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 10 octobre 2016
N° CERTFR-2016-ACT-041

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-041

1 - Industrialisation de déni de service distribué, le cas particulier des objets connectés

Contexte de l'analyse

Lors des dernières semaines, une recrudescence des dénis de service distribués à l'encontre de journalistes ou d'opérateurs a été constaté.

Une des particularités de ces attaques récentes est leur provenance.

En effet, ces attaques provenaient d'objets connectés mal sécurisés, constituant un réseau de machines zombies.

D'autre part, suite à l'attention médiatique attirée par ces attaques, un utilisateur a publié le code source d'un des codes malveillants utilisé pour compromettre ces objets connectés et permettre ces attaques via un service à la demande payant.

Le réseau mondial des objets connectés

Depuis quelques années, de nombreux fabricants d'équipements permettent de les connecter sur la toile. Les logiciels embarqués dans ces objets peuvent contenir des vulnérabilités, ou présenter des défauts de configuration permettant d'en prendre le contrôle.

Si ces objets sont connectés directement sur Internet, ils peuvent représenter des cibles faciles pour des attaquants qui pourront les utiliser soit comme vecteur d'attaque, soit comme rebond pour compromettre le réseau interne.

Ainsi, sur le grand nombre de nouveaux équipements qui vont être connectés cette année aux quatre coins du monde, sur tous ces équipements qui ne sont que rarement mis à jour, que deviendront les vôtres?

Déni de service distribué

Le déni de service distribué est une attaque relativement connue consistant à saturer les connexions de la "cible" pour la rendre injoignable.

Afin de réaliser cette attaque, l'attaquant peut utiliser un grand nombre de machines compromises qui émettent des requêtes au même instant vers un site ciblé, surpassant ainsi les capacités de ce site, et le rendant indisponible pour les utilisateurs légitimes. Dans un autre domaine, le déni de service distribué peut être comparé à un infarctus digital, les machines contrôlées par l'attaquant représentant les plaques de cholestérol bloquant une artère (la connexion) du coeur (le service visé).

Analyse du code malveillant *MIRAI*

Moyen de propagation

Chaque membre du réseau zombie effectue une recherche exhaustive sur internet d'équipements laissant un accès ouvert, et essaye de s'y connecter en utilisant la force brute via un dictionnaire de quelques dizaines de couples utilisateur - mot de passe.

Les équipements ciblés sont majoritairement des caméras connectées, des récepteurs vidéos (`DVR`), mais également des routeurs ou des imprimantes réseau.

Une fois une cible identifiée, le code malveillant envoie à un serveur spécialisé les informations sous la forme `ip:port username:password`.

Ce serveur se charge ensuite d'infecter les hôtes identifiés en y téléchargeant le code malveillant via les utilitaires `tftp`, `wget` ou un utilitaire personnalisé (nommé `Echo loader`).

Coeur du code malveillant

La charge du code malveillant s'exécute sur un objet connecté compromis.

Cette charge peut s'exécuter sur un grand nombre d'architectures distinctes, ce qui lui permet de diversifier les cibles.

Le rôle principal de cette charge est non seulement de récupérer les commandes d'attaques depuis le serveur de contrôle, mais aussi d'effectuer un balayage du réseau pour découvrir de nouvelles victimes.

Ce balayage réseau vise les ports `23`(service `telnet`), mais également le port `2323`.

Il utilise quelques techniques pour complexifier l'analyse et pour s'adapter aux machines embarqués. En particulier, il complexifie l'usage du débogueur `GDB`, et utilise les signaux `Unix` pour dérouter le flot de contrôle.

Serveur de contrôle

Le serveur de contrôle permet à l'attaquant de monétiser l'accès au réseau de machines compromises, via un service d'interface programmable.

Cette particularité montre une évolution des cybercriminels qui s'inspirent de pratiques déployées dans l'industrie informatique afin de maximiser le revenu et de minimiser les risques encourus.

