



30 octobre 2023

Analyse en aval d'un cyberincident

Attaques DDoS «NoName057(16)» de juin 2023

Le présent rapport analyse les attaques par déni de service distribué (attaques DDoS) survenues durant les deux premières semaines de juin 2023 (semaines 23 et 24) contre des organisations et des autorités suisses. Il explique en détail la variante d'attaque DDoS utilisée au niveau de la couche applicative.

La Suisse a surmonté ces attaques DDoS du groupe «NoName057(16)» sans dommages durables. La plupart des organisations et des autorités suisses prises pour cible s'étaient dûment préparées contre des attaques DDoS et ont donc réagi de manière adéquate. On peut en déduire que la mise en œuvre de mécanismes de sécurité adaptés aux besoins permet de réduire considérablement les dommages potentiels.

Les médias ont abondamment parlé de ces attaques DDoS, en raison tant de la variété de leurs cibles que du caractère politiquement sensible du discours prononcé devant le Parlement par Volodymyr Zelensky. Cette couverture médiatique a permis au groupe de capter l'attention du grand public, ce qui était son intention première. Le groupe de pirates prorusse «NoName057(16)» tenait à exprimer ses préoccupations politiques, en réaction à plusieurs décisions du Parlement suisse (par ex. transfert à des États tiers de matériel de guerre, annonce du discours de Volodymyr Zelensky au Parlement).

Les attaques DDoS visaient à perturber la disponibilité des sites web (par épuisement de ressources, en anglais *resource exhaustion*). Aucune fuite d'informations n'est à déplorer au niveau des données productives.

Table des matières

1	Résumé.....	3
2	Introduction.....	4
2.1	Contexte géopolitique.....	4
2.2	Catégorisation.....	5
3	Description de l'attaque.....	6
3.1	Type d'attaque DDoS.....	6
3.2	Groupe «NoName057(16)».....	6
3.3	Description technique.....	13
4	Déroulement de l'attaque.....	17
5	Effets de la cyberattaque.....	21
5.1	Résonance médiatique.....	21
5.2	Conséquences politiques.....	22
5.3	Effets juridiques.....	22
5.4	Dommmages effectifs.....	23
6	Recommandations.....	24
7	Bilan.....	27
8	Annexes.....	29

1 Résumé

Au cours des deux premières semaines de juin 2023 (semaines 23 et 24), des attaques par déni de services distribué (attaques DDoS)¹ ont été menées contre des organisations et des autorités suisses. Ce cyberactivisme (hacktivisme) contre la Suisse est intervenu à la suite de plusieurs décisions prises par le Parlement fédéral dans le contexte de la guerre en Ukraine (voir chap. 8 [1] et [2]). Les hacktivistes comptent beaucoup sur l'effet de signal de leurs attaques DDoS pour faire connaître leurs préoccupations politiques et atteindre ainsi leurs objectifs.

Le groupe avait pris pour cible des autorités ou des organisations proches de l'administration fédérale et jouissant d'une bonne réputation auprès du public (par ex. Parlement suisse, La Poste Suisse SA, Chemins de fer fédéraux CFF). Ces attaques DDoS ont paralysé certains sites web pendant une courte période (quelques heures). Dans le pire des cas, les interruptions de service ont duré quelques jours. Il n'y a pas eu de dommage permanent causé aux infrastructures informatiques ou d'autre préjudice économique; ce n'était d'ailleurs pas le but premier du groupe, qui voulait surtout attirer l'attention des médias, de la société et du monde politique.

Il s'agit du groupe d'hacktivistes prorusse «NoName057(16)» qui, depuis mars 2022, enchaîne dans le monde entier les attaques DDoS contre diverses cibles jugées «critiques à l'égard de la Russie» (par ex. administrations publiques et autorités, entreprises et autres organisations). Les attaques fructueuses sont à chaque fois publiées sur le canal Telegram du même nom.

Le groupe «NoName057(16)» mobilise pour ses attaques des cyberactivistes («heroes») qui mettent à disposition, contre rémunération, leur propre ordinateur pour les attaques DDoS. Ceux-ci peuvent en outre proposer des cibles à attaquer. Le groupe leur fournit le client DDoS «DDoSia». Les «heroes» bénéficient d'un soutien technique sur le canal Telegram «DDoSia-Project».

Les attaques basées sur Internet se sont concentrées au niveau de la couche applicative (couche 7 OSI)². Le mode opératoire de «NoName057(16)» a consisté à surcharger la capacité de traitement des sites (épuisement des ressources, en anglais *resource exhaustion*), pour rendre certains services inaccessibles au public (par ex. vente en ligne de billets CFF). La vague d'attaques a duré au total deux semaines et n'a pas évolué d'un point de vue technique durant cette période. Seules les cibles attaquées changeaient d'un jour à l'autre. Les victimes étaient plus ou moins bien préparées à de telles attaques DDoS. Certaines ont ainsi pu réagir plus rapidement que d'autres aux attaques et en réduire l'impact.

Il est possible de limiter les effets de telles attaques DDoS par des mesures aussi bien techniques (par ex. pare-feu pour applications web: adaptation de la configuration des règles de pare-feu afin que le client DDoS puisse être détecté et bloqué, voir chap. 3.3) qu'organisationnelles (par ex. plan de continuité d'activité - PCA³).

La menace latente de telles attaques DDoS justifie de suivre en permanence les développements spécifiques du cyberspace, d'en évaluer les risques et, si nécessaire, d'adapter les dispositifs de sécurité. Les pannes survenues et leurs comptes rendus dans les médias ont révélé qu'il reste parfois un potentiel d'amélioration, quand il s'agit de préparer la réaction à ce genre d'attaques. Certaines victimes ont déjà mis en œuvre des mesures utiles.

¹ https://fr.wikipedia.org/wiki/Attaque_par_déni_de_service

² <https://fr.wikipedia.org/wiki/Modèle OSI>

³ [https://fr.wikipedia.org/wiki/Plan_de_continuité_d'activité_\(informatique\)](https://fr.wikipedia.org/wiki/Plan_de_continuité_d'activité_(informatique))

2 Introduction

2.1 Contexte géopolitique

La Russie a attaqué militairement l'Ukraine à la fin de février 2022. Dans ce conflit, l'Ukraine subit également des attaques dans le cyberspace, dues tant à des acteurs étatiques qu'au cyberactivisme (hacktivisme). La Russie aussi fait l'objet de cyberattaques lancées par divers cyberactivistes et par d'autres organisations. D'autres pays sont dans la même situation, à commencer par les États membres de l'OTAN.

Dans le sillage du conflit ukrainien, la cyberactivité émanant de hacktivistes et visant la Suisse ou des cibles basées en Suisse est demeurée globalement marginale. Le nombre d'incidents et leur intensité sont restés conformes à l'analyse de la menace faite par le Centre national pour la cybersécurité (NCSC) et le Service de renseignements de la Confédération (SRC). La réalisation d'une menace potentielle ne change rien à la situation de la menace, et la Suisse reste susceptible d'être ponctuellement confrontée à une cyberactivité relevant de l'hacktivisme. Mais jusqu'à présent, des mesures de sécurité et de lutte conventionnelles (atténuation des attaques) ont permis d'y faire face. Par conséquent, les dommages subis par la Suisse restent mineurs à ce jour.

Dans son rapport de situation «La sécurité de la Suisse 2023»⁴, le SRC explique en détail la situation. La carte ci-après indique les cyberattaques menées par des hacktivistes durant la première année de guerre (attaques affectant la disponibilité/DDoS):

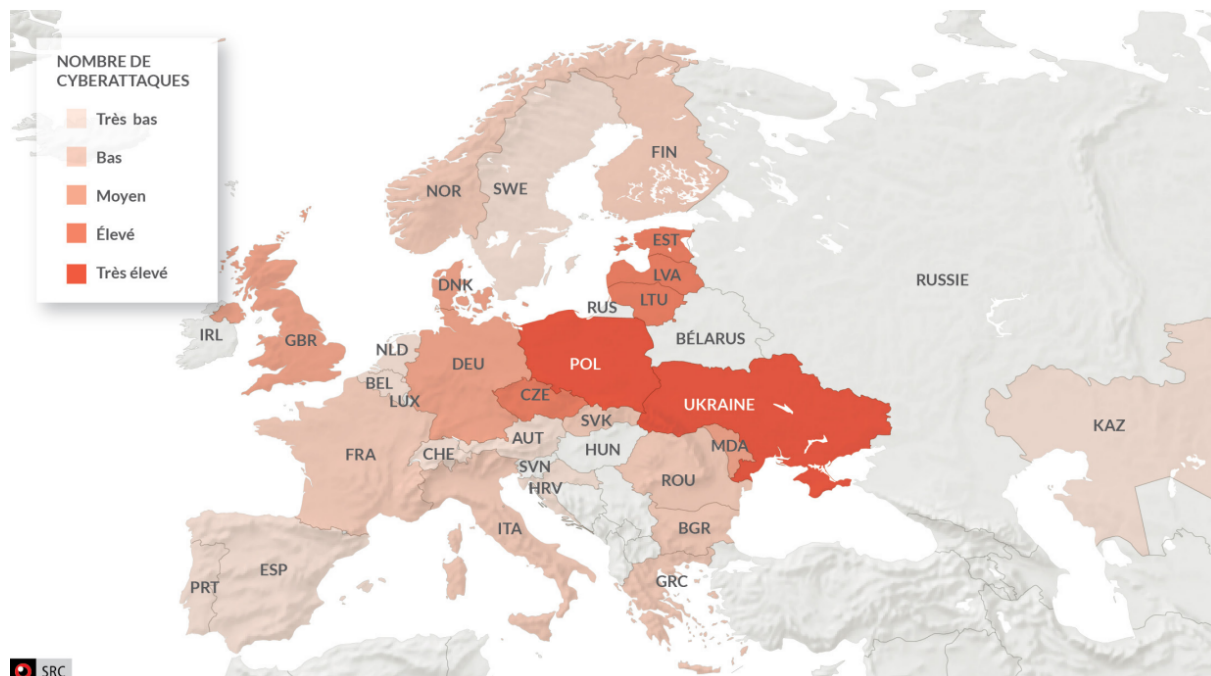


Figure 1: Attaques DDoS menées par des hacktivistes durant la première année de guerre, source: SRC, Rapport de situation 2023

Le terme «cyberguerre»⁵ est un mot-valise formé de **cyber**espace et **guerre**. Il désigne l'usage offensif des technologies de l'information sur une longue période par deux États en conflit (militaire).

⁴ https://www.vbs.admin.ch/fr/ddps/organisation/unites-administratives/service-renseignement.detail.document.html/vbs-internet/fr/documents/service_renseignement/rapports_des_situation/NDB-Lagebericht-2023-f.pdf.html

⁵ <https://fr.wikipedia.org/wiki/Cyberguerre>

Selon cette définition, les attaques par déni de service distribué (DDoS) que le groupe «NoName057(16)» a commises en juin dernier contre différentes cibles situées en Suisse ne peuvent être assimilées à un événement belliqueux s’inscrivant dans une cyberguerre, mais relèvent plutôt du cyberactivisme (voir chap. 2.2).

