'authentifier pour accéder à un ensemble de ressources (sites, applications), induisant ainsi la création d'un identifiant unique, censé faciliter la navigation (unique portail d'authentification, gestion des préférences utilisateur, etc.). On peut citer par exemple *Facebook Connect*, *Windows Live ID*, *Google Account*, etc.
– Identification statistique : certaines données issues du navigateur, de l'application ou encore du système d'exploitation permettent le calcul d'une empreinte entraînant la capacité à singulariser l'utilisateur. Ce calcul peut par exemple s'appuyer sur le *User-Agent*, la valeur du champ *HTTP Accept*, la politique de gestion des *cookies*, la résolution de l'écran, ou encore les extensions installées [8].

Recommandations

La directive 2002/58 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9][10] précise que l'utilisation de *cookies* est autorisée à condition que l'utilisateur se voie donner des informations claires et précises sur la finalité de ces *cookies* ainsi que les informations placées sur l'équipement terminal qu'il utilise. L'utilisateur pourra refuser l'utilisation de ces dispositifs, cependant cette disposition ne fait pas obstacle au stockage de données utilisées à des fins exclusivement techniques.

Techniquement, des solutions amont ont été proposées, comme l'en-tête HTTP *"Do Not Track"* (DNT, 2009), pour permettre d'indiquer à un site web qu'un utilisateur ne souhaite pas être tracé. Cependant, bien qu'intégré dans tous les navigateurs modernes, il est purement déclaratif et peut être ignoré par le site visité.

D'un point de vue pratique, une des solutions les plus simples afin de limiter ces traces est de bloquer les *cookies* tiers. Ces *cookies* ne sont généralement pas utiles pour la navigation et il est recommandé de les refuser par défaut [11].

Enfin, de nombreuses extensions pour navigateur permettent de limiter le suivi d'un utilisateur existant. Elles ont principalement pour effet :

– le blocage des traceurs (*DoNotTrackME*, *Disconnect*, *uBlock Origin*, *AdBlock*),
– le blocage des scripts (*NoScript*, *ScriptNo*),
– la génération de fausses informations afin de brouiller le calcul des empreintes numériques (*Random Agent Spoofer*),
– le basculement automatique vers HTTPS si disponible (*HTTPS Everywhere*).

Références

1. Bulletin d'actualité CERTA-2010-ACT-005 (05 février 2010)

   http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-005/CERTA-2010-ACT-005.html
2. RFC 6265 (HTTP State Management Mechanism) (avril 2011)

   https://www.rfc-editor.org/rfc/rfc6265.txt
3. RFC 6797 (HSTS) (novembre 2012)

   https://tools.ietf.org/html/rfc6797section-14.9
4. How HSTS supercookies make you choose between privacy or security (02 février 2015)

   https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
5. Evercookie (github)

   https://github.com/samyk/evercookie
6. IAB Cookie White Paper (janvier 2014)

   http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
7. Web beacon (9 janvier 2014)

   https://www.iab.net/wiki/index.php/Web$_beacon$
8. Browser uniqueness

   https://panopticlick.eff.org/browser-uniqueness.pdf
9. Directive 2002/58/CE (12 juillet 2002)

   http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
10. Sites web, cookies et autres traceurs (CNIL)

    http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/
11. Conseils aux internautes (CNIL)

    http://www.cnil.fr/vos-droits/vos-traces/les-cookies/conseils-aux-internautes/

Vulnérabilités critiques au sein de Juniper ScreenOS

Contexte

Le 18/12/2015, le CERT-FR a émis l'alerte CERTFR-2015-ALE-014 [1] concernant plusieurs vulnérabilités critiques impactant le système ScreenOS des équipements Juniper. D'après le bulletin de sécurité publié par Juniper [2], ces vulnérabilités ont été découvertes suite à un audit de code interne et auraient été introduites volontairement pour affaiblir la sécurité de ScreenOS. Il s'agit en l'occurrence de deux portes dérobées qui permettent de :

- contourner le mécanisme d'authentification en place au niveau des services SSH et Telnet,
- déchiffrer les communications entre un client et le service VPN d'un équipement Juniper vulnérable.

Marqueurs de détection

La société Fox-It propose des signatures au format Snort afin d'identifier toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée. Ces signatures sont cependant limitées au service Telnet. De plus, la vulnérabilité liée au service VPN étant exploitable après une interception passive du trafic chiffré, il n'est pas possible de détecter son exploitation.

Versions affectées

La porte dérobée permettant d'accéder à l'interface d'administration de l'équipement via le protocole Telnet ou SSH impacte le logiciel Juniper ScreenOS de la version 6.3.0r17 à 6.3.0r20.

La vulnérabilité permettant de déchiffrer les communications réseau liées au service VPN impacte le logiciel Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18 et les versions 6.3.0r12 à 6.3.0r20.

Ces vulnérabilités permettant un accès illégitime sont respectivement référencées par les identifiants CVE-2015-7755 et CVE-2015-7756.

Description des portes dérobées

CVE-2015-7755

La porte dérobée permettant d'accéder à l'interface d'administration d'un équipement Juniper vulnérable est localisée au sein du code de vérification des identifiants de connexion. Ce code compare le mot de passe saisi par l'utilisateur avec une chaîne de caractères codée en dur dans le système ScreenOS. Si ils sont identiques, l'accès est autorisé.

CVE-2015-7756

La seconde porte dérobée reposait sur une faiblesse du générateur de nombres aléatoires utilisé par l'algorithme de chiffrement et permettait à un attaquant d'accéder au contenu des communications VPN, obtenues à partir d'une écoute passive du trafic réseau.

Corrections

Le CERT-FR recommande d'appliquer les mesures préconisées dans le bulletin d'alerte CERTFR-2015-ALE-014.

Documentation

1 Bulletin d'alerte du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-014/index.html
2 Bulletin de sécurité de l'éditeur :
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
3 Versions de ScreenOS vulnérable :
https://isc.sans.edu/diary/Infocon+Yellow%3A+Juniper+Backdoor+(CVE-2015-7755+and+CVE-2015-7756)/20521

1 - Rappel des avis émis

Dans la période du 21 au 27 décembre 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-ALE-015 : Campagne de messages électroniques non sollicités de type TeslaCrypt
– CERTFR-2015-AVI-554 : Multiples vulnérabilités dans le noyau Linux de Debian
– CERTFR-2015-AVI-555 : Vulnérabilité dans VMWare
– CERTFR-2015-AVI-556 : Multiples vulnérabilités dans Citrix XenServer
– CERTFR-2015-AVI-557 : Multiples vulnérabilités dans Cisco IOS et IOS XE
– CERTFR-2015-AVI-558 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
– CERTFR-2015-AVI-559 : Vulnérabilité dans Xen
– CERTFR-2015-AVI-560 : Vulnérabilité dans Cisco IOS XE
– CERTFR-2015-AVI-561 : Multiples vulnérabilités dans le noyau Linux de Fedora
– CERTFR-2015-AVI-562 : Multiples vulnérabilités dans ISC Bind
– CERTFR-2015-AVI-563 : Multiples vulnérabilités dans le noyau Linux de SUSE

Durant la même période, les publications suivantes ont été mises à jour :

– CERTFR-2015-ALE-014-1 : Vulnérabilité dans Juniper ScreenOS (ajout de règles Snort dans les contournements provisoires.)

Gestion détaillée du document

28 décembre 2015 version initiale.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-052