Une autre partie du serveur de contrôle permet de récupérer les cibles repérées par les zombies et de leur envoyer une charge active, et montre une démarche visant à simplifier et automatiser la compromission de nouvelles victimes.

Motifs d'attaques

Différentes attaques sont implémentées dans ce code malveillant, certaines étant relativement simples (saturation de port simple, ou *SYN Flood*), d'autres mettant en oeuvre des prototoles plus complexes tels que le protocole de jeu `Valve`, ou le protocole d'encapsulation `GRE`.

Autres familles de codes malveillants spécialisées dans le déni de service

Le code source de la famille *Mirai* ayant été publié, une recrudescence des attaques par force brute sur des objets connectés est attendue.

Toutefois, de nombreux autres codes malveillants possédant des capacités de déni de service distribués existent, tels que *Rex*, qui se propage via des sites compromis, ou encore *XorDDOS* qui se propage via une attaque force brute sur le service `SSH`.

Impacts

L'impact de ces codes malveillants visant les objets connectés est multiple. Tout d'abord, lors de leur utilisation pour un déni de service distribué, la disponibilité de l'accès Internet du réseau hébergeant cet objet peut être mise à mal, mais surtout la disponibilité du site visé.

D'autre part, la compromission de cet objet peut représenter un danger en terme de confidentialité, en particulier dans le cas des caméras connectées.

En effet, l'attaquant peut ainsi récupérer les images enregistrées par cette caméra, et ainsi exploiter les images reçues à des fins néfastes.

Enfin, l'accessibilité de codes d'exploitation abaisse le niveau requis par un attaquant pour mener de telles attaques.

On peut donc en conclure qu'en l'absence de contremesures, un attaquant de faible niveau pourra non seulement utiliser ces caméras de surveillance ou autres objets connectés pour rendre inaccessible un site visé, mais aussi pour mener des actions malveillant à l'encontre des propriétaires de ces équipements.

Recommandations

Au vu des impacts potentiels, le CERT-FR recommande la plus grande prudence lors de l'installation d'objets connectés sur Internet.

De même, une politique de mise à jour régulière des logiciels embarqués sur ces équipements doit être mise en oeuvre.

D'autre part, le CERT-FR recommande de changer les mots de passe de connexion sur ces objets, ainsi que la mise en place de restrictions au niveau réseau sur les interfaces d'administration des équipements susmentionnés.

Documentation

- https://www.ovh.com/fr/news/articles/a2367.goutte-ddos-n-apas-fait-deborder-le-vac
- https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-d dos/
- https://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/
- https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-definition-dune-politique-de-filtrage-reseau-dun-pare-feu/
- https://www.ssi.gouv.fr/administration/guide/mot-de-passe/
- https://thisissecurity.net/2016/08/17/from-website-locker-to-ddos-rex/
- https://blog.checkpoint.com/wp-content/uploads/2015/10/sb-report-threat-intelligence-groundhog.pdf

2 - Rappel des avis émis

Dans la période du 03 au 09 octobre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-325 : Vulnérabilité dans les produits Cisco
- CERTFR-2016-AVI-326 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-327 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-328 : Vulnérabilité dans Xen
- CERTFR-2016-AVI-329 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2016-AVI-330 : Vulnérabilité dans les produits F5
- CERTFR-2016-AVI-331 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-332 : Vulnérabilité dans Citrix License Server
- CERTFR-2016-AVI-333 : Multiples vulnérabilités dans les produits BlueCoat

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

- CERTFR-2016-ALE-006 : Campagne de messages électroniques non sollicités de type Zepto/Odin (ajout marqueurs supplémentaires ;)
- CERTFR-2016-ALE-006 : Campagne de messages électroniques non sollicités de type Zepto/Odin (ajout marqueurs supplémentaires ;)

Gestion détaillée du document

10 octobre 2016 version initiale.