Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC
Bereich Analyse

30. Oktober 2023

Nachgelagerte Vorfallanalyse

DDoS-Angriffe «NoName057(16)», Juni 2023

Dieser Bericht analysiert die Distributed Denial of Service-Angriffe (DDoS-Angriffe), welche sich auf Schweizer Organisationen und Behörden im Zeitraum der ersten zwei Juniwochen 2023 (Wochen 23 und 24) ereignet haben. Die eingesetzte DDoS Angriffsvariante auf der Applikationsebene wird detailliert erläutert.

Die Schweiz hat diese DDoS-Angriffe des Akteurs «NoName057(16)» ohne nachhaltige Schäden überstanden. Die angegriffenen Schweizerischen Organisationen und Behörden waren mehrheitlich auf DDoS-Angriffe vorbereitet und konnten deshalb adäquat reagieren. Daraus erschliesst sich, dass durch das bedarfsgerechte Implementieren von Sicherheitsmechanismen der potenzielle Schaden massgebend minimiert werden kann.

Aufgrund der vielfältigen Ziele des Akteurs sowie der politischen Brisanz der Rede im Parlament von Wolodymyr Selenskyj, wurden über die DDoS-Angriffe in den Medien intensiv berichtet. Durch diese flächendeckende Berichterstattung erhielt der Akteur die grosse Aufmerksamkeit in der Bevölkerung, die er mit seiner Aktion gesucht hat. Ziel der prorussischen Hackergruppe «NoName057(16)» war die Vermittlung ihrer politischen Anliegen, dies als Reaktion auf mehrere Entscheidungen des Schweizer Parlaments (z. B. Weitergabe von Kriegsmaterial an Drittstaaten, Ankündigung der Rede von Wolodymyr Selenskyj im Parlament).

Die DDoS-Angriffe zielten auf die Beeinträchtigung der Verfügbarkeit von Webauftritten (Erschöpfung der vorhandenen Ressourcen, engl. Resource Exhaustion) hin. Ein Informationsabfluss von produktiven Daten fand nicht statt.

Inhaltsverzeichnis

1 Management Summary

Während der ersten beiden Juniwochen 2023 (Woche 23 und 24) haben sich Distributed Denial of Service-Angriffe (DDoS-Angriffe)1 gegen Schweizer Organisationen und Behörden ereignet. Auslöser für diesen Cyberaktivismus (Hacktivismus) gegen die Schweiz waren mehrere Entscheidungen des Schweizer Parlaments im Zusammenhang mit dem Ukraine-Krieg (siehe Kapitel 8 [1] und [2]). Die Hacktivisten versprechen sich eine hohe Signalwirkung ihrer DDoS-Angriffe, damit sie ihre politischen Anliegen kundtun und ihre Absichten erreichen können.

Der Akteur hatte es insbesondere auf Behörden oder Organisationen abgesehen, welche eine gewisse Nähe zur Bundesverwaltung haben und ein hohes Ansehen in der Öffentlichkeit geniessen (z. B. das Schweizer Parlament, die Schweizerische Post AG und die Schweizerische Bundesbahnen SBB). Durch diese DDoS-Angriffe waren einzelne Webauftritte kurzzeitig (während wenigen Stunden) nicht erreichbar. Der maximale Schaden stellte sich in Form von Ausfällen über mehrere Tage dar. Ein permanenter Schaden an IKT-Infrastrukturen oder anderweitige wirtschaftliche Schäden sind nicht entstanden, dies war bei diesen Angriffen auch nicht das primäre Ziel des Akteurs, welches in erster Linie darin bestand, mediale, gesellschaftliche und politische Aufmerksamkeit zu erregen.

Beim Akteur handelt es sich um die prorussische Hacktivismusgruppierung «NoName057(16)», welche seit März 2022 DDoS-Angriffe gegen verschiedene Ziele weltweit (z. B. öffentliche Verwaltungen und Behörden, Firmen und weitere Organisationen) ausführt, die sie als «russland-kritisch» betrachtet. Die erfolgreich durchgeführten Angriffe werden jeweils über den gleichnamigen Telegram-Kanal veröffentlicht.

«NoName057(16)», mobilisiert für ihre Angriffe sogenannte Cyberaktivisten («heroes»), welche ihre eigenen Rechner für die DDoS-Angriffe gegen Bezahlung zur Verfügung stellen. Die sogenannten «heroes», können zudem Ziele vorschlagen, die angegriffen werden sollen. Der Akteur stellt den DDoS-Client namens «DDoSia» zur Verfügung. Die «heroes» werden über den Telegram-Kanal «DDoSia-Project» technisch unterstützt.

Die internetbasierten Angriffe haben sich auf die Applikationsebene (OSI Layer-7)2 konzentriert. «NoName057(16)» wollte dabei gezielt Ausfälle von Webauftritten durch die Überlastung der vorhandenen Kapazitäten (Erschöpfung von Ressourcen, engl. Resource Exhaustion) erzeugen, damit bestimmte Services für die Öffentlichkeit nicht mehr verfügbar sind (z. B. den Onlinekauf von SBB-Tickets). Die gesamte Angriffswelle dauerte zwei Wochen und hat sich während dieser Zeit aus technischer Perspektive nicht verändert. Im Tagesrhythmus veränderten sich jedoch die angegriffenen Ziele. Die Betroffenen waren unterschiedlich gut auf solche DDoS-Angriffe vorbereitet. Entsprechend konnten einige schneller als andere auf die Angriffe reagieren und so die Auswirkungen minimieren.

Die Auswirkungen eines solchen DDoS-Angriffes können mit technischen Massnahmen (z. B. mittels Web Application Firewall: konfigurative Anpassung der Firewall-Regeln, damit der DDoS-Client erkannt und gesperrt wird, siehe Kapitel 3.3) und organisatorischen Massnahmen (z. B. Business Continuity Management - BCM[3]) minimiert werden.

Die latente Gefahr solcher DDoS-Angriffe bedingt, dass die spezifischen Entwicklungen im Cyberraum permanent verfolgt, die Risiken evaluiert und die Sicherheitsdispositive bei Bedarf angepasst werden. Aufgrund der verursachten Ausfälle sowie den dadurch erzeugten medialen Berichterstattungen wurde ersichtlich, dass bei einzelnen Betroffenen weiteres Verbesserungspotential bei der Vorbereitung der Reaktion auf solche Angriffe besteht. Einzelne Betroffene haben auch bereits Massnahmen umgesetzt.

[1] https://de.wikipedia.org/wiki/Denial_of_Service

[2] https://de.wikipedia.org/wiki/OSI-Modell

[3] https://de.wikipedia.org/wiki/Betriebliches_Kontinuitätsmanagement

2 Einführung

2.1 Geopolitischer Kontext

Ende Februar 2022 hat Russland die Ukraine militärisch angegriffen. Die Ukraine wird im Rahmen dieses Krieges ebenfalls im Cyberraum angegriffen, sei dies durch staatliche Akteure oder Cyberaktivismus (Hacktivismus). Russland seinerseits ist ebenfalls Ziel von Cyberangriffen, die von unterschiedlichen Cyberaktivisten und anderen Organisationen verübt werden. Auch andere Länder, insbesondere NATO-Staaten, stehen im Fokus von Cyberangriffen.

Insgesamt wurden im Rahmen des Ukraine-Krieges bisher nur wenige aktivistisch-motivierte Cyberaktivitäten gegen die Schweiz und gegen schweizerische Ziele festgestellt. Die Anzahl und die Intensität der Cyberaktivitäten entsprach der Bedrohungseinschätzung des Nationalen Zentrums für Cybersicherheit (NCSC) und des Nachrichtendienstes des Bundes (NDB. Durch eine Realisierung der Bedrohung ändert sich die Bedrohungslage nicht. Die Schweiz kann weiterhin zeitweise von aktivistisch motivierten Cyberaktivitäten betroffen werden. Diesen Cyberaktivitäten konnte bisher mit konventionellen Sicherheits- und Bekämpfungsmassnahmen (Mitigation) begegnet werden. Dementsprechend sind die Schäden in der Schweiz bisher klein.

Im Lagebericht «Sicherheit Schweiz 2023»[4] stellt der NDB die Situation detailliert dar. Die nachfolgende Darstellung zeigt die Cyberangriffe durch Cyberaktivisten im ersten Kriegsjahr (DDoS/Überlastungsangriffe) auf:

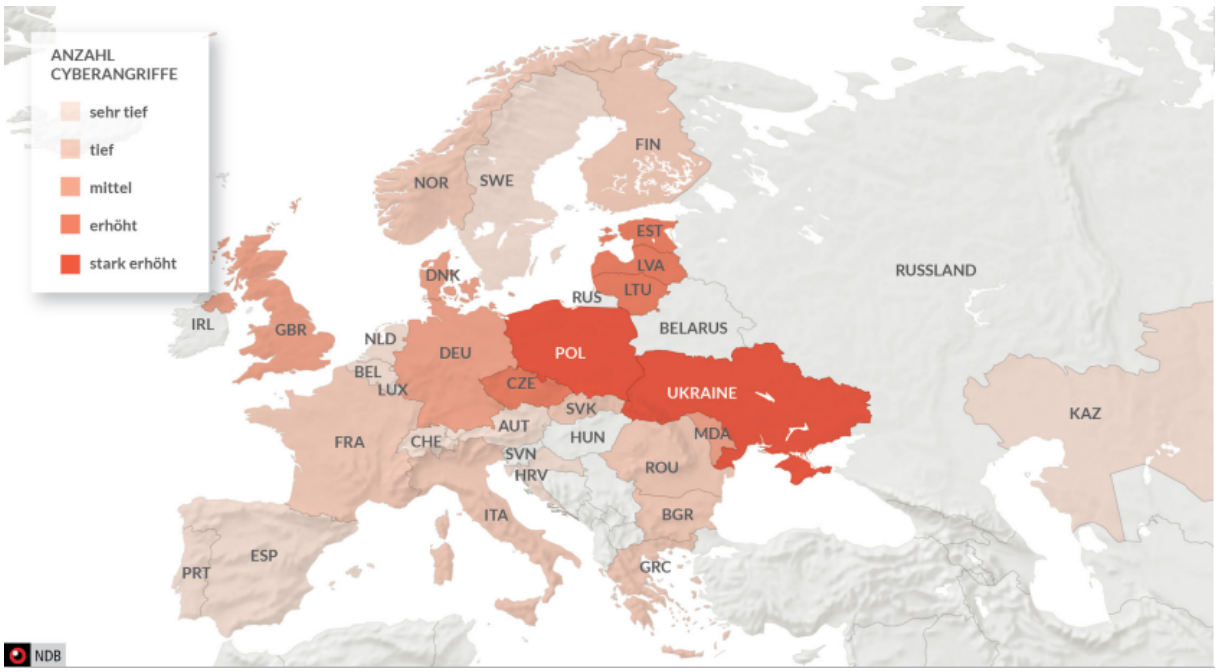

Abbildung 1: DDoS-Angriffe durch Cyberaktivisten im ersten Kriegsjahr, Quelle: NDB Lagebericht 2023

Der Begriff Cyberkrieg[5] setzt sich aus den Begriffen **Cyber**raum und **Krieg** zusammen. Er bezeichnet eine kriegerische (militärische) Auseinandersetzung, welche mit den Mitteln der Informationstechnologie über eine gewisse Zeit und zwischen zwei Staaten erfolgt.

