TLP:WHITE

INFRASTRUCTURE D'ATTAQUE DU GROUPE CYBERCRIMINEL TA505

AOÛT 2019 - FÉVRIER 2021

Version 1.0

10/02/2021

TLP:WHITE

Sommaire

Threat Actor 505 (TA505) est un groupe cybercriminel, actif depuis 2014. Il mène des campagnes d'hameçonnage, qui sont depuis 2019, régulièrement suivies d'actions de chiffrement par rançongiciel.

Un précédent rapport publié par l'ANSSI [1] en 2020 fournit une synthèse de la connaissance acquise sur ce groupe cybercriminel.

Ce document détaille l'infrastructure utilisée par TA505 lors des campagnes de distribution des implants **Get2** et **SDBbot** depuis 2019. Il contient également des indicateurs de compromission et des méthodes de détection.

1 Structure générale de l'infrastructure

L'activité du groupe cybercriminel TA505 remonterait à au moins 2014. Jusqu'en 2017, son activité semblait se concentrer sur la distribution de chevaux de Troie bancaires (**Dridex**, **TrickBot**) et de rançongiciels (**Locky**).

L'année 2018 a marquée un tournant dans ses méthodes d'attaques, TA505 distribuant de plus en plus de portes dérobées et cherchant désormais à déployer le rançongiciel **Clop** chez des entités à même de payer des rançons de montants élevés (*Big game hunting*).

De septembre 2019 à septembre 2020, le groupe cybercriminel TA505 a mené des campagnes de distribution de l'outil d'administration à distance **SDBbot**, apparemment spécifique à lui.

SDBbot est habituellement le précurseur du déploiement du rançongiciel **Clop**.

TA505 est également connu pour utiliser **TinyMet**/**Metasploit** et **CobaltStrike** après avoir obtenu un accès grâce à **SDBbot** [2].

1.1 Différents types de serveurs

Lors de ces campagnes, TA505 met en œuvre quatre types de serveurs communiquant directement avec les cibles et victimes :

- un serveur compromis utilisé afin de rediriger les victimes vers un serveur d'hameçonnage. Il est nommé serveur de redirection dans la suite du document ;
- un serveur d'hameçonnage qui délivre un fichier XLS contenant le téléchargeur **Get2** ;
- un serveur de commande et de contrôle pour **Get2** : le serveur et l'implant sont utilisés afin de délivrer **SDBbot** ;
- un serveur de commande et de contrôle pour la porte dérobée **SDBbot**.

Les analyses de l'ANSSI sur cette infrastructure ont permis de constater certains liens et usages généraux.

Ordre de grandeur du nombre de serveurs par types observés depuis août 2019 :

- serveurs de redirection : 600 ;
- serveurs d'hameçonnage : 120 ;
- serveurs **Get2** : 120 ;
- serveurs **SDBbot** : 25.

1.1.1 Relations entre types de serveurs

Généralement et à un instant donné, plusieurs serveurs de redirection pointent vers un même serveur d'hameçonnage [3] (relation *-1).

Au cours du temps, un serveur de redirection peut être réutilisé pour rediriger vers de nouveaux serveurs d'hameçonnage (relation 1-*).

Un serveur d'hameçonnage est exclusif à un serveur **Get2** et réciproquement (relation 1-1).

Un serveur **Get2** est exclusif à un serveur **SDBbot** mais plusieurs serveurs **Get2** peuvent délivrer des implants **SDBbot** utilisant le même serveur de commande et de contrôle (relation *-1).

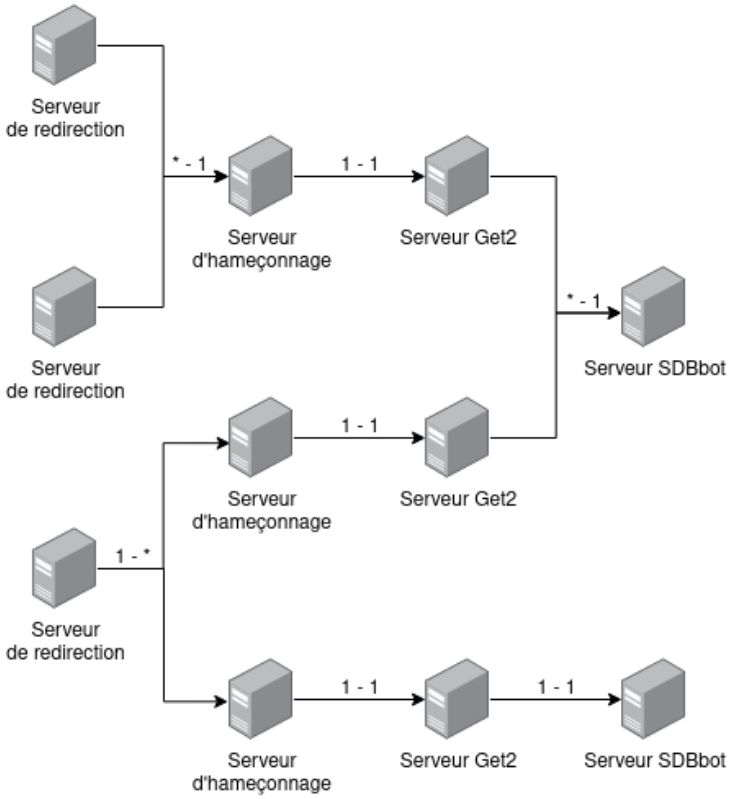

Fig. 1.1 : Liens entre les types de serveurs

1.1.2 Durée d'usage

Les serveurs d'hameçonnage et **Get2** sont généralement utilisés pendant une journée.

Les serveurs **Get2** délivrent différents implants **SDBbot** pointant vers le même serveur de commande et de contrôle pendant une à deux semaines. Les serveurs **SDBbot** restent ensuite actifs, mais aucun nouvel implant lié à ceux-ci n'est distribué par **Get2** [4]. Les serveurs **SDBbot** peuvent être utilisés durant plusieurs semaines et rester actifs plusieurs mois.

1.2 Noms de domaine

TA505 attribue un nom de domaine à chacun des serveurs de la chaîne d'infection, hormis les serveurs de redirection. Les serveurs de redirection sont des serveurs HTTP compromis et utilisés pour héberger un fichier HTML, leur nom de domaine original est utilisé.

2 Caractéristiques des serveurs par type

2.1 Serveurs de redirection

Depuis mars 2020, les liens présents dans les pièces jointes des courriels d'hameçonnage pointent vers des fichiers HTML au nom aléatoire hébergés sur des serveurs compromis [5]. Ces fichiers HTML font usage de JavaScript afin de rediriger les victimes vers un serveur d'hameçonnage.

Avant l'usage de serveurs de redirection, les pièces jointes contenaient un lien direct vers les serveurs d'hameçonnage. Des services de raccourcissement d'URLs ont ensuite été utilisé par le groupe cybercriminel.

Les investigations ont permis de découvrir 575 serveurs compromis utilisés comme serveurs de redirection, leur noms de domaine sont disponibles en annexe 7.2.

Le nombre élevé de serveurs HTTP compromis pourrait indiquer que le groupe cybercriminel TA505 achèterait des accès à d'autres groupes cybercriminels. La majorité des serveurs de redirection sont des serveurs HTTP délivrant du contenu statique et n'utilisant pas de système de gestion de contenu, ce qui rend leur exploitation plus complexe et difficilement automatisable. La méthode de compromission des serveurs HTTP est inconnue, mais est potentiellement indirecte, via la récupération d'identifiants FTP par exemple.