2.2 Catégorisation

Les attaques DDoS menées contre la Suisse étaient dues à des hacktivistes animés de mobiles politiques. Durant ce cyberincident, ils ont relayé des éléments de propagande prorusse. Le groupe est ponctuellement parvenu à paralyser les sites web pris pour cible (voir chap. 3.2). C’est ce qui a amené le NCSC à ranger les attaques DDoS de juin dans le **cyberactivisme**⁶:

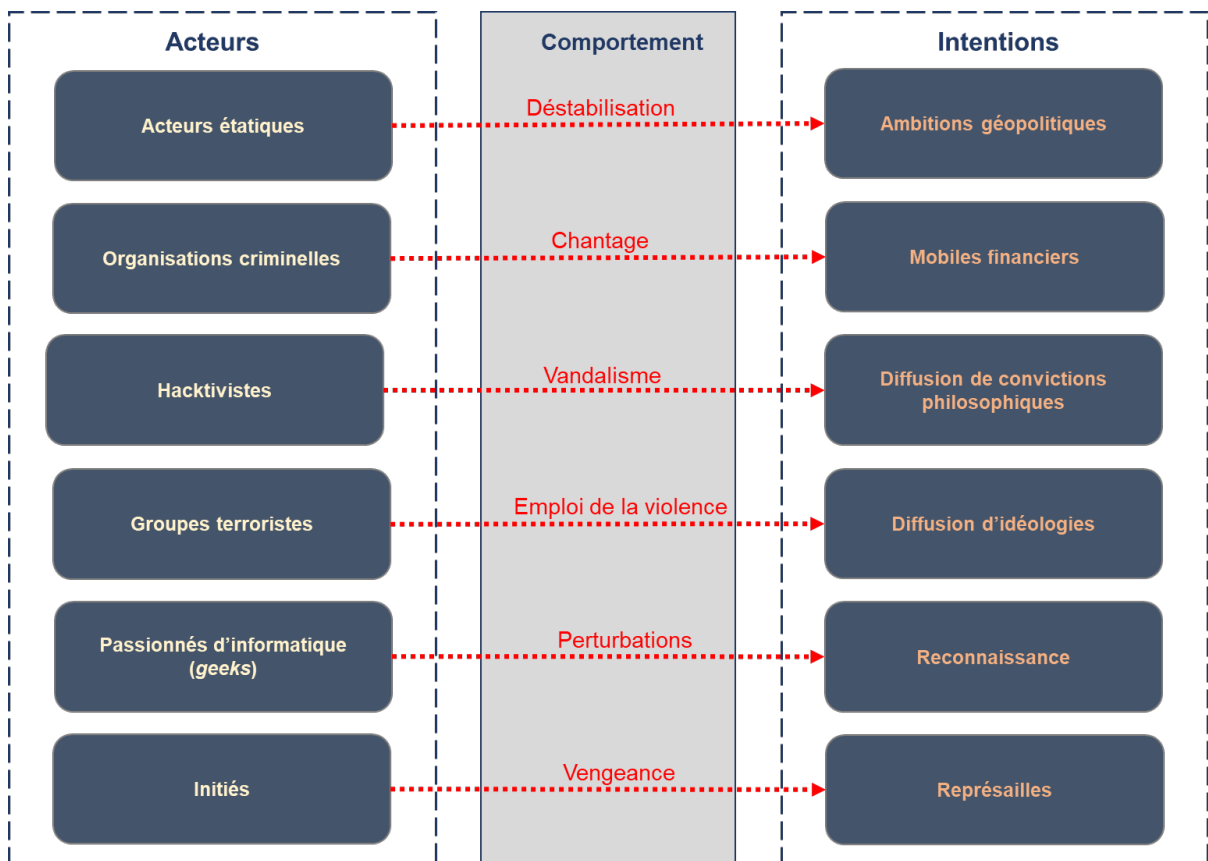


Figure 2: Acteurs, comportements et intentions

Le groupe «NoName057(16)» fait connaître ses succès potentiels par le service de messagerie instantanée Telegram. Cet acteur vise ainsi à attirer l’attention sur ses activités inspirées par un mobile politique. La diffusion médiatique des succès obtenus et la captation de l’attention politique et sociale qui s’ensuit, dans le pays agressé, relèvent de facto d’opérations d’information (*Info Ops*).

⁶ <https://fr.wikipedia.org/wiki/Cybermilitantisme>

3 Description de l'attaque

3.1 Type d'attaque DDoS

Il existe différentes possibilités de surcharger les ressources de systèmes lors d'attaques DDoS. Les attaques commises cherchaient à imiter le comportement d'utilisateurs humains légitimes de sites Internet, en appelant automatiquement des services tels que les formulaires de recherche ou d'inscription, au détriment de la logique métier située en aval. Il faut dire que la logique métier et les composants du réseau en amont, à l'instar des serveurs d'applications, des équilibreurs de charge (*Loadbalancer*) ou des pare-feu pour applications web (*Web Application Firewall - WAF*), sont dimensionnés pour des raisons économiques en fonction du nombre d'utilisateurs attendus. Ces ressources risquent donc d'être sollicitées au-delà de leurs limites de performance par de tels accès générés artificiellement et de ne plus pouvoir offrir leurs services aux utilisateurs réels. Quant aux sites web, ils ne peuvent être utilisés comme d'habitude, voire restent inaccessibles.

Un examen technique plus approfondi figure au chap. 3.3.

3.2 Groupe «NoName057(16)»

Le groupe «NoName057(16)» a publiquement revendiqué sur Telegram ces attaques DDoS. Il s'agit d'un collectif prorusse actif depuis mars 2022. Apparue pour la première fois lors de l'invasion russe de l'Ukraine (février 2022), ce groupe a déclaré la «cyberguerre» à la «guerre de l'information menée contre la Russie». Il communique essentiellement par Telegram et signale également ses cibles par ce canal. En outre, ses abonnés peuvent faire part de leurs souhaits sur Telegram quant à la prochaine cible attaquée.

Approche générale

Le graphique ci-après désigne l'approche générale en trois phases du groupe (voir la description technique au chap. 3.3):

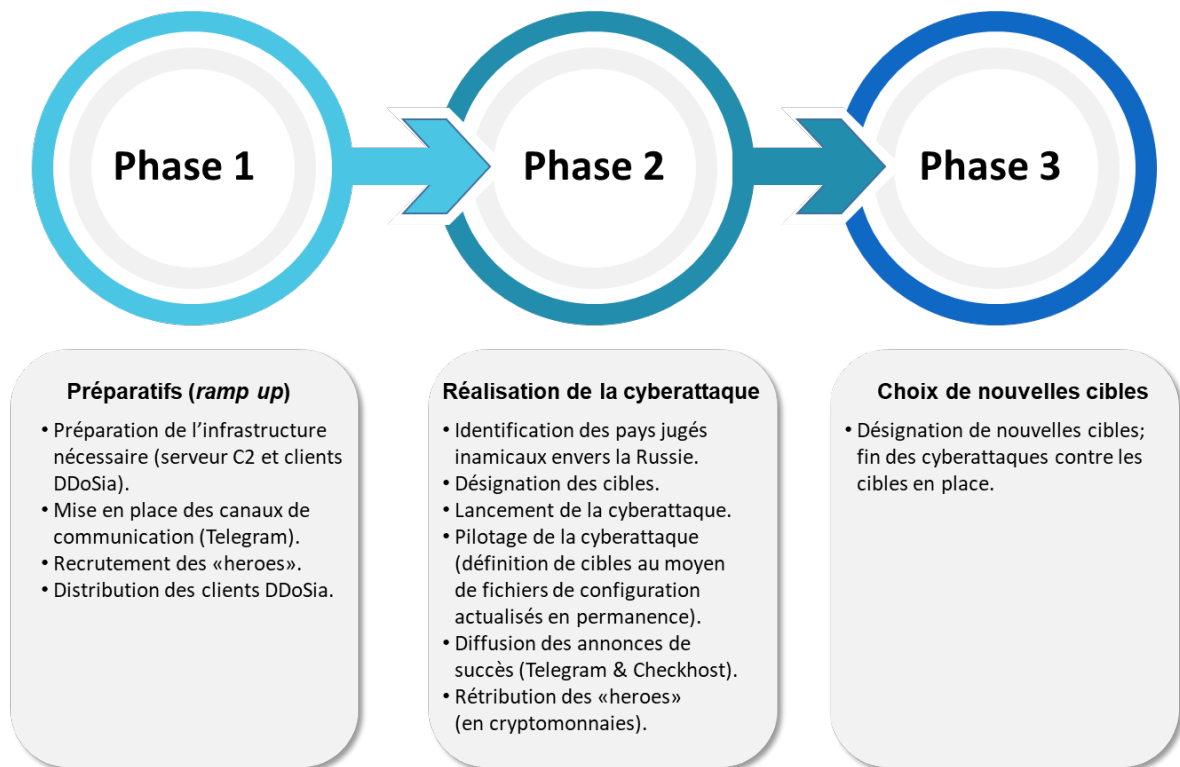


Figure 3: Approche générale

Cibles attaquées

Le groupe s'en prend essentiellement à des sites web hébergés en Ukraine ou dans des pays de l'OTAN et de l'UE. Il s'est avéré que les pays qui soutiennent l'Ukraine ou qui prennent des sanctions contre la Russie peuvent également être pris pour cible. La Suisse l'a elle aussi brièvement appris à ses dépens, à la suite de deux décisions des Chambres fédérales jugées trop favorables à l'Ukraine (voir chap. 8, [1] et [2]). Les attaques DDoS contre la Suisse ne reposaient sur aucun motif économique, et donc n'étaient pas liées à la prospérité helvétique. La Suisse n'a été prise pour cible que pendant une semaine. Tout indique qu'à l'avenir aussi le groupe s'attaquera à des États à des fins de propagande.

Le diagramme ci-après indique toute une série d'États pris pour cibles entre le 1^{er} avril et le 24 juin 2023 par le groupe:

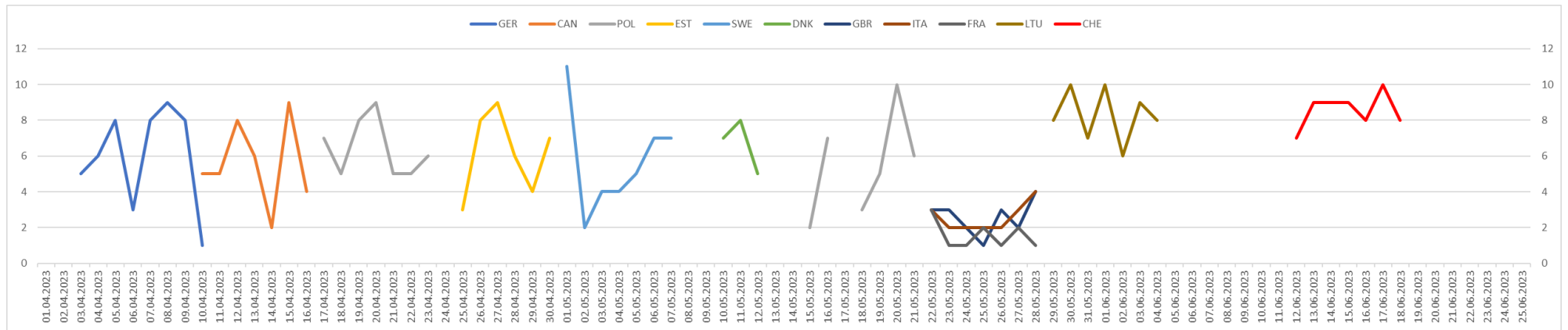


Figure 4: Attaques DDoS contre d'autres États avant, pendant et après sa cyberattaque contre la Suisse (liste non exhaustive)

On voit bien que la Suisse (abréviation CHE selon la norme ISO) n'est que l'un des nombreux pays pris pour cibles. On remarque encore qu'avant même ses attaques DDoS contre la Suisse, menées du 12 au 18 juin 2023, le collectif «NoName057(16)» était déjà actif contre d'autres pays.

