LE GROUPE CYBERCRIMINEL SILENCE

Date de création	22/10/2019
Date de publication	23/04/2020
Acteur(s) offensif(s) concerné(s)	Criminalité
Secteur(s) d'activité concerné(s)	Finance
Résumé opérationnel	Silence est un groupe de cybercriminels supposément russophone, actif depuis 2016, et ciblant des institutions financières à travers le monde. Depuis ses débuts, leur degré de sophistication s'est accru, de sorte qu'ils utilisent désormais une infrastructure d'attaque qu'ils ont eux-même créé afin d'opérer des retraits frauduleux aux distributeurs automatiques de billets.

	Acronyme	Désignation	Définition
Faits	**(C)**	Constaté	Informations vérifiées par l'agence ou des partenaires nationaux.
	(NV)	Non vérifiable	Non vérifiable avec les capacités de l'agence.
Commentaires	**(I)**	Interprétation	Information déduite des éléments constatés ou non vérifiables à la disposition de l'agence.
	(HYP)	Hypothèse	Hypothèse.

Sommaire

1 Ciblage privilégié de Silence : les banques

Silence[1] est un groupe de cybercriminels, supposément russophones et indépendants, actif depuis 2016. Il ciblait alors en particulier des banques de pays de la CEI (Russie, Biélorussie, Moldavie, Arménie, Kazakhstan, etc.) et d'Ukraine, mais a depuis étendu son périmètre à une trentaine de pays en Europe (dont l'Allemagne, la Suisse, le Royaume-Uni et l'Autriche), en Asie (dont Israël, la Turquie, Taïwan, la Malaisie et la Corée du Sud) et en Afrique (dont le Ghana et le Kenya) [1].

D'après Group-IB [1, 2], des adresses IP localisées en France auraient communiqué avec l'infrastructure de commande et de contrôle (C2) de Silence en 2019, ce qui était apparemment déjà le cas en 2016 et 2017.

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'adresse IP 5.39.30.110 (OVH) a été utilisée comme serveur C2 de Silence.Downloader en septembre 2016. Cette adresse IP a été résolue entre août 2012 et juin 2019 par le nom de domaine « `cours-a-domicile.fr` ». Cependant, une résolution DNS observée pendant aussi longtemps peut être le signe que le nom de domaine a été "abandonné". En outre, au cas où Silence ait utilisé le C2 pour faire de l'hameçonnage ciblé, cela pourrait indiquer un ciblage d'entités francophones. Ainsi, bien que l'ANSSI n'en ait pas eu connaissance, il n'est pas exclu que la France puisse être ciblée, ou qu'elle l'ait déjà été.

L'une des sources de profit de ce groupe cybercriminel réside dans la manipulation de distributeurs automatiques de billets (DAB), bien qu'ils ne se limitent pas qu'à cette activité, adaptant leurs outils à l'environnement compromis. En effet, alors que lors de ses première attaques, Silence utilisait des outils développés par d'autres cybercriminels[2] les outils et codes malveillants qu'il utilise actuellement ont majoritairement été développés par ses membres (Silence, Atmosphere, Farse et Cleaner[3]) [2, 1].

Généralement, après compromission du SI de la victime, le serveur C2 de Silence propage une charge utile contenant plusieurs modules et permettant aux attaquants :

- soit d'accroître les plafonds de retraits aux DAB, ainsi que les plafonds de découverts des cartes de clients via l'intrusion dans le système de traitement de cartes bancaires (*card processing*) de la banque ;
- soit de prendre le contrôle des DAB de la banque, via l'intrusion dans son application de gestion des DAB.

Des retraits simultanés sont dans les deux cas réalisés par des mules[4].

En 2016, le groupe Silence a également cherché à deux reprises à émettre des virements frauduleux depuis le système de transfert interbancaire russe AWS CBR (équivalent russe de Swift) [2].

Au total, de juin 2016 à juin 2019, Silence aurait dérobé environ 4,2 millions de dollars à des banques [1].