2.2 Serveurs d'hameçonnage

Les serveurs d'hameçonnage usurpent l'apparence de plateformes de partage de fichiers (OneDrive, DropBox, Box, OneHub...), afin d'amener la victime à télécharger un fichier XLS malveillant. Ce fichier contient le téléchargeur **Get2**. Les victimes sont amenées à visiter un serveur d'hameçonnage via des courriels d'hameçonnage.

Les noms de domaine des serveurs d'hameçonnage identifiés lors de nos analyses sont disponibles en annexe 7.1 et dans le fichier CSV joint à ce mémo.

2.3 Serveurs Get2

Les serveurs de commande et de contrôle **Get2** ont pour but de délivrer la porte dérobée **SDBbot** aux victimes d'intérêt de TA505.

Les noms de domaine des serveurs de commande et de contrôle **Get2** identifiés lors de nos analyses sont disponibles en annexe 7.1 et dans le fichier CSV joint à ce mémo.

2.4 Serveurs SDBbot

Les serveurs **SDBbot** permettent aux opérateurs de TA505 de contrôler les machines infectées. L'implant **SDBbot** offre plusieurs fonctionnalités aux opérateurs : l'exécution de commandes système, l'enregistrement vidéo de l'écran, l'accès au bureau à distance, la redirection de ports et l'accès au système de fichiers [6].

Les noms de domaine et adresses IP des serveurs de commande et de contrôle **SDBbot** identifiés lors de nos analyses sont disponibles en annexe 7.1 et dans le fichier CSV joint à ce mémo.

3 Utilisation d'hébergeurs « bulletproof »

Le groupe cybercriminel TA505 utilise régulièrement **TinyMet/Metasploit** et **CobaltStrike** après avoir obtenu un accès grâce à **SDBbot**.

TA505 a utilisé au moins deux hébergeurs *bulletproof*[1] pour héberger des serveurs de commande et de contrôle **Metasploit** et **CobaltStrike**.

3.1 VPSSC

IBM X-Force et Vikas Singh ont relevé l'utilisation de l'hébergeur *bulletproof* VPSSC Networks LTD par TA505 [7] [8]. Les adresses IP suivantes ont été attribuées à TA505 : « `91.214.124.20` », « `91.214.124.25` », « `91.214.124.64` » et « `91.214.124.5` ».

VPSSC Networks LTD n'a qu'un système autonome, « `AS210119` », correspondant à la plage d'adresses IP « `91.214.124.0/24` ».

Le tableau suivant contient les adresses IP du système autonome « `AS210119` » ayant été détectées par l'ANSSI comme serveurs de commande et de contrôle **Metasploit** et **CobaltStrike**.

Adresse IP	Service	Date de première vue	Date de dernière vue
91.214.124.5	Metasploit	2019-07-31	2020-02-03
91.214.124.13	Metasploit	2019-10-07	2020-02-01
91.214.124.18	Metasploit	2019-08-14	2019-10-15
91.214.124.20	Metasploit	2019-09-11	2020-02-07
91.214.124.22	Metasploit	2019-10-04	2019-10-24
91.214.124.25	Metasploit	2019-12-19	2020-02-05
91.214.124.29	Metasploit	2019-08-10	2019-11-03
91.214.124.53	Metasploit	2019-09-03	2019-10-30
91.214.124.54	Metasploit	2019-08-04	2020-01-10
91.214.124.57	Metasploit	2020-01-29	2020-02-25
91.214.124.64	Metasploit	2019-11-13	2020-01-15
91.214.124.64	CobaltStrike	2019-12-21	2020-01-23

Il est possible que certaines de ces adresses IP aient été contrôlées par TA505. Il est également possible que d'autres acteurs cybercriminels utilisent cet hébergeur et y déploient des outils d'attaque communs.

TA505 semble avoir arrêté d'utiliser cet hébergeur en février 2020.

3.2 FlowSpec

Intel471 indique que TA505 a l'habitude de recourir aux services de l'hébergeur *bulletproof* FlowSpec [9]. L'éditeur donne deux adresses IP utilisées par TA505 : « `176.121.14.175` » et « `176.121.14.238` ». Ces adresses IP correspondent à des serveurs de commande et de contrôle **Metasploit**.

L'hébergeur FlowSpec n'a qu'un système autonome, « `AS210138` », correspondant à la plage d'adresses IP « `176.121.14.0/24` ».

Le tableau suivant contient les adresses IP du système autonome « `AS210138` » ayant été détectées par l'ANSSI comme serveurs de commande et de contrôle **Metasploit** et **CobaltStrike**.

[1] Services d'hébergement qui proposent de louer des serveurs dans des juridictions hors d'atteinte des traités de coopération judiciaire. Ces hébergeurs sont, de plus, peu regardants quant à la finalité d'utilisation des serveurs.

Adresse IP	Service	Date de première vue	Date de dernière vue
176.121.14.140	CobaltStrike	2020-09-20	2021-02-04
176.121.14.229	CobaltStrike	2020-08-22	2021-01-31
176.121.14.251	CobaltStrike	2020-10-25	2021-01-30
176.121.14.232	Metasploit	2020-10-09	2021-01-15
176.121.14.235	Metasploit	2021-01-06	2021-01-14
176.121.14.249	CobaltStrike	2020-10-06	2021-01-09
176.121.14.226	Metasploit	2020-03-10	2020-12-22
176.121.14.175	Metasploit	2020-03-06	2020-12-20
176.121.14.241	Metasploit	2020-03-21	2020-12-18
176.121.14.238	Metasploit	2020-06-03	2020-12-16
176.121.14.234	Metasploit	2020-11-05	2020-11-27
176.121.14.197	CobaltStrike	2020-11-23	2020-11-26
176.121.14.183	Metasploit	2020-03-11	2020-11-13
176.121.14.183	CobaltStrike	2020-03-13	2020-11-08
176.121.14.226	CobaltStrike	2020-10-07	2020-10-07
176.121.14.237	CobaltStrike	2020-08-19	2020-09-10
176.121.14.208	Metasploit	2020-04-12	2020-09-05
176.121.14.231	CobaltStrike	2020-07-28	2020-08-06
176.121.14.199	Metasploit	2020-03-09	2020-05-16
176.121.14.228	CobaltStrike	2020-05-08	2020-05-08
176.121.14.237	Metasploit	2020-03-21	2020-03-21
176.121.14.173	Metasploit	2019-09-23	2019-10-01
176.121.14.132	CobaltStrike	2019-07-17	2019-08-06
176.121.14.112	Metasploit	2019-07-31	2019-07-31

Il est possible que certaines de ces adresses IP soient ou aient été contrôlées par TA505. Il est également possible que d'autres acteurs cybercriminels utilisent cet hébergeur et y déploient des outils communs.

On remarque une augmentation du nombre de serveurs de commande et de contrôle à partir de mai 2020. Ceci est concomitant au passage par TA505 de l'hébergeur VPSSC à FLOWSPEC pour la constitution de son infrastructure.

4 Nouveaux liens avec le rançongiciel Clop

En supplément des liens déjà décrits dans la publication de l'ANSSI en 2020 [1], des indices techniques liant TA505 à **Clop** ont été découverts.

