Cybercrime : l'ANSSI attire l'attention sur Silence

Nom : Silence. Origine : supposément russophone. Âge : au moins quatre ans. Cible de prédilection : les banques. Rayon d'action : Afrique, Asie et Europe.

L'ANSSI a récemment dédié un rapport à ce groupe cybercriminel qu'elle dit avoir été « particulièrement actif au cours de l'année 2019 ».

L'élargissement de son périmètre d'attaque est allé de pair avec sa montée en compétence.

Dans l'affaire, la France n'a peut-être pas été épargnée. L'ANSSI en veut pour preuve une dizaine d'adresses IP qui ont communiqué avec l'infrastructure de commande et de contrôle (C2) de Silence.

IP	Fournisseur	Pays	Programme	Annee
5.39.30.110	OVH	France	Silence.Downloader	09-2016
54.36.191.97	OVH	France	Silence.Downloader	10-2017
164.132.228.29	OVH	France	Silence.Downloader	06-2017
137.74.224.142	OVH	France	Silence.Downloader	08-2017
92.222.68.32	OVH	France	Silence.Downloader	04-2017
139.99.156.100	OVH	France	Exploit	10-2017
149.56.131.140	OVH	France	Meterpreter	08/10-2017
51.255.200.161	OVH	France	Exploit CVE-2017-0199	06-2017
109.13.212.72	SFR SA	France	pakovelli@mail.com	08-2017

L'une de ces adresses (5.39.30.110) a été résolue, entre août 2012 et juin 2019, par le nom de domaine cours-a-domicile.fr. Ce qui peut trahir une tentative de hameçonnage ciblé contre des entités francophones.

Mode opératoire : ça commence par du *phishing*

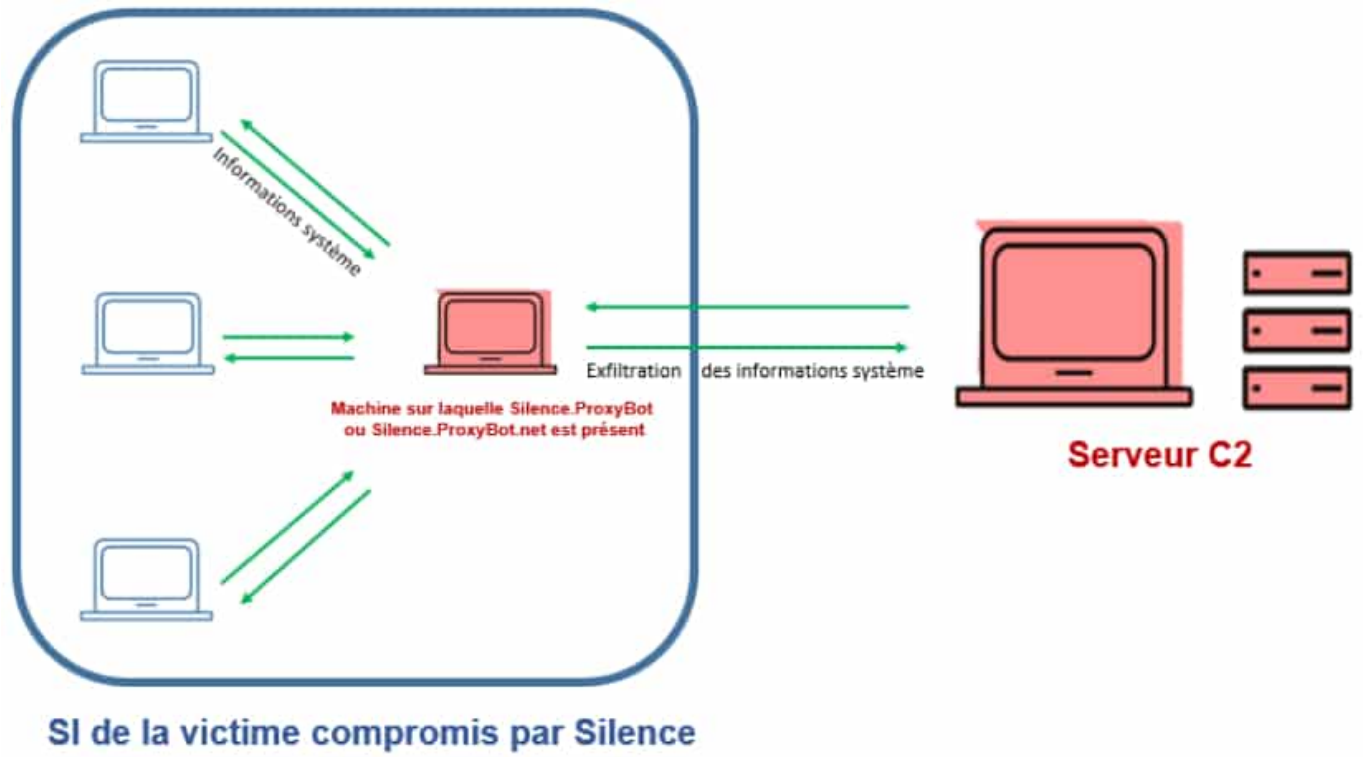
Silence cible généralement ses victimes au travers d'e-mails usurpant l'image d'institutions financières. Y compris en utilisant les adresses d'employés d'institutions dont le SI a déjà été compromis.