Analyse de la menace

Le graphique ci-après présente les résultats de l'analyse de la menace (*threat assessment*) effectuée par le NCSC pour «NoName057(16)». On y voit par exemple que la vague d'attaques présentait une complexité (*threat level*) plutôt faible, mais que les attaques DDoS ont été menées avec une intensité élevée (*attack frequency*):

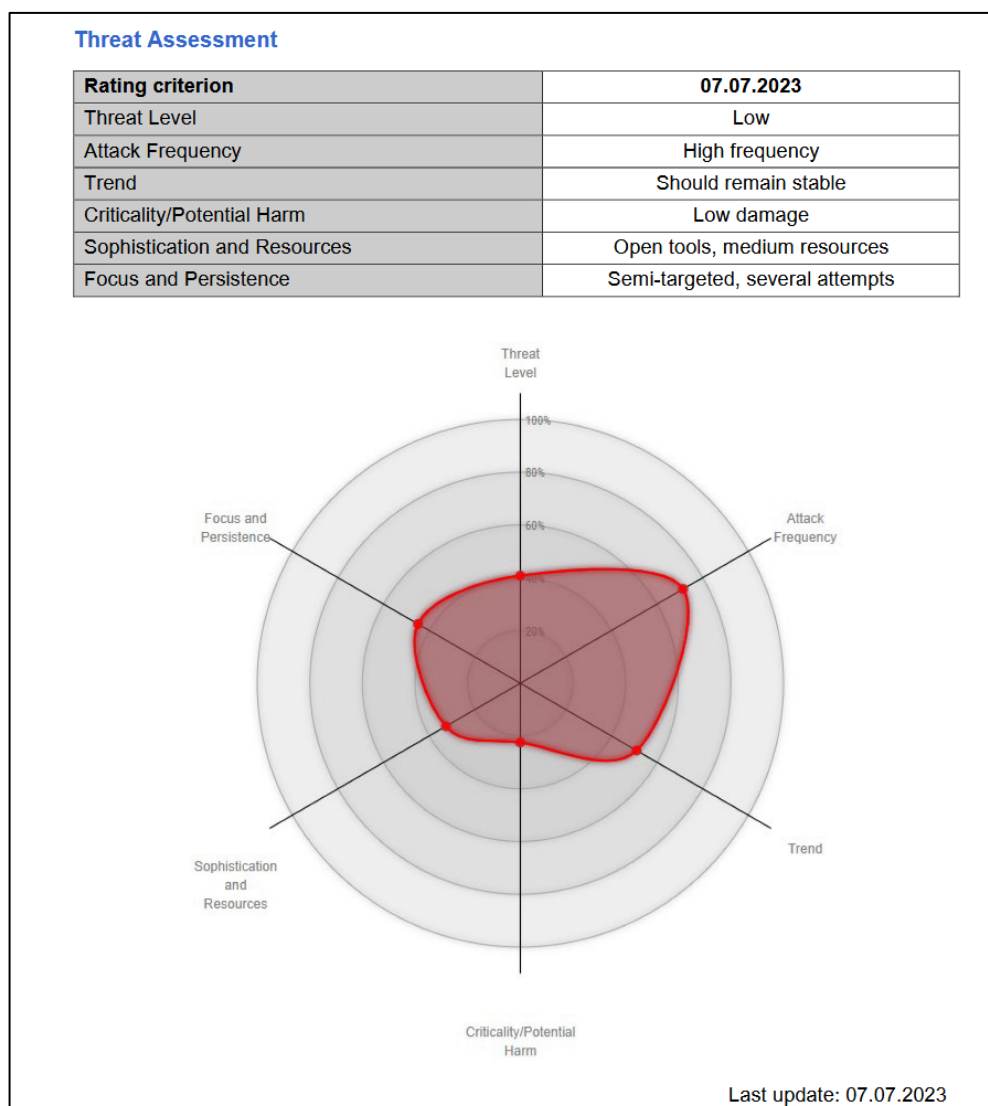



Figure 5: Analyse par le NCSC de la menace émanant de «NoName057(16)»

Motifs du groupe

Le 11 mars 2022, le collectif «NoName057(16)» a lui-même publié dans Telegram la charte suivante portant sur ses activités:



ГREETINGS, COMRADES!

The hacker group NoName057(16) is on the warpath with Ukrainian under-hackers and their corrupt henchmen!

These fans of the neo-fascists who seized power in Ukraine are trying to attack the Internet resources of our country and intimidate our compatriots with their attacks on social networks and other communication channels. In response to their miserable attempts, we are carrying out massive attacks on dire propaganda resources that blatantly lie to people about Russia's special operation in Ukraine, as well as on the websites of Ukrainian unfortunate hackers who are trying to support Zelensky's neo-Nazi regime and a handful of drug addicts and Nazis from his pack!

We have a number of successful attacks on Ukrainian resources behind us, as a result of which users' access to them was paralyzed. And this is just the beginning.

Enemies, we want to recall the words of the famous Russian commander Alexander Nevsky: "Whoever comes to us with a sword will die by the sword!"

Here we will talk about our cases and attacks.

Figure 6: Traduction anglaise d'un post publié par «NoName057(16)»

Pour faire entendre ses préoccupations politiques et atteindre ses objectifs, le groupe lance et coordonne des attaques DDoS visant à attirer la plus grande attention possible.

Dans un autre post publié dans Telegram, le groupe explique la méthode d'attaque choisie de la manière suivante:

Motif invoqué par le groupe	Qualification par le NCSC	Succès selon le NCSC
«Si les serveurs d'entreprises se trouvent dans le nuage, le trafic réseau supplémentaire aboutit à des frais accrus.»	Le groupe vise à causer un dommage financier.	But en partie atteint. Aucun préjudice économique majeur n'est à signaler.
«Si un site web reste déconnecté du réseau pendant plus de deux jours, sa visibilité dans les moteurs de recherche est nettement moins bonne.»	Le groupe veut rendre les sites web plus difficiles à trouver.	But non atteint. La visibilité dans les moteurs de recherche n'a pas souffert.
«Le site web a beau être à nouveau disponible, la réputation de son exploitant continue de souffrir.»	Le groupe cherche à nuire à la réputation de ses cibles.	But non atteint. La réputation des victimes a souffert tout au plus lors de la cyberattaque.
«Les systèmes attaqués sont susceptibles de divulguer des informations vers l'extérieur par des messages générés automatiquement (par ex. information interne sur les banques de données).»	Le groupe vise à provoquer une fuite d'informations techniques.	But en partie atteint. Le NCSC ne peut exclure que de telles informations aient été divulguées durant la cyberattaque.

Tableau 1: Raisons invoquées par «NoName057(16)» et appréciation du NCSC

Chaque fois qu'une cyberattaque aboutit, un message posté à titre de preuve sur le canal Telegram **@noname05716** signale le site web attaqué, en ajoutant le drapeau du pays et un lien vers un compte rendu du site check-host.net.

Le site web check-host.net indique si les sites web de différents pays sont atteignables (en ligne). Il permet encore de générer une succession d'instantanés pour voir si à un moment donné, des sites étaient consultables ou non. Le groupe présente le message indiquant que la cible attaquée n'était pas accessible à un moment donné comme preuve de la réussite de la cyberattaque (trophée). Ce message dans Telegram est complété par divers messages et des encouragements à rejoindre et à soutenir le groupe.

Canaux de communication

Le groupe utilise essentiellement deux canaux Telegram pour sa communication:

- **@noname05716**: canal de discussions générales en langue russe (le plus souvent: copies d'écran des attaques DDoS réussies).
- **@noname05716eng**: traduction en anglais de nombreux messages du principal canal de discussion.

La communication élargie emprunte des canaux supplémentaires:

Nom d'origine du canal	Traduction française
DDoSia - мануалы + актуальное ПО	DDoSia – manuels + logiciels actuels
DDoSia - поддержка	Soutien du projet DDoSia
Полезные материалы	Matériel utile
Общий чат	Discussion générale
English support	Assistance en anglais
Предложение целей	Propositions d'objectifs
Ваши видео и скриншоты работы с клиентом DDoSia	Vidéos et copies d'écran de votre travail avec le client DDoSia

Tableau 2: Liste des canaux Telegram, avec traduction française

Modèle d'exploitation du groupe

Le groupe n'utilise pas de réseau de zombies (*botnet*) classique⁷, mais compte sur le soutien de volontaires, appelés «heroes». Ceux-ci installent sur leur propre ordinateur le client DDoSia (voir plus loin), qui est utilisé pour lancer les cyberattaques.

Les «heroes» s'enregistrent à l'aide d'un logiciel robot opérant dans Telegram. Celui-ci leur envoie ensuite un lien URL servant à télécharger les fichiers DDoSia exécutables et un fichier texte avec un identifiant unique des nouveaux «heroes» enregistrés.

Les «heroes» ont la possibilité de s'enregistrer avec leur numéro d'identification et un portefeuille cryptographique auprès du robot Telegram. Le groupe promet aux «heroes» un paiement en cryptomonnaies basé sur le nombre de cyberattaques qu'ils ont réalisées. La rémunération dépend du nombre total d'attaques lancées un jour donné par tous les volontaires actifs.

Un post du groupe publié en mars 2023 sur Telegram révèle le schéma de paiement en place:

- 80 000 roubles pour la première place
- 50 000 roubles pour la deuxième place
- 20 000 roubles pour la troisième place

Les «heroes» s'étant classés entre la quatrième et la dixième places devaient se partager un budget total de 50 000 roubles.

Les paiements s'effectuent en cryptomonnaies comme l'Ethereum, le Bitcoin et le Tether. Les «heroes» peuvent se procurer par le canal DDoSia de Telegram des informations sur leurs statistiques de productivité (liste des dix meilleurs).

L'identité du bailleur de ces moyens financiers reste obscure. Contrairement à d'autres

⁷ <https://fr.wikipedia.org/wiki/Botnet>

cyberactivistes, le groupe n'a pas lancé à ce jour d'appels aux dons, par exemple dans les médias sociaux.