[4] https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.detail.document.html/vbs-internet/de/documents/nachrichtendienst/lageberichte/NDB-Lagebericht-2023-d.pdf.html

[5] https://de.wikipedia.org/wiki/Cyberkrieg

Die zeitlich befristeten Distributed Denial of Service (DDoS)-Angriffe, die der Akteur «NoName057(16)» im vergangenen Juni auf verschiedene Ziele in der Schweiz verübt hatten, können gemäss Definition nicht als kriegerisches Ereignis unter dem Begriff Cyberkrieg verstanden werden, sondern ist vielmehr dem Cyberaktivismus zuzuordnen (siehe Kapitel 2.2).

2.2 **Kategorisierung**

Die DDoS-Angriffe auf die Schweiz wurden durch politisch motivierte Hacktivisten ausgeführt. Sie betreiben in diesem Cybervorfall prorussische Propaganda. Der Akteur konnte mit seinen DDoS-Angriffen die fokussierten Webauftritte teilweise beeinträchtigen (siehe Kapitel 3.2). Deshalb ordnet das NCSC die DDoS-Angriffe im Juni dem **Cyberaktivismus**[6] zu:

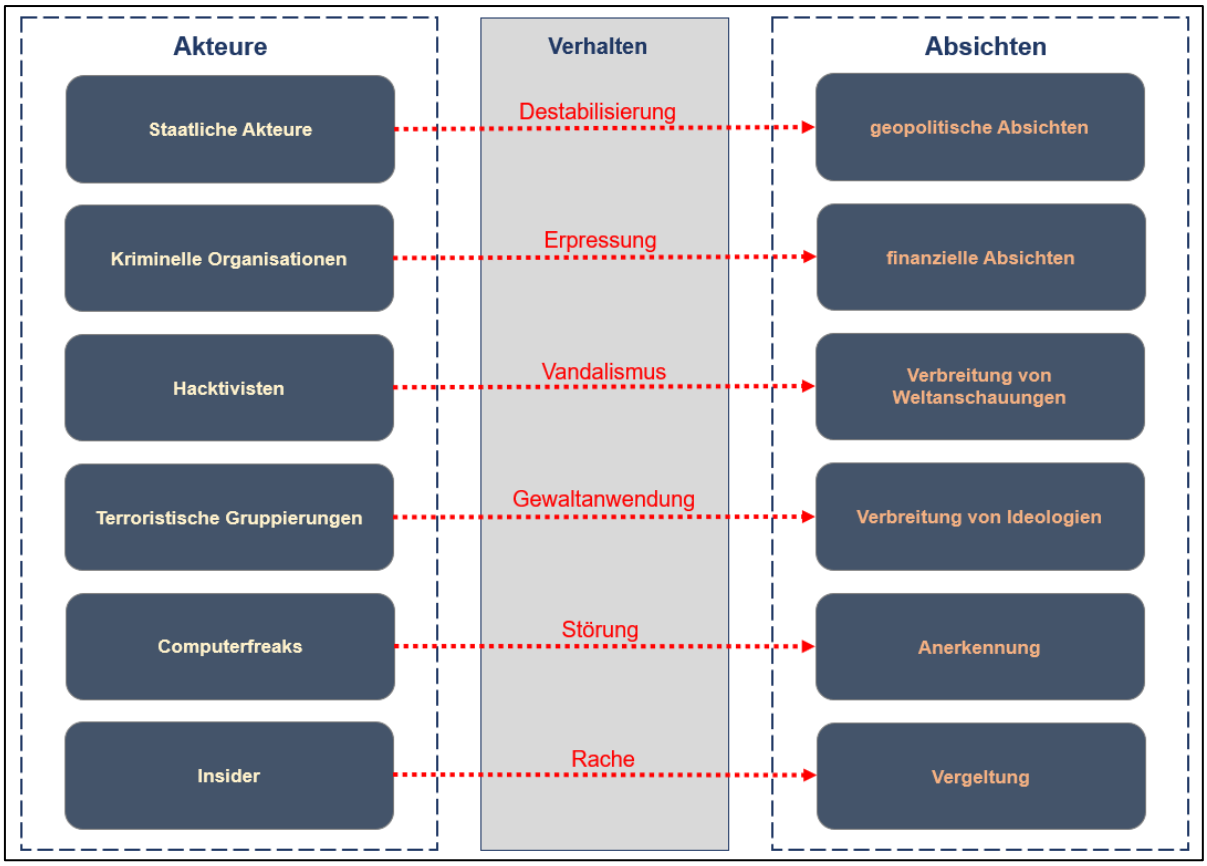

Abbildung 2: Akteure, deren Verhalten und Absichten

Der Akteur «NoName057(16)» verbreitet seine potentiellen Erfolge jeweils über den Instant-Messaging-Dienst Telegram. Der Akteur will dadurch eine hohe Aufmerksamkeit für seine politisch motivierten Aktivitäten erreichen. Das mediale Verbreiten der Erfolge und das Auslösen der politischen und gesellschaftlichen Aufmerksamkeit im Zielstaat ist daher de facto den Informationsoperationen (Info Ops) zuzuordnen.

[6] https://de.wikipedia.org/wiki/Cyberaktivismus

3 Beschreibung des Angriffs

3.1 Art des DDoS-Angriffs

Um die Ressourcen von Systemen mittels DDoS zu erschöpfen, bestehen verschiedene Möglichkeiten. Die verübten Angriffe verfolgte das Ziel, legitimes menschliches Nutzungsverhalten auf Webauftritte nachzuahmen. Hierzu wurden automatisiert Webservices wie z. B. Such- oder Anmeldeformulare aufgerufen, welche jeweils eine gewisse Last in der nachgelagerten Business-Logik verursachen. Da die Businesslogik resp. die vorgelagerten Netzwerkkomponenten wie Applikationsserver, Loadbalancer oder Web Applikation Firewalls (WAF) aus wirtschaftlichen Gründen auf der Basis von erwarteten Nutzerzahlen dimensioniert werden, können diese aufgrund der künstlich erzeugten Zugriffe über ihre vorgesehenen Leistungsgrenzen belastet werden und dadurch den eigentlichen Benutzern ihren Service nicht mehr anbieten und die Webauftritte lassen sich nicht wie gewöhnlich nutzen oder sind nicht erreichbar.

Eine technisch tiefere Betrachtung ist im Kapitel 3.3 einsehbar.

3.2 Akteur «NoName057(16)»

Der Akteur «NoName057(16)» bekennt sich auf Telegram öffentlich als Initiant dieser DDoS-Angriffe. «NoName057(16)» ist eine prorussische Gruppierung, welche seit März 2022 aktiv ist. Die Gruppierung trat in den Kriegswirren um die russische Invasion in der Ukraine (Februar 2022) erstmals in Erscheinung und erklärte den «Cyberkrieg» gegen den «Informationskrieg gegen Russland». Die Gruppe kommuniziert primär via Telegram und gibt über diesen Kanal auch ihre Ziele bekannt. Ausserdem können die Followers auf Telegram ihre Wünsche äussern, welches Ziel als nächstes angegriffen werden soll.

Generelles Vorgehen

Die nachfolgende Grafik beschreibt das generelle Vorgehen des Akteurs in drei Phasen (siehe technische Beschreibung im Kapitel 3.3):

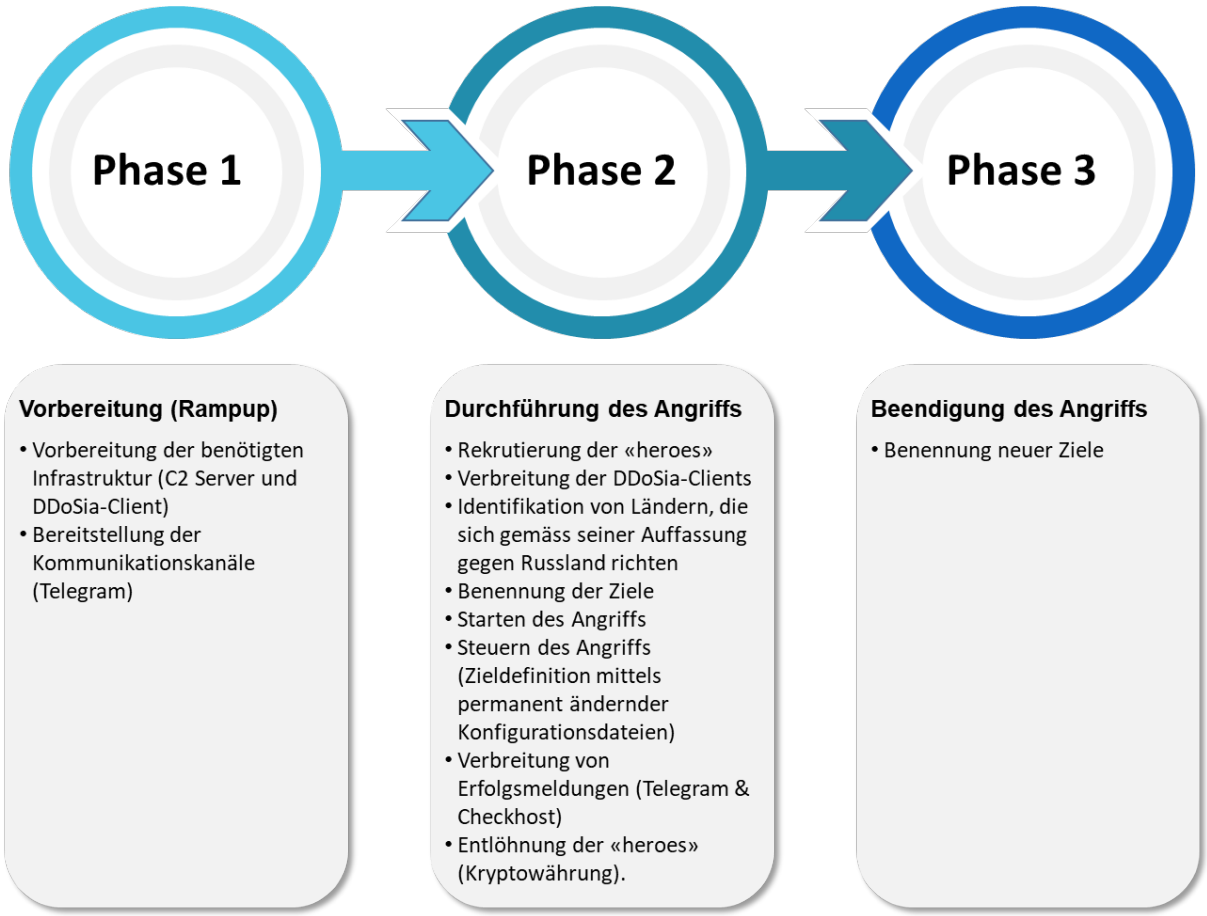

Abbildung 3: Generelles Vorgehen

Angegriffene Ziele

Als Ziele greift der Akteur primär Webauftritte der Ukraine sowie solche von NATO- und EU-Ländern an. Es hat sich gezeigt, dass auch Länder, welche die Ukraine unterstützen respektive Sanktionen gegen Russland ergreifen, zum Ziel werden können. Wegen der beiden Entscheidungen des Parlamentes zum vermeintlichen Vorteil der Ukraine (siehe Kapitel 8, [1] und [2]) wurde auch die Schweiz kurzzeitig zu einem Ziel. Die DDoS-Angriffe auf die Schweiz erfolgten nicht aus wirtschaftlichen Gründen respektiv wegen des schweizerischen Wohlstands. Die Schweiz war nur eine Woche lang Ziel des Akteurs. Es ist zu erwarten, dass der Akteur auch in Zukunft Staaten zu propagandistischen Zwecken angreifen wird.