Le groupe Silence est apparu particulièrement actif au cours de l'année 2019 et mérite donc une attention particulière. En effet, de septembre 2018 à août 2019, Group-IB décompte déjà 16 campagnes de Silence [1], et au moins 7 campagnes concluantes :

[1] FireEye dénomme TEMP.TruthTeller ce qu'il considère être une partie de l'activité de Silence. Pour Crowdstrike, Silence se réfère à Whisper Spider.
[2] Par exemple, ils utilisaient la porte dérobée Kikothac, développée par un tiers, avant de concevoir leur porte dérobée Silence.MainModule.
[3] Cet outil sert à supprimer les traces d'une connexion à distance des attaquants au sein du SI de la victime.
[4] Individu qui transfère des fonds d'origine frauduleuse via différents comptes bancaires dans différents pays.

- en mai 2018 et février 2019, le groupe Silence a attaqué deux banques indiennes ;
- en février 2019, il a dérobé à la banque russe Omsk IT Bank environ 400000 dollars ;
- en mai 2019, il a dérobé à la banque bangladaise Dutch-Bangla Bank environ 3 millions de dollars ;
- en juin 2019, il a attaqué des banques russes ;
- en juillet 2019, il a attaqué des banques au Chili, au Costa Rica, en Bulgarie et au Ghana.

2 Mode opératoire

2.1 Compromission

Silence cible ses victimes au travers de courriels d'hameçonnage usurpant l'image d'institutions financières. Parfois, les courriels proviennent d'adresses légitimes d'employés d'institutions dont le SI a déjà été compromis [3], les rendant d'autant plus crédibles.

Ces courriels contiennent une pièce jointe malveillante :

- soit sous la forme d'un document Word contenant une macro ou un exploit ;
- soit sous la forme d'un fichier ZIP ou RAR contenant un fichier CHM[5] ;
- soit sous la forme d'un document exploitant les CVE-2017-0199[6] et CVE-2017-11882[7] qui télécharge et exécute un fichier HTA contenant un VBScript ;
- soit sous la forme d'un fichier .lnk[8].

En guise de phase préparatoire, il arrive également que Silence envoie massivement des milliers de courriels à travers le monde dans le but de mettre à jour sa base de données des adresses courriel actives de ses cibles et d'étendre son périmètre géographique d'attaque. Ces courriels contiennent une image ou un lien mais sont dépourvus de charge malveillante [1]. Group-IB a ainsi constaté trois campagnes de ce type visant la Russie, les pays de l'ex-Union soviétique, l'Asie, l'Europe et la Nouvelle-Zélande en 2018.

2.2 Propagation

En cliquant sur la pièce jointe malveillante, la victime déclenche la propagation automatique au sein du système d'information (SI) de l'outil d'administration à distance Truebot (ou Silence.Downloader). Ce code malveillant, en communiquant avec le C2, est utilisé pour propager d'autres charges utiles.

Lors de campagnes plus récentes (en mai 2019), Group-IB a identifié la propagation du code malveillant Ivoke en tant que première charge utile, plutôt que celle de Truebot [1].

En outre, Silence utilise parfois un utilitaire proxy, Silence.ProxyBot (Turncard) ou Silence.ProxyBot.net (Fourthstreet), qui forme un proxy entre les machines compromises et le serveur C2, afin de pouvoir atteindre les éléments locaux du réseau compromis qui ne sont pas accessibles à distance.

[5] Les fichiers CHM sont des fichiers HTML compilés. Lorsqu'un utilisateur Windows ouvre un fichier CHM, Windows lance le programme d'aide HTML de Microsoft afin d'afficher le fichier HTML compilé. En modifiant le fichier d'aide légitime pour inclure un contenu malveillant se déclenchant lorsque la documentation est affichée (par exemple lancement d'une commande PowerShell), un attaquant peut compromettre un SI.

[6] Faille dans Office découverte en mars 2017 permettant de dissimuler des instructions malveillantes dans un document sauvegardé au format .RTF.

[7] Vulnérabilité d'exécution de code à distance existant dans le logiciel Microsoft Office lorsque celui-ci ne parvient pas à gérer correctement les objets en mémoire, découverte en novembre 2017.

