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 septembre 2015
N° CERTFR-2015-ACT-039

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-039

1 - Porte dérobée *SYNful Knock*

Le 15 septembre 2015, la société FireEye a annoncé avoir découvert des routeurs Cisco dont le logiciel constructeur a été modifié pour intégrer une porte dérobée (baptisée "*SYNful Knock*").

Architecture générale et fonctionnalités

Cette porte dérobée résiste au redémarrage du routeur et peut être personnalisée par l'adjonction de composants enfichables installables à distance qui, eux, ne sont pas résilients. Les auteurs de ce code malveillant ont conçu le protocole utilisé lors du déploiement des modules additionnels pour qu'il puisse ressembler à `HTTP`.

La porte dérobée

L'une des fonctionnalités de base de "*SYNful Knock*" consiste à donner un accès privilégié à tout utilisateur qui saisirait un mot de passe inclus dans la porte dérobée, soit lors d'une connexion `telnet` (mais pas `SSH`), soit par la console ou bien après avoir saisi la commande `enable`. Les commandes de base supportées par "*SYNful Knock*" offrent les services suivants :

- énumération des modules chargés et de leur état ;
- allocation de mémoire en vue du chargement d'un nouveau module ;
- chargement d'un module en mémoire ;
- activation d'un module ;
- suppression d'un module.

Les modules

Les modules peuvent s'insérer dans le flux d'exécution normal du système afin d'en modifier le comportement ou fournir des services utilisables sans interférer avec le fonctionnement du routeur.

Installation et mises à jour

Installation

La modification de l'image Cisco IOS passe vraisemblablement par les étapes suivantes :

- passage des permissions de certaines zones mémoires en lecture/écriture ;
- modification voire remplacement de certaines fonctions du système ;
- écrasement de données légitimes par des chaînes de caractères et des données de configuration utilisées par la porte arrière.

Les modifications de permissions permettent de modifier le code d'origine et de détourner le flux d'exécution originel en s'y intercalant. L'écrasement de certaines parties de l'image a lui pour but de ne pas modifier la taille de l'image d'origine.

Accès et mise à jour par le réseau

Au niveau du réseau, l'accès aux routeurs compromis avec cette version du logiciel constructeur malveillant passera vraisemblablement par l'utilisation du port 80 ou du protocole `telnet`. Dans le premier cas, la poignée de main entre l'attaquant et un routeur compromis débute par l'envoi, vers le port 80 du routeur, d'un paquet `TCP SYN` pour lequel la différence entre le numéro de séquence et le numéro d'acquittement est égale à `0xC123D` (`791101`). Le routeur répond par un paquet `TCP` ayant les caractéristiques suivantes :

- les drapeaux `SYN` et `ACK` sont mis ;
- son numéro de séquence est égal au numéro d'acquittement initialement envoyé par le client ;
- le pointeur de fin des données urgentes est égal à 1 ;
- le drapeau d'urgence n'est pas mis ;
- les options TCP sont égales à "`02 04 05 b4 01 01 04 02 01 03 03 05`" (taille maximale de segment=`1460`, 2x`NOP`, `SACK` permis, `NOP`, échelle de fenêtre=`5`).

Le client termine cet échange en envoyant un paquet `TCP` contenant la commande à exécuter et ayant comme particularités :

- l'activation des drapeaux `PUSH` et `ACK` ;
- la présence de la chaîne "`text`" au décalage `98` (`0x62`).