Das folgende Diagramm zeigt eine Auflistung von Staaten, welche im Zeitraum vom 1. April 2023 bis am 24. Juni 2023 durch den Akteur angegriffen worden sind:

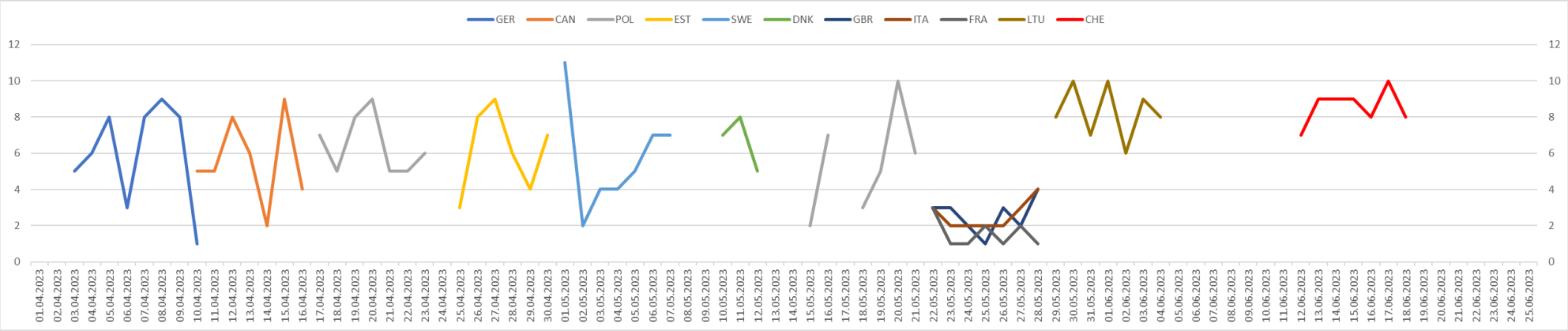

Abbildung 4: DDoS-Angriffe auf andere Staaten vor, während und nachdem die Schweiz angegriffen worden war (Auflistung nicht abschliessend)

Dabei ist ersichtlich, dass die Schweiz (Kennzeichnung CHE gemäss ISO) eines von vielen Ländern ist, welche durch den Akteur angegriffen worden sind. Auch zu erkennen ist, dass der Akteur bereits vor den DDoS-Angriffen gegen die Schweiz vom 12. Juni 2023 bis am 18. Juni 2023 gegen andere Staaten aktiv war.

Threat Assessment über den Akteur

Die nachfolgende Grafik visualisiert die Bedrohungsanalyse (Threat Assessment) des NCSC über den Akteur «NoName057(16)». Diese zeigt beispielsweise auf, dass die Komplexität (Threat Level) der Angriffswelle eher klein war, jedoch die DDoS-Angriffe in einer hohen Intensität erfolgten (Attack Frequency):

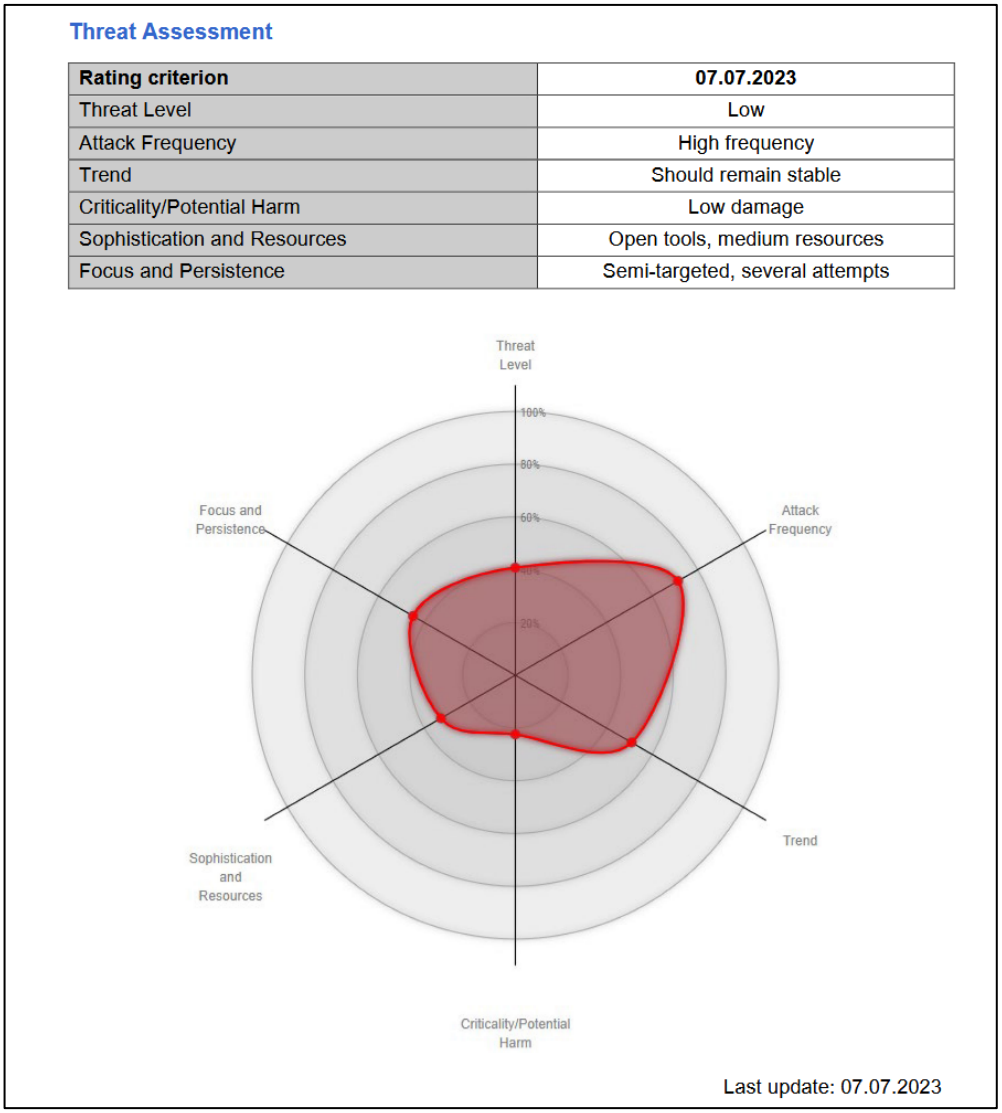

Abbildung 5: Threat Assessment des NCSC zu «NoName057(16)»

Motivation des Akteurs

Das nachfolgende Leitbild zu den Aktivitäten der Gruppierung hat der Akteur am 11. März 2022 auf Telegram publiziert:

Abbildung 6: Telegram-Post vom Akteur übersetzt ins Englische

Damit der Akteur sein politisches Anliegen und seine Absichten umsetzen kann, initiiert und koordiniert er DDoS-Angriffe, um eine möglichst grosse Aufmerksamkeit zu erreichen.

Der Akteur führt in einem weiteren Telegram-Post die folgenden Motivationen für die Wahl dieser Angriffsmethodik auf:

Formulierte Motivation des Akteurs	Einordnung der Motivation durch das NCSC	Erreichung der Motivation aus Sicht NCSC
«Wenn die Firmenserver in der Cloud laufen, führt der erhöhte Netzwerkverkehr zu höheren Kosten.»	Der Akteur will einen finanziellen Schaden verursachen.	Teilweise erreicht. Es entstand kein wesentlicher wirtschaftlicher Schaden.
«Wenn eine Webseite für mehr als 2 Tage offline ist, wird ihre Sichtbarkeit in Suchmaschinen relevant schlechter.»	Der Akteur will die Auffindbarkeit von Webauftritten beeinträchtigen.	Nicht erreicht. Die Sichtbarkeit in Suchmaschinen wurde nicht beeinträchtigt.
«Auch wenn die Webseite wieder verfügbar ist, verbleibt die Reputation des Betreibers geschwächt.»	Der Akteur will die Reputation seiner Ziele beeinträchtigen.	Nicht erreicht. Die Reputation der Betroffenen wurde höchstens während der Angriffszeit geschwächt.
«Angegriffene Systeme können aufgrund von automatisch generierten Fehlermeldungen Angaben nach aussen preisgeben (z. B. interne Information über Datenbanken).»	Der Akteur will einen Abfluss von technischen Informationen erzielen.	Teilweise erreicht. Das NCSC kann nicht ausschliessen, dass solche Informationen während der Angriffszeit preisgegeben wurden.

Tabelle 1: Motivation des Akteurs und Einschätzung des NCSC

Wenn der Angriff erfolgreich ist, wird als Beweis auf dem Telegram-Kanal **@noname05716** eine Nachricht über den angegriffenen Webauftritt mit der Fahne des Landes und einem Link auf einen Bericht der Webseite check-host.net gepostet.

Auf der Webseite check-host.net ist ersichtlich, ob Webauftritte aus verschiedenen Ländern erreichbar (online) sind. Es lassen sich auch im Nachhinein konsultierbare Momentaufnahmen generieren, ob Webauftritte zu einem bestimmten Zeitpunkt erreichbar waren. Die Meldung, dass das angegriffene Ziel zu einem gewissen Zeitpunkt nicht verfügbar war, wird vom Akteur als Beweis für den erfolgreichen Angriff (als Trophäe) präsentiert. Ergänzt wird diese Telegram-Mitteilung mit verschiedenen Grussbotschaften und Aufforderungen, der Gruppierung zu folgen und sie zu unterstützen.

Kommunikationskanäle des Akteurs

Der Akteur setzt zur Kommunikation hauptsächlich zwei Telegram-Kanäle ein:

- **@noname05716:** Allgemeiner Chat-Kanal (meist Screenshots von erfolgreichen DDoS-Attacken) in russischer Sprache.
- **@noname05716eng:** Englische Übersetzungen vieler Posts aus dem Haupt-Chat-Kanal.

Die erweiterte Kommunikation erfolgt über zusätzliche Kanäle:

Name des Kanals inkl. Originaltext	Übersetzung
DDoSia - мануалы + актуальное ПО	DDoSia - Handbücher + aktuelle Software
DDoSia - поддержка	DDoSia-Unterstützung
Полезные материалы	Nützliche Materialien
Общий чат	Allgemeiner Chat
English support	Englischer Support
Предложение целей	Vorschlag von Zielen
Ваши видео и скриншоты работы с клиентом DDosia	Ihre Videos und Screenshots von der Arbeit mit dem DDoSia-Client

Tabelle 2: Auflistung und Übersetzung der Telegram-Kanäle

Betriebsmodell des Akteurs

Der Akteur verwendet kein klassisches Botnetz[7], sondern zählt auf die Unterstützung von Freiwilligen, den sogenannten «heroes». Diese «heroes» installieren auf ihren Computern den DDoSia-Client (siehe weiter unten), der für die Angriffsdurchführung eingesetzt wird.

Die «heroes» registrieren sich über einen Telegram-Bot. Nach der Registrierung sendet der Telegramm-Bot eine URL für den Download der ausführbaren DDoSia-Dateien und eine Textdatei mit einer eindeutigen ID zur Identifizierung des registrierten «heroes».