[8] Fichier utilisé pour diriger vers un fichier exécutable sous Windows.

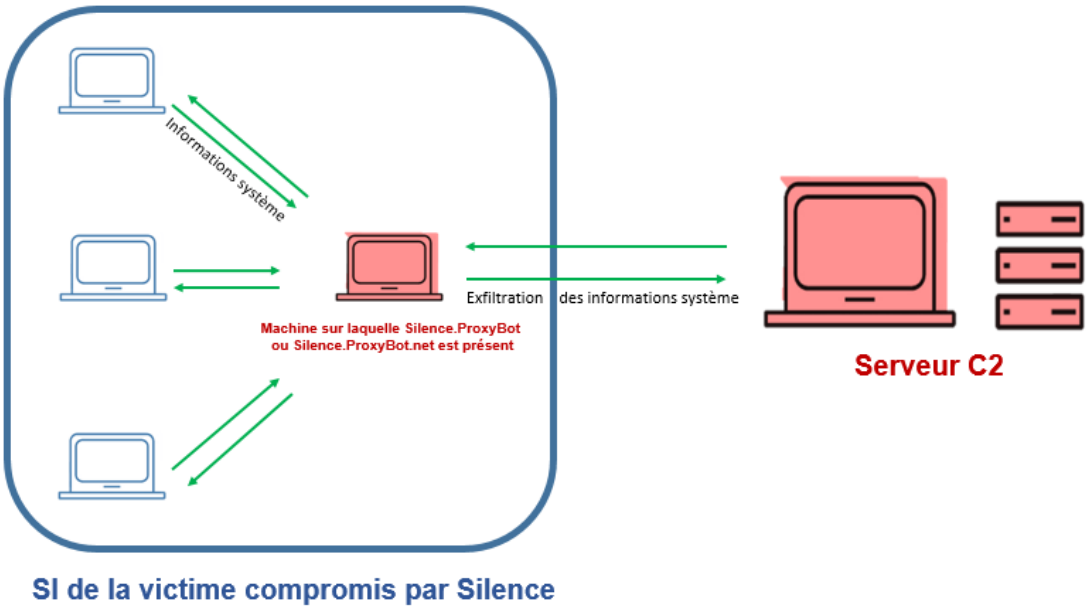

Fig. 2.1 : Exfiltration d'informations système via un utilitaire proxy

Silence récupère des informations, exfiltre des données ou télécharge des fichiers au sein du SI par le biais d'au moins trois codes malveillants possibles :

- Slowroll (Silence.Mainmodule) : cette porte dérobée communique directement avec le serveur C2 ou par le biais d'un serveur proxy ;
- EmpireDNSAgent (EDA) : cet outil, basé sur Empire et sur dnscat2te, est une porte dérobée, distribuée par Slowroll, et communiquant avec le serveur C2 par tunnel DNS ;
- Cardcam[9] : cet utilitaire réalise des captures d'écran ainsi que des enregistrements vidéo du système compromis, afin de permettre aux attaquants de comprendre le fonctionnement de l'entité victime et d'identifier les logiciels qu'elle utilise.

2.3 Exécution de l'attaque

2.3.1 Accès à l'application de gestion des DAB

CEN/XFS est un standard avec lequel la majorité des fabricants de DAB (Diebold, Wincor, NCR) sont en conformité. Du fait de l'interprétation variée que ces fabricants avaient de ce standard, il est devenu répandu d'utiliser le gestionnaire XFS (*XFS manager*). C'est un intergiciel (*middleware*) qui fournit une architecture client-serveur pour l'application Windows qui gère les DAB. Il représente donc l'interface entre l'application et le DAB.

[9] Identifié par Kaspersky en novembre 2017, il est dénommé Cardcam par FireEye.