Enfin, dans les cas connus publiquement, la réponse du routeur compromis après exécution de la commande est préfixée des entêtes `HTTP` suivants :

```
HTTP/1.1 200 OK
Server: Apache/2.2.17 (Ubuntu)
X-Powered-By: PHP/5.3.5-1ubuntu7.7
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Modèles concernés

La société FireEye mentionne avoir connaissance que les modèles suivants sont - a minima - concernés :

- Cisco 1841 ;
- Cisco 2811 ;
- Cisco 3825.

On notera que ces trois modèles de routeurs à services intégrés ne sont plus vendus par le constructeur aujourd'hui, mais :

- cette liste est évidemment non exhaustive puisqu'ils n'ont trouvé que 14 cas de routeurs compromis alors que près de 200 seraient accessibles via Internet ;
- cela pourrait être un signe que cette version de logiciel constructeur modifié est un ancien projet remplacé depuis par une version moins facilement détectable.

Concernant ce dernier point, le lecteur attentif aura noté que la mise en éveil numéro 40411 de Cisco datant du 11 août 2015 et concernant l'évolution des attaques contre les plateformes Cisco IOS fait état de cas avérés d'images `ROM Monitor` (aussi appelées `ROMMON`, *boot software*, *boot image*, *boot helper*) malveillantes, cas qui sont donc différents du médiatique "*SYNful Knock*", une version modifiée de Cisco IOS Software.

Cibles connues

Plusieurs entités ont effectué un balayage du réseau Internet afin de tenter de détecter, dénombrer et localiser les routeurs compromis. Ces initiatives ont été suivies de publications de résultats allant de 14 hôtes compromis dans 4 pays à 199 adresses IP uniques appartenant à 163 hôtes uniques dans 31 pays. Il ne semble pas qu'il y ait de point commun flagrant entre les cibles ainsi trouvées si ce n'est que la France, parmi d'autres, fait partie des pays qui n'apparaissent pas dans ces résultats. Néanmoins, il serait hâtif de se baser sur cette observation pour déduire, de sa simple position géographique, qu'une entité n'est pas touchée :

- la disparité des résultats obtenus montre que ces balayages ne sont pas exhaustifs ;

– seuls des équipements accessibles via Internet à l'heure des tests ont pu être interrogés alors que cette porte dérobée a pu être installée sur un routeur désormais installé au coeur du réseau interne d'une entreprise ;
– l'heuristique utilisée pour obtenir ces résultats est basée sur des traits très spécifiques du code malveillant, traits que l'on ne retrouve peut-être pas dans d'autres versions et certainement pas dans d'autres programmes malveillants.

Détection

Détection active via le réseau

La poignée de main `TCP` décrite supra est suffisamment spécifique pour être utilisée comme moyen de détection. Plusieurs outils ont ainsi été développés et mis à disposition par FireEye et Cisco.

Détection passive et surveillance du réseau

Des règles de détection gratuites (FireEye) et payantes (Cisco) sont disponibles pour des sondes réseau de détection d'intrusion (`NIDS`) courantes mais, au-delà de ces règles très spécifiques à une menace, la surveillance par les administrateurs des activités sur le réseau dont ils ont la charge est indispensable. Par exemple, être capable de détecter que quelqu'un tente d'accéder à un routeur depuis une adresse non explicitement autorisée par la politique de sécurité contribue grandement à se prémunir de menaces similaires. De la même façon, les protocoles `telnet` et `HTTP` ayant probablement été bannis de tout réseau d'administration moderne, le simple fait qu'ils puissent être utilisés devrait lever une alerte.

Détection et analyse à partir des routeurs

Les bits de permissions présents dans le cache des entrées de la table des pages (le *translation lookaside buffer* ou `TLB`) étant modifiés pour rendre les pages mémoires accessibles en écriture et ces permissions pouvant être visualisées, cela donne une méthode de détection possible pour certains modèles de routeurs. En effet, le code exécutable étant typiquement dans des pages mémoire uniquement accessibles en lecture, l'absence de pages en lecture seule pourrait indiquer qu'une modification des permissions a été effectuée.

En pratique, sur les routeurs la supportant, la commande suivante devrait retourner des résultats sur un routeur sain :

```
show platform tlb | include RO, Valid
```

Les possesseurs de matériels Cisco équipés de *Multilayer Switching Feature Card* (MSFC) pourront étendre cette vérification à cette dernière :