Les domaines « `get-proof-service.com` » et « `outside-service.com` » correspondent aux caractéristiques des domaines utilisés par TA505. Ils ont résolu les adresses IP « `169.239.129.112` » et « `169.239.129.100` » qui servaient le site de fuites de données du rançongiciel **Clop** [10] [11] [12].

Les noms de domaine « `support-iron.com` » et « `support-box.com` » ont été utilisés par **Clop** comme serveur de messagerie pour des négociations [13]. Ces deux noms de domaine correspondent aux caractéristiques des domaines utilisés par TA505.

5 Activités récentes

De septembre à mi-novembre 2020, la chaîne d'infection **Get2/SDBbot** était à l'arrêt. Cependant, TA505 est resté actif. Le 12 novembre 2020, l'Australian Cyber Security Centre a émis une alerte sur des attaques ciblant le secteur médical par un acteur utilisant **SDBbot** [14]. Ce dernier est spécifique au groupe cybercriminel TA505.

Plusieurs serveurs d'hameçonnage et **Get2** ont fait leur apparition mi-novembre puis mi-décembre. Leur utilisation a été accompagnée d'un nouveau serveur C2 **SDBbot** (« `135.181.97.81` ») fin novembre.

Depuis mi-décembre, aucun nouveau serveur lié à TA505 n'a été identifié. La mise en pause de la chaîne de compromission pourrait signifier que TA505 concentre actuellement ses activités sur le déploiement de **Clop**, ce que son site internet de fuite de données semble confirmer, avec les entreprises Amey plc et the7stars récemment chiffrées.

6 Recommandations et détection réseau

Il est recommandé de bloquer les plages d'adresses IP « `91.214.124.0/24` » et « `176.121.14.0/24` » correspondant aux hébergeurs *bulletproof* utilisés par TA505, ainsi que les indicateurs liés aux serveurs de commande et de contrôle **SDBbot**.

Les domaines liés aux serveurs d'hameçonnage et **Get2** sont utilisés durant un laps de temps très court et ne devraient pas être réutilisés par TA505, leur blocage n'est donc pas obligatoire. Cependant, il est conseillé d'effectuer une recherche de présence passée de ceux-ci dans les journaux de connexion.

Sur les noms de domaine fournis, ces éléments permettent de préciser le comportement attendu lors d'une détection réseau :

- serveur d'hameçonnage : téléchargement d'un fichier XLS/XLSX sur le port 443 du domaine ;
- serveur **Get2** : téléchargement d'une DLL sur le port 443 du domaine avec le user-agent « `Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36` » ou « `Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36` » ;
- serveur **SDBbot** : communications sur le port 443 du domaine et requête vers « `http://ip-api.com/json` » avec le user-agent « `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36` ».

7 Annexes

7.1 Indicateurs techniques : serveurs d'hameçonnage, Get2 et SDBbot

Type de serveur	Indicateur technique	Date d'enregistrement	Source
C2 SDBbot	drm-google-analtyic.com	2019-08-07	https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	facebook-drm-server3.com	2019-08-07	https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	news-server-drm-google.com	2019-08-07	https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	static-google-analtyic.com	2019-08-07	https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 Get2	windows-update-02-en.com	2019-09-02	Twitter : @kyleehmke
C2 Get2	update365-office-ens.com	2019-09-03	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	office-teml-en.com	2019-09-11	Twitter : @KorbenD_Intel
C2 Get2	windows-dev-sec.com	2019-09-11	Twitter : @KorbenD_Intel
C2 Get2	office365-en-gb.com	2019-09-16	Twitter : @KorbenD_Intel
C2 Get2	office365-update-en-gb.com	2019-09-16	Twitter : @JAMESWT_MHT
C2 Get2	windows-several-update.com	2019-09-18	Twitter : @James_inthe_box
C2 Get2	windows-update-sdfw.com	2019-09-20	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	windows-update-sdbt.com	2019-09-20	Twitter : @B1naryG
C2 Get2	update-ms-en-office365.com	2019-09-23	Twitter : @B1naryG
C2 Get2	update-msoffice365.com	2019-09-23	ANSSI
C2 Get2	office365-update-en.com	2019-09-25	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	windows-avs-update.com	2019-09-25	Twitter : @B1naryG
C2 Get2	office365-update-eu.com	2019-09-26	Twitter : @58_158_177_102
C2 Get2	windows-wsus-en.com	2019-09-30	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
Hameçonnage	cdn-onedrive-live.com	2019-10-01	Twitter : @killamjr
Hameçonnage	dropbox-download.com	2019-10-01	Twitter : @killamjr
Hameçonnage	googledrive-en.com	2019-10-01	Twitter : @h51un6
Hameçonnage	onedrive-cdn.com	2019-10-01	Twitter : @abuse_ch
Hameçonnage	windows-cnd-update.com	2019-10-01	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	windows-msd-update.com	2019-10-01	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	windows-fsd-update.com	2019-10-07	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
Hameçonnage	onedrive-sdn.com	2019-10-08	Twitter : @dark_moon2019
C2 Get2	windows-sys-update.com	2019-10-08	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
Hameçonnage	googledrive-gb.com	2019-10-09	Twitter : @kyleehmke
C2 Get2	windows-me-update.com	2019-10-09	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
C2 Get2	windows-se-update.com	2019-10-09	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
Hameçonnage	googledrive-eu.com	2019-10-10	Twitter : @kyleehmke
C2 Get2	windows-upgrade-en.com	2019-10-10	Twitter : @kyleehmke
C2 SDBbot	drm-server13-login-microsoftonline.com	2019-10-11	https ://vblocalhost.com/uploads/VB2020-24.pdf