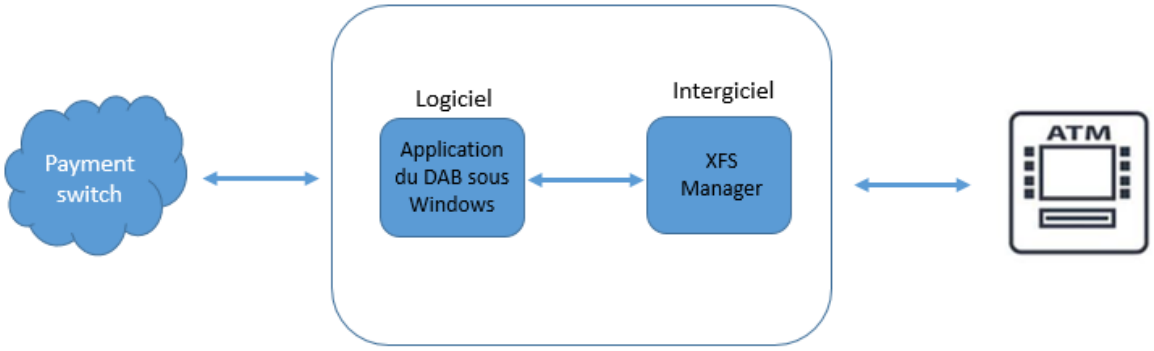

Fig. 2.2 : Interactions avec le DAB

Commentaire : toute application développée en conformité avec le standard XFS pourrait prendre le contrôle d'un DAB. En effet, le standard XFS unifie le fonctionnement des applications avec tout DAB. Développé en tenant compte de la logique de ce standard, une application, légitime ou malveillante, est capable d'administrer des objets de bas niveau au niveau d'un DAB [4].

Truebot distribue Atmosphere.Dropper dans le SI de la victime. Atmosphere.Dropper repère l'application de gestion des DAB et son processus dont la fonction est de transmettre des commandes aux DAB. Par exemple, pour les DAB du fabricant Wincor-Nixdorf, ce processus s'appelle fwmain32.exe.

Une fois le processus repéré, Atmosphere.Dropper ou Atmosphere.Injector (lui-même distribué par Atmosphere.Dropper), y injecte la *dynamic link library* (DLL)[10] Atmosphere. Celle-ci permet à l'attaquant d'activer la charge utile Atmosphere.

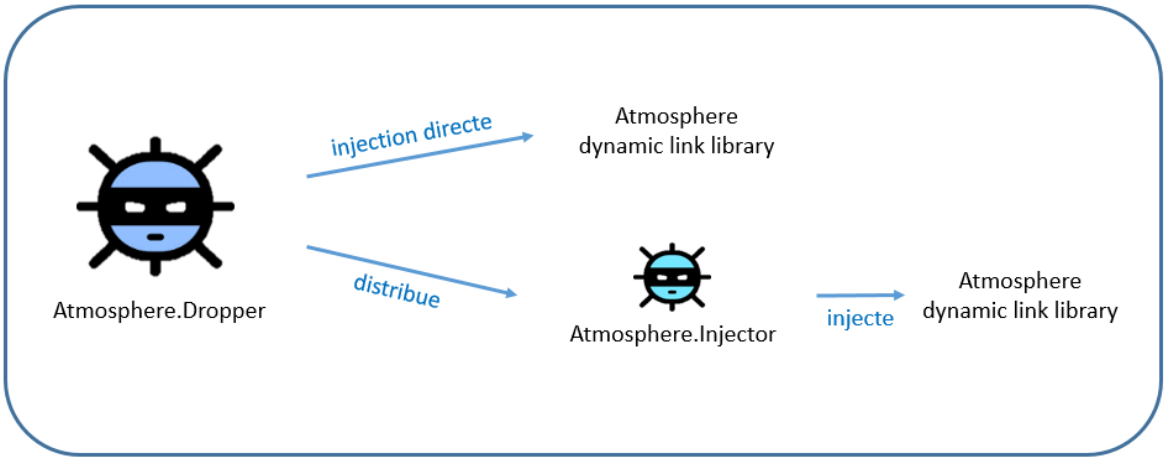

Fig. 2.3 : Injection de la DLL malveillante au sein du processus légitime de commande aux DAB

Une fois activée, elle permet aux attaquants :

- d'exécuter une commande pour récupérer des informations sur le contenu des cassettes du DAB ;
- de contrôler à distance les retraits d'argent, en envoyant une commande au DAB ;
- ou de contrôler physiquement le DAB, en tapant une combinaison spécifique sur le clavier du DAB.