3.3 Description technique

Au début de la guerre en Ukraine, le NCSC a constaté une recrudescence d'activités DDoS menées avec le maliciel «Bobik»⁸. Les victimes ignoraient que leur ordinateur avait été infecté et participait à des attaques DDoS malveillantes. «NoName057(16)» a entre-temps changé de philosophie et appelle publiquement, dans les médias sociaux, les volontaires à se servir en tant que «heroes» d'un client DDoS spécial baptisé «DDoSia».

Le passage de Bobik à ce client DDoS spécifique a sensiblement réduit les frais d'exploitation supportés par le groupe, car il n'a plus besoin d'appareils infectés. Le changement obéit donc à une logique économique.

Les attaques DDoS du groupe s'inscrivent dans le projet DDoSia⁹, formé de serveurs de commande et de contrôle (serveurs C2) et de clients DDoSia. DDoSia a vu le jour en septembre 2022 pour donner aux soi-disant «heroes» la possibilité, via Telegram, de mettre volontairement à disposition leur ordinateur et leur connexion Internet afin de lancer des cyberattaques.

Description du client DDoSia

Le client DDoSia, qui fait l'objet de perfectionnements constants, est programmé en langage «Go» et fonctionne sur les plateformes Linux, Windows, MacOS et Android.

Le client DDoSia utilise par défaut l'agent utilisateur (*User-Agent*) «Go-http-client/1.1» du langage de programmation «Go». L'identifiant correspondant n'a pas changé du début à la fin des attaques DDoS. L'identification univoque de l'agent utilisateur a simplifié l'atténuation à l'aide de pare-feu pour applications web (WAF). En effet, il a suffi d'adapter la configuration du pare-feu pour bloquer cet agent utilisateur.

Aucun cas de dissimulation de l'adresse IP du client DDoSia par usurpation d'identité¹⁰ n'a été constaté. Autrement dit, les «heroes» sont potentiellement identifiables à l'aide de leur adresse IP. Le groupe recommande donc dans ses canaux d'assistance pour Telegram d'utiliser VPN pour rendre l'identification des «heroes» plus difficile.

Des informations plus complètes sur le client DDoSia, y compris sa rétro-ingénierie, peuvent être consultées sur le blog de l'éditeur de cybersécurité Sekoia (voir chap. 8, [4]).

⁸ <https://decoded.avast.io/martinchlumecky/bobik/>

⁹ <https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/>

¹⁰ https://fr.wikipedia.org/wiki/Attaque_par_usurpation_d'identit%C3%A9

Description de la communication de commande et de contrôle

Le schéma ci-dessous montre le déroulement de la communication entre les clients DDoSia et les serveurs de commande et de contrôle (C2)¹¹:

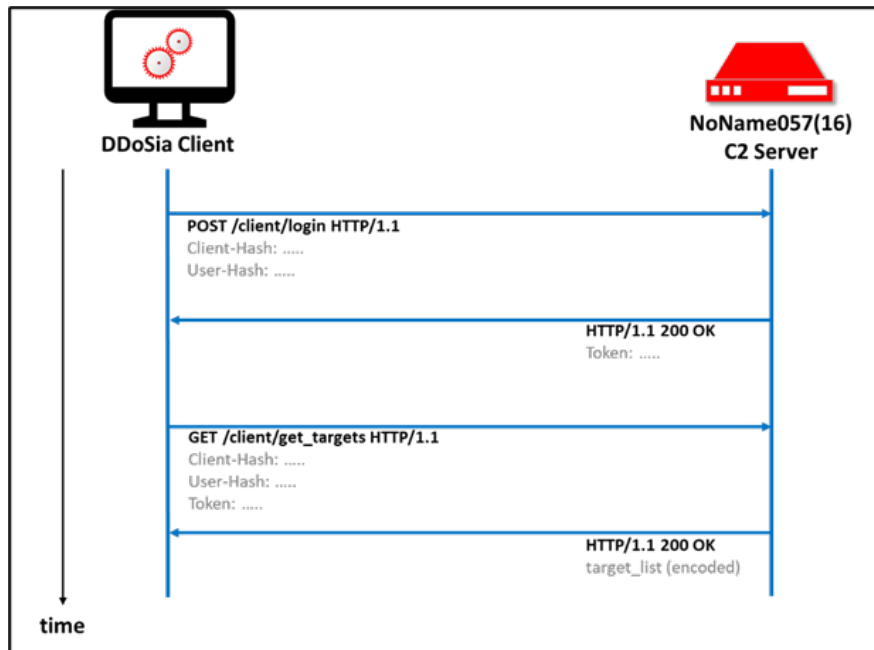


Figure 7: «Communication entre DDoSia et le serveur C2»

La communication entre les clients DDoSia et les serveurs C2 est personnalisée au moyen d'un double hachage, le premier au niveau de l'utilisateur (*user hash*) et le deuxième au niveau de sa machine (*client hash*), qui permet d'identifier le participant et son ordinateur. Le premier sert également à identifier l'utilisateur en vue du paiement des «heroes». Le client DDoSia reçoit ensuite la liste des cibles à attaquer (*target_list (encoded)*).

¹¹ <https://www.techtarget.com/whatis/definition/command-and-control-server-CC-server>

Communication avec la cible de l'attaque

Le client DDoSia génère les requêtes concrètes auprès des sites web en question à partir des instructions figurant dans la liste des cibles à attaquer (récupérées sur les serveurs C2).

À cet effet, il utilise un modèle, complété par des chaînes de caractères aléatoires. Le groupe veille dans la conception de ses modèles et des contenus générés de façon aléatoire à ce que le trafic de données ressemble beaucoup à des requêtes web légitimes afin de déjouer la détection automatique des attaques DDoS.

Le schéma ci-dessous indique comment le client DDoSia imite le trafic légitime, trompant ainsi les mécanismes de protection et empêchant le trafic malveillant d'être intercepté. Il s'ensuit que les mécanismes de protection, à l'instar de la protection DDoS et des pare-feu, ne parviennent généralement pas à détecter et bloquer automatiquement ce trafic de données:

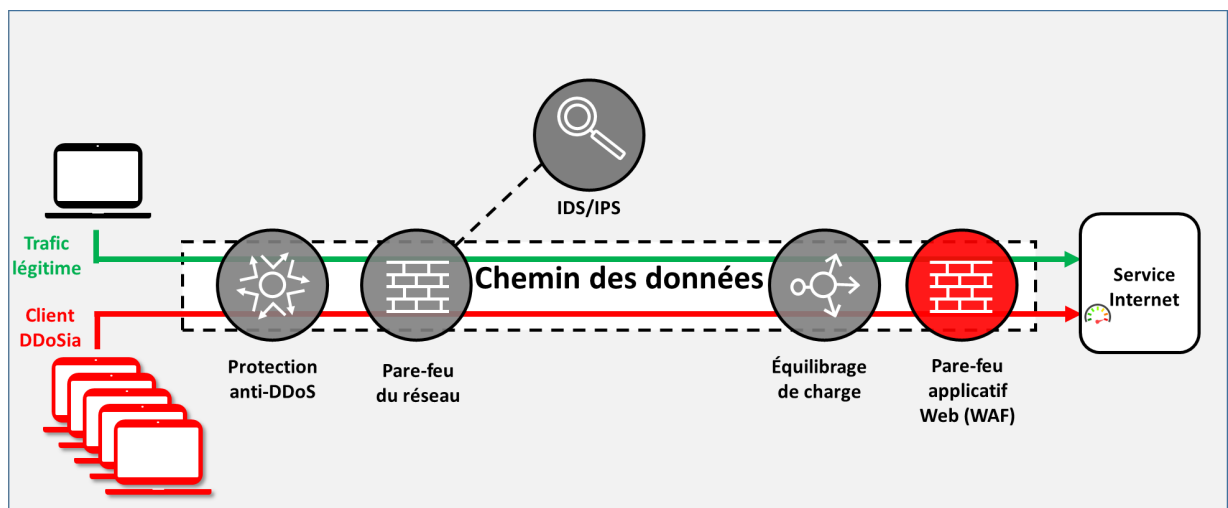


Figure 8: Trafic malveillant en provenance du client DDoSIA

Les exemples suivants montrent des modèles complétés par des chaînes de caractères aléatoires:

Exemple 1:

- Modèle: "hxxp[s]://www.webseite.ch/de/search/?term=\$_1"
- \$_1 est une chaîne de 6 à 12 caractères aléatoires (par ex. ici: kenuab)

URL consultée: "hxxp[s]://www.webseite.ch/de/search/?term=kenuab"

Exemple 2:

- Modèle: "hxxp[s]://www.webseite.ch/de/register/?name=\$_1.\$_1@\$_2.ch"
- \$_1 est une chaîne de 6 à 8 caractères aléatoires en lettres minuscules, et \$_2 une chaîne de 10 à 12 caractères aléatoires également en lettres minuscules (par ex. ici \$1: goenza.leurebe et \$2: pahelsnwmni)

URL consultée:

"hxxp[s]://www.webseite.ch/de/register/?name=goenza.leurebe@pahel
snwmni.ch"

Autrement dit, le client DDoSia génère en permanence des requêtes web dont les paramètres diffèrent à chaque fois et dont la charge de traitement se répercute sur les infrastructures informatiques en aval (par ex. banques de données utilisées dans les processus d'affaires). En raison de leur structure dynamique, ces requêtes sont très difficiles à distinguer du trafic légitime.

Réaction technique à l'attaque DDoS (*mitigation*)

L'analyse des modèles d'attaque (par ex. par filtrage des fichiers journaux de l'agent utilisateur du client DDoSia) permet de dresser une liste d'adresses IP des «heroes» impliqués. Grâce à cette liste, il est possible de bloquer le trafic réseau malveillant au niveau du routeur Internet (*edge router*) de l'organisation touchée, voire même déjà au stade du fournisseur de services Internet (par ex. en reroutant le trafic vers un trou noir¹²).

Dans le cadre des attaques DDoS examinées, les fournisseurs de services Internet suisses ont neutralisé le trafic DDoS dans leur réseau dorsal. À cet effet, ils ont bloqué des plages d'adresses IP et des systèmes autonomes, en adaptant continuellement les blocages au cours des cyberattaques. Les blocages ont été effectués sur la base de l'échange d'informations approfondi mis en place par le NCSC.

Comme les processus de sécurité et d'exploitation (gestion des réponses aux incidents, gestion du changement et gestion des versions) demandent tout un travail manuel (par ex. définition des règles de blocage), il faut compter un certain temps entre la détection et l'atténuation de telles attaques DDoS. Selon les expériences et témoignages actuels, un temps de réaction d'environ deux heures est à prévoir.

Le groupe ne peut pas toujours connaître les mesures de protection déployées dans les organisations concernées. Il faut donc s'attendre à ce que ses attaques se poursuivent sans relâche, mais sans produire de nouvelle panne.

Quantification

Les attaques DDoS menées contre l'administration fédérale provenaient de 20 000 adresses IP différentes. Statistiques à l'appui, seuls 3 % de ces adresses se situaient dans des plages IP appartenant à la Suisse.