Les mails peuvent contenir plusieurs types de pièces jointes malveillantes :

- un document Word avec une macro ou un exploit ;
- une archive zip ou rar contenant un fichier CHM (HTML compilé, ouvert par défaut avec le programme d'aide HTML de Microsoft) ;
- un document qui exploite les failles CVE-2017-0199 (compromission d'Office par dissimulation d'instructions malveillantes dans un fichier RTF) et CVE-2017-11882

(exécution de code à distance dans Office lorsque celui-ci ne parvient pas à gérer correctement les objets en mémoire) ;
- un fichier .lnk (utilisé pour diriger vers un exécutable sur Windows).

Tous ces vecteurs déclenchent la propagation de l'outil d'administration à distance Truebot, qui va communiquer avec le C2.
Silence a parfois recours à un utilitaire proxy pour pouvoir atteindre les éléments locaux du réseau compromis qui ne sont pas accessibles à distance.



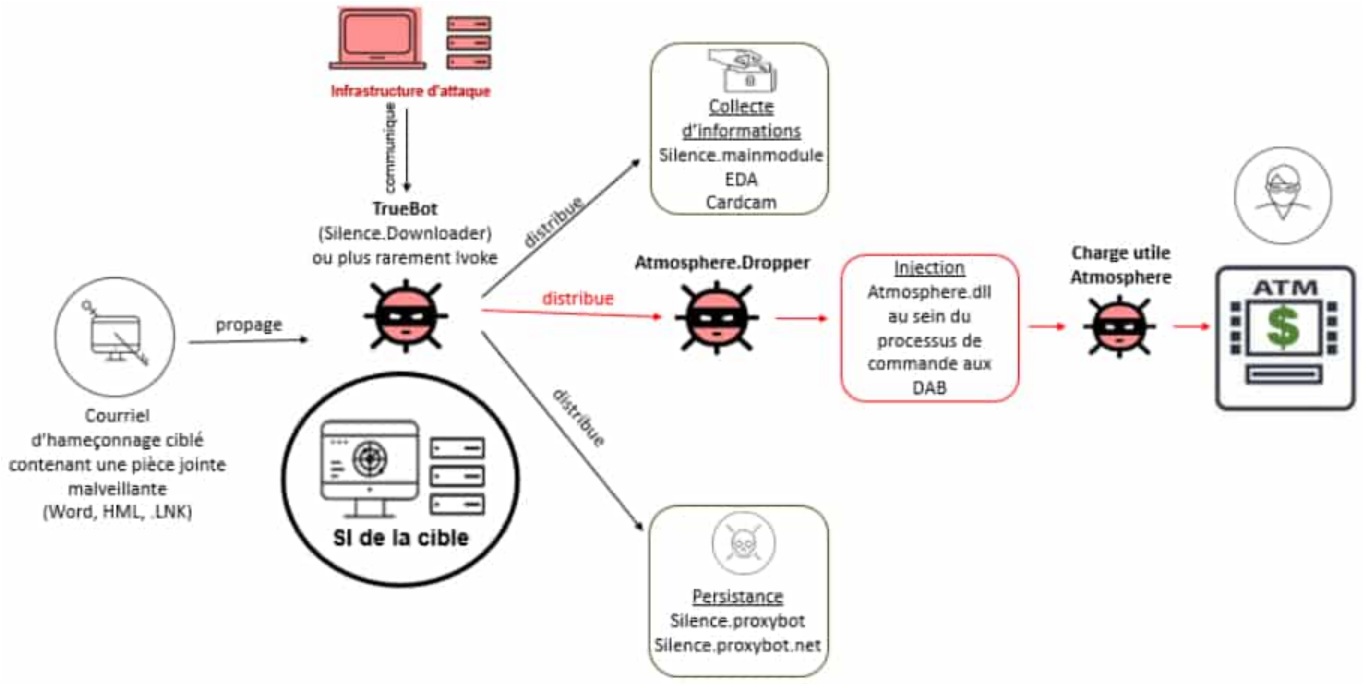
Plafond relevé

Plusieurs codes malveillants permettent la récupération et l'envoi de données sur le SI infecté. Dont l'utilitaire de capture d'écran et de vidéo Cardcam.

À partir de là, Silence peut tenter une intrusion dans l'application de gestion des distributeurs automatiques de billets (DAB) de la banque visée.

Truebot distribue une charge utile qui repère ladite application et son processus qui transmet des commandes au DAB. Il y injecte une DLL qui permet de :

- Récupérer des informations sur le contenu des cassettes
- Contrôler à distance les retraits
- Contrôler physiquement le DAB en tapant une combinaison spécifique sur le clavier



Silence s'en prend parfois aussi à des systèmes de traitement de cartes bancaires. Objectif : accroître les plafonds de retrait et de découvert de CB préalablement activées. Ces accroissements ont l'avantage d'être valables sur tout DAB, peu importe sa localisation et sa banque gestionnaire.

Entre juin 2016 et juin 2019, Silence aurait dérobé l'équivalent de 4,2 millions de dollars. Avec un hold-up à 3 millions contre la banque bangladaise Dutch-Bangla Bank.
Dénominateur commun à de nombreuses banques infectées : l'absence de conformité PCI DSS. Ce qui fait de l'Asie une cible d'intérêt premier.

Illustration principale © slimmer_jimmer via *VisualHunt / CC BY-NC-ND*