Die «heroes» haben die Möglichkeit, sich mit ihrer ID-Nummer und einer Krypto-Wallet beim Telegram-Bot zu registrieren. Der Akteur verspricht den «heroes» eine Auszahlung in Kryptowährungen basierend auf der Anzahl der von ihm durchgeführten Angriffe. Diese werden im Vergleich zur Gesamtzahl, der von allen aktiven Freiwilligen an einem bestimmten Tag durchgeführten Angriffe, festgelegt.

Ein Telegram-Post des Akteurs vom März 2023 beschreibt das Auszahlungsschema wie folgt:

- 80.000 Rubel für den ersten Platz
- 50.000 Rubel für den zweiten Platz
- 20.000 Rubel für den dritten Platz

Ein Budget von 50.000 Rubel wurde zwischen dem vierten und zehnten Platz aufgeteilt.

Die Zahlungen werden in Kryptowährungen wie Ethereum, Bitcoin und Tether vorgenommen. Die «heroes» können Informationen über ihre Gesamtstatistiken (TopTen-Liste) im DDoSia-Telegram-Kanal abrufen.

Wer der Sponsor dieser finanziellen Mittel ist, bleibt unklar. Im Gegensatz zu anderen Cyberaktivisten führte der Akteur bislang keinen Spendenaufruf z. B. über Social Media durch.

[7] https://de.wikipedia.org/wiki/Botnet

3.3 Technische Beschreibung

Zu Beginn des Ukraine-Krieges stellte das NCSC eine Zunahme der DDoS-Aktivitäten mittels der Schadsoftware «Bobik»[8] fest. Die Opfer wussten nicht, dass ihre Computer mit dieser Schadsoftware infiziert worden waren und zur Durchführung von DDoS-Angriffen missbraucht wurden. «NoName057(16)» hat seine Philosophie inzwischen geändert und ruft die «heroes» in den sozialen Medien öffentlich zur Nutzung eines speziellen DDoS-Clients namens «DDoSia» auf.

Durch den Wechsel von Bobik zu diesem speziellen DDoS-Client verringert sich der Betriebsaufwand für den Akteur erheblich, da für ihn die Beschaffung von infizierten Geräten entfällt. Der Wechsel hat damit wirtschaftliche Gründe.

Zur Ausführung der DDoS-Angriffe nutzt der Akteur das DDoSia-Projekt[9], welches aus Command & Control Servern (C2 Server) und DDoSia-Clients besteht. DDoSia wurde im September 2022 entwickelt, damit die sogenannten «heroes» via Telegram die Möglichkeit erhalten, als Freiwillige ihre Computer und ihre Internetanschlüsse zur Angriffsausführung zur Verfügung zu stellen.

Beschreibung DDoSia-Client

Der DDoSia-Client wird dauernd weiterentwickelt, ist in der Programmiersprache «Go» programmiert und ist auf den Plattformen Linux, Windows, MacOS und Android lauffähig.

Der DDoSia-Client verwendet standardmässig den User Agent «Go-http-client/1.1» der Programmiersprache «Go». Während der gesamten DDoS-Angriffe wurde die HTTP User-Agent Kennung «Go-http-client/1.1» nicht verändert. Die eindeutige Erkennung des User-Agents vereinfachte die Mitigation mittels Web Application Firewalls (WAF's). Auf den Web Application Firewalls konnte dieser User-Agent durch eine konfigurative Anpassung gesperrt werden.

Es wurde keine Verschleierung der DDoSia-Client IP-Adresse mittels Spoofing[10] festgestellt. Als Konsequenz sind die «heroes» anhand ihrer IP-Adresse potentiell identifizierbar. Der Akteur empfiehlt auf seinen Telegram-Supportkanälen die Verwendung von VPN, damit eine Identifizierung der «heroes» erschwert wird.

Detailliertere Informationen über den DDoSia-Client inklusive Reverse Engineering können auf dem Blog des Sicherheitsdienstleisters Sekoia (siehe Kapitel 8, [4]) nachgelesen werden.

[8] https://decoded.avast.io/martinchlumecky/bobik/

[9] https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

[10] https://de.wikipedia.org/wiki/Spoofing

Beschreibung Command & Control-Kommunikation

Die nachfolgende Darstellung zeigt den Kommunikationsablauf der DDoSia-Clients mit den Command and Control-Servern (C2)[11] auf:

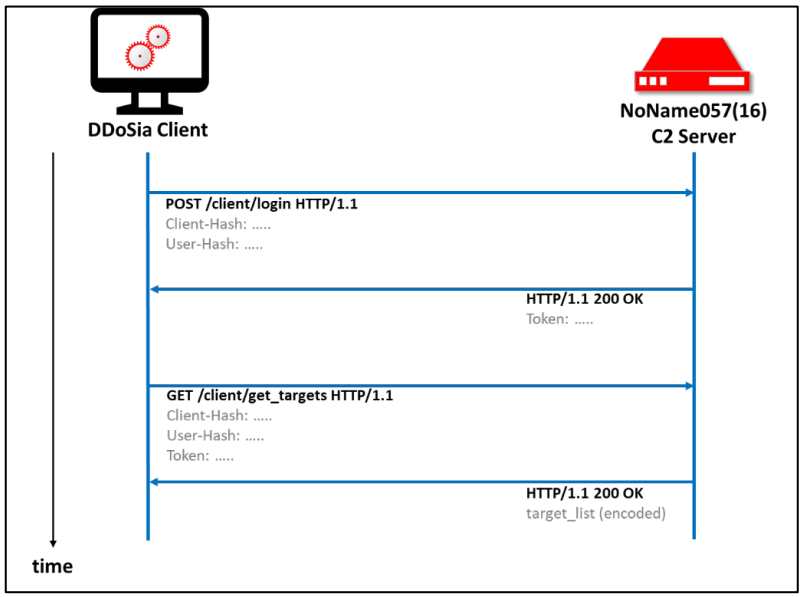

Abbildung 7: «DDoSia-C2-Kommunikation»

Die Kommunikation zwischen DDoSia-Clients und den C2-Servern ist mittels eines User-Hashs personalisiert, welcher den Teilnehmer identifiziert, sowie eines Client-Hashes, welcher den Computer des Teilnehmers identifiziert. Der User-Hash wird auch zur Identifikation des jeweiligen Benutzers verwendet, um die Bezahlung der «heroes» durchzuführen. Der DDoSia-Client empfängt abschliessend die Liste mit den Angriffszielen `(target_list(encoded))`.

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

Kommunikation mit dem Angriffsziel

Der DDoSia-Client generiert aufgrund von Anweisungen in der Liste der Angriffsziele (abgerufen bei den C2-Servern) die konkreten Abfragen bei den anzugreifenden Webauftritt.

Dabei wird ein Template verwendet, welches durch parametrierte Zufalls-Zeichenketten ergänzt wird. Der Akteur legt bei dem Design dieser Templates sowie der zufällig generierten Inhalte besonderes Augenmerk darauf, dass dieser Datenverkehr sehr ähnlich zu legitimen Web-Abfragen aussieht, um eine automatisierte Erkennung der DDoS-Angriffe zu erschweren.

Die nachfolgende Darstellung zeigt auf, wie der DDoSia-Client legitimen Datenverkehr imitiert, dadurch Schutzmechanismen täuscht und deshalb der schadhafte Datenverkehr nicht unterbunden wird. Daher kann dieser Datenverkehr von Schutzmechanismen wie DDoS-Protection und Firewalls meist nicht automatisiert erkannt und blockiert werden:

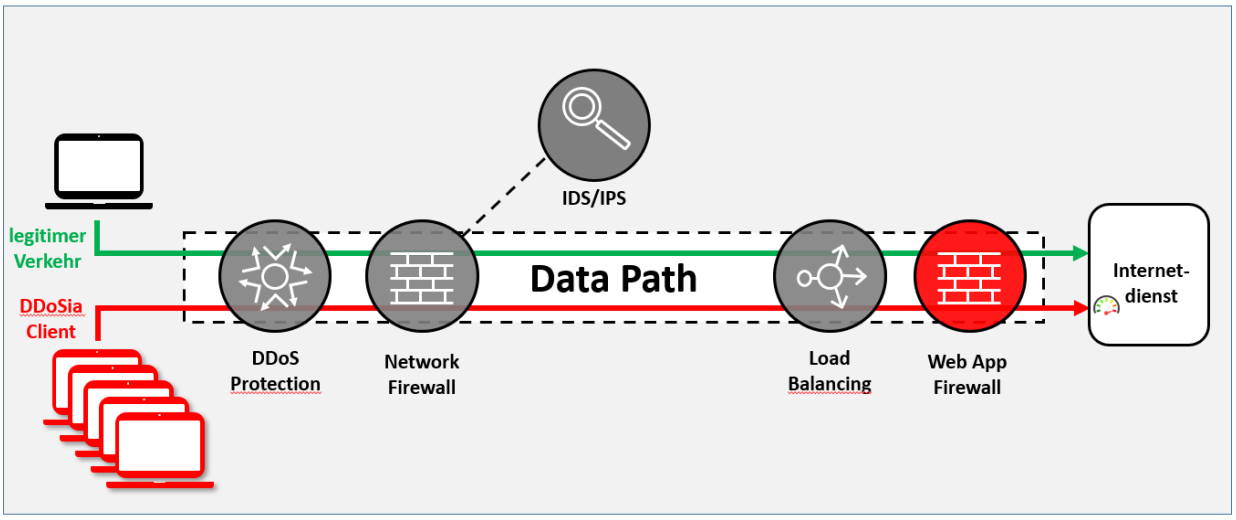

Abbildung 8: Schadhafter Datenverkehr des DDoSIA-Clients

Die folgenden Beispiele zeigen Templates, welche durch parametrierte Zufalls-Zeichenketten ergänzt werden:

Beispiel 1:

- Template: `"hxxp[s]://www.webseite.ch/de/search/?term=$_1"`
- $_1 ist ein zufälliger String der Länge 6-12 (z. B. hier: kenuab)

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

Beispiel 2:

- Template: `"hxxp[s]://www.webseite.ch/de/register/?name=$_1.$_1@$_2.ch"`
- $_1 ist ein zufälliger String der Länge 6-8 bestehend aus Kleinbuchstaben, $_2 ist ein zufälliger String der Länge 10-12 bestehend aus Kleinbuchstaben (z. B. hier $1: goenza.leurebe und $2 pahelsnwmni)

Aufgerufene URL: `"hxxp[s]://www.webseite.ch/de/register/?name=goenza.leurebe@pahelsnwmni.ch"`

Somit werden durch den DDoSia-Client laufend Web-Abfragen generiert, welche sich in den Parametern unterscheiden und deren Verarbeitungslast in den nachgelagerten IKT-Infrastrukturen (z. B. in Datenbanken, welche in Business-Prozessen verwendet werden) verursachen. Die Anfragen sind durch ihren dynamischen Aufbau daher nur schwer von legitimem Datenverkehr unterscheidbar.

Technische Reaktion auf den DDoS-Angriff (Mitigation)

Durch Analyse der Angriffsmuster (z. B. durch Filtern der Log-Dateien auf den User-Agent des DDoSia-Clients) kann eine Liste der IP-Adressen von beteiligten «heroes» erstellt werden. Mittels dieser Liste kann der schadhafte Netzwerkverkehr bereits beim Internet-Router (Edge-Router) der betroffenen Organisation, respektive beim Internet Service Provider (ISP) selbst, blockiert werden (z. B. mittels Null-Routing[12]).

