

GOURAUD Elie

KOWAL Jérémy

DUT RT Chalons en Champagne

Année universitaire 2020-2021

Rapport de projet : sécurité offensive

Remerciements

Merci à Madame Gobillard Delphine et Monsieur Melcior Michel.

Mots clés

Botnet : « Botnet » est une contraction des termes « robot » et « network » (réseau). Les cyber-criminels utilisent des chevaux de Troie spéciaux pour violer la sécurité des ordinateurs de différents utilisateurs, prendre le contrôle de chacun de ces ordinateurs infectés et les regrouper au sein d'un réseau de « bots » gérables à distance.

Bot : Hôte infecté et faisant partie du botnet.

Botnet Master : Entité de contrôle d’un botnet

Obfuscation : Méthode de camouflage de code et de dissimulation d’action.

Payload : « Charge utile » élément permettant un piratage.

Exploit : Désigne l’exploitation d’une faille de sécurité.

Combolist : C’est une liste regroupant login et mot de passe sous la forme login :password

ESX : serveur VMware pour faire de la virtualisation.

Sommaire

**Introduction**

**1.Etude de cas**

- Analyse d’un squelette

- Environnement de déploiement

**2. Master et serveur C&C**

- Infrastructure

- Charge utile

- Détection et camouflage

- Structure et analyse

**3. Scénario et infection**

- Infrastructure de test

- Environnement de déploiement

Introduction

Le sujet vise à développer un Botnet à usage éducatif, dans le but d’occuper un réseau type entreprise, de recueillir des informations sensibles, ainsi que d’asservir les hôtes à différentes tâches.

Dans le bus d’étudier l’utilité ainsi que les méthodes utilisées actuellement par les pirates pour comprendre et envisager des contre-mesures.

Le sujet répond donc à la probatique :

**Peut-on privilégier l’attaque pour mieux défendre ?** ou l’étude et le développement d’un botnet pour en étudier les contre-mesures à adopter.

1. **Etude de cas**

**A - Analyse d’un squelette**

Mirai Botnet

Type d’architecture : auto-propagation

Infrastructure : C&C

Spécificités :

- Blacklist composé d’adresse IP des sites gouvernementaux.

- Table de type combolist de login par défaut d’IoT.

Carte de prolifération : **Annexe A1**

Le Botnet Mirai est le plus connus des botnets, car il a sévèrement sévi sur internet, réalisant des attaques DDoS sur des infrastructures web et serveurs, notamment pour avoir DDoS le site web d’un journaliste ayant critiqué le botnet dans un article. Il est également connu pour être l’architecture de base des botnets actuels.

Rustock Botnet

Type d’architecture : auto-propagation

Infrastructure : C&C

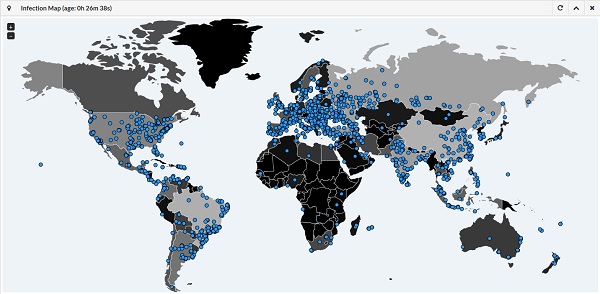
Spécificités : propagation accrue

Carte de prolifération : **Annexe A2**

Rustock est connu pour avoir été l’un des premiers botnets démantelé par Microsoft et le FBI, il reste aujourd’hui le botnet avec la vitesse de propagation la plus élevé de l’histoire avec 12 millions de spams par minutes, soit 17.28 milliards de spams par jours

**ANNEXES**

**A1**



**A2**