C2 Get2	office365-eu-update.com	2019-10-13	https ://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader
Hameçonnage	onedrive-en.com	2019-10-13	ANSSI
C2 Get2	office365-us-update.com	2019-10-13	Twitter : @James_inthe_box
Hameçonnage	dropbox-en.com	2019-10-14	Twitter : @killamjr
Hameçonnage	onedrive-download-en.com	2019-10-14	Twitter : @kyleehmke
Hameçonnage	onedrive-download.com	2019-10-14	Twitter : @kyleehmke
C2 Get2	windows-en-us-update.com	2019-10-14	Twitter : @kyleehmke
Hameçonnage	dropbox-eu.com	2019-10-15	Twitter : @killamjr
Hameçonnage	onedrive-sd.com	2019-10-15	Twitter : @killamjr
Hameçonnage	onedrive-sn.com	2019-10-15	Twitter : @killamjr
C2 Get2	windows-afx-update.com	2019-10-15	Twitter : @kyleehmke
C2 SDBbot	drm-server-booking.com	2019-10-16	https ://vblocalhost.com/uploads/VB2020-24.pdf
Hameçonnage	onedrive-en-live.com	2019-10-17	Twitter : @killamjr
C2 Get2	windows-wsus-update.com	2019-10-17	Twitter : @kyleehmke
C2 Get2	windows-service-en.com	2019-10-20	Twitter : @kyleehmke
Hameçonnage	dropbox-sdn.com	2019-10-20	Twitter : @kyleehmke
Hameçonnage	dropbox-er.com	2019-10-21	Twitter : @killamjr
Hameçonnage	onedrive-fn.com	2019-10-23	Twitter : @killamjr
C2 Get2	windows-update-sys.com	2019-10-23	Twitter : @killamjr
Hameçonnage	dropbox-download-eu.com	2019-10-24	Twitter : @kyleehmke
Hameçonnage	onedrive-us-en.com	2019-10-24	Twitter : @killamjr
C2 Get2	windows-office365.com	2019-10-24	Twitter : @James_inthe_box
Hameçonnage	googledrive-download.com	2019-10-27	Twitter : @KorbenD_Intel
Hameçonnage	syncdownloading.com	2019-10-28	Twitter : @James_inthe_box
C2 Get2	office-en-service.com	2019-10-28	Twitter : @James_inthe_box
C2 Get2	microsoft-online-en-us.com	2019-10-31	ANSSI
C2 Get2	microsoft-live-us.com	2019-11-03	Twitter : @killamjr
Hameçonnage	sync-share.com	2019-11-03	Twitter : @killamjr
Hameçonnage	syncdownload.com	2019-11-03	ANSSI
Hameçonnage	own-eu-cloud.com	2019-11-05	Twitter : @killamjr
C2 Get2	microsoft-hub-us.com	2019-11-06	Twitter : @killamjr
Hameçonnage	box-en.com	2019-11-08	Twitter : @killamjr
Hameçonnage	box-cnd.com	2019-11-11	Twitter : @killamjr
C2 Get2	microsoft-cnd-en.com	2019-11-13	Twitter : @James_inthe_box
Hameçonnage	onehub-en.com	2019-11-13	Twitter : @killamjr
C2 Get2	microsoft-cnd.com	2019-11-18	Twitter : @0xkyle

Hameçonnage	onedrive-live-en.com	2019-11-18	Twitter : @killamjr
Hameçonnage	box-en-au.com	2019-11-19	Twitter : @killamjr
C2 Get2	microsoft-store-en.com	2019-11-19	Twitter : @James_inthe_box
C2 Get2	ms-home-live.com	2019-11-20	Twitter : @kyleehmke
Hameçonnage	sharefile-cnd.com	2019-11-20	Twitter : @killamjr
C2 Get2	microsoft-home-en.com	2019-11-21	Twitter : @Nocturnus
Hameçonnage	sharefile-us.com	2019-11-25	Twitter : @killamjr
C2 Get2	windows-service-us.com	2019-11-25	Twitter : @kyleehmke
Hameçonnage	dropbox-cnd.com	2019-11-26	Twitter : @killamjr
C2 Get2	live-en.com	2019-11-26	Twitter : @58_158_177_102
Hameçonnage	boxfiles-en.com	2019-11-28	Twitter : @kuermelecke
C2 Get2	msonebox.com	2019-11-28	Twitter : @kuermelecke
C2 Get2	online-office365.com	2019-11-28	Twitter : @0xkyle
Hameçonnage	sharefiles-eu.com	2019-11-28	Twitter : @killamjr
C2 SDBbot	jp-microsoft-store.com	2019-11-30	https ://vblocalhost.com/uploads/VB2020-24.pdf
Hameçonnage	sharefiles-en.com	2019-11-30	Twitter : @kyleehmke
C2 Get2	onms-home.com	2019-12-05	Twitter : @kyleehmke
Hameçonnage	onedrive-en-eu.com	2019-12-10	Twitter : @CTI_Marc
C2 Get2	upgrade-ms-home.com	2019-12-10	Twitter : @AdamTheAnalyst
Hameçonnage	onedrive-eu.com	2019-12-11	Twitter : @CTI_Marc
C2 Get2	windows-appstore-en.com	2019-12-11	Twitter : @AdamTheAnalyst
C2 Get2	geo-st-microsoft.com	2019-12-16	Twitter : @Bl4ng3l
Hameçonnage	daumcdnf.com	2019-12-16	Twitter : @AdamTheAnalyst
Hameçonnage	daumcdns.com	2019-12-16	Twitter : @CTI_Marc
Hameçonnage	daumcdnr.com	2019-12-18	Twitter : @CTI_Marc
C2 Get2	ms-en-microsoft.com	2019-12-18	Twitter : @CTI_Marc
C2 SDBbot	eu-global-online.com	2020-01-13	https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	eu-global.com	2020-01-13	https ://vblocalhost.com/uploads/VB2020-24.pdf
Hameçonnage	fileshare-cnd.com	2020-01-13	Twitter : @ffforward
C2 Get2	ms-global-store.com	2020-01-13	Twitter : @ffforward
C2 Get2	studio-stlsdr.com	2020-01-14	Twitter : @ffforward
Hameçonnage	file-shares.com	2020-01-14	Twitter : @AdamTheAnalyst
Hameçonnage	egnytefs.com	2020-01-15	Twitter : @CTI_Marc
C2 Get2	selling-group.com	2020-01-15	Twitter : @CTI_Marc
Hameçonnage	share-stores.com	2020-01-15	Twitter : @CTI_Marc
C2 Get2	xbox-en-cnd.com	2020-01-15	Twitter : @AdamTheAnalyst

Hameçonnage	fileshare-storage.com	2020-01-16	Twitter : @AdamTheAnalyst
C2 Get2	reselling-corp.com	2020-01-17	Twitter : @AdamTheAnalyst
C2 Get2	general-lcfd.com	2020-01-20	Twitter : @ffforward
Hameçonnage	share-downloading.com	2020-01-20	Twitter : @ffforward
C2 Get2	integer-ms-home.com	2020-01-21	Twitter : @ffforward
Hameçonnage	one-drive-storage.com	2020-01-21	Twitter : @ffforward
C2 Get2	global-logic-stl.com	2020-01-22	Twitter : @AdamTheAnalyst
Hameçonnage	shared-download.com	2020-01-22	Twitter : @AdamTheAnalyst
Hameçonnage	shared-downloads.com	2020-01-23	Twitter : @AdamTheAnalyst
Hameçonnage	files-downloads.com	2020-01-25	Twitter : @AdamTheAnalyst
C2 Get2	store-in-box.com	2020-01-25	Twitter : @AdamTheAnalyst
Hameçonnage	download-shares.com	2020-01-28	Twitter : @rcwht_
C2 Get2	stt-box.com	2020-01-28	Twitter : @AdamTheAnalyst
Hameçonnage	clouds-share.com	2020-01-29	Twitter : @AdamTheAnalyst
C2 Get2	microsoft-store-drm-server.com	2020-01-29	Twitter : @ffforward
Hameçonnage	clouds-doanload-cnd.com	2020-01-31	Twitter : @ffforward
Hameçonnage	cloud-store-cdn.com	2020-02-01	Twitter : @ffforward
C2 Get2	microsoft-sback-server.com	2020-02-03	Twitter : @ffforward
C2 SDBbot	auxin-box.com	2020-02-04	https ://vblocalhost.com/uploads/VB2020-24.pdf
Hameçonnage	live-msr.com	2020-02-04	Twitter : @ffforward
Hameçonnage	one-drive-ms.com	2020-02-04	Twitter : @ffforward
C2 Get2	wpad-home.com	2020-02-04	Twitter : @killamjr
C2 Get2	mainten-ferrum.com	2020-02-05	Twitter : @ffforward
Hameçonnage	shared-cnd.com	2020-02-05	Twitter : @ffforward
Hameçonnage	download-cdn.com	2020-02-07	Twitter : @ffforward
C2 Get2	ms-break.com	2020-02-07	Twitter : @ffforward
Hameçonnage	fileshare-cdns.com	2020-02-09	Twitter : @ffforward
C2 Get2	ms-home-store.com	2020-02-09	Twitter : @ffforward
C2 Get2	ms-upgrades.com	2020-02-14	Twitter : @stoerchl
Hameçonnage	sharefiles-download.com	2020-02-14	Twitter : @stoerchl
Hameçonnage	dl-sharefile.com	2020-02-16	Twitter : @ffforward
C2 Get2	home-storages.com	2020-02-16	Twitter : @stoerchl
Hameçonnage	cdn-box.com	2020-02-18	Twitter : @stoerchl
Hameçonnage	dl-sync.com	2020-02-18	Twitter : @AdamTheAnalyst
C2 Get2	ms-rdt.com	2020-02-18	Twitter : @rcwht_
C2 Get2	microsoft-ware.com	2020-02-20	Twitter : @ffforward