Im Rahmen der untersuchten DDoS-Angriffe wurde durch Schweizer Internet Service Provider der DDoS-Datenverkehr in ihrem Backbone blockiert. Dies erfolgte durch das Sperren von IP-Ranges und von Autonomous Systems (AS). Diese Sperrungen wurden während der Angriffe kontinuierlich angepasst. Basis für die Sperrungen war der umfassende Informationsaustausch, welcher durch das NCSC ermöglicht wurde.

Da die Sicherheits- und Betriebsprozesse (Incident Response Management, Change Management und Release Management) manuelle Arbeit erfordern (z. B. Definition von Blockierungsregeln), muss mit einer gewissen Zeitspanne zwischen Erkennung und Mitigation von solchen DDoS-Angriffen gerechnet werden. Aktuelle Erfahrungen und Aussagen zeigen, dass mit einer Reaktionszeit von ca. zwei Stunden zu rechnen ist.

Da der Akteur implementierte Schutzmassnahmen bei den betroffenen Organisationen nicht in jedem Fall feststellen kann, muss damit gerechnet werden, dass die Angriffe unvermindert weitergehen – jedoch keine Ausfälle mehr verursachen.

Quantifizierung

Während der DDoS-Angriffe auf die Bundesverwaltung wurden ca. 20'000 IP-Adressen festgestellt. Statistiken über die Angriffe auf die Bundesverwaltung zeigen einen Anteil von 3% IP-Adressen, welche dem Schweizer IP-Adressenbereich zugeordnet werden.

Mit einem Durchschnitt von 20'000 pps bis 25'000 pps (packets per seconds) und weniger als 200 Mbit/s (Megabits per second) war der Datenverkehr der DDoS-Angriffe eher gering. Diese Kennzahlen sind für DDoS-Angriffe auf Applikationsebene typisch.

[12] https://en.wikipedia.org/wiki/Black_hole

4 Verlauf des Angriffs

Mit dem Beginn der DDoS-Angriffe gegen die Schweiz am Mittwoch, 7. Juni 2023 um 8:00 Uhr, erscheint in der C2-Target-Liste die Webseite https://www.parlament.ch als erstes Ziel.

Grund für dieses neue Ziel sind:

- Diskussionen im Schweizer Parlament über Waffenexporte [13].
- Die Ankündigung vom 5. Juni bezüglich der Videobotschaft von Wolodymyr Selenskyj im Schweizer Parlament am 15. Juni 2023[14].

Die Followers wurden über den Telegram-Kanal des Akteurs informiert:

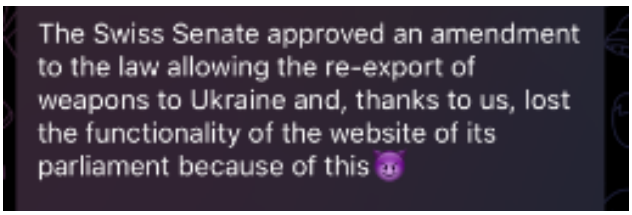

Abbildung 9: Erste Nachricht in Telegram-Kanal, Quelle: Telegram

Auch die Ankündigung der Videobotschaft von Wolodymyr Selenskyj wurde mit einer Telegram-Nachricht kommentiert:

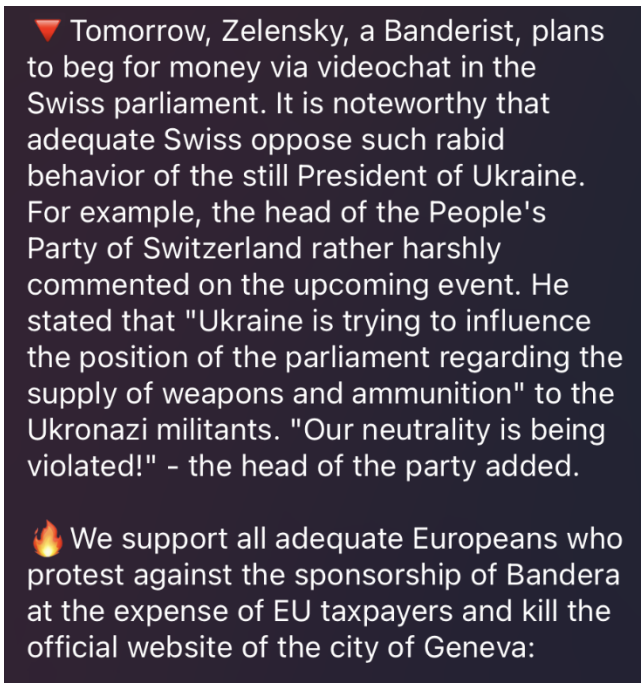

Abbildung 10: Zweite Telegram-Kanal Nachricht, Quelle: Telegram

[13] https://www.parlament.ch/de/services/news/Seiten/2023/20230308171441079194158159038_bsd143.aspx
[14] https://www.parlament.ch/de/services/news/Seiten/2023/20230606100706116194158159038_bsd044.aspx

Chronologischer Ablauf

Die DDoS-Angriffe erfolgten während rund zwei Wochen. Dabei ist zu erwähnen, dass der Akteur schon vorher andere Staaten in ungefähr gleichem Umfang (zeitlich, technisch sowie inhaltlich) angegriffen hat und die Angriffe weiter anhalten.

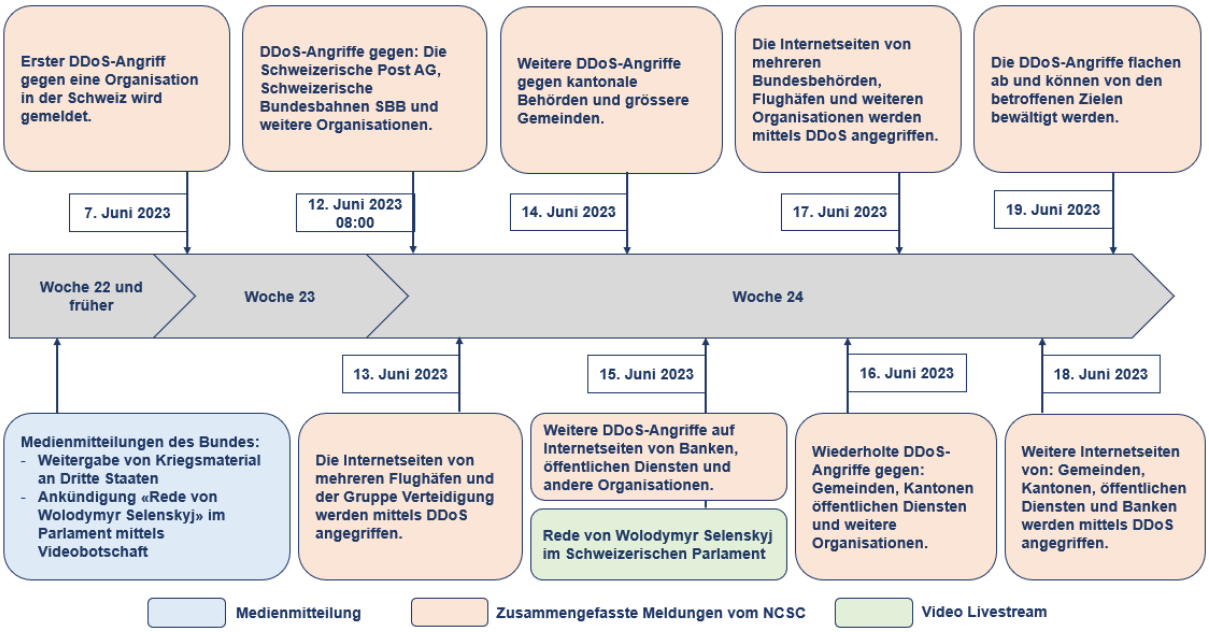

Abbildung 11: Chronologischer Ablauf der Ereignisse (zusammengefasst)

Die folgende Tabelle zeigt die erfolgreichen DDoS-Angriffe auf:

Ziele	Datum						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Bundesverwaltung	4	1		1		2	
Kantone			2		3		
Städte			6				6
Public Service	2		1	1			1
Flughafen		8				6	
Finanzsektor				5		2	1
Andere				1	3		
Rüstung				1			
Total 57	**6**	**9**	**9**	**9**	**6**	**10**	**8**

Tabelle 3: Darstellung der erfolgreichen DDoS-Angriffe

Daraus lässt sich erkennen, dass sich im Schnitt rund acht erfolgreiche DDoS-Angriffe pro Tag ereignet haben. Die Konzentration auf Webauftritte von Flughäfen, Organisationen aus dem Finanzsektor und von Städten ist offensichtlich. Zusätzlich ist zu erkennen, dass Anfang Woche 24 eher Behörden und erst nach der zweiten Wochenhälfte privatwirtschaftliche Angriffsziele im Fokus waren.

Eine weitere Darstellung zeigt die dem NCSC gemeldeten Angriffe im Vergleich zu den erfolgreich gemeldeten DDoS-Angriffen (siehe Tabelle 4):

Datum	Quellen	
	Gemeldete Angriffe beim NCSC	Als erfolgreich publizierte DDoS-Angriffe
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**

Tabelle 4: Meldungen beim NCSC im Vergleich zu den Publikationen auf Telegram durch den Akteur

Vergleicht man das Total der erfolgreichen 57 DDoS-Angriffe gemäss Tabelle 3 mit dem Total der gemeldeten DDoS-Angriffe beim NCSC (85 Meldungen, siehe Tabelle 4), wird eine Differenz ersichtlich. Daraus wird erkenntlich, dass einige Organisationen und Behörden die DDoS-Angriffe erfolgreich mitigieren respektive bemerkbare Ausfälle verhindern konnten.

Die nachfolgende Tabelle (siehe Tabelle 5) dient als Ergänzung zum chronologischen Ablauf (im Tagesrhythmus aufsteigend):

Datum	Beim NCSC gemeldete Angriffe auf Schweizer Behörden und Organisationen	Bemerkung
12.06.2023	• 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	Am ersten Tag der Cyberangriffe wurden insbesondere Behörden und staatsnahe Organisationen angegriffen.
13.06.2023	• www.vtg.admin.ch • www.flughafen-zuerich.ch • www.gva.ch	Am zweiten Tag sind die Webauftritte der Gruppe Verteidigung im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) und von verschiedenen Flughäfen angegriffen worden.
14.06.2023	• www.geneve.com • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch	Am dritten Tag waren insbesondere Städte im Fokus des Akteurs.

Datum	Beim NCSC gemeldete Angriffe auf Schweizer Behörden und Organisationen	Bemerkung
	• www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch	
15.06.2023	• www.ncsc.admin.ch • www.ruag.com • www.postauto.ch • www.zvv.ch • www.swissid.ch	Am vierten Tag der Angriffswelle wurden wieder Behörden und Organisationen angegriffen.
16.06.2023	• www.nw.ch • www.steuern-nw.ch • etax-login.nw.ch • www.stans.ch • www.buochs.ch • www.snb.ch	Am fünften Tag hatte es der Akteur vorwiegend auf die Behörden des Kantons Nidwalden abgesehen.
17.06.2023	• 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	Am sechsten Tag sind wieder Bundesbehörden in den Fokus geraten.
18.06.2023	• 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	Am letzten Tag der Angriffswelle wurden erneut Städte angegriffen.