[10] Une DLL est une bibliothèque logicielle, contenant du code et des données, dont les fonctions sont chargées en mémoire par un programme au besoin lors de son exécution.

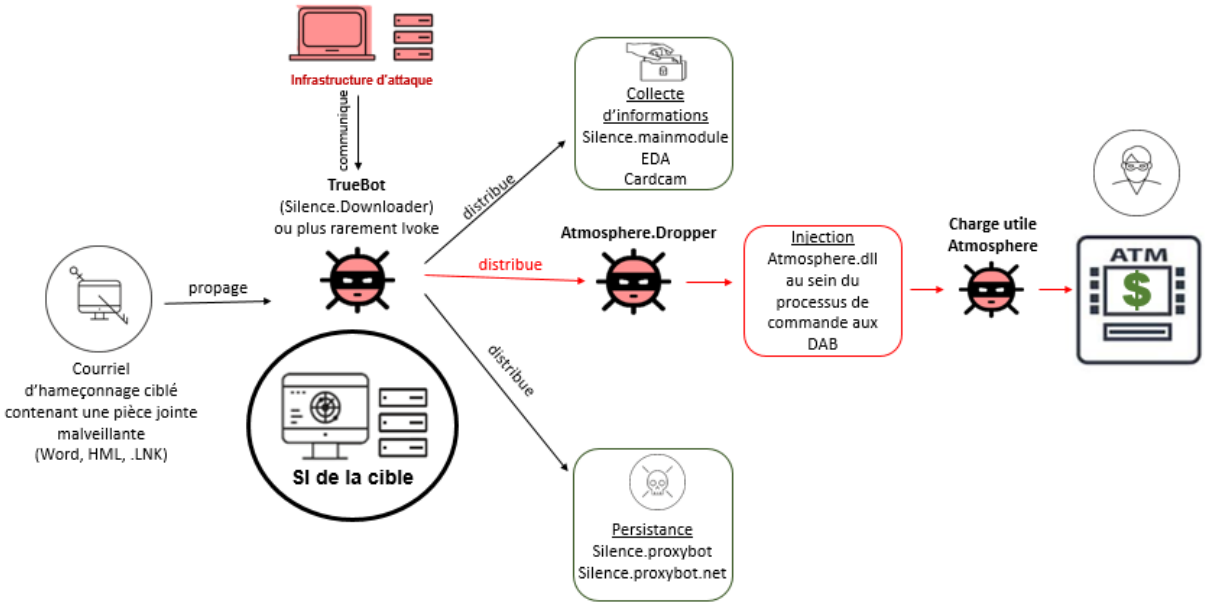

Fig. 2.4 : Mode opératoire de Silence résultant en des retraits frauduleux aux DAB

Commentaire : Cette technique de repérage du processus de commande des DAB et d'injection d'une DLL malveillante n'a semble-t-il pas été inventée par Silence, comme en attestent des éléments en source ouverte, datant de 2009 [5]. En outre, cette technique n'est pas la seule permettant de compromettre un DAB. Le MOA Lazarus utiliserait par exemple un code malveillant interceptant les demandes de retraits frauduleuses de leurs mules afin d'autoriser le retrait sans que l'application légitime de la banque n'en ait eu connaissance.

2.3.2 Accès au système de traitement de cartes bancaires

Afin d'effectuer des retraits frauduleux aux DAB, Silence essaierait parfois d'accéder au système de traitement de cartes bancaires (*card processing*) au sein du SI de la banque victime afin de retirer les plafonds de retrait et de découvert de cartes bancaires préalablement activées, puis enverrait des mules retirer l'argent.