Hameçonnage	owncloud-cdn.com	2020-02-20	Twitter : @ffforward
Hameçonnage	clouds-cdn.com	2020-02-21	Twitter : @0xkyle
Hameçonnage	att-download.com	2020-02-24	Twitter : @stoerchl
C2 Get2	glr-ltd.com	2020-02-24	Twitter : @stoerchl
C2 Get2	mays-ltd.com	2020-02-24	Twitter : @stoerchl
Hameçonnage	share-clouds.com	2020-02-24	Twitter : @stoerchl
Hameçonnage	int-download.com	2020-02-25	Twitter : @stoerchl
C2 Get2	rdmsom.com	2020-03-02	Twitter : @ffforward
Hameçonnage	shares-cloud.com	2020-03-02	Twitter : @stoerchl
Hameçonnage	cdn-downloads.com	2020-03-03	Twitter : @stoerchl
C2 Get2	into-box.com	2020-03-03	Twitter : @stoerchl
Hameçonnage	shares-cdns.com	2020-03-06	Twitter : @ffforward
C2 Get2	tnrff-home.com	2020-03-06	Twitter : @reecdeep
Hameçonnage	dl-icloud.com	2020-03-09	Twitter : @stoerchl
C2 Get2	dysoool.com	2020-03-09	Twitter : @ffforward
C2 Get2	get-downloads.com	2020-03-09	Twitter : @stoerchl
Hameçonnage	i-sharecloud.com	2020-03-10	Twitter : @stoerchl
Hameçonnage	sharespoint-en.com	2020-03-10	Twitter : @stoerchl
C2 Get2	clietns-download.com	2020-03-13	Twitter : @ffforward
Hameçonnage	onedrives-en-live.com	2020-03-17	Twitter : @stoerchl
Hameçonnage	stat-downloads.com	2020-03-18	Twitter : @stoerchl
Hameçonnage	clients-share.com	2020-03-19	Twitter : @stoerchl
C2 Get2	static-downloads.com	2020-03-19	Twitter : @stoerchl
C2 Get2	getlink-service.com	2020-03-20	Twitter : @stoerchl
Hameçonnage	dyn-downloads.com	2020-03-23	Twitter : @stoerchl
Hameçonnage	mslinks-downloads.com	2020-04-09	Twitter : @stoerchl
C2 Get2	corp-downloads.com	2020-04-12	Twitter : @stoerchl
C2 SDBbot	us-microsoft-store.com	2020-04-21	Twitter : @tbarabosch
C2 SDBbot	s3-ap-southeast-1-amazonaws.com	2020-05-21	https ://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
C2 SDBbot	s3-ap-southeast-2-amazonaws.com	2020-05-21	https ://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
C2 Get2	corp-storage.com	2020-06-01	Twitter : @stoerchl
Hameçonnage	fasts-downloads.com	2020-06-01	Twitter : @stoerchl
C2 Get2	filessz.com	2020-06-02	Twitter : @stoerchl
Hameçonnage	rmt-downloads.com	2020-06-02	Twitter : @stoerchl
C2 Get2	shr-links.com	2020-06-02	Twitter : @stoerchl
Hameçonnage	store-downloads.com	2020-06-02	Twitter : @stoerchl

Hameçonnage	downloads-links.com	2020-06-03	Twitter : @stoerchl
C2 Get2	sharefileszz.com	2020-06-03	Twitter : @stoerchl
Hameçonnage	eu-download.com	2020-06-07	Twitter : @stoerchl
C2 Get2	sdff-corp.com	2020-06-07	Twitter : @JAMESWT_MHT
C2 Get2	def-update.com	2020-06-08	Twitter : @stoerchl
C2 SDBbot	s77657453-onedrive.com	2020-06-08	https ://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
C2 SDBbot	s89065339-onedrive.com	2020-06-08	https ://www.telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104
Hameçonnage	sl-downloads.com	2020-06-08	Twitter : @stoerchl
Hameçonnage	md-downloads.com	2020-06-15	Twitter : @stoerchl
C2 Get2	nffsd-corp.com	2020-06-15	Twitter : @stoerchl
C2 SDBbot	music-server11-facebook.com	2020-06-16	Twitter : @tbarabosch
C2 SDBbot	music-server17-facebook.com	2020-06-16	Twitter : @tbarabosch
Hameçonnage	data-downloads.com	2020-06-16	Twitter : @stoerchl
Hameçonnage	ex-downloads.com	2020-06-16	Twitter : @stoerchl
C2 Get2	mgrs-service.com	2020-06-16	Twitter : @stoerchl
C2 Get2	wire-share.com	2020-06-16	Twitter : @stoerchl
Hameçonnage	dropboxscdn.com	2020-06-19	https ://www.hornetsecurity.com/en/security-information/clop-clop-ta505-html-malspam-analysis/
C2 Get2	get-hlinks.com	2020-06-21	Twitter : @tbarabosch
Hameçonnage	dropboxccdn.com	2020-06-22	Twitter : @AdamTheAnalyst
C2 Get2	rapid-stores.com	2020-06-22	Twitter : @stoerchl
Hameçonnage	dropboxwcdn.com	2020-06-23	Twitter : @stoerchl
C2 Get2	fast-gl-backups.com	2020-06-23	Twitter : @stoerchl
Hameçonnage	dropboxrcdn.com	2020-06-24	Twitter : @stoerchl
C2 Get2	ex-stores.com	2020-06-24	Twitter : @stoerchl
C2 Get2	alpha-telemetry-microsoft.com	2020-06-26	Twitter : @stoerchl
Hameçonnage	boxrcdn.com	2020-06-26	Twitter : @stoerchl
Hameçonnage	google-us-cdn.com	2020-06-28	Twitter : @stoerchl
C2 Get2	usr-telemetry-microsoft.com	2020-06-28	Twitter : @stoerchl
C2 Get2	direct-upt.com	2020-06-29	Twitter : @stoerchl
Hameçonnage	google-eu-cdn.com	2020-06-29	Twitter : @stoerchl
Hameçonnage	direct-share.com	2020-06-30	Twitter : @stoerchl
C2 Get2	mira-store.com	2020-06-30	Twitter : @stoerchl
Hameçonnage	global-downloads.com	2020-07-02	Twitter : @stoerchl
C2 Get2	limo-ones.com	2020-07-02	Twitter : @stoerchl
Hameçonnage	fast-bits.com	2020-07-05	Twitter : @stoerchl
C2 Get2	personal-dss.com	2020-07-05	Twitter : @stoerchl