Tabelle 5: Auflistung der angegriffenen Webauftritte vom 12. Juni 2023 bis am 18. Juni 2023

5 Wirkung des Angriffs

Die Meldungen auf dem russisch-sprachigen Telegram-Kanal des Akteurs wurden jeweils von ca. 5'500 Teilnehmern und auf dem englischen-sprachigen Telegram-Kanal von ca. 1'000 bis 1'500 Teilnehmern gelesen. Über Social Media Kanäle (z. B. über Twitter) wurden die Erfolgsmeldungen des Akteurs während der Angriffsdauer − im Vergleich zur medialen Berichterstattung in der Schweiz (siehe Kapitel 5.1) − nicht massgebend kolportiert.

Aufgrund der zielspezifischen Angriffe auf der Applikationsebene sind die Webauftritte, welche nicht durch Sperrung ganzer Adress-Ranges (mittels Quell-IP-Adressen oder mittels Sperrung von Autonomous System - AS[15]) abgesichert werden können (z. B. Auslandschweizer, welche auf die Behördenportale zugreifen müssen), besonders gefährdet. Der Grund dafür ist, dass die Konfiguration der Web Application Firewalls (WAF) zuerst an den spezifischen Angriff angepasst werden müssen. Bis diese Konfigurationen erfolgt sind, ist das Ziel dem Angriff ausgesetzt. Das NCSC geht davon aus, dass für solche Konfigurationsanpassungen rund zwei Stunden Arbeitszeit aufgewendet werden muss. Die angewandten Prozesse (z. B. Analyse – Staging – Rollout) richten sich nach den Sicherheits- und Betriebsprozessen (Incident Response Management, Change Management und Release Management) der jeweiligen Organisation respektive den Vereinbarungen im relevanten Service Level Agreement bei ausgelagerten Managed Security Services (Prozess und Reaktionszeit).

Als Beispiel ist hier das E-Konto der Stadt Basel zu erwähnen, welches am Mittwoch, 14. Juni 2023, durch massive gleichzeitige Login-Versuche überlastet wurde. Auch das E-Tax Login des Kantons Nidwalden wurde am Freitag, 16. Juni 2023, in der gleichen Art und Weise überlastet. Die angegriffenen Webauftritte waren in der Schweiz nach den Anpassungen der Schutzmassnahmen wieder zeitnah erreichbar.

Der effektive Schaden setzte sich für die betroffenen Angriffsziele aus dem Reputationsschaden und dem Aufwand zur Mitigation der DDoS-Angriffe zusammen.

Viele der betroffenen Unternehmungen haben in der Folge ihr Risiko-Management überprüft und in einigen Fällen eine stärkere Einbindung ihres Internet Service Providers (ISP)[16] in das eigene Schutzdispositiv umgesetzt (z. B. durch das Abonnieren eines DDoS-Schutzmechanismus).

5.1 Mediale Wirkung

Am 5. Juni 2023 hat das Schweizer Parlament die Rede von Wolodymyr Selenskyj für den 15. Juni angekündigt. Diese Ankündigung sowie der Parlamentsentscheid zur Weitergabe von Kriegsmaterial lösten den Beginn der DDoS-Aktivitäten von NoName057(16) aus. Als eine der ersten Organisationen wurde die Website des Parlaments (parlament.ch) angegriffen, wie die Parlamentsdienste am 7. Juni 2023 um 15:05 Uhr via Twitter bekannt gegeben haben. Nachdem am Montag 12. Juni 2023 weitere Webseiten der Bundesverwaltung nicht erreichbar waren veröffentlichte das NCSC eine Pressemitteilung zu den DDoS-Angriffen. Diese Mitteilung wurde von den Schweizer Medien breit aufgenommen. So zählte das NCSC rund 50 Artikel in den Printmedien und über 370 Online-Artikel.

Durch die Berichterstattung in den Schweizer Medien wurden die DDoS-Angriffe und deren dahinterstehende politische Botschaft in der breiten Schweizer Bevölkerung verstärkt wahrgenommen. Dies führte jedoch zu Verunsicherungen und Fragen bei der Bevölkerung. Insgesamt erreichten über 40 Medienanfragen die NCSC-Medienstelle. Der Delegierte des Bundes für

[15] https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[16] https://de.wikipedia.org/wiki/Internetdienstanbieter

Cybersicherheit Florian Schütz stand in diesen Tagen im medialen Fokus, da er verschiedenen Medien Interviews gegeben hat, in denen er DDoS erklärte um diese Verunsicherung der Bevölkerung zu minimieren.

Die intensive mediale Berichterstattung flachte nach der Rede von Wolodymyr Selenskyj am 15. Juni 2023 ab und bei der Einstellung der DDoS-Angriffe am 19. Juni 2023 waren diese kaum Thema mehr.

Einige Medien vermischten in ihrer Berichterstattung den unabhängigen, jedoch zeitgleich bekannt gewordenen Ransomware-Angriff auf die Firma Xplain. Das NCSC betonte in seiner Medienarbeit immer, dass verschiedene Gruppierungen hinter den Angriffen standen. So stand hinter dem Angriff auf Xplain (einem IT-Zulieferer der Bundesverwaltung) die Gruppe «Play» und zum DDoS-Angriff auf die Parlamentsdienst-Webseite hat sich auf Telegramm die Gruppe «NoName» bekannt. Ebenfalls wurde unterstrichen, dass die Motive der Akteure hinter einem Ransomware-Angriff (Xplain) und einer politisch motivierten DDoS-Attacke grundsätzlich unterschiedlich sind.

5.2 Politische Wirkung

In den eidgenössischen Räten erfolgte auf die DDoS-Angriffe selber keine starke Reaktion. Der Nationalratspräsident Martin Candinas, sowie die Ständeratspräsidentin. Brigitte Häberli-Koller, haben die DDoS-Angriffe in den jeweiligen Räten erwähnt.

Am 15. Juni 2023 hat die Nationalrätin Doris Fiala einen Vorstoss (Ip. 23.3755 «Befinden wir uns bereits im Cyberkrieg. Auch auf Stufe Bund?»)[17] eingereicht. Der Bundesrat betonte in seiner Antwort, dass die DDoS-Angriffe als Akt des Vandalismus zu klassifizieren seien und nur geringe Schäden verursacht hätten. Sie seien damit deutlich von gravierenden Fällen abzugrenzen. Der Bundesrat warnte zudem explizit davor, diese Angriffe als «Cyberkrieg» zu bezeichnen. Eine solche Bezeichnung «überhöht ihre Gefahr und unterstützt damit die Absicht der Angreifer, Verunsicherung zu streuen»[18].

Es ist davon auszugehen, dass sich das Parlament weiterhin aktiv über die Massnahmen des Bundes gegen Cyberangriffe generell und im Nachgang auf die erfolgten Angriffe speziell zum Thema des Schutzes gegen DDoS-Angriffe informieren wird. Weitere politische Auswirkungen der Angriffe sind nicht zu erwarten.

5.3 Rechtliche Wirkung

Die Bundesanwaltschaft hat wegen des DDoS-Angriffes auf die Website des Schweizer Parlaments ein Verfahren eröffnet.[19] Das NCSC verweist auf das laufende Verfahren.

5.4 Effektiver Schaden

Das NCSC führte nach den DDoS-Angriffen bei den betroffenen Unternehmen eine Umfrage durch. Die erhaltenen Rückmeldungen zeigten auf, dass der grösste Schaden bei der Unzufriedenheiten der Kunden lag, da betroffene Webauftritte vorübergehend nicht erreichbar waren. Diese Ausfälle erstreckten sich hauptsächlich über wenige Stunden und in einem Einzelfall über maximal drei Tage, begleitet von Instabilitäten. Ein allfälliger monetärer Schaden kann

[17] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233755#tab-panel-acc-1

[18] https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233755#tab-panel-acc-2

[19] https://www.inside-it.ch/bundesanwaltschaft-untersucht-ddos-angriff-auf-parlamentsdienste-20230612

nicht näher beziffert werden. Es wurde bestätigt, dass keine dauerhaften Schäden an der IKT-Infrastruktur entstanden sind.

Die betroffenen Behörden und Organisation mussten zur Bekämpfung der DDoS-Angriffe keine zusätzlichen personellen Ressourcen aufbauen, jedoch leisteten die Mitarbeitenden zusätzliche Arbeitszeiten.

Dem NCSC ist nicht bekannt, dass aufgrund der DDoS-Angriffe eine Organisation (z. B. ein KMU) zur Geschäftsaufgabe gezwungen worden wäre.

Die DDoS-Angriffe haben bestätigt, dass solche Attacken jedes beliebige Ziel treffen und zumindest kurzfristig stören können. Das NCSC empfiehlt deshalb, ein proaktives Schutzdispositiv zu pflegen (siehe Schutzmassnahmen im Kapitel 6).

6 Empfehlungen

Im Vergleich zu komplexen Angriffen (z. B. Advanced Persistent Threats), die auf das Eindringen in Computersysteme abzielen, weisen DDoS-Angriffe eine geringere technische Komplexität auf. Die Herausforderungen beim Schutz vor DDoS-Angriffen liegen bei der Skalierbarkeit der Angriffe und der Entwicklung neuer Techniken, um DDoS-Schutzmechanismen zu umgehen. Deshalb sind robuste Sicherheitsmassnahmen und ein proaktiver Ansatz von entscheidender Bedeutung, um sich vor den Auswirkungen von DDoS-Angriffen zu schützen.

Das NCSC gibt verschiedene Empfehlungen ab, welche in der Form von proaktiven Massnahmen zum Schutz vor oder als reaktive Massnahmen im Anschluss an DDoS-Angriffe umgesetzt werden können.

Proaktive Massnahmen

Folgende Massnahmen (nicht abschliessend) sollten je nach Bedarf zur Vorbereitung auf einen potenziellen DDoS-Angriff umzusetzen:

Proaktive Massnahmen	Beschreibung / Nutzen	Wirkung bei den vorliegenden DDoS-Angriffen
Prüfen Sie die Relevanz von DDoS-Angriffen in Ihrem IT-Risikomanagement und IT-Service Continuity Management.	DDoS-Angriffe werden im IT-Risikomanagement Prozess auf ihre Relevanz geprüft und gegebenenfalls als Risiko aufgenommen.	Gegen dieses Risiko werden vor dem Angriff angemessene technische und organisatorische Massnahmen umgesetzt.
Identifizieren Sie Ihre potentiell bedrohten Webauftritte im Rahmen einer Business Impact Analyse (BIA).	Eine BIA liefert die Anforderungen an die Verfügbarkeit von Webauftritten.	Die businesskritischen Webauftritte sind bekannt und können entlang der Businessanforderungen geschützt werden.
Stimmen Sie sich bezüglich Schutzmassnahmen zur Gewährleistung der Verfügbarkeit mit Ihrem ISP oder Managed Security Service Provider (MSSP) ab.	Massnahmen zur Einhaltung der Anforderungen an die Verfügbarkeit von Webauftritten werden mit dem jeweiligen Service Provider vereinbart und periodisch auf ihre Aktualität geprüft.	Die Schutzmassnahmen sind vertraglich vereinbart und stehen bei einem potenziellen Angriff zur Verfügung.
Berücksichtigen Sie die Schutzmassnahmen vor DDoS-Angriffen in Ihrer Sicherheitsarchitektur (Security by Design).	Massnahmen zum Schutz vor DDoS-Angriffen werden bereits beim Design eines Webauftrittes implementiert. Zum Beispiel kann ein Content Delivery Network (CDN) dazu beitragen, die Auswirkungen von DDoS-Angriffen zu mildern, indem es den Verkehr über eine Vielzahl von Servern weltweit verteilt.	Die Berücksichtigung der Sicherheitsanforderungen in der Sicherheitsarchitektur minimiert die Wahrscheinlichkeit, dass der DDoS-Datenverkehr Webauftritte erreichen und überlasten.
Setzen Sie für potentiell bedrohte Webauftritte eine Web Application Firewall (WAF) ein.	WAFs überwachen den Datenverkehr auf Anwendungsebene und blockieren schädliche Anfragen, bevor sie den Webauftritt erreichen können.	Erst durch das Vorhandensein einer WAF, kann man Webauftritte rasch gegen DDoS-Angriffe schützen. WAF's können konfigurativ an den spezifischen DDoS-Angriff

Proaktive Massnahmen	Beschreibung / Nutzen	Wirkung bei den vorliegenden DDoS-Angriffen
		angepasst werden.
Arbeiten Sie einen Notfallplan aus und testen Sie diesen.	Ein Notfallplan schafft strukturierte Anweisungen im Falle eines DDoS-Angriffs. Er umfasst das IT-Service Continuity Management und das Business Continuity Management (BCM).	Ein Notfallplan erlaubt die geplante und strukturierte Reaktion auf den DDoS Angriff.