Commentaire : Lorsque des attaquants ont accès au système de traitement de carte, l'argent peut être retiré dans n'importe quel DAB de n'importe quelle banque depuis n'importe quel pays. En revanche, lorsque des attaquants compromettent directement l'application de gestion de DAB, les mules doivent se déplacer là où se trouve la banque victime afin de pouvoir retirer l'argent. Ce fût le cas lors de l'attaque de Silence contre la banque bangladaise DBBL en mai 2019 [6].

Afin d'accéder au système de traitement de carte, Silence compromettrait le compte avec privilèges d'un employé de la banque victime, en récupérant son mot de passe par le biais de l'outil Farse. Cet outil est une version modifiée de Mimikatz (dont le code source est disponible sur Github).

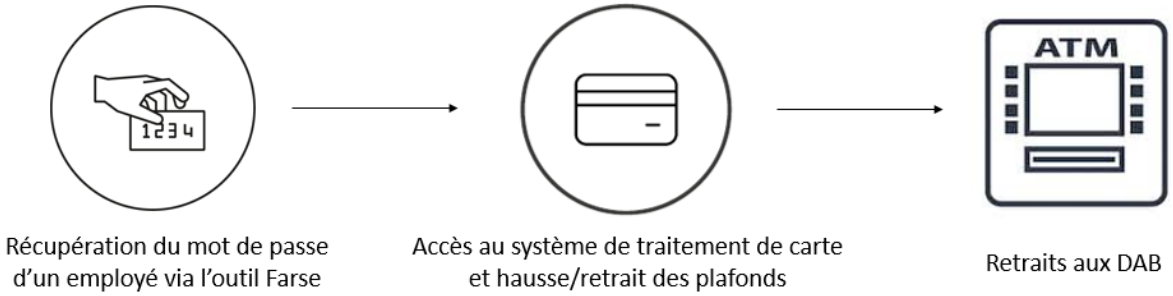

Fig. 2.5 : Compromission du système de traitement de carte

Commentaire : Des exfiltrations de données clients au sein d'entreprises de système de paiement/retrait tels que Mastercard ou Visa peuvent conduire à leur vente sur le Dark Web, et à leur utilisation par des cybercriminels à des fins de clonage de cartes bancaires. Ces cartes peuvent ensuite servir aux mules lors de retraits frauduleux aux DAB. Par exemple, l'exfiltration de données dont a été victime MasterCard en août 2019 pourrait avoir servi à de telles fins.

3 Liens entre Silence et TA505

D'après Group-IB, Truebot et FlawedAmmyy.Downloader[11] auraient été développés par une même personne russophone. Or, FlawedAmmyy.Downloader aurait été utilisé depuis 2016 au cours de campagnes d'hameçonnage aussi bien massives que ciblées, dont la plupart serait le fait de TA505 [7, 8, 9]. .

Commentaire : FlawedAmmyy et Truebot auraient d'ailleurs été développés en 2016, année au cours de laquelle le groupe Silence a émergé, alors que TA505 était déjà actif depuis 2014.

Enfin, aussi bien TA505 que Silence utilisent parfois des fichiers .lnk en guise de pièce jointe malveillante au sein de leurs courriels d'hameçonnage, pour respectivement délivrer FlawedAmmyy.downloader et Truebot. Or l'usage de ce format de fichier est rare.

Comme évoqué par Group-IB [10], il se pourrait que les liens entre TA505 et Silence soient dus au fait que Silence achète des accès aux SI de banques, notamment à TA505. Cet achat d'accès serait corrélé à la baisse d'envois de courriels d'hameçonnage par Silence.

A ce titre, fin 2019, TA505 aurait ouvert l'accès au SI d'au moins une banque en Europe à Silence [11].

4 Conclusion

A ses débuts, Silence commettait des erreurs au cours de ses attaques, et mimait des techniques provenant d'autres groupes. Par exemple, le fait de prendre des captures d'écran des postes infectés des employés de la banque victime proviendrait de Carbanak[12]. Aujourd'hui, Silence est l'un des groupes cybercriminels les plus actifs et sophistiqués contre le secteur bancaire.