Le trafic de données de ces attaques DDoS était plutôt faible, avec une moyenne de 20 000 à 25 000 pps (paquets par seconde) et moins de 200 Mbit/s (mégabits par seconde). De tels paramètres sont typiques des attaques DDoS menées au niveau de la couche applicative.

¹² [https://fr.wikipedia.org/wiki/Black_hole_\(informatique\)](https://fr.wikipedia.org/wiki/Black_hole_(informatique))

4 Dérroulement de l'attaque

Le mercredi 7 juin 2023 vers 8 heures, quand débutent les attaques DDoS contre la Suisse, le site <https://www.parlament.ch> est le tout premier à figurer dans la liste des cibles du serveur C2.

Deux raisons semblent avoir conduit au choix de cette nouvelle cible:

- les discussions menées au Parlement suisse sur les réexportations d'armes¹³;
- l'annonce le 5 juin du discours en visioconférence que Volodymyr Zelensky tiendrait le 15 juin 2023 devant le Parlement suisse¹⁴.

Les abonnés au canal Telegram du groupe ont eu droit à l'information suivante:

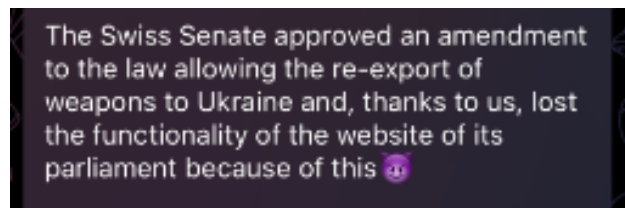


Figure 9: Premier message diffusé par le canal Telegram, source: Telegram

L'annonce du discours en visioconférence de Volodymyr Zelensky a elle aussi fait l'objet d'un message dans Telegram:

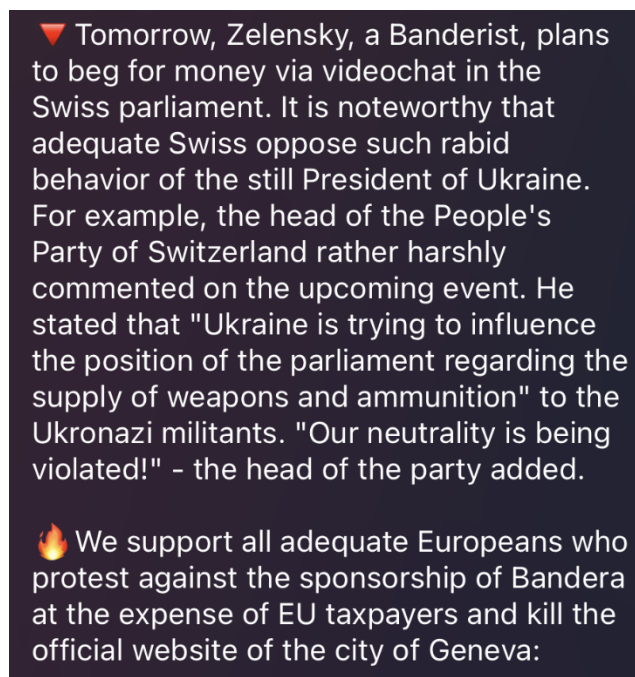


Figure 10: Second message diffusé par le canal Telegram, source: Telegram

¹³ https://www.parlament.ch/fr/services/news/Pages/2023/20230607121944115194158159038_bsf078.aspx

¹⁴ <https://www.parlament.ch/press-releases/Pages/mm-info-2023-05-31.aspx?lang=1036>

Chronologie des faits

Les attaques DDoS ont duré près de deux semaines. Il convient de signaler ici que le groupe avait déjà lancé auparavant des attaques à peu près équivalentes (en termes de durée, sur le plan technique comme par le contenu) contre d'autres États et que ses attaques perdurent.

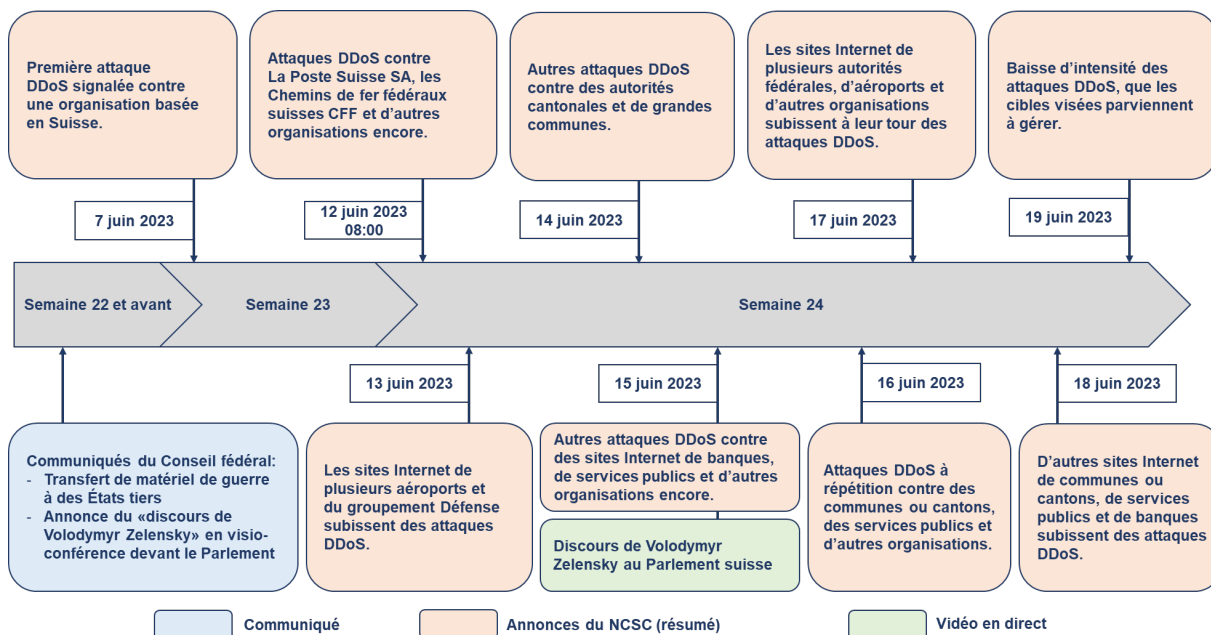


Figure 11: Brève chronologie des événements

Le tableau ci-après montre les attaques DDoS réussies:

Cibles	Date						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Administration fédérale	4	1		1		2	
Cantons			2		3		
Villes			6				6
Service public	2		1	1			1
Aéroports		8				6	
Secteur financier				5		2	1
Autres				1	3		
Armement				1			
Total 57	6	9	9	9	6	10	8

Tableau 3: Liste récapitulative des attaques DDoS réussies

On voit ainsi qu'il y a eu en moyenne huit attaques DDoS réussies par jour. Celles-ci se sont clairement concentrées sur les sites Internet d'aéroports, d'organisations du secteur financier et de villes. En outre, elles ont privilégié des autorités au début de la semaine 24, et s'en sont surtout prises en fin de semaine à des cibles du secteur privé.

Un autre tableau met en regard les attaques signalées au NCSC avec les attaques DDoS signalées comme réussies (voir Tableau 4):

Date	Sources	
	Attaques annoncées au NCSC	Attaques DDoS signalées comme réussies
12.06.2023	11	6
13.06.2023	11	9
14.06.2023	10	9
15.06.2023	11	9
16.06.2023	10	6
17.06.2023	16	10
18.06.2023	16	8
Total	85	57

Tableau 4: Comparaison entre les annonces reçues par le NCSC et les publications du groupe sur Telegram

Si l'on compare les 57 attaques DDoS réussies du Tableau 3 au total des attaques DDoS signalées au NCSC (85 annonces, voir Tableau 4), on constate une différence significative. Il en ressort que quelques organisations et autorités ont su atténuer les attaques DDoS ou, du moins, éviter des interruptions de service notables.

Le tableau ci-après (voir Tableau 5) précise la chronologie des faits qui précède (l'intensité des attaques allant croissant de jour en jour):

Date	Attaques lancées contre des autorités ou des organisations et signalées au NCSC	Remarque
12.06.2023	<ul style="list-style-type: none"> • login.swisspass.ch • www.swisspass.ch • account.post.ch • www.post.ch • www.sob.ch • www.sbb.ch • www.edi.admin.ch • www.fedpol.admin.ch • www.bazg.admin.ch • www.ejpd.admin.ch • www.parlament.ch 	Le premier jour, les cyberattaques se sont concentrées sur des autorités et des organisations proches de l'État.
13.06.2023	<ul style="list-style-type: none"> • www.vtg.admin.ch • www.flughafen-zuerich.ch • www.gva.ch 	Le deuxième jour, les sites web du groupement de la Défense au Département fédéral de la défense, de la protection de la population et des sports (DDPS) ainsi que de différents aéroports ont été attaqués.
14.06.2023	<ul style="list-style-type: none"> • www.geneve.com • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch 	Le troisième jour, le groupe s'est surtout attaqué aux villes.

Date	Attaques lancées contre des autorités ou des organisations et signalées au NCSC	Remarque
	<ul style="list-style-type: none"> • www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch 	
15.06.2023	<ul style="list-style-type: none"> • www.ncsc.admin.ch • www.ruag.com • www.postauto.ch • www.zvv.ch • www.swissid.ch 	La vague d'attaques du quatrième jour a submergé à nouveau des autorités et des organisations.
16.06.2023	<ul style="list-style-type: none"> • www.nw.ch • www.steuern-nw.ch • etax-login.nw.ch • www.stans.ch • www.buochs.ch • www.snb.ch 	Le cinquième jour, le groupe s'est surtout attaqué aux autorités du canton de Nidwald.
17.06.2023	<ul style="list-style-type: none"> • www.ejpd.admin.ch • www.fedpol.admin.ch • www.bazg.admin.ch • sob.ch • www.post.ch • gva.ch • www.edi.admin.ch • www.vtg.admin.ch 	Le sixième jour, les autorités fédérales ont à nouveau été prises pour cibles.
18.06.2023	<ul style="list-style-type: none"> • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.montreux.ch • www.stadt.sg.ch • www.stmoritz.com • stadt.winterthur.ch • bellinzona.ch • www.ville-fribourg.ch • www.stadt-schaffhausen.ch 	Des villes ont encore été visées le dernier jour de la vague d'attaques.

Tableau 5: Liste des sites Internet attaqués du 12 au 18 juin 2023

5 Effets de la cyberattaque

Les messages publiés par le groupe sur son canal Telegram en russe ont été lus à chaque fois par près de 5500 participants. En outre, entre 1000 et 1500 personnes les ont lus sur son canal Telegram en anglais. Le groupe n'a toutefois guère relayé ses succès sur les réseaux sociaux (par ex. Twitter) – alors qu'au moment de l'attaque, les médias suisses en ont abondamment parlé (voir chap. 5.1).