Tabelle 6: Proaktive Massnahmen

Reaktive Massnahmen

Das NCSC empfiehlt, die folgenden Massnahmen bedarfsgerecht zur Reaktion auf einen potenziellen DDoS-Angriff umzusetzen:

Massnahmen zur Reaktion auf DDoS-Angriffe	Beschreibung / Nutzen	Wirkung bei den vorliegenden DDoS-Angriffen
Überwachen Sie die exponierten Webauftritte und richten Sie eine automatisierte Erkennung von Anomalien ein.	Die Überwachung des Datenverkehrs hilft ungewöhnliche Muster oder erhöhten Netzwerkverkehr zu erkennen.	Diese Massnahme unterstützt das frühzeitige Erkennen und Abwehren von DDoS-Angriffen.
Stellen Sie sicher, dass Sie technisch und organisatorisch rasch auf DDoS-Angriffe reagieren können.	Technische Schutzmassnahmen dienen vorwiegend der Detektion und Abwehr von DDoS-Angriffen. Die Sicherheitsprozesse regeln die organisatorischen Aspekte (z. B. Security Incident Management, Eskalation, Medienarbeit).	Durch die rasche Implementierung von Schutzmassnahmen (z. B. blockieren von IP-Adressen, konfigurative Anpassungen von Sicherheitsmechanismen durch die Pikettorganisation) können DDoS-Angriffe zeitnah mitigiert werden.
Stellen Sie sicher, dass ihre Webauftritte in der Sicherheitsarchitektur bereits vorgelagert (Schutz in der Tiefe) vor automatisierten Angriffen geschützt sind.	Durch die Implementierung von CAPTCHA[20]-Technologien kann sichergestellt werden, dass z. B. ein Webformular eines Webauftrittes nicht automatisiert ausgefüllt werden kann.	Vorgelagerte Schutzmassnahmen verhindern, dass der automatisierte DDoS-Angriff die Webauftritte erreicht.
Sperrung von IP-Ranges und Autonomous Systems (AS's) anhand der Indicators of Compromise (IOC's).	Grundlage für eine solche Sperrung sind die IOC's, die Cyber Security Hub des NCSC verfügbar sind. Durch die oben erwähnte Anomalie-Erkennung können die IOC's organisationsspezifisch erkannt werden.	Der schädliche Datenverkehr kann dadurch unterbunden werden.

[20] https://de.wikipedia.org/wiki/Captcha

Massnahmen zur Reaktion auf DDoS-Angriffe	Beschreibung / Nutzen	Wirkung bei den vorliegenden DDoS-Angriffen
Blockierung der spezifischen Angriffe auf Applikationsebene.	Anhand der Informationen aus verschiedenen Quellen (z. B. Security Incident und Event Management (SIEM) und diversen Log-Dateien) können die Sicherheitsmechanismen (z. B. WAF) spezifisch für die Abwehr des Angriffs angepasst werden.	Durch das Blockieren des DDoSia-Clients (User Agent) kann der DDoS-Angriff bereits bei der WAF abgewehrt werden.

Tabelle 7: Massnahmen zur Reaktion auf DDoS-Angriffe

Das NCSC publiziert weitere Handlungsempfehlungen und vorbeugende Massnahmen auf seiner Internetseite (siehe Kapitel 8, [3]).

7 Fazit

Die klassischen Anti-DDoS-Sicherheitsstrategien, welche traditionell eher gegen volumetrische DDoS-Angriffe[21] ausgerichtet sind, reichen zum Schutz vor dem aktuellen Akteur mit den Angriffen auf der Applikationsebene nicht aus.

In vorliegenden Fall waren die angreifenden Systeme der Cyberaktivisten zu grossen Teilen über IP-Ranges und Autonomous Systems (AS) identifizierbar und konnten deshalb weitgehend gezielt gesperrt werden. Dies sorgte dafür, dass die angegriffenen Webauftritte relativ zeitnah wieder verfügbar waren. Ein wichtiger zusätzlicher Sicherheitsmechanismus waren Web Application Firewalls (WAF's, wenn vorhanden), welche spezifisch auf das Angriffsmuster nachkonfiguriert werden konnten.

Falls bei einer künftigen DDoS-Attacke die teilnehmenden Cyberaktivisten geografisch noch stärker verteilt agieren sollten, muss mit einem grösseren Schadensausmass gerechnet werden. Es wird schwieriger sein, alle IP-Ranges und/oder AS zu identifizieren und zu blockieren. Deshalb ist in einem solchen Fall mit zeitlich ausgedehnteren Beeinträchtigungen der angegriffenen Webauftritte zu rechnen.

Lessons learned

Folgende Lessons learned sind aus Sicht des NCSC's erwähnenswert:

- Der Akteur führte − trotz weit verbreiteten / implementierten DDoS-Sicherheitsmechanismen − seine Angriffe teilweise und über eine gewisse Zeit erfolgreich um. Als Konsequenz müssen die Sicherheitsdispositive geprüft und bedarfsgerecht angepasst werden;
- DDoS-Angriffe können auch das Business von Dritten beeinträchtigen, sofern ein Webauftritt erfolgreich angegriffen wird, welcher für die korrekte Funktionsweise eines anderen Webauftrittes oder Business Prozesses benötigt wird. Eine Business Impact Analyse (BIA) dient als Grundlage, damit solche Abhängigkeiten erkannt und im Business Continuity Management (BCM) berücksichtigt werden können;
- Der Einfluss von Sperrungen (z. B. mittels IP-Ranges) auf die Geschäftstätigkeit der jeweiligen Unternehmung (z. B. Beeinträchtigung des Zugriffs für legitime Benutzer, gesetzlich geregelte Webauftritte), muss im Rahmen einer Business Impact Analyse geprüft werden;
- Die Koordination und der detaillierte Informationsaustausch des NCSC mit den Betroffenen war sehr wichtig;
- Die Verbreitung von angriffsspezifischen Informationen (z. B. Namen des Akteurs) muss alle Vor- und Nachteile berücksichtigen;
- Die Auswirkungen eines DDoS-Angriffs können mit den gängigen Sicherheitsmechanismen (z. B. Sperrung von IP-Ranges, Geoblocking, Web Application Firewalls, Rate Limitierung) relativ zeitnah minimiert werden, sobald die Angriffsmuster in ausreichender Tiefe bekannt sind;
- Können Vertrauensstellungen zwischen isolierten Netzwerken etabliert werden, welche über das Internet kommunizieren, können auch neuere Technologien wie z. B. SCiON[22] eingesetzt werden. Die SCiON-Technologie verfügt über einen integrierten Schutz vor DDoS-Angriffen;
- Die breite mediale Berichterstattung hatte zur Folge, dass die Schweizer Behörden und Organisationen bezüglich der Thematik «DDoS» sensibilisiert wurden;
- Aus den Antworten auf die NCSC-Umfrage konnte entnommen werden, dass die betroffenen Unternehmen ihr Risiko hinsichtlich DDoS-Angriffe neu bewerten und die entsprechenden Massnahmen überprüfen werden.

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

[22] https://scion-architecture.net/

Abschliessende Bemerkungen

Grössere Organisationen, welche z. B. über ein Security Operation Center (SOC) verfügen, konnten relativ rasch reagieren, sobald die Angriffsmuster bekannt waren. Ob technische Fragestellungen oder fehlende Sicherheitsprozesse teilweise zu zeitlich längeren Beeinträchtigungen geführt haben (z. B. Ausfälle von Webauftritten über mehrere Tage), kann nachträglich nicht mehr schlüssig eruiert werden.

Die jeweiligen Unternehmen stehen in der Verantwortung, im Rahmen des kontinuierlichen Verbesserungsprozesses die benötigen Anpassungen vorzunehmen. Das NCSC empfiehlt, die in diesem Bericht empfohlenen Massnahmen und die Lessons Learned zu prüfen und in Eigenverantwortung bedarfsgerecht umzusetzen.

8 Anhänge

Informationen und Erläuterungen zu DDoS-Angriffen

Das NCSC publiziert auf seiner Webseite generelle Informationen und Erläuterungen zu DDoS-Angriffen[23].

Die verschiedenen Varianten von DDoS-Angriffen (z. B. volumetrische Angriffe oder Layer-7 Angriffe) werden in einem Dokument des Multi State Information Sharing & Analysis Centers (MS-ISAC[24], in Kooperation mit der US Cybersecurity & Infrastructure Security Agency CISA[25] und dem Center for Internet Security CIS[26]) detailliert erläutert.

Referenzierte Informationsquellen

Nummer	Erläuterung und URL
[1]	Präsident Selenskyi wird sich am 15. Juni an die Schweizer Ratsmitglieder richten, https://www.parlament.ch/press-releases/Pages/mm-info-2023-05-31.aspx
[2]	Ständerat will Weitergabe von Schweizer Kriegsmaterial erleichtern, https://www.parlament.ch/de/services/news/Seiten/2023/20230607124254254194158159038_bsd093.aspx
[3]	Empfehlungen des NCSC gegen DDoS-Angriffe, https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/ddos.html
[4]	Sekoia - Detailliertere Informationen über den DDoSia-Client, https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

Tabelle 8: Referenzierte Informationsquellen

Kategorisierung der Akteure und deren Motivationen

Um die Auswirkungen von Cyberangriffen einschätzen zu können, ist es zunächst wichtig festzustellen, welche Bedrohungsakteure die Angriffe durchführen. Diese wiederum lassen sich nach ihrer Motivation unterscheiden und in folgende Kategorien einordnen:

Bedrohungsakteure (Threat Actors)	Motivationen
Staatliche Akteure	Staatliche Akteure haben meist geopolitische Absichten. Dabei werden systemrelevante Infrastrukturen der Gegenpartei angegriffen. Das Ziel dabei ist, die Gegenpartei zu destabilisieren und zu annektieren.
Kriminelle Organisationen	Kriminelle Organisationen haben meist finanzielle Absichten. Durch ihre betrügerischen Aktivitäten wollen sie ihre Opfer in ihre Gewalt bringen. Das Ziel dabei ist, Lösegeldzahlungen zu erpressen.
Hacktivisten	Hacktivisten wollen Aufmerksamkeit erregen und ihre politischen oder religiösen Weltanschauungen verbreiten. Durch gezielten Vandalismus und ihre Informationsoperationen (Info Ops)[27] wollen sie ihre Opfer destabilisieren und für

[23] https://www.ncsc.admin.ch/ncsc/de/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

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

	ihre Ideologie gewinnen. Das Ziel dabei ist, Aufmerksamkeit für ihre Weltanschauungen in der Öffentlichkeit zu erlangen.
Terroristische Gruppierungen	Terroristische Gruppierungen wollen Angst und Schrecken verbreiten.
Computerfreaks	Computerfreaks wollen ein Machtgefühl zur persönlichen Befriedigung oder Bestätigung der eigenen Kompetenz erlangen. Regelmässig geht es ihnen auch darum, Anerkennung in bestimmten Kreisen zu erlangen.
Insider	Insider sind Akteure, die im Gegensatz zu Aussenstehenden privilegierten Zugang zum Opfer haben (z. B. Angestellte, Beauftragte). Sie nutzen diesen Zugang, um Schaden zu verursachen oder um sich ungerechtfertigt zu bereichern.