Les attaques de Silence seraient facilitées par l'absence de conformité PCI DSS[13] des banques victimes. Par exemple, une attaque récente de Silence sur la Dutch Bangladesh Bank Limited (DBBL) ayant provoqué le retrait de 3 millions de dollars, a été facilitée par le fait que la DBBL n'appliquait pas la norme PCI DSS, tout comme 95% des banques présentes au Bangladesh, mais aussi comme un certain nombre de banques en Asie. Ces banques sont par conséquent des cibles plus propices aux attaques de Silence que les banques européennes, bien que Silence s'en prenne depuis le second semestre 2018 à des banques de tous horizons, Europe incluse. Cet élargissement du périmètre d'attaque de Silence est concomitant à sa montée en compétence.

[11] FlawedAmmyy est un outil d'accès à distance (*remote access trojan*) basé sur la fuite du code source du logiciel légitime Ammyy Admin en 2016, et contenant un *downloader* et une charge utile.

[12] Le code source de la porte dérobée Carbep, active depuis 2010, a fuité en 2013. De Carbep auraient été dérivés les codes malveillants Anunak et Carbanak. Ces deux codes malveillants ont été utilisés de 2013 à 2015 par le groupe communément appelé Carbanak dans le cadre d'attaques ciblées sur des banques et des systèmes de paiement dans une trentaine de pays afin de dérober plus d'un milliard de dollars.

[13] Certification mondiale assurant la sécurité des données (cartes et données bancaires) traitées. Elle s'applique aux différents acteurs de la chaîne monétique, et incite à 300 contrôles de sécurité. Être en conformité avec PCI DSS c'est notamment sauvegarder les données de cartes bancaires des clients de manière sécurisée, notamment via le chiffrement, le contrôle en continu et les tests de sécurité de l'accès aux données des cartes.

5 Bibliographie

[1] Group-IB, “SILENCE 2.0”. In : (août 2019).

[2] Group-IB, “Silence : Moving into the Darkside”. In : (sept. 2018).

[3] ReaQta. *Silence Group Targeting Russian Banks via Malicious CHM*. 24 jan. 2019. URL : https://reaqta.com/2019/01/silence-group-targeting-russian-banks/ (visité le 22/10/2019).

[4] Kaspersky. *Le Jackpot des distributeurs automatiques de billets : malwares et autres méthodes d’enrichissement*. 26 avr. 2016. URL : https://securelist.fr/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/64949/ (visité le 24/12/2019).

[5] Ne scrie caiafa verde. *Study on ATM Security : Code Injection on Wincor Nixdorf ATMs*. 3 juin 2009. URL : http://caiafaverde.blogspot.com/2009/06/study-on-atm-security-code-injection-on.html (visité le 30/10/2019).

[6] Bleeping Computer. *Silence Group Likely Behind Recent $3M Bangladesh Bank Heist*. 3 juil. 2019. URL : https://www.bleepingcomputer.com/news/security/silence-group-likely-behind-recent-3m-bangladesh-bank-heist/ (visité le 03/07/2019).

[7] Trend Micro. *FlawedAmmyy Malware Information*. 31 juil. 2019. URL : https://success.trendmicro.com/solution/1123301-flawedammyy-malware-information (visité le 04/11/2019).

[8] Proofpoint. *Leaked Ammyy Admin Source Code Turned into Malware*. 7 mar. 2018. URL : https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware (visité le 04/11/2019).

[9] TrendMicro. *TA505 At It Again - Variety Is the Spice of ServHelper and FlawedAmmyy*. 27 août 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/ (visité le 27/08/2019).

[10] Group-IB. *Group-IB Presents Its Annual Report on Global Threats to Stability in Cyberspace*. 29 nov. 2019. URL : https://www.group-ib.com/media/gib-2019-2020-report/ (visité le 24/12/2019).

[11] Group-IB, “New Financially Motivated Attacks in Western Europe Traced to Russian-Speaking Threat Actors”. In : (27 mar. 2020).