Comme les attaques se concentrent sur la couche applicative, la menace est bien réelle au cas où le site Internet ne pourrait être sécurisé par le blocage de plages d'adresses (à l'aide d'adresses IP sources ou par blocage de systèmes autonomes¹⁵), par exemple parce que les Suisses de l'étranger doivent pouvoir y accéder. En effet, il faut d'abord adapter la configuration des pare-feu pour applications web (WAF) à l'attaque spécifique. La cible reste vulnérable jusqu'à ce que ces configurations soient effectuées. Le NCSC estime que de telles adaptations prennent deux heures. Les processus utilisés (par ex. analyse, préparation, déploiement) dépendent des processus de sécurité et d'exploitation internes (gestion de la réponse aux incidents, gestion du changement et gestion des versions) ou bien des dispositions prévues dans l'accord de niveau de service en vigueur pour les services de sécurité gérés ayant été externalisés (processus et temps de réaction).

On peut citer ici comme exemple le compte électronique de la Ville de Bâle qui, le mercredi 14 juin 2023, a été surchargé par des tentatives d'ouverture de session simultanées. Le surlendemain, le portail des finances du canton de Nidwald connaissait pareil sort. Les sites web attaqués sont rapidement redevenus accessibles aux internautes suisses, après l'adaptation des mesures de protection.

Les victimes des cyberattaques ont subi un double préjudice, entre le dommage réputationnel et les efforts consentis pour atténuer les attaques DDoS.

Par la suite, beaucoup d'entreprises concernées ont revu leur gestion des risques et, parfois, mieux intégré leur fournisseur de services Internet¹⁶ dans leur propre dispositif de protection (par ex. en s'abonnant à un mécanisme de protection contre les attaques DDoS).

5.1 Résonance médiatique

Le 5 juin 2023, le Parlement suisse a annoncé que Volodymyr Zelensky s'exprimerait en visioconférence dans son hémicycle le 15 juin 2023. Cette annonce et la décision du Parlement relative aux réexportations de matériel de guerre ont été l'événement déclencheur des activités DDoS déployées par NoName057(16) contre la Suisse. Le Parlement (parlement.ch) fait partie des premières organisations visées, comme l'ont annoncé les Services du Parlement sur Twitter le 7 juin 2023 à 15 h 05. Le lundi 12 juin 2023, comme d'autres sites web de l'administration fédérale n'étaient plus accessibles, le NCSC a publié un communiqué de presse sur les attaques DDoS. Les médias suisses ont largement repris ce communiqué. Le NCSC a ainsi compté une cinquantaine d'articles parus dans la presse écrite et plus de 370 articles publiés en ligne.

Les comptes rendus des médias ont attiré l'attention du grand public suisse sur les attaques DDoS et le message politique véhiculé, suscitant des incertitudes et de nombreuses questions parmi la population. Au total, plus de 40 demandes des médias sont parvenues au service de presse du NCSC. Durant ces quelques jours, Florian Schütz, le délégué fédéral à la cybersécurité, a été sous les feux des médias et a accordé une série d'interviews où il a donné

¹⁵ https://fr.wikipedia.org/wiki/Autonomous_System

¹⁶ https://fr.wikipedia.org/wiki/Fournisseur_d'accès_à_Internet

des explications sur les attaques DDoS, afin d'apaiser les craintes de la population.

L'intense couverture médiatique s'est atténuée après le discours prononcé par Volodymyr Zelensky, le 15 juin 2023. Puis, quand les attaques DDoS ont cessé, le 19 juin 2023, il n'en a plus guère été question.

Certains médias ont fait l'amalgame avec l'attaque par rançongiciel dirigée contre la société Xplain et rendue publique au même moment. Or le NCSC a toujours répété, dans ses relations avec les médias, que des groupes différents étaient à l'origine de ces deux attaques. Celle contre Xplain (fournisseur informatique de l'administration fédérale) était due au groupe «Play», tandis que le groupe «NoName» avait reconnu sur Telegram s'en être pris au site des services du Parlement. Le NCSC a également souligné qu'une attaque par rançongiciel (Xplain) obéit à une autre logique qu'une attaque DDoS inspirée par un mobile politique.

5.2 Conséquences politiques

Les attaques DDoS elles-mêmes n'ont pas suscité de forte réaction au sein des Chambres fédérales. Martin Candinas, le président du Conseil national, et Brigitte Häberli-Koller, la présidente du Conseil des États, en ont parlé dans leur conseil respectif.

Le 15 juin 2023, la conseillère nationale Doris Fiala a déposé une intervention à ce sujet (Ip. 23.3755 «Sommes-nous déjà en état de cyberguerre à l'échelon de la Confédération?»)¹⁷. Le Conseil fédéral a souligné dans sa réponse que les attaques DDoS devaient être considérées comme des actes de vandalisme et qu'elles n'avaient causé que des dommages minimes. Il a ajouté que «qualifier ces attaques de cyberguerre était excessif, car cela confortait les cybercriminels dans leur intention de semer le trouble»¹⁸.

Le Parlement continuera vraisemblablement de s'informer activement sur les mesures prises par la Confédération contre les cyberattaques en général et, à la suite des attaques, sur la protection contre les attaques DDoS en particulier. Les attaques ne devraient toutefois pas avoir d'autres conséquences politiques.

5.3 Effets juridiques

Le Ministère public de la Confédération a ouvert une procédure suite à l'attaque DDoS menée contre le site web du Parlement fédéral¹⁹. Le NCSC renvoie à la procédure en cours.

¹⁷ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20233755#tab-panel-acc-1>

¹⁸ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefte?AffairId=20233755#tab-panel-acc-2>

¹⁹ <https://www.inside-it.ch/bundesanwalt-schaft-untersucht-ddos-angriff-auf-parlamentsdienste-20230612>

5.4 Dommages effectifs

Le NCSC a mené une enquête auprès des entreprises touchées par les attaques DDoS. Selon les réponses reçues, celles-ci ont surtout déploré le mécontentement de leur clientèle, temporairement privée d'accès à leur site Internet. La plupart des pannes n'ont duré que quelques heures. Dans un seul cas, la panne s'est prolongée durant trois jours, accompagnée d'une instabilité du système. Les éventuels dommages monétaires sont impossibles à chiffrer. Les entreprises ont encore confirmé qu'aucun dommage durable n'avait été causé à leur infrastructure informatique.

Même si les autorités et les organisations touchées n'ont pas eu besoin de renforts pour combattre les attaques DDoS, leurs collaborateurs ont effectué des heures de travail supplémentaires.

À la connaissance du NCSC, aucune organisation (par ex. une PME) n'a été contrainte de cesser ses activités en raison des attaques DDoS.

L'incident confirme que nul n'est à l'abri d'attaques DDoS, qui peuvent paralyser au moins à court terme n'importe quel site web. Le NCSC recommande donc de prévoir un dispositif proactif pour assurer sa protection (voir les mesures de protection décrites au chap. 6).

6 Recommandations

Les attaques DDoS sont techniquement moins sophistiquées que les attaques complexes (par ex. *advanced persistent threats*, APT), qui visent à pénétrer les systèmes informatiques. Les défis posés par la protection contre les attaques DDoS tiennent à leur évolutivité et aux nouvelles techniques développées pour contourner les mécanismes anti-DDoS. Des mesures de sécurité robustes et une approche proactive s'avèrent par conséquent décisives pour se protéger des effets des attaques DDoS.

Le NCSC formule diverses recommandations en matière de protection, sous forme de mesures proactives ou de mesures réactives à prendre à la suite d'une attaque DDoS.

Mesures proactives

Les mesures suivantes (liste non exhaustive) doivent être mises en place en fonction des besoins, afin de déjouer une attaque DDoS potentielle:

Mesures proactives	Description / utilité	Effets sur les attaques DDoS en question
Vérifiez la pertinence des attaques DDoS dans votre gestion des risques informatiques et dans votre gestion de la continuité des services informatiques.	Les attaques DDoS jugées pertinentes dans le processus de gestion des risques informatiques seront assimilées à des risques, le cas échéant.	Des mesures tant techniques qu'organisationnelles sont mises en œuvre contre un tel risque, en amont de toute cyberattaque.
Identifiez vos sites Internet potentiellement menacés, lors d'un bilan d'impact sur votre activité (BIA).	Un BIA vous indique les exigences de disponibilité de vos sites Internet.	Les sites Internet critiques sont connus et peuvent être protégés en fonction des exigences de l'entreprise.
Consultez votre fournisseur de services Internet / votre fournisseur de services de sécurité gérés (MSSP) sur les mesures à prendre pour garantir la disponibilité de votre site web.	Les mesures visant à assurer le respect des exigences en matière de disponibilité des sites web sont convenues avec le fournisseur concerné, et leur actualité est vérifiée à intervalles réguliers.	Les mesures de protection sont fixées par contrat et peuvent être prises en cas d'attaque potentielle.
Tenez compte des mesures de protection contre les attaques DDoS dans votre architecture de sécurité (<i>security by design</i>).	Les mesures de protection contre les attaques DDoS sont mises en œuvre dès la conception des sites web. Par exemple, un réseau de diffusion de contenu (CDN) contribuera à atténuer l'impact des attaques DDoS, en répartissant le trafic entre de nombreux serveurs situés dans le monde entier.	La prise en compte, dans l'architecture de sécurité, des exigences en matière de sécurité réduit la probabilité que le trafic DDoS parvienne jusqu'aux sites web et puisse les surcharger.
Utilisez un pare-feu d'applications web (WAF) pour les sites web potentiellement menacés.	Les WAF surveillent le trafic au niveau des applications et bloquent les requêtes malveillantes avant qu'elles ne	Seule la présence d'un WAF permet de protéger rapidement les sites web contre les attaques DDoS. Il est possible d'adapter à chaque

Mesures proactives	Description / utilité	Effets sur les attaques DDoS en question
	parviennent au site web.	fois la configuration du WAF aux attaques DDoS spécifiques.
Élaborez un plan d'urgence et testez-le.	Un plan d'urgence comporte des instructions structurées en cas d'attaque DDoS. Il comprend la gestion de la continuité des services informatiques et la gestion de la continuité des activités (BCM).	Un plan d'urgence permet de réagir à une attaque DDoS de manière planifiée et structurée.

