



30 October 2023

Downstream incident analysis

DDoS attacks by NoName057(16), June 2023

This report analyses the distributed denial of service (DDoS) attacks on Swiss organisations and authorities in the first two weeks of June 2023 (weeks 23 and 24). The type of application-layer DDoS attack deployed is explained in detail.

Switzerland sustained no lasting damage from these DDoS attacks perpetrated by the actor NoName057(16). Most of the Swiss organisations and authorities targeted were prepared for DDoS attacks and were therefore able to respond appropriately. This shows that the potential damage can be significantly minimised by implementing security mechanisms as required.

The actor's multiple targets and the political sensitivity of Ukrainian President Volodymyr Zelenskyy's address to the Swiss Parliament led to the DDoS attacks garnering wide media coverage. As a result of this comprehensive reporting, the actor received the high level of public attention that it was seeking. The aim of pro-Russian hacker group NoName057(16) was to convey its political grievances in response to a series of decisions by the Swiss Parliament, including the transfer of war materiel to third countries and the announcement of President Zelenskyy's address to Parliament.

The DDoS attacks were intended to impair the availability of websites through resource exhaustion. No productive data was leaked.

Contents

1	Management summary	3
2	Introduction.....	4
2.1	Geopolitical context.....	4
2.2	Categorisation	5
3	Description of the attacks	6
3.1	Nature of the DDoS attacks	6
3.2	NoName057(16).....	6
3.3	Technical description	12
4	How the attacks unfolded	16
5	Impact of the attacks	20
5.1	Media impact	20
5.2	Political impact.....	21
5.3	Legal impact.....	21
5.4	Actual damage.....	21
6	Recommendations.....	23
7	Conclusion	26
8	Appendices	28

1 Management summary

The first two weeks of June 2023 (weeks 23 and 24) saw a series of distributed denial of service (DDoS) attacks¹ targeting Swiss organisations and authorities. This cyberactivism (hacktivism) against Switzerland was triggered by several decisions of the Swiss Parliament in connection with the war in Ukraine (see section 8, and). The hacktivists intended their DDoS attacks to send out a strong signal as a way of making their political grievances known and achieving their objectives.

The actor primarily targeted authorities and organisations close to the Federal Administration and held in high esteem by the public (e.g. the Swiss Parliament, Swiss Post and Swiss Federal Railways SBB). As a result of these DDoS attacks, a number of websites were down for a short period (a few hours). The worst damage involved outages lasting several days. There was no permanent damage to ICT infrastructure or other economic damage, nor was this the actor's primary objective in these attacks, which were mainly aimed at attracting media, public and political attention.

The perpetrator was the pro-Russian hacktivist group NoName057(16), which since March 2022 has been carrying out DDoS attacks against a range of targets worldwide that it considers to be critical of Russia, including public administrations and authorities, companies and other organisations. Successful attacks are posted on the Telegram channel of the same name.

To wage its DDoS attacks, NoName057(16) mobilises cyberactivists known as "heroes", who make their own computers available for the attacks in return for payment. The "heroes" can also suggest potential targets. The actor provides the DDoS client, called DDoSia, and the "heroes" receive technical support via the DDoSia project Telegram channel.

The web-based attacks focused on the application layer (OSI layer 7)². NoName057(16) aimed to cause targeted website outages by overloading the available capacities (resource exhaustion) so that certain services would no longer be available to the public (e.g. the online purchase of SBB tickets). The entire wave of attacks lasted two weeks, with no change from a technical perspective over this period. However, the attacked targets changed day by day. Some victims were well prepared for such DDoS attacks, others less so. Accordingly, some were able to respond to the attacks faster than others and thus minimise the impact.

The impact of such a DDoS attack can be minimised with technical measures (e.g. by means of a web application firewall: reconfiguring the firewall rules so that the DDoS client is detected and blocked, see section 3.3) and organisational measures (e.g. business continuity management, BCM³).