C2 Get2	main-boost.com	2020-07-06	Twitter : @stoerchl
C2 SDBbot	news-server17-yahoo.com	2020-07-13	ANSSI
C2 Get2	going-tr.com	2020-07-31	ANSSI
Hameçonnage	direct-space.com	2020-08-04	Twitter : @AdamTheAnalyst
C2 Get2	nellscorp.com	2020-08-04	Twitter : @stoerchl
C2 Get2	definite-limits.com	2020-08-05	Twitter : @stoerchl
Hameçonnage	mop-shere.com	2020-08-05	Twitter : @stoerchl
C2 Get2	none-class.com	2020-08-06	Twitter : @stoerchl
Hameçonnage	river-store.com	2020-08-06	Twitter : @stoerchl
C2 Get2	band-switch.com	2020-08-10	Twitter : @Supre31539665
Hameçonnage	tremd-space.com	2020-08-10	Twitter : @Supre31539665
C2 Get2	siron-del.com	2020-08-11	Twitter : @ffforward
C2 Get2	transff-reddon.com	2020-08-11	Twitter : @S0lari1
Hameçonnage	long-space.com	2020-08-12	Twitter : @S0lari1
Hameçonnage	url-space.com	2020-08-17	Twitter : @Supre31539665
Hameçonnage	one-drives.com	2020-08-19	Twitter : @stoerchl
Hameçonnage	onesdrives.com	2020-08-19	Twitter : @BushidoToken
C2 Get2	see-back.com	2020-08-19	Twitter : @stoerchl
Hameçonnage	digitals-space.com	2020-08-19	Twitter : @Supre31539665
C2 Get2	backup-place.com	2020-08-21	Twitter : @stoerchl
C2 SDBbot	store-000846-live.com	2020-08-21	Twitter : @tbarabosch
C2 SDBbot	store-003774-live.com	2020-08-21	Twitter : @tbarabosch
Hameçonnage	filesharess.com	2020-08-24	Twitter : @stoerchl
C2 Get2	near-fast.com	2020-08-24	Twitter : @stoerchl
Hameçonnage	box-cdn.com	2020-08-26	Twitter : @stoerchl
Hameçonnage	dropbox-cdns.com	2020-08-26	Twitter : @stoerchl
C2 Get2	first-destin.com	2020-08-26	Twitter : @stoerchl
C2 Get2	groms-dat.com	2020-08-26	Twitter : @stoerchl
C2 Get2	toppon-studio.com	2020-08-26	Twitter : @stoerchl
Hameçonnage	dropbox-cdnn.com	2020-08-30	Twitter : @ffforward
C2 Get2	west-dat.com	2020-08-30	Twitter : @stoerchl
C2 Get2	fosdommtoi.com	2020-09-02	Twitter : @stoerchl
Hameçonnage	onehub-cdn.com	2020-09-02	Twitter : @stoerchl
C2 Get2	bak-home.com	2020-09-07	Twitter : @Supre31539665
Hameçonnage	short-share.com	2020-09-07	Twitter : @cocaman
C2 Get2	nels-ltd.com	2020-09-08	Twitter : @stoerchl

Hameçonnage	shortcut-links.com	2020-09-08	Twitter : @stoerchl
C2 Get2	near-back.com	2020-09-09	Twitter : @stoerchl
C2 SDBbot	news-37876-mshome.com	2020-09-10	https ://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
C2 SDBbot	news-389767-mshome.com	2020-09-10	https ://www.telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546
Hameçonnage	dropbox-cdnt.com	2020-09-13	Twitter : @stoerchl
C2 Get2	pssd-ltdgroup.com	2020-09-13	Twitter : @stoerchl
Hameçonnage	shared-filez.com	2020-09-29	Twitter : @stoerchl
C2 Get2	microsoft-debug-098.com	2020-11-16	Twitter : @AdamTheAnalyst
C2 Get2	bak0-store.com	2020-11-16	Twitter : @sS55752750
C2 SDBbot	xbox-ms-store-debug.com	2020-11-21	Twitter : @tbarabosch
C2 Get2	res-backup.com	2020-12-11	Twitter : @stoerchl
Hameçonnage	ms-downloading.com	2020-12-11	Twitter : @stoerchl
C2 Get2	ms-debug-services.com	2020-12-14	Twitter : @sS55752750
Hameçonnage	local-download.com	2020-12-14	Twitter : @fffforward
C2 Get2	ms-pipes-service.com	2020-12-16	Twitter : @James_inthe_box
Hameçonnage	docs-downloading.com	2020-12-16	Twitter : @stoerchl
C2 SDBbot	92.38.135.217		https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	158.255.208.148		https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	158.255.208.168		https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	185.17.121.188		https ://vblocalhost.com/uploads/VB2020-24.pdf
C2 SDBbot	135.181.97.81		Twitter : @CTI_Marc

7.2 Serveurs de redirection

Serveurs de redirection				
174.143.146.246	fangirlmag.com	morenorubio.com	telefoniabologna.it	www.garethwalker.plus.com
190.184.198.151	fbd.de	motorocio.com	telusplanet.net	www.gatesofhell.plus.com
192.198.92.131	fedup.tv	moveyourmarket.com	test.ishine.cz	www.gbinnie.plus.com
195.34.73.29	fepete.ch	moz.execulink.net	testensie.de	www.georgewatson.plus.com
198.91.87.97	filateliadimauro.com	mwt.net	tewxda71.secure.ne.jp	www.gm4pgv.plus.com
202.164.235.127	filipelucio.com	nakladatelstvi-brazda.wz.cz	texas-diesel.com	www.greencentral.plus.com
208.74.201.75	flbox.net	naturainmente.com	thamescom.com	www.hansvanderwerf.nl
209.182.199.2	fliplens.com	naxnet.or.jp	thebitcrew.com	www.hieroglyph.freeuk.com
211.202.2.87	floratelecom.com	neo-kikaku.jp	theestatehouse.co.uk	www.hiroden-con.jp
212.159.9.151	fnp-smellingerlan.nl	neszmely.eu	theotime.net	www.i-younet.ne.jp
2819.linux2.testsider.dk	forsi.net	neumanns-installation.de	theswimshop.co.za	www.ili.net
38.106.32.161	fotoseiten.heimat.eu	new.lerian-nti.be	throwingsevens.co.uk	www.inyes.com.tw
89.161.181.116	fructa.nl	nhn.dk	timetunnel.net	www.isistech.com.tw
aaa-architecten.nl	ftpadmin.edv-stumpf.de	nlink.com.br	tommasobuglioni.com	www.izmsj.co.jp
aaa-arcobaleno.it	fvaweb.it	nottinghamsuburbanrailway.co.uk	tomsonguitars.co.uk	www.izu.co.jp
abi83-schramberg.de	g7.com.tw	nozawashoten.com	travelhub.com.sg	www.jrhayley.plus.com
academy-internet.net	garant.bos.ru	ns.netnet.or.jp	tridentenvironmental.co.uk	www.k-macs.ne.jp
addstock.co.uk	garciaestelles.com	ns38541.ovh.net	trucksong.com.au	www.katch.ne.jp
agriturismoilcascinone.com	giles.uk.net	ntskeptics.org	ts-shimada.com	www.kenkudo.plus.com
agt.net	grandeweddings.com	nyittc.com	tsbm.ch	www.knell.plus.com
alexanderjonesi.com	hamiltonpainters.ca	nytva-nmz.ru	tsp2002.com	www.kolks.nl
alfa-tel.sk	hapax.qc.ca	obuse-apple.com	twofish.freeuk.com	www.leklicht.net
amusun.com	haslundalsted.dk	oiseau-perdu.fr	udec.cl	www.lincolnshirefitness.co.uk
angelfire.com	healthfood.syoutikubai.com	okclub.org.uk	ulusalofis.com	www.lysabarnard.plus.com
appswiss.ch	hgusler.com	oldftp.otenet.gr	unclechunk.com	www.ma-kaeser.ch
arcadia1998.web.fc2.com	hhcj.co.uk	olioeroli.it	unser-en.de	www.macatawa.org
archifaktura.hu	hhvdds.com	ondermaat.nl	users.cuci.nl	www.medhiartis.com
assostudiosrl.it	hieroglyph.freeuk.com	optimaconsulting.com.au	users.tpg.com.au	www.merijntjeaanderijn.nl
asumedo.jp	hiustensiirto.org	organic-harmony.com	v-support.free.bg	www.mikaeljigmo.com
audicat.net	hmw42.host-my-website.com	orpheus.cuci.nl	valsgaard-kofod.dk	www.miqsoft.hu
audio-pa-service.de	home.foni.net	pageplop.com	vanbenthem.org	www.miyazaki-catv.ne.jp
bacskateszov.hu	home.gelsennet.de	papageienseite.de	vdbunt.net	www.mjonkers.nl
balkanwide-assistance.rs	home.townisp.com	parafiaukta.pl	vhowland.co.uk	www.mr-mondial.com
baskidunyasi.net	host81-138-7-108.in-addr.btopenworld.com	paulomatosconsultores.com.br	victorlutte.cl	www.ms247.plus.com