Tableau 6: Mesures proactives

Mesures réactives

Le NCSC recommande d'adopter les mesures suivantes en fonction des besoins pour répondre à une attaque DDoS potentielle:

Mesures réactives à prévoir en réponse aux attaques DDoS	Description / utilité	Effets sur les attaques DDoS en question
Surveillez les sites web exposés et mettez en place une détection automatisée des anomalies.	La surveillance du trafic de données permet de détecter des envois inhabituels ou une hausse du trafic réseau.	Cette mesure aide à la détection précoce des attaques DDoS et permet une défense efficace.
Veillez à pouvoir réagir rapidement aux attaques DDoS sur le plan technique et organisationnel.	Les mesures de protection techniques servent avant tout à détecter les attaques DDoS et à s'en protéger. Les processus de sécurité règlent les aspects organisationnels (par ex. gestion des incidents de sécurité, escalade, relations avec les médias).	Il est possible d'atténuer les attaques DDoS en temps réel, en adoptant rapidement des mesures de protection (par ex. blocage des adresses IP, adaptation de la configuration des mécanismes de sécurité par l'organisation de piquet).
Veillez à assurer en amont, dans l'architecture de sécurité, la protection des sites web contre les attaques automatisées (protection en profondeur).	La mise en œuvre des technologies CAPTCHA ²⁰ permet d'éviter qu'un formulaire en ligne d'un site web, par ex., ne puisse être rempli de manière automatisée.	Des mesures de protection en amont empêchent les attaques DDoS automatisées d'atteindre les sites web.
Bloquez les plages d'adresses IP et les systèmes autonomes sur la base des indicateurs de compromission (IoC).	Les IoC, disponibles sur le Cyber Security Hub du NCSC, servent de base à un tel blocage. Grâce à la détection d'anomalies mentionnée ci-dessus, les IoC peuvent être reconnus de manière spécifique à	Le trafic malveillant peut ainsi être bloqué.

²⁰ <https://fr.wikipedia.org/wiki/CAPTCHA>

	chaque organisation.	
Bloquez les attaques au niveau de la couche applicative.	Il est indiqué d'adapter les mécanismes de sécurité (par ex. WAF) pour contrer l'attaque spécifique sur la base d'informations tirées de différentes sources (par ex. gestion des informations et des événements de sécurité SIEM, fichiers journaux).	Le blocage du client DDoSia (agent utilisateur) permet de neutraliser l'attaque DDoS au niveau du WAF déjà.

Tableau 7: Mesures à prévoir en réaction aux attaques DDoS

Le NCSC publie sur son site Internet d'autres recommandations pratiques et mesures préventives (voir chap. 8, [3]).

7 Bilan

Les stratégies classiques de sécurité anti-DDoS, traditionnellement plutôt orientées contre les attaques DDoS volumétriques²¹, n'offrent pas une protection suffisante face au groupe actuel et à ses cyberattaques déployées au niveau de la couche applicative.

Dans le cas présent, les systèmes attaquants des cyberactivistes étaient en grande partie identifiables par leurs plages d'adresses IP et leurs systèmes autonomes, et ont ainsi pu faire l'objet d'un blocage largement ciblé. Les sites web attaqués sont donc redevenus disponibles assez rapidement. Un autre mécanisme de sécurité s'est avéré précieux, les pare-feu pour applications web (WAF). Partout où ils étaient disponibles, ils ont pu être reconfigurés en fonction du modèle d'attaque.

Si lors d'une future attaque DDoS, les cyberactivistes impliqués devaient être davantage dispersés géographiquement, de plus sévères dommages seraient à prévoir. Car il serait plus difficile d'identifier et de bloquer toutes les plages d'adresses IP et/ou les systèmes autonomes. Il faudrait donc s'attendre en pareil cas à des perturbations plus durables des sites web attaqués.

Leçons à tirer

De l'avis du NCSC, les leçons suivantes méritent d'être retenues:

- Le groupe a mené ses attaques avec succès en partie, et même pendant un certain temps, malgré les mécanismes de sécurité anti-DDoS adoptés à large échelle. Par conséquent, il faudra vérifier les dispositifs de sécurité et les adapter aux besoins;
- Les attaques DDoS peuvent également perturber la marche des affaires de tiers, si le site web attaqué avec succès est nécessaire au bon fonctionnement d'un autre site ou d'un processus d'entreprise. Un bilan d'impact sur les activités (BIA) servira de base pour identifier de tels liens de dépendance et en tenir dûment compte dans la gestion de la continuité des activités (BCM);
- Un autre bilan d'impact sur les activités (BIA) s'impose pour juger de l'influence des blocages (par ex. au moyen de plages IP) sur la marche des affaires de l'entreprise touchée (par ex. accès refusé aux utilisateurs légitimes, présence sur le web fixée dans la loi);
- La coordination ainsi que les échanges d'informations détaillées entre le NCSC et les cibles des attaques ont joué un rôle très important;
- La diffusion d'informations spécifiques à l'attaque (par ex. nom du groupe) présente des avantages et des inconvénients, qui demandent un examen systématique;
- Les mécanismes de sécurité courants (par ex. blocage des plages IP, géoblocage, pare-feu d'applications web, limitation de débit) peuvent atténuer assez rapidement les effets d'une attaque DDoS, une fois les modèles d'attaque suffisamment connus;
- Si des relations d'approbation peuvent être établies entre des réseaux isolés qui communiquent par Internet, des technologies plus récentes telles que SCiON²² pourront également être utilisées. La technologie SCiON dispose d'une protection intégrée contre les attaques DDoS;
- Les nombreux comptes rendus dans les médias ont eu pour effet de sensibiliser les autorités et les organisations suisses au thème des attaques DDoS;
- Les réponses à l'enquête du NCSC indiquent que les entreprises concernées réévalueront le risque encouru d'attaques DDoS et qu'elles réexamineront les mesures à prendre.

²¹ <https://www.cisecurity.org/insights/white-papers/ms-isac-guide-to-ddos-attacks>

²² <https://scion-architecture.net/>

Remarques finales

Les grandes organisations disposant, par exemple, d'un centre des opérations de sécurité (*security operations center*, SOC) ont pu réagir relativement rapidement, une fois que les modèles d'attaque ont été connus. Il n'est pas possible de déterminer a posteriori si des questions techniques ou l'absence de processus de sécurité ont ponctuellement entraîné des perturbations plus longues (par ex. pannes de plusieurs jours de sites web).

Il incombe aux entreprises concernées d'effectuer les adaptations nécessaires, dans le cadre du processus d'amélioration continue. Le NCSC les invite à examiner les mesures recommandées et les leçons à tirer qui figurent dans le présent rapport, et leur recommande de les mettre en œuvre sous leur propre responsabilité, en fonction de leurs besoins.

8 Annexes

Informations et explications sur les attaques DDoS

Le NCSC publie sur son site web des informations générales avec des explications sur les attaques DDoS²³.

Les différentes variantes d'attaques DDoS (par ex. attaques volumétriques ou attaques au niveau de la couche 7) sont expliquées en détail dans un document du Multi State Information Sharing & Analysis Center (MS-ISAC)²⁴, publié en collaboration avec l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA)²⁵ et le Centre pour la sécurité d'Internet (CIS)²⁶.

Sources d'information référencées

N°	Explication et adresse URL
[1]	Le président Zelensky s'adressera aux parlementaires suisses le 15 juin, https://www.parlament.ch/press-releases/Pages/mm-info-2023-05-31.aspx?lang=1036
[2]	Le Conseil des États confirme sa ligne sur les réexportations, https://www.parlament.ch/fr/services/news/Pages/2023/20230607121944115194158159038_bsf078.aspx
[3]	Recommandations du NCSC contre les attaques DDoS, https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ddos.html
[4]	Sekoia – informations détaillées concernant le client DDoSia, https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

Tableau 8: Sources d'information référencées

Catégorisation des acteurs et de leurs motivations

Pour évaluer l'impact des cyberattaques, il est important dans un premier temps de déterminer quels acteurs malveillants mènent les attaques. Ceux-ci peuvent à leur tour être distingués en fonction de leur motivation et classés dans les catégories suivantes:

Acteurs malveillants (<i>threat actors</i>)	Motivations
Acteurs étatiques	Les acteurs étatiques ont en général des ambitions géopolitiques. Ils s'attaquent aux infrastructures d'importance systémique de la partie adverse afin de la déstabiliser et de l'annexer.
Organisations criminelles	Les organisations criminelles sont en général mues par des mobiles financiers. Elles cherchent à travers leurs activités frauduleuses à mettre leurs victimes sous leur emprise. Le but est ici de leur extorquer une rançon.
Hacktivistes	Les hacktivistes cherchent à attirer l'attention et à imposer à la société leur vision politique ou religieuse du monde. Leur vandalisme ciblé et leurs opérations d'information

²³ <https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/ddos.html>

²⁴ <https://www.cisecurity.org/insights/white-papers/ms-isac-guide-to-ddos-attacks>

²⁵ <https://www.cisa.gov>

²⁶ <https://www.cisecurity.org>

	(Info Ops) ²⁷ visent à déstabiliser leurs victimes et à les rallier à leur idéologie.
Groupes terroristes	Les groupes terroristes visent à entretenir un climat de panique.
Passionnés d'informatique (geeks)	Les geeks sont en quête d'un sentiment de puissance, pour leur satisfaction personnelle ou afin de se prouver à eux-mêmes leurs capacités. Ils cherchent aussi à obtenir une reconnaissance dans certains cercles.
Initiés	Contrairement aux tiers, les initiés ont un accès privilégié à la victime (par ex. employés, mandataires). Ils tirent parti de cet accès pour causer des dommages ou s'enrichir indûment.

Tableau 9: Catégorisation des acteurs malveillants et de leurs motifs d'agir

Détails au jour le jour des attaques DDoS menées

Date du rapport	Titre	Description	Commentaires
12.06.2023	Attaques DDoS du 12.06.2023 par NoName057(16) contre sites suisses inclus administration fédérale	<p>Lundi 12.06.2023 à 08:20, des attaques DDoS ont lieu de la part de NoName057(16) envers des sites de l'administration (OFDF et DFJP). La liste des sites visés a été postée quelques minutes plus tard et se compose comme suit:</p> <ul style="list-style-type: none"> • login.swisspass.ch • www.swisspass.ch • account.post.ch • www.post.ch • www.sob.ch • www.sbb.ch • www.edi.admin.ch • www.fedpol.admin.ch • www.bazg.admin.ch • www.ejpd.admin.ch • www.parlament.ch <p>À 10:03, NoName057(16) a revendiqué sur son canal Telegram des attaques à l'encontre de la Suisse en indiquant le site du parlement [1] avec un rapport de check-host.net du 12.06.2023 09:28 (UTC: 07:28) [2]. Le rapport indique que la connexion ne fonctionne que depuis la Suisse (protection DDoS via geofencing). NoName057(16) justifie son action par les remerciements adressés par Zelensky à la Suisse pour leur adhésion au</p>	<ul style="list-style-type: none"> • Type d'attaque: layer 7 attacks (HTTP POST and GET flood). • Origine du trafic des attaques DDoS: traffic originates from Russian IP space and MIRhosting (AS206932, AS52000) as well as Stark Industries (AS44477). • Autres recommandations: mitigation can also include searching for anomalies in the HTTP Header as well as protecting resource intensive functions using a captcha. <p>Sur son canal Telegram, NoName057(16) a revendiqué les attaques contre DFJP (11:23), OFDF (12:35), fedpol (13:47), EDI (15:00), SOB (16:04) et La Poste (17:11). Les rapports de check-host [3] ont été établis vers 09:30 (UTC: 07:31) à l'exception de celui de La Poste, établi vers 13:47 (UTC 11:47).</p> <p>[3] https://check-host.net/check-report/103a5159k82c https://check-host.net/check-report/103a4fdakb51 https://check-host.net/check-report/103a4fdakb51</p>