The latent threat posed by such DDoS attacks requires specific developments in cyberspace to be permanently monitored, risks to be evaluated and security arrangements to be adapted as necessary. As the outages caused and the resulting media coverage made clear, there is further scope for improving the preparation of the response to such attacks among some of the parties affected. Some have already implemented measures.

¹ https://en.wikipedia.org/wiki/Denial-of-service_attack

² https://en.wikipedia.org/wiki/OSI_model

³ https://en.wikipedia.org/wiki/Business_continuity_planning

2 Introduction

2.1 Geopolitical context

In late February 2022, Russia launched a military attack on Ukraine. The ensuing war has also seen Ukraine attacked in cyberspace, whether by state actors or cyberactivism (hacktivism). Russia too has been the target of cyberattacks, carried out by various cyberactivists and other organisations. Other countries, especially NATO members, have likewise been the focus of cyberattacks.

Overall, only a few activist-motivated cyberactivities against Switzerland and Swiss targets have been detected so far in the context of the Ukraine war. The number and intensity of cyberactivities have been in line with the threat assessment issued by the National Cybersecurity Centre (NCSC) and the Federal Intelligence Service (FIS). Materialisation of the threat does not alter the threat situation. Switzerland may continue to be affected by activist-motivated cyberactivities from time to time. So far, it has been possible to counter these cyberactivities with conventional security and mitigation measures. Accordingly, the damage in Switzerland to date has been minor.

The FIS presents the situation in detail in its situation report "Switzerland's Security 2023".⁴ The following diagram shows cyberattacks (DDoS) by cyberactivists in the first year of the war:

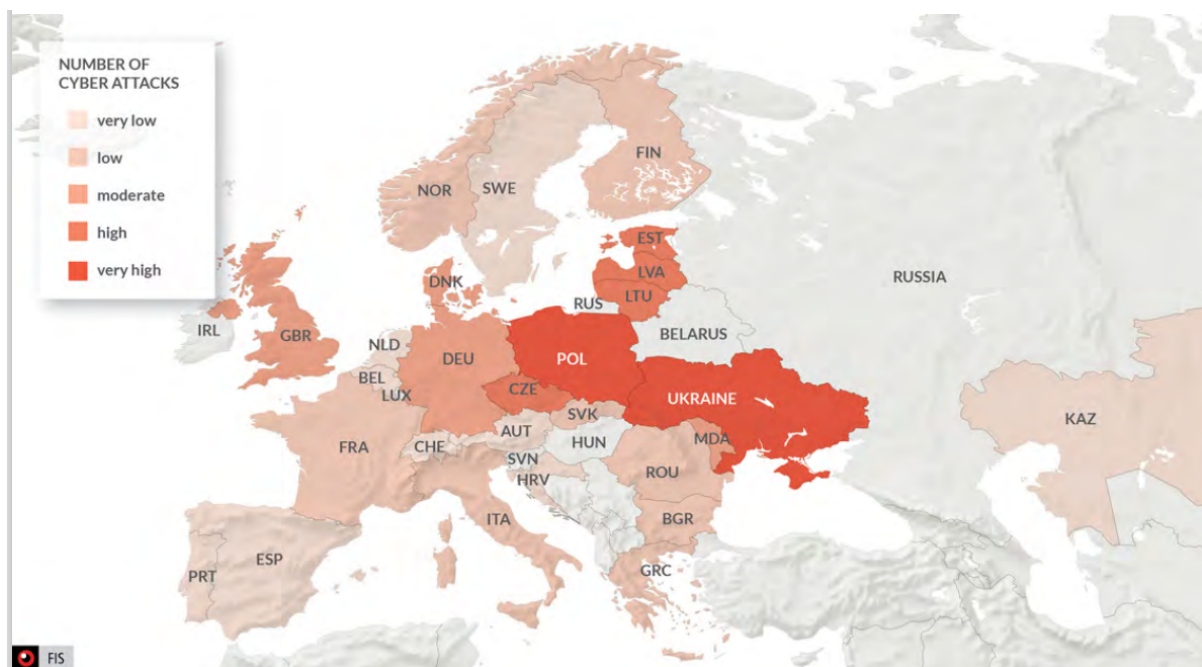


Figure 1: DDoS attacks by cyberactivists in the first year of war; source: FIS situation report 2023

The term "cyberwarfare"⁵ or "cyberwar" (a portmanteau of **cyberspace** and **war**) refers to a military conflict waged with information technology between two states over a certain period.

The temporary DDoS attacks perpetrated by NoName057(16) on various targets in Switzerland in June 2023 cannot be understood as an act of war falling within the definition of the term cyberwarfare, but should rather be classed as cyberactivism (see section 2.2).

⁴ <https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.detail.document.html/vbs-inter-net/de/documents/nachrichtendienst/lageberichte/NDB-Lagebericht-2023-d.pdf.html>

⁵ <https://en.wikipedia.org/wiki/Cyberwarfare>

2.2 Categorisation

The DDoS attacks on Switzerland were carried out by politically motivated hacktivists, who engaged in pro-Russian propaganda as part of the cyberincident. The actor was able to cause some impairment to the targeted websites (see section 3.2). The NCSC therefore classifies the June DDoS attacks as **cyberactivism**.⁶

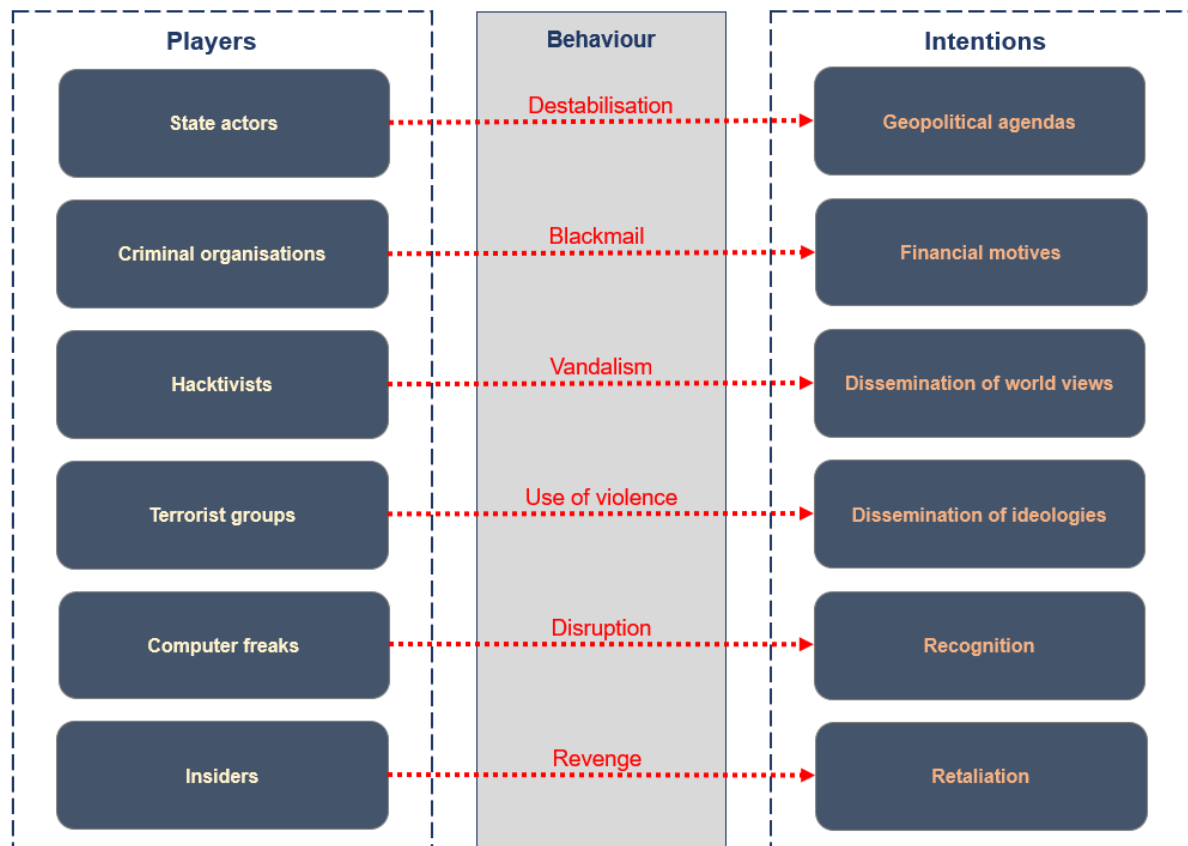


Figure 2: Actors, their behaviour and intentions

NoName057(16) disseminates its potential successes on the instant messaging service Telegram, with a view to attracting a high level of attention for its politically motivated activities. The media dissemination of successes and the garnering of political and public awareness in the target country can therefore de facto be classified as information operations (Info Ops).

⁶ https://en.wikipedia.org/wiki/Internet_activism

3 Description of the attacks

3.1 Nature of the DDoS attacks

There are several ways to exhaust system resources by means of DDoS. The aim of the June attacks was to imitate legitimate human user behaviour on websites. To this end, web services such as search or registration forms were invoked by automated means, each causing a certain load in the downstream business logic. Given that the business logic or upstream network components such as application servers, load balancers or web application firewalls (WAFs) are, for economic reasons, sized based on the expected number of users, they can be loaded beyond their intended performance limits by artificially created access requests, meaning that they are no longer able to offer their service to the actual users. As a result, the websites cannot be used as normal or become unavailable.

A more detailed technical examination can be found in section 3.3.

3.2 NoName057(16)

The actor NoName057(16) publicly admitted on Telegram to being behind these DDoS attacks. NoName057(16) is a pro-Russian group that has been active since March 2022. It first emerged in the turmoil surrounding Russia's invasion of Ukraine (February 2022), declaring "cyberwar" in response to the "information war against Russia". The group communicates primarily on Telegram and also announces its targets via this channel. Moreover, its Telegram followers can have their say about which target they want to see attacked next.

General modus operandi

The following diagram sets out the actor's general modus operandi in three phases (see technical description in section 3.3):

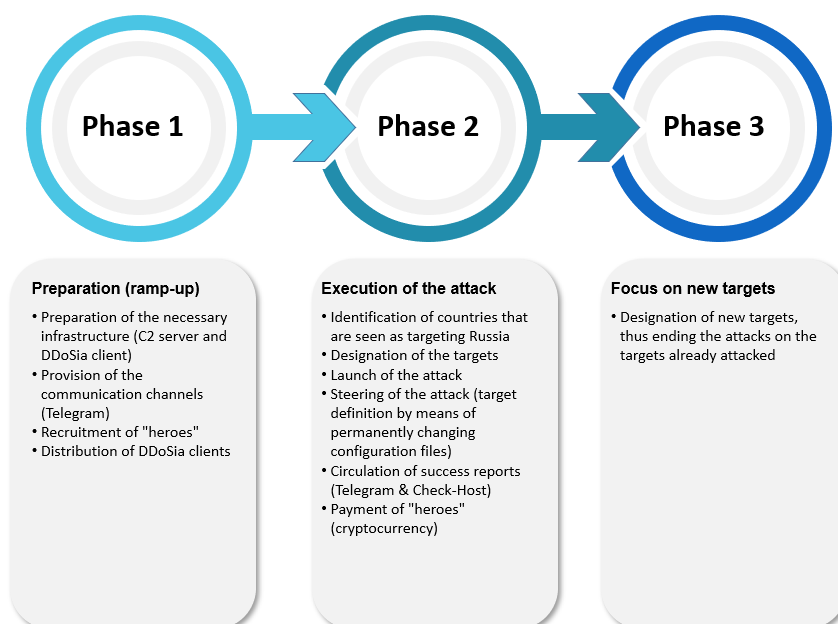


Figure 3: General modus operandi

Targets attacked

The actor's primary targets are Ukrainian websites as well as those of NATO and EU countries. It has become apparent that countries that support Ukraine or impose sanctions on Russia can also become targets. As a result of two decisions by the Swiss Parliament, perceived as benefiting Ukraine (see section 8, and), Switzerland was also briefly targeted. The DDoS attacks on Switzerland were not carried out for economic reasons or because of its prosperity, and the country was in the actor's sights for only one week. It is to be expected that the actor will continue to attack states for propaganda purposes in the future.

The following diagram shows the countries attacked by the actor between 1 April and 24 June 2023:

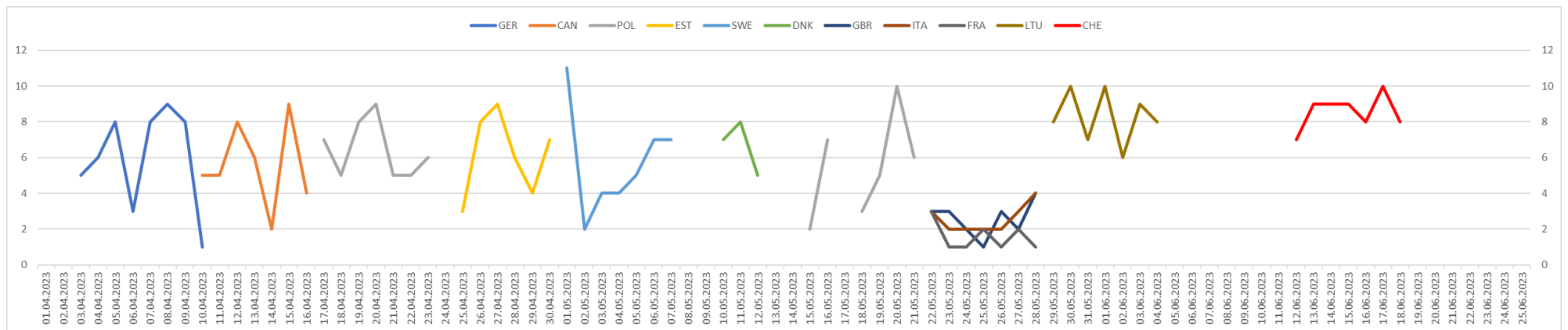


Figure 4: DDoS attacks on other countries before, while and after Switzerland was targeted (not exhaustive)

It can be seen that Switzerland (indicated by its ISO country code CHE) is one of many countries to have been hit. Moreover, the actor was already targeting other states prior to the DDoS attacks on Switzerland between 12 and 18 June 2023.

Threat assessment for the actor

The diagram below illustrates the NCSC's threat assessment for NoName057(16). It shows, among other things, that the complexity (threat level) of the attack wave was relatively low, but that the DDoS attacks occurred at high intensity (attack frequency):

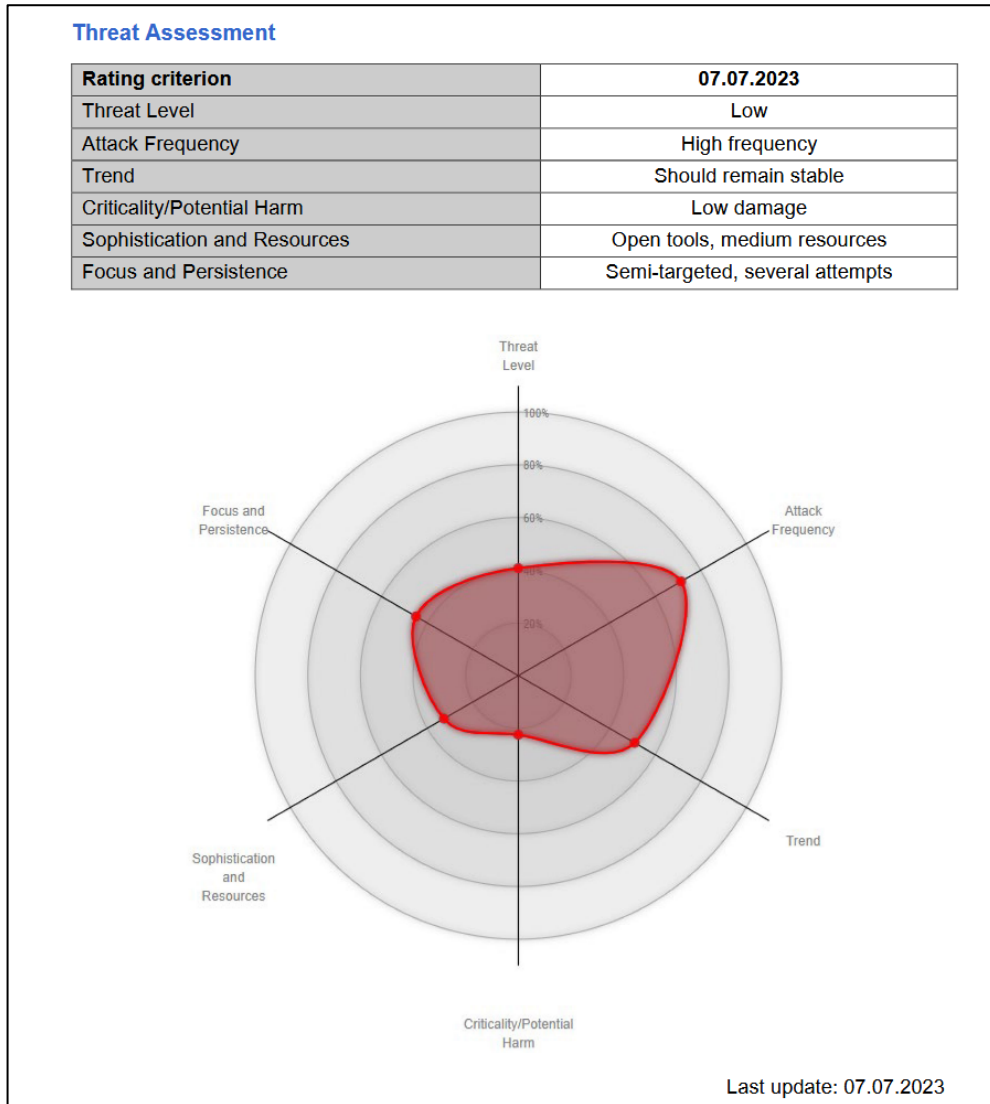



Figure 5: NCSC threat assessment for NoName057(16)

Actor's motivation

The following manifesto for the group's activities was posted by the actor on Telegram on 11 March 2022:



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: English translation of the actor's Telegram post

With a view to achieving its objectives and political goals, the actor initiates and coordinates DDoS attacks in order to generate as much attention as possible.

In another Telegram post, the actor cites the following motivations for its choice of attack methodology:

Declared motivation of actor	Classification of motivation by NCSC	Achievement of motivation in NCSC's view
"If company servers run in the cloud, the increased network traffic leads to higher costs."	The actor wants to cause financial damage.	Partially achieved. There was no significant economic damage.
"If a website is offline for more than two days, its search engine visibility declines significantly."	The actor wants to impair websites' findability.	Not achieved. Search engine visibility was not impaired.
"Even once the website is available again, the operator's reputation remains tarnished."	The actor wants to damage its targets' reputation.	Not achieved. Any reputational damage was confined to the duration of the attack period.
"Attacked systems can disclose information to the outside world (e.g. internal database information) through automatically generated error messages."	The actor wants to cause a leak of technical information.	Partially achieved. The NCSC cannot rule out the possibility that such information was disclosed during the attack period.

Table 1: Actor's motivation and NCSC assessment

If the attack is successful, a message is posted on the Telegram channel **@noname05716** by way of proof, featuring the attacked website with the country's flag and a link to a report on the website Check-Host.net.

Check-Host.net shows whether websites from different countries are available (online). It is also possible to generate ex-post snapshots indicating whether websites were available at a certain point in time. A screenshot showing that the attacked target was unavailable at a certain time is presented by the actor as proof of the successful attack (i.e. as a trophy). This Telegram message is accompanied by various greetings and calls to follow and support the group.

Actor's communication channels

The actor mainly uses two Telegram channels for communication:

- **@noname05716**: general chat channel (mostly screenshots of successful DDoS attacks) in Russian.
- **@noname05716eng**: English translations of many posts from the main chat channel.

Further communication takes place via additional channels:

Name of channel (in original language)	Translation
DDoSia - мануалы + актуальное ПО	DDoSia manuals + current software
DDoSia - поддержка	DDoSia support
Полезные материалы	Useful materials
Общий чат	General chat
English support	English support
Предложение целей	Suggestions for targets
Ваши видео и скриншоты работы с клиентом DDoSia	Your videos and screenshots from working with the DDoSia client

Table 2: List of Telegram channels with their English translations

Actor's operating model

Rather than using a conventional botnet,⁷ the actor relies on the support of volunteers known as "heroes". The "heroes" install the DDoSia client (see below) – used to carry out the attacks – on their computers.

The "heroes" register via a Telegram bot. After registration, the Telegram bot sends a URL for downloading the DDoSia executables and a text file with a unique ID to identify the registered "hero".

The "heroes" can register with the Telegram bot using their ID number and a crypto wallet. The actor promises them a payout in cryptocurrency based on the number of attacks it carries out. The payment is set in relation to the total number of attacks carried out by all active volunteers on a given day.

A Telegram post by the actor from March 2023 describes the payout system as follows:

- RUB 80,000 for first place
- RUB 50,000 for second place
- RUB 20,000 for third place

Fourth to tenth places shared a budget of RUB 50,000.

Payments are made in cryptocurrencies such as Ethereum, Bitcoin or Tether. The "heroes" can access information about their overall statistics (top-ten list) on the DDoSia Telegram channel.

It remains unclear who sponsors these financial resources. Unlike other cyberactivists, the actor has not yet made any appeals for donations, e.g. via social media.

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

3.3 Technical description

At the start of the war in Ukraine, the NCSC noted an increase in DDoS activity using Bobik⁸ malware. The victims were unaware that their computers had been infected with the malware and were being used to carry out DDoS attacks. NoName057(16) has since changed its approach, asking the "heroes" publicly on social media to use a special DDoS client called DDoSia.

Switching from Bobik to this DDoS client significantly reduces the operational burden on the actor by eliminating the need for it to procure infected devices. Thus there are economic reasons for the change.

To perpetrate its DDoS attacks, the actor uses the DDoSia project,⁹ consisting of command-and-control (C2) servers and DDoSia clients. DDoSia was developed in September 2022 to allow the "heroes", via Telegram, to volunteer their computers and internet connections to carry out attacks.

Description of the DDoSia client

Continually upgraded, the DDoSia client is programmed in the Go programming language and can run on the Linux, Windows, macOS and Android platforms.

Its default user agent is Go-http-client/1.1 (written in Go). The HTTP user agent identifier Go-http-client/1.1 remained unchanged throughout the DDoS attacks. Unambiguous identification of the user agent made mitigation using WAFs easier by adjusting their configuration to block the agent.

No obfuscation of the DDoSia client IP address by means of spoofing¹⁰ was detected. Consequently, the "heroes" are potentially identifiable from their IP addresses. On its Telegram support channels, the actor recommends using virtual private networks (VPNs) to make such identification more difficult.

More detailed information about the DDoSia client, including reverse engineering, can be found on the blog of the security service provider Sekoia (see section 8,).

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

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

¹⁰ https://en.wikipedia.org/wiki/Spoofing_attack

Description of command-and-control communication

The following diagram shows the communication flow of the DDoSia clients with the command-and-control (C2) servers:¹¹