```
show msfc tlb | include RO, Valid
```

Les modifications apportées à l'image Cisco IOS pourraient être détectées :
– en ligne en comparant les empreintes `MD5` "*Embedded Hash*" et "*Computed Hash*" données par la commande `verify` ;
– hors ligne en comparant l'empreinte `SHA-512` de l'image Cisco IOS utilisée pour la dernière mise à jour de l'équipement avec celle indiquée dans la zone "Support et Téléchargements" du site de l'éditeur ;
– en comparant l'empreinte "`CCO`" calculée par la commande `verify` avec celle fournie par l'éditeur sur son site.

Des données légitimes, dont des chaînes de caractères, étant écrasées lors de l'installation, il peut arriver qu'un routeur compromis affiche ou journalise des messages non standards ou incohérents. Les administrateurs doivent donc être alertés par ce type d'errements. Les zones écrasées pourraient être choisies en fonction des fonctionnalités utilisées sur le routeur. Par conséquent, ces modifications de comportements peuvent varier d'un équipement à l'autre. Aussi, l'obtention d'un vidage de l'image du routeur permet de conserver une copie des modules chargés en mémoire volatile à des fins d'analyse et est une des étapes nécessaires à une correcte évaluation de l'impact d'une attaque. En effet, les actions réalisables par un attaquant dépendent des modules installés.

Limites

Il convient de garder à l'esprit les limites suivantes :
– les attaquants ont pu mettre à jour la porte dérobée afin que les signatures mentionnées supra ne soient plus adaptées ;
– le comportement des commandes saisies sur le routeur pour recueillir des informations a pu être modifié par le code malveillant.

Impacts

Selon le positionnement du routeur compromis au sein du réseau, la présence de cet outil peut autoriser un attaquant à (cette liste n'étant pas exhaustive) :

- accéder de façon récurrente au réseau interne d'une entreprise ;
- obtenir une copie de flux réseau ;
- mener d'autres attaques en se faisant passer pour une de ses victimes ;
- annoncer des préfixes réseau via `BGP` pour détourner du trafic ou tenter de masquer une autre attaque.

Aussi, la découverte d'un tel implant sur un équipement doit conduire à penser qu'il n'est pas le seul à être compromis.

Prévention et réaction

Vecteur d'infection initiale

D'après les sources publiques, le vecteur d'infection initiale ne serait pas basé sur l'exploitation d'une vulnérabilité des routeurs, mais plutôt sur l'utilisation de données de connexion légitimes (mots de passe faibles, par défaut, ou obtenus par un autre biais) ou en accédant physiquement au matériel.

Prévention

Étant donné le vecteur d'infection initiale supposé, la prévention passera par la sécurisation de l'accès aux équipements réseau (a minima: mots de passe forts, non stockés en clair) ainsi que leurs locaux et de façon plus générale, par le durcissement de la configuration des périphériques (suppression des services inutiles, journalisation des événements, etc.). Il conviendra de respecter scrupuleusement (et mettre en place le cas échéant) les procédures visant à s'assurer que le socle de base que constituent les équipements réseau est solide. Notamment, concernant les systèmes installés sur ces équipements :

- ils doivent provenir directement du constructeur (et pas d'un réseau pair-à-pair ou d'un site non officiel) ;
- leur intégrité doit être vérifiée avant installation (et périodiquement après) ;
- les modifications de leur configuration doivent être maîtrisées et contrôlées ;
- les mises à jour de sécurité doivent être appliquées.

Sur les équipements supportés, l'activation du démarrage sécurisé (*secure boot*) est devenue indispensable.

En cas de détection

Les victimes sont invitées à prendre contact avec le CERT-FR.

Documentation

- SYNful Knock - A Cisco router implant - Part I
  https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html
- SYNful Knock - A Cisco router implant - Part II
  https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis0.html
- SYNful Knock - A CISCO IMPLANT
  https://www2.fireeye.com/rs/848-DID-242/images/rpt-synful-knock.pdf
- In Search of SYNful Routers
  https://zmap.io/synful/
- SYNful Knock
  http://blog.shadowserver.org/2015/09/21/synful-knock/
- SYNful Knock: Detecting and Mitigating Cisco IOS Software Attacks
  https://blogs.cisco.com/security/synful-knock
- Talos Rules 2015-09-15
  https://snort.org/advisories/talos-rules-2015-09-15
- Cisco IOS Software Integrity Assurance
  https://www.cisco.com/web/about/security/intelligence/integrity-assurance.html
- Offline Analysis of IOS Image Integrity
  https://blogs.cisco.com/security/offline-analysis-of-ios-image-integrity

- Cisco Trust Anchor Technologies
  https://www.cisco.com/web/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf
- Cisco Guide to Harden Cisco IOS Devices
  https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- Outils de détection de "SYNful Knock" mis à disposition par FireEye
  https://github.com/fireeye/synfulknock
- Talos Intel - Synful Knock Scanner
  http://talosintel.com/scanner/
- Evolution in Attacks Against Cisco IOS Software Platforms
  http://tools.cisco.com/security/center/viewAlert.x?alertId=40411
- Cisco Event Response: SYNful Knock Malware
  https://www.cisco.com/web/about/security/intelligence/ERP_SYNfulKnock.html

2 - Rappel des avis émis

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

- CERTFR-2015-AVI-402 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2015-AVI-403 : Multiples vulnérabilités dans Moodle
- CERTFR-2015-AVI-404 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2015-AVI-405 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2015-AVI-406 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-407 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-408 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2015-AVI-409 : Multiples vulnérabilités dans Google Chrome

Gestion détaillée du document

28 septembre 2015 version initiale.