bestwatersystems.net	hot.useractive.com	peever.myzen.co.uk	vinkelvej12.dk	www.nas-k.co.jp
blackbass.mx	hp1.tcbnet.ne.jp	pension-pentacon.de	vodoustoichivshperplat.com	www.ndbsoft.be
blackqpid.org.uk	hrnecek.com	perso.menara.ma	volksaddiction.nl	www.nebulus30.plus.com
bmgiventures.com	ht-srl.com	petzel.be	vpm.hu	www.neszmely.eu
bootsstation-reiherhals.de	hungfei.com	philippschoch.ch	w-chat.xf.cz	www.newmedia.plus.com
bosmafamily.nl	hurricaneprotection.com	phobia.net	wallflore.de	www.newnorth.net
braccom.ch	iceman30.de	phoenixinvestigations.ca	waoptions.com.au	www.newtrees.plus.com
brandveiligheidsexperts.nl	icmserver.net	phones4you.be	weather.fixitpro.ro	www.nozawashoten.com
bravanian.hk	igrs.ca	pipslab.nl	web123.webhotelli.fi	www.odyssey.on.ca
brekus.org	import43.com	pitakchon.com	webtj.net	www.olioeroli.it
bs.url.tw	indyscribe.com	pitbull-marketing.com	wellnessnaturopathic.com	www.ozonatory24.pl
bufetgarrigosa.com	injuredworkersadvocates.com	planearconsultoria.com.br	werinussa.net	www.pedigree1.plus.com
buresova-obrazy.wz.cz	inkoleasing.ru	pollet-rauen.de	westbridges.net	www.perso.ch
cabrerapelaez.com	inlinefascia.com	pomp-buerotechnik.de	workaccount.free.bg	www.peteralexander.plus.com
carnegienet.net	intertech.co.jp	praktijkewalts.info	www.0202.com.tw	www.peterfishwick.free-online.co.uk
cbango.com.ar	ishinomakicatering.web.fc2.com	praktijkmariekehuisman.nl	www.1120.com.tw	www.pitakchon.com
ccb.myzen.co.uk	ismailersoz.com	pratik.com.tr	www.aandgwright.plus.com	www.planet.eon.net
cckgate.com	izmsj.co.jp	predskolaci.cz	www.abc-tax.jp	www.pomp-buerotechnik.de
cdbs.com.tr	jav.ee	primusbelgium.com	www.adrianwaldock.plus.com	www.praktijkmariekehuisman.nl
cekornapred.org	jerry.proweb.net	profiline-berlin.de	www.aero-source.net	www.prtc.net
cgmt.co.id	jesamcorp.com	promoreclame.info	www.agt.net	www.reusenproject-n.nl
channelvue.com.au	jkcontrols.co.uk	promoreclame.nl	www.akiko.f9.co.uk	www.riskybus.f9.co.uk
cinelario.com	jl-mag.de	prospectnews.com	www.alexrc.plus.com	www.robm674.plus.com
citlink.net	jlcarral.com	proweb.co.uk	www.andyhawk.free-online.co.uk	www.rpepin.plus.com
clausing-advies.nl	jlijten.nl	quickandeasy.co.za	www.andymurray.plus.com	www.ryosuke.plus.com
clb.bazzacco.net	jmvisuals.com	rassegnavermentino.it	www.angelfire.com	www.salter51.plus.com
cloudserver098095.home.pl	jrfa.net	razor.arnes.si	www.apogara.plus.com	www.sarge05.plus.com
cntmc.com	jrsa.net	redir9.alteabz.it	www.area043.com	www.schemml.de
col-med.com	jsfactory.net	reninet.com	www.baba-t.com	www.scottofyork.plus.com
colddry.com	justdeckshamilton.ca	reynders.info	www.balnakiel.plus.com	www.servitemequipos.cl
collegiogeometri.it	kaharmonie.nl	rf-arch.com	www.benhamlyn.plus.com	www.seward.net
computersoostynaarlo.nl	kanzlei-borchers.de	rimaje.nl	www.billcarthy.f9.co.uk	www.sgtwilko.f9.co.uk
conexionesymanguerashidrocalidas.com.mx	karat.hu	rjr-rs.com.br	www.blossomtel.com	www.shaunfennings.plus.com
consulturias.com	karinart.de	robbiblubber.org	www.bluecrabhosting.co.uk	www.shichihukuudon.com
coolnovelties.co.uk	kasumikarate.hanagasumi.net	route31.org	www.bretby.plus.com	www.shorthouse.com
corbalanlopez.com	katch.ne.jp	ruegenfleisch.de	www.bryantaylor.free-online.co.uk	www.silcom.com