Tabelle 9: Kategorisierung der Bedrohungsakteuren und ihre Motivation

Details der DDoS-Angriffe im Tagesrhythmus

Meldedatum	Titel	Beschreibung	Kommentare
12.06.2023	DDoS-Angriffe vom 12.06.2023 durch NoName057(16) auf Internetseiten der Schweiz inklusive der Bundesverwaltung	Am Montag, dem 12.06.2023, um 8.20 Uhr finden DDoS-Angriffe durch NoName057(16) auf Internetseiten der Bundesverwaltung (BAZG und EJPD) statt. Einige Minuten später wird die Liste der anvisierten Seiten gepostet, die sich wie folgt zusammensetzt: • 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 Um 10.03 Uhr bekennt sich NoName057(16) auf seinem Telegram-Kanal zu den Angriffen auf die Schweiz. Dabei gibt er die Internetseite des Parlaments [1] mit einem Bericht von check-host.net vom 12.06.2023, 9.28 Uhr (UTC: 07:28) [2] an. Der Bericht zeigt, dass die Verbindung nur von der Schweiz aus funktioniert (DDos-Schutz durch Geofencing). NoName057(16) rechtfertigt seine Aktion mit den Dankesworten, die Selenskyj dafür an die Schweiz gerichtet hat, dass diese dem 10. Sanktionspaket	• Angriffsart: layer 7 attacks (HTTP POST and GET flood). • Herkunft des Datenverkehrs bei den DDoS-Angriffen: traffic originates from Russian IP space and MIRhosting (AS206932, AS52000) as well as Stark Industries (AS44477). • Andere Empfehlungen: mitigation can also include searching for anomalies in the HTTP Header as well as protecting resource intensive functions using a captcha. Auf seinem Telegram-Kanal bekennt sich NoName057(16) zu den Angriffen auf das EJPD (11:23), das BAZG (12:35), fedpol (13:47), das EDI (15:00), die SOB (16:04) und Die Post (17:11). Die Berichte von Check-Host [3] werden um 9.30 Uhr (UTC: 07:31) erstellt, mit Ausnahme desjenigen zu Die Post, der um 13.47 Uhr (UTC: 11:47) erstellt wird. [3] https://check-host.net/check-report/103a5159k82c https://check-host.net/check-report/103a4fdakb51 https://check-host.net/check-report/103a4edck891

Meldedatum	Titel	Beschreibung	Kommentare
		gegen Russland zugestimmt hatte. Diese Zustimmung vonseiten der Schweiz war am 29.03.2023 erfolgt. [1] www.parlament.ch [2] https://check-host.net/check-report/103a4c6aka29	https://check-host.net/check-report/103a53afk272 https://check-host.net/check-report/103a523fk4ec https://check-host.net/check-report/103af460ka6b
13.06.2023	DDoS-Angriffe vom 13.06.2023 durch NoName057(16) auf Internetseiten der Schweiz inklusive der Bundesverwaltung	Am Dienstag, dem 13.06.2023, um 9.20 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • flyedelweiss.com • www.vtg.admin.ch • www.flughafen-zuerich.ch • peoples.ch • engadin-airport.ch • www.bernairport.ch • airport-grenchen.ch • www.gva.ch Um 11.10 Uhr wird diese Liste um die folgenden neuen Ziele erweitert: • www.swisshelicopter.ch • zimex.com • www.pc7-team.ch	Auf seinem Telegram-Kanal bekennt sich NoName057(16) zu den Angriffen auf 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 (Flughafen St. Gallen, 15:58), www.swisshelicopter.ch (16:19), zimex.com (17:27) und www.pc7-team.ch (18:01). Die Berichte von Check-Host [1] werden um 9.30 Uhr (UTC: 07:30) erstellt, mit Ausnahme derjenigen zu www.swisshelicopter.ch, zimex.com und www.pc7-team.ch, die um 11.10 Uhr (UTC: 09:10) erstellt werden. Bei der Analyse des Telegram-Kanals von NoName057(16) fällt auf, dass die nach den Angriffen vom 12.06.2023 von «Followern» geposteten Kommentare etwas mit der Schweiz zu tun haben. Das erhöht die Wahrscheinlichkeit, dass die darin genannten Organisationen das Ziel künftiger Angriffe sein werden. Die betroffenen Kantone werden vor diesen Kommentaren gewarnt (11:35, 11:39). [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-

Meldedatum	Titel	Beschreibung	Kommentare
			report/103d87c3k56c https://check-host.net/check-report/103dc68ek21e https://check-host.net/check-report/103dc78ak788 https://check-host.net/check-report/103dc833k3f3
14.06.2023	DDoS-Angriffe vom 14.06.2023 durch NoName057(16) auf Internetseiten der Schweiz	Am Mittwoch, dem 14.06.2023, um 8.00 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • www.geneve.com Um 08.20 Uhr wird diese Liste um die folgenden neuen Ziele erweitert: • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch Um 11.15 Uhr um die folgenden neuen Ziele: • www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch Dabei ist anzumerken, dass die Seite www.geneve.com die touristische Seite von Genf darstellt und nicht die offizielle Seite der Stadt bzw. des Kantons Genf, die unter der Adresse www.ge.ch zu finden ist.	Auf seinem Telegram-Kanal bekennt sich NoName057(16) zu den Angriffen auf www.geneve.com (10:10), www.stadt-schaffhausen.ch (11:45), www.bs.ch (12:02), e-konto.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) und www.bellinzona.ch (16:02). Die Berichte von Check-Host [1] werden um 9.30 Uhr (UTC: 07:30) erstellt, mit Ausnahme derjenigen zu www.stadt-schaffhausen.ch, www.lausanne.ch, www.montreux.ch, www.stadt.sg.ch und www.bellinzona.ch, die um 10.50 Uhr (UTC: 08:50) erstellt werden. Als NoName057(16) den Angriff auf www.geneve.com öffentlich macht, spielt er auf die für den 15.06.2023 in der Bundesversammlung vorgesehene Ansprache von Präsident Selenskyj per Videokonferenz an. [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 https://check-host.net/check-

Meldedatum	Titel	Beschreibung	Kommentare
			report/1040e788k29 https://check-host.net/check-report/1040e84ck7ed
15.06.2023	DDoS-Angriffe vom 15.06.2023 durch NoName057(16) auf Internetseiten der Schweiz	Am Donnerstag, dem 15.06.2023, um 8.00 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • 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	Auf seinem Telegram-Kanal bekennt sich NoName057(16) zu den Angriffen auf 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), und www.geneve-finance.ch (17:09). Die Berichte von Check-Host [1] werden um 9.15 Uhr (UTC: 07:15) erstellt. [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/10440aadk1ad https://check-host.net/check-report/10440b9ak78e https://check-host.net/check-report/10440c2fkb4c
16.06.2023	DDoS-Angriffe vom 16.06.2023 durch NoName057(16) auf Internetseiten der Schweiz	Am Freitag, dem 16.06.2023, um 9.20 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • www.nw.ch • www.steuern-nw.ch • etax-login.nw.ch • www.pilatus-aircraft.com • www.stans.ch • www.buochs.ch	Auf seinem Telegram-Kanal bekennt sich NoName057(16) zu den Angriffen auf 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) und www.lakelucerne.ch (15:52). Die Seite www.autofaehre.ch taucht nicht in der Liste der Ziele auf, die von dem Botnet von NoName057(16) angegriffen werden, und sie ist aktuell

Meldedatum	Titel	Beschreibung	Kommentare
		• www.snb.ch • www.zentralbahn.ch • www.lakelucerne.ch Um 10.00 Uhr wird der Liste eine zusätzliche Seite hinzugefügt: • www.vsz.ch	auch erreichbar (15:00). Wahrscheinlich handelt es sich hierbei um einen Kommunikationsfehler von NoName057(16). Die Berichte von Check-Host werden um 9.15 Uhr (UTC: 07:15) erstellt.
18.06.2023	DDoS-Angriffe vom 17.–18.06.2023 durch NoName057(16) auf Internetseiten der Schweiz	Am Samstag, dem 17.06.2023, um 9.20 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • 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 Um 10.30 Uhr wird der Liste eine zusätzliche Seite hinzugefügt: • www.edi.admin.ch Um 14.00 Uhr werden der Liste zusätzliche Seiten hinzugefügt: • www.vtg.admin.ch • www.swisshelicopter.ch • www.zimex.com • www.heliswissinternational.com • www.pc7-team.ch Am Sonntag, dem 18.06.2023, um 10.45 Uhr wird von NoName057(16) eine neue Liste mit Zielen für DDoS-Angriffe verwendet. Die Liste setzt sich wie folgt zusammen: • 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	Die grosse Mehrheit der Seiten, die am Samstag und am Sonntag anvisiert werden, sind schon während der gesamten Woche anvisiert worden. Auf seinem Telegram-Kanal bekennt sich NoName057(16) am Samstag, dem 17.06.2023, zu den Angriffen auf 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) und www.pc7-team.ch (19:47). Die Berichte von Check-Host werden von 9.30–10.00 Uhr (UTC: 07:30–08:00) erstellt, mit Ausnahme derjenigen zu gva.ch, vtg.admin.ch, www.swissprivatebankers.com, www.swisshelicopter.ch, www.zimex.com und www.pc7-team.ch, die um 14.00 Uhr (UTC: 12:00) erstellt werden. Auf seinem Telegram-Kanal bekennt sich NoName057(16) am Sonntag, dem 18.06.2023, zu den Angriffen auf 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) und www.zvv.ch (18:34). Die Berichte von Check-Host werden von 9.30–10.00 Uhr (UTC: 07:30–08:00) erstellt, mit Ausnahme derjenigen zu www.swissprivatebankers.com

Meldedatum	Titel	Beschreibung	Kommentare
		• www.ville-fribourg.ch • www.stadt-schaffhausen.ch Um 15.15 Uhr werden der Liste zusätzliche Seiten hinzugefügt: • www.juliusbaer.com • sasd.ch • www.swissprivatebankers.com • www.zvv.ch • www.myswitzerland.com	und www.zvv.ch, die um 14.30 Uhr (UTC: 12:30) erstellt werden.

Tabelle 10: Tägliche DDoS-Meldungen mit Ergänzungen vom 12. Juni 2023 bis am 18. Juni 2023