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 02 mai 2017
N° CERTFR-2017-ACT-018

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-018

1 - Utilisation du *Domain Fronting* pour obscurcir une empreinte réseau

Description

Dans une communication HTTPs, le nom de domaine que le client souhaite contacter apparait trois fois :

1. dans la requête DNS permettant de trouver l'adresse IP numérique du serveur à contacter ;
2. dans le champ *TLS-SNI* quand le client demande le certificat TLS du serveur ;
3. dans le champ *Host* de l'en-tête de la requête HTTP envoyé dans le tunnel chiffré.

Les deux premières instances apparaissent en clair sur le réseau, mais la troisième est protégée par le chiffrement TLS.

Le *Domain Fronting* consiste à remplacer ces deux instances visibles en clair par un autre nom de domaine *A*, tout en conservant la troisième à la valeur originale *B*. Si ces deux noms de domaine pointent vers l'adresse IP d'un serveur publiant les deux sites web, la connexion TLS sera établie, puis le serveur se basera sur le contenu du champ *Host* pour choisir quel contenu fournir.

Ainsi le client obtiendra le contenu qu'il attend provenant du site *B*, tout en semblant, pour un observateur extérieur se basant sur les métadonnées du trafic, communiquer avec le site *A*. Cette configuration est possible avec des serveurs d'hébergements mutualisés, où de nombreux sites partagent la même adresse IP, ou encore pour des sites utilisant un CDN tel que cloudflare, akamai, etc. Cette technique est utilisée et documentée depuis plusieurs années par le logiciel d'anonymisation TOR afin de contourner des mécanismes mis en place par certains états pour en interdire l'usage.

Utilisation malveillante

Le CERT-FR a constaté l'utilisation de cette technique dans plusieurs incidents, dans lesquelles un logiciel malveillant s'en sert pour dissimuler ses communications avec son serveur de contrôle et de commandes.

Dans ce cas, les seules traces visibles dans les journaux DNS et dans les journaux proxy ne font apparaitre que le site *A* qui est un site légitime, quand le domaine malveillant *B* n'apparait nulle part, rendant plus complexe la détection et le confinement de cette menace.

Contre-mesures

Lors de recherches de traces réseau, il est important de prendre en compte non seulement les noms de domaines malveillants, mais également de rechercher directement les adresses IP derrière ces noms de domaines.

Il convient également d'apporter une attention particulière aux noms de domaines et IPs de CDNs qui se prêtent particulièrement à ce type de pratiques. Ces éléments sont également à prendre en compte lors de la mise en place de listes noires pour le blocage de sites malveillants.

Documentation

- Blocking-resistant communication through domain fronting :
  http://www.icir.org/vern/papers/meek-PETS-2015.pdf

2 - Rappel des avis émis

Dans la période du 23 au 30 avril 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-128 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-129 : Multiples vulnérabilités dans IBM Domino
- CERTFR-2017-AVI-130 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTFR-2017-AVI-131 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-132 : Vulnérabilité dans NVIDIA GeForce Experience
- CERTFR-2017-AVI-133 : Vulnérabilité dans Ghostscript

Gestion détaillée du document

02 mai 2017 version initiale.