creditperformance.com.br	katcol.co.uk	sabre.com.tw	www.btalbot.plus.com	www.skegness.net
crsystems.it	katofer.axelero.net	sarahshuckburgh.com	www.btvm.ne.jp	www.skvarsani.plus.com
cs-cart.jp	kawabe.es	sauna-verdeclub.jp	www.cabrerapelaez.com	www.sky-net.or.jp
cs-kn.de	kawarayu.net	scegli-vinci.it	www.cadvision.com	www.skywin.com.tw
cue4you.nl	kdconstructionusa.com	scgis.co.uk	www.camion.idps.co.uk	www.smailes.plus.com
cukierniatylczynscy.lh.pl	kelder.nl	scnet.tv	www.capturedcovers.com	www.ssquire.plus.com
cumc-hmb.com	kodu.neti.ee	seapower-italia.it	www.carnegienet.net	www.studiomugnaini.eu
cyberfaery.com	krasnaya.co.uk	sedlec.unas.cz	www.cati.com.tw	www.sun-inet.or.jp
d-road.com	kvision.tv	seiyuu.ne.jp	www.chartercare.plus.com	www.teltech.hu
daretodreamfarm.com	laborex.hu	server44.dubhosting.co.uk	www.chienhung.url.tw	www.telusplanet.net
dashingleather.com	laltraimmagine.ss.it	setrise.nl	www.chiyih.com	www.thepringlefamily.plus.com
dataidea.it	larcocultura.it	seward.net	www.cliftons.plus.com	www.tlauder.f9.co.uk
deal-courrier.be	larossola.it	seyatosan.iaigiri.com	www.cotc.net	www.topsecretmagic.co.uk
decor8.ie	leklicht.net	sh2070.evanzo-server.de	www.courtneywalker.plus.com	www.topworld.nl
deechtebol.com	lesrivesdechambesy.ch	shichihukuudon.com	www.csalikft.hu	www.tranzit124.cz
demetnagement.com	lessentieldelimmo.fr	shinedns.net	www.ctaz.com	www.trips75.nl
demo1.lerian-nti.be	lewell.fr	shorthouse.com	www.cuci.nl	www.ts-shimada.com
dentistsinyourarea.com	limonecomunicacao.com.br	silcom.com	www.cyberfaery.com	www.tutka.net
diaita.ch	lincolnshirefitness.co.uk	sinseisyoji.co.jp	www.dalesnewzealand.co.nz	www.twofish.freeuk.com
diamond-water.hk	linkit.biz	sistemishop.it	www.danair.es	www.users.dialstart.net
diesilberamis.meeriwelt.de	loadesecoparc.co.uk	skaluneris.com	www.davion.plus.com	www.users.freenetname.co.uk
dmatica.it	lovedonesproducts.com	sky.od.ua	www.debbo.plus.com	www.vandenberghider.plus.com
doctorschoicenursing.com	lovittco.com.au	slhk23.0101host.com	www.deelen-wageningen.nl	www.vanguard-art.com
dondolino.it	lpa.myzen.co.uk	smarine.mu	www.derekrjones.plus.com	www.veritaspartners.co.jp
dorianbaroque.org	lucker.co	smitt.nl	www.devenney.plus.com	www.victorlutte.cl
draco-artgallery.wz.cz	ma-kaeser.ch	soarpower.com	www.devon38.plus.com	www.wctc.net
drivingschoolburlington.ca	macatawa.org	socom.es	www.diaita.ch	www.webtj.net
dylanwong.com	madeleinekrook.nl	solartia.com	www.dunlop.force9.co.uk	www.wessexgrange.plus.com
eatondesigns.com	mama.pipi.ne.jp	sortis.lt	www.eastwood35.idps.co.uk	www.wu4652.com.tw
eddy.noneto.com	margaretanddavid.com	spadework.org	www.edv-waldherr.at	www.wwt-ag.ch
edog2017.karyamedia.net	martinsmith.nl	speeltuintalud.nl	www.emadesign.net	www.yuzuni.com
eduardorodrigues.adv.br	mcsgrp.com	spiralfolderrollers.com	www.estpak.ee	www.ywmc.com.tw
eduthermas.sk	mdunker.gmxhome.de	sportreisen.de	www.eva.hi-ho.ne.jp	www1.amigo2.ne.jp
ej.progresas.lt	medhiartis.com	staceydodge.com	www.everestgroupcorp.com	www2.arnes.si
elzaservis.cz	media-angel.de	stanbridgeestate.com	www.expoteam.net	www2.tpgi.com.au
emeraldtiger.com	members.chello.at	studiomugnaini.eu	www.ezl.com	www2.udec.cl

entrenador-personal.com	members.chello.nl	studiospa.com.pl	www.ezlink.ca	www3.telus.net
erp.garan.pro	members.iinet.net.au	su.valley.ne.jp	www.firemouth.plus.com	www4176uc.sakura.ne.jp
ertopcu.com	members.upc.nl	summer.ntua.edu.tw	www.firered.plus.com	wwwroot.doorenbos.net
esoterik-lenormand.com	mettelindberg.dk	superlecker.info	www.flowerdevon.idps.co.uk	wwwroot.forent.sk
evroteplo.ru	mezmerband.com	surfindave.com	www.ford7.plus.com	yas-jr.com
ezl.com	mh-miyoshi.jp	svava.eu	www.formosahappiness.org	yhti.net
fachadasalaire.com	mjlunalaw.com	t-o-kitano.com	www.fra19.plus.com	yu.ac.kr
falcon1.net	mjonkers.nl	takeoneaudio.jp	www.framar.plus.com	zlhoteckelinie.wz.cz
famwillems.nl	monarchy.nl	taouxis.gr	www.funkydoowop.plus.com	zoeandjo.co.uk

8 Bibliographie

[1] ANSSI. *Évolution de l'activité du groupe cybercriminel TA505*. 22 juin 2020.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-006/.

[2] Korean Financial Security Institute. *TA505 Group Profiling*. 28 février 2020.
URL : https://www.fsec.or.kr/common/proc/fsec/bbs/163/fileDownLoad/2298.do.

[3] urlscan.io.
URL : https://urlscan.io/search/#one-drives.com.

[4] Fox-IT. *TA505 : A Brief History Of Their Time*. 16 novembre 2020.
URL : https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/.

[5] AdamTheAnalyst. 3 mars 2020.
URL : https://twitter.com/AdamTheAnalyst/status/1234848328170557440.

[6] Dennis Schwarz, Kafeine, Matthew Mesa, Axel F. *TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader*. 16 octobre 2019.
URL : https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader.

[7] IBM X-Force. *TA505 Continues to Infect Networks With SDBbot RAT*. 14 avril 2020.
URL : https://securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/.

[8] vikas891. 7 février 2020.
URL : https://twitter.com/vikas891/status/1225759078976118784.

[9] Intel471. *Flowspec – TA505's bulletproof hoster of choice*. 15 juillet 2020.
URL : https://public.intel471.com/blog/bulletproof-hoster-of-choice/.

[10] urlscan.io. 8 août 2020.
URL : https://urlscan.io/result/0625e3e4-3e34-41ec-8b56-a740d2df5b25.

[11] urlscan.io. 26 août 2020.
URL : https://urlscan.io/result/8017d88e-e636-43ee-b686-96a9be76d6b2.

[12] urlscan.io. 8 août 2020.
URL : https://urlscan.io/result/c13f0941-cb9c-4435-8e38-81068b462650.

[13] S2W LAB. *[S2W LAB] Analysis of Clop Ransomware suspiciously related to the Recent Incident*. 23 novembre 2020.
URL : https://www.notion.so/S2W-LAB-Analysis-of-Clop-Ransomware-suspiciously-related-to-the-Recent-Incident-c26daec604da4db6b3c93e26e6c7aa26.

[14] Australian Cyber Secuirty Center. *SDBBot Targeting Health Sector*. 12 novembre 2020.
URL : https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector.

Version 1.0 - 10/02/2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN