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 26 décembre 2014
N° CERTFR-2014-ACT-052

**Affaire suivie par :**
CERT-FR

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTFR-2014-ACT-052**

## 1 - Le *DNS sinkholing*

### Introduction

Le *DNS sinkholing* (littéralement « trou d'évier DNS ») ou *DNS blackhole* (« trou noir DNS »), est une technique utilisée principalement dans la lutte contre les programmes malveillants. Le principe est de rediriger les noms de domaine malveillants vers un ou plusieurs serveurs non maîtrisés par les attaquants, afin d'empêcher les postes compromis de recevoir des commandes.

### Intérêts

Le *DNS sinkholing* a plusieurs utilités. Tout d'abord, il vise à neutraliser certains effets indésirables des logiciels malveillants. En effet, certains programmes, tels que les *Remote Administration Tools* (RAT), s'ils sont déconnectés de leurs serveurs de commandes et de contrôle (CC), peuvent totalement cesser de fonctionner. Dans d'autres cas, le programme pourra garder une certaine autonomie, mais il échappera tout de même au contrôle de l'attaquant et ne pourra probablement plus exfiltrer de données.

Le deuxième intérêt du *sinkholing* est la possibilité d'analyser le trafic reçu. Le protocole peut potentiellement être décodé afin de récupérer les informations transmises par le client compromis. Des statistiques peuvent aussi être compilées, telles que le nombre de postes touchés, la répartition par pays, par domaine d'activité d'entreprises, etc. De nombreuses sociétés travaillant dans le domaine de la lutte contre la cybercriminalité utilisent cette technique pour réaliser leurs statistiques et pour démanteler des *botnets*. Toutefois, le détournement de domaines compromis sur Internet pose des questions de confidentialité, puisque le détenteur du « faux » serveur de CC peut être amené à récupérer des données issues des systèmes compromis.

Lors de l'analyse réseau d'un domaine, si l'on observe une adresse IP qui résout de nombreux domaines malveillants, il est possible que cela corresponde à un *sinkhole*. Pour s'en assurer, un *whois* ou une requête DNS inverse pourra lever le doute.

### Description technique

#### Serveurs

La première étape de la création d'un *DNS sinkhole* se fait par l'installation d'un serveur DNS qui va rediriger les noms de domaine configurés vers un ou plusieurs serveurs d'analyse. Il est également recommandé d'installer un second serveur qui va écouter sur les ports classiques utilisés par les programmes malveillants (80, 443, 8080, etc.) et envoyer une réponse standard pour toutes les requêtes reçues. En plus de répondre aux requêtes, une capacité de capture de trafic peut être utilisée pour enregistrer et analyser les informations envoyées par le client infecté préalablement prévenu.

**Redirection DNS**

Afin de détourner le trafic CC vers le serveur d'analyse choisi, il faut que la réponse DNS apportée au client soit modifiée. Cette réponse peut être modifiée à différents niveaux :

- sur un SI maîtrisé, le serveur cache DNS récursif peut posséder des entrées statiques redirigeant les domaines entrés vers une adresse IP interne. Cela permet de protéger les utilisateurs de son propre réseau ;
- sur Internet, la seule solution est de passer par une société d'enregistrement DNS. On peut modifier l'enregistrement du domaine malveillant ou bien demander à un niveau de domaine supérieur, par exemple au niveau du TLD. Mais cela nécessite de prouver à la société en charge du nom de domaine la légitimité de la demande.

L'adresse IP retournée au client peut être soit une IP non routable, par exemple 127.0.0.1, qui permet d'empêcher la communication avec le CC, soit une IP interne, typiquement le serveur chargé d'analyser le trafic malveillant.

**Documentation**


1 Description du *DNS sinkholing* par le SANS :
http://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523
2 Règles Emerging Threats sur les plages d'adresses IP *sinkhole* Microsoft :
http://doc.emergingthreats.net/bin/view/Main/2016102
3 Règles Emerging Threats sur les plages d'adresses IP *sinkhole* Google :
http://doc.emergingthreats.net/bin/view/Main/2016104
4 Règles Emerging Threats sur les plages d'adresses IP *sinkhole* Anubis :
http://doc.emergingthreats.net/bin/view/Main/2018455


# 2 - Rappel des avis émis

Dans la période du 22 au 25 décembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-537 : Multiples vulnérabilités dans NTP ntpd
- CERTFR-2014-AVI-538 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2014-AVI-539 : Multiples vulnérabilités dans Apple OS X
- CERTFR-2014-AVI-540 : Vulnérabilité dans PHP
- CERTFR-2014-AVI-541 : Multiples vulnérabilités dans Huawei

# Gestion détaillée du document

**26 décembre 2014** version initiale.