²⁷ <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-34.pdf>

Date du rapport	Titre	Description	Commentaires
		<p>10e paquet de sanctions envers la Russie. Cette adhésion a été communiquée par la Suisse le 29.03.2023.</p> <p>[1] www.parlament.ch [2] https://check-host.net/check-report/103a4c6aka29</p>	<p>report/103a4edck891 https://check-host.net/check-report/103a53afk272 https://check-host.net/check-report/103a523fk4ec https://check-host.net/check-report/103af460ka6b</p>
<p>13.06.2023</p>	<p>Attaques DDoS du 13.06.2023 par NoName057(16) contre sites suisses inclus administration fédérale</p>	<p>Mardi 13.06.2023 à 09:20, nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS.</p> <p>La liste se compose comme suit:</p> <ul style="list-style-type: none"> • flyedelweiss.com • www.vtg.admin.ch • www.flughafen-zuerich.ch • peoples.ch • engadin-airport.ch • www.bernairport.ch • airport-grenchen.ch • www.gva.ch <p>Cette liste a été actualisée à 11 h 10 avec les nouvelles cibles suivantes:</p> <ul style="list-style-type: none"> • www.swisshelicopter.ch • zimex.com • www.pc7-team.ch 	<p>Sur son canal Telegram, NoName057(16) a revendiqué les attaques contre vtg.admin.ch (10:03), bernairport.ch (11:12), airport-grenchen.ch (12:27), gva.ch (13:34), engadin-airport.ch (14:47), peoples.ch (aérodrome de Saint-Gall, 15:58), www.swisshelicopter.ch (16:19), zimex.com (17:27), www.pc7-team.ch (18:01).</p> <p>Les rapports de check-host [1] ont été établis vers 09:30 (UTC 07:30), à l'exception de ceux de www.swisshelicopter.ch, zimex.com et www.pc7-team.ch qui ont été établis vers 11:10 (UTC 09:10)</p> <p>En analysant le canal Telegram de NoName057(16) , des commentaires postés par des «followers » à la suite des attaques du 12.06.2023 ont un lien avec la Suisse, augmentant les chances des organisations citées d'être la cible de futures attaques.</p> <p>Les cantons concernés ont été avertis de ces commentaires (11:35, 11:39).</p> <p>[1] https://check-host.net/check-report/103d8aafk44 https://check-host.net/check-report/103d83b0keb8 https://check-host.net/check-report/103d8574kb67 https://check-host.net/check-report/103d8603k4c6 https://check-host.net/check-report/103d86f8kbb2 https://check-host.net/check-report/103d87c3k56c</p>

Date du rapport	Titre	Description	Commentaires
			https://check-host.net/check-report/103dc68ek21e https://check-host.net/check-report/103dc78ak788 https://check-host.net/check-report/103dc833k3f3
14.06.2023	Attaques DDoS du 14.06.2023 par NoName057(16) contre sites suisses	<p>Mercredi 14.06.2023 à 08:00, nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS.</p> <p>La liste se compose comme suit:</p> <ul style="list-style-type: none"> • www.geneve.com <p>Cette liste a été actualisée à 08:20 avec les nouvelles cibles suivantes:</p> <ul style="list-style-type: none"> • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch <p>Puis à 11:15 avec les nouvelles cibles suivantes:</p> <ul style="list-style-type: none"> • www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch <p>À noter que le site www.geneve.com correspond au site touristique de Genève et non pas au site officiel de la Ville/République de Genève, qui est www.ge.ch</p>	<p>Sur son canal Telegram, NoName057(16) a revendiqué les attaques contre www.geneve.com (10:10), www.stadt-schaffhausen.ch (11:45), www.bs.ch (12:02), ekonto.egov.bs.ch (12:48), www.stadt-zuerich.ch (13:22), www.lausanne.ch (14:02), www.montreux.ch (14:49), www.stadt.sg.ch (15:23) et www.bellinzona.ch (16:02). Les rapports de check-host [1] ont été établis vers 09:30 (UTC: 07:30) à l'exception de ceux de www.stadt-schaffhausen.ch, www.lausanne.ch, www.montreux.ch, www.stadt.sg.ch et www.bellinzona.ch qui ont été établis vers 10:50 (UTC: 08:50)</p> <p>Dans sa publication sur l'attaque contre www.geneve.com, NoName057(16) fait allusion à l'allocution du Président Zelensky par vidéoconférence à l'Assemblée fédérale prévue pour le 15.06.2023.</p> <p>[1] https://check-host.net/check-report/1040acf6k148 https://check-host.net/check-report/1040e8e8k532 https://check-host.net/check-report/1040aff4k575 https://check-host.net/check-report/1040b0dak8f1 https://check-host.net/check-report/1040af59k432 https://check-host.net/check-report/1040e3a7kf79 https://check-host.net/check-report/1040e4b4k497</p>

Date du rapport	Titre	Description	Commentaires
			https://check-host.net/check-report/1040e788k29 https://check-host.net/check-report/1040e84ck7ed
15.06.2023	Attaques DDoS du 15.06.2023 par NoName057(16) contre sites suisses	<p>Jeudi 15.06.2023 à 08:00, nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS.</p> <p>La liste se compose comme suit:</p> <ul style="list-style-type: none"> • ncsc.admin.ch • www.myswitzerland.com • www.ruag.com • www.postauto.ch • www.zvv.ch • www.swissid.ch • www.swissprivatebankers.com • sasd.ch • www.juliusbaer.com • www.swissbanking.ch • www.geneve-finance.ch 	<p>Sur son canal Telegram, NoName057(16) a revendiqué les attaques contre www.myswitzerland.com (09:57), www.zvv.ch (11:02), www.swissid.ch (11:02), www.ruag.com (12:34), www.swissprivatebankers.com (13:22), sasd.ch (14:19), www.juliusbaer.com (15:15), www.swissbanking.ch (16:12), www.geneve-finance.ch (17:09).</p> <p>Les rapports de check-host [1] ont été établis vers 09:15 (UTC 07:15).</p> <p>[1] https://check-host.net/check-report/10440470kc60 https://check-host.net/check-report/104406b8kbe1 https://check-host.net/check-report/1044088ek60d https://check-host.net/check-report/10440518kcd6 https://check-host.net/check-report/10440971k53e https://check-host.net/check-report/10440a00ke63 https://check-host.net/check-report/10440aadc1ad https://check-host.net/check-report/10440b9ak78e https://check-host.net/check-report/10440c2fkb4c</p>
16.06.2023	Attaques DDoS du 16.06.2023 par NoName057(16) contre sites suisses	<p>Vendredi 16.06.2023 à 09:20, une nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS.</p> <p>La liste se compose comme suit:</p> <ul style="list-style-type: none"> • www.nw.ch • www.steuern-nw.ch • etax-login.nw.ch • www.pilatus-aircraft.com • www.stans.ch • www.buochs.ch • www.snb.ch 	<p>Sur son canal Telegram, NoName057(16) a revendiqué les attaques contre www.nw.ch (10:05), www.steuern-nw.ch (11:13), etax-login.nw.ch (12:24), www.vsz.ch (13:37), www.autofaehre.ch (14:41), www.lakelucerne.ch (15:52).</p> <p>Le site www.autofaehre.ch ne figure pas dans la liste des cibles attaquées par le BotNet de NoName057(16) et le site est</p>

Date du rapport	Titre	Description	Commentaires
		<ul style="list-style-type: none"> www.zentralbahn.ch www.lakelucerne.ch <p>Un site supplémentaire a été ajouté à la liste à 10:00:</p> <ul style="list-style-type: none"> www.vsz.ch 	<p>actuellement accessible (15:00). Il est plutôt probable qu'il s'agisse d'une erreur de communication de NoName057(16) .</p> <p>Les rapports de check-host ont été établis vers 09:15 (UTC 07:15).</p>
18.06.2023	Attaques DDoS du 17.-18.06.2023 par NoName057(16) contre sites suisses	<p>Samedi 17.06.2023 à 09:20, une nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS. La liste se compose comme suit:</p> <ul style="list-style-type: none"> www.ejpd.admin.ch www.fedpol.admin.ch www.bazg.admin.ch sob.ch www.post.ch gva.ch airport-grenchen.ch bernairport.ch engadin-airport.ch peoples.ch <p>Un site supplémentaire a été ajouté à la liste à 10:30:</p> <ul style="list-style-type: none"> www.edi.admin.ch <p>Des sites supplémentaires ont été ajoutés à la liste à 14:00:</p> <ul style="list-style-type: none"> www.vtg.admin.ch www.swisshelicopter.ch www.zimex.com www.heliswissinternational.com www.pc7-team.ch <p>Dimanche 18.06.2023 à 10:45, une nouvelle liste de cibles est utilisée par NoName057(16) pour des attaques DDoS. La liste se compose comme suit:</p> <ul style="list-style-type: none"> www.stadt-zuerich.ch www.bs.ch ekonto.egov.bs.ch www.lausanne.ch www.montreux.ch www.stadt.sg.ch www.stmoritz.com stadt.winterthur.ch bellinzona.ch www.ville-fribourg.ch www.stadt-schaffhausen.ch 	<p>La grande majorité des sites ciblés samedi et dimanche avaient déjà été ciblés durant la semaine écoulée. Sur son canal Telegram, NoName057(16) a revendiqué samedi 17.06.2023 les attaques contre edi.admin.ch (10:07), www.bernairport.ch (11:14), airport-grenchen.ch (12:27), engadin-airport.ch (13:34), gva.ch (14:46), vtg.admin.ch (15:44), www.swissprivatebankers.com (16:55), www.swisshelicopter.ch (18:03), www.zimex.com (19:01) et www.pc7-team.ch (19:47).</p> <p>Les rapports de check-host ont été établis vers 09:30-10:00 (UTC 07:30-08:00) à l'exception de ceux de gva.ch, vtg.admin.ch, www.swissprivatebankers.com, www.swisshelicopter.ch et www.zimex.com et www.pc7-team.ch qui ont été établis vers 14:00 (UTC 12:00).</p> <p>Sur son canal Telegram, NoName057(16) a revendiqué dimanche 18.06.2023 les attaques contre www.montreux.ch (10:05), www.stadt.sg.ch (11:16), www.stadt-schaffhausen.ch (12:27), www.lausanne.ch (13:38), www.stmoritz.com (14:49), www.ville-fribourg.ch (15:50), www.swissprivatebankers.com (17:15) et www.zvv.ch (18:34)</p> <p>Les rapports de check-host ont été établis vers 09:30-10:00 (UTC 07:30-08:00) à l'exception de ceux de</p>

Date du rapport	Titre	Description	Commentaires
		Des sites supplémentaires ont été ajoutés à la liste à 15:15: <ul style="list-style-type: none"> • www.juliusbaer.com • sasd.ch • www.swissprivatebanke rs.com • www.zvv.ch • www.myswitzerland.com 	www.swissprivatebankers.com et www.zvv.ch vers 14:30 (12:30 UTC).

Tableau 10: Annonces d'attaques DDoS avec ajouts effectués au quotidien, entre le 12 et le 18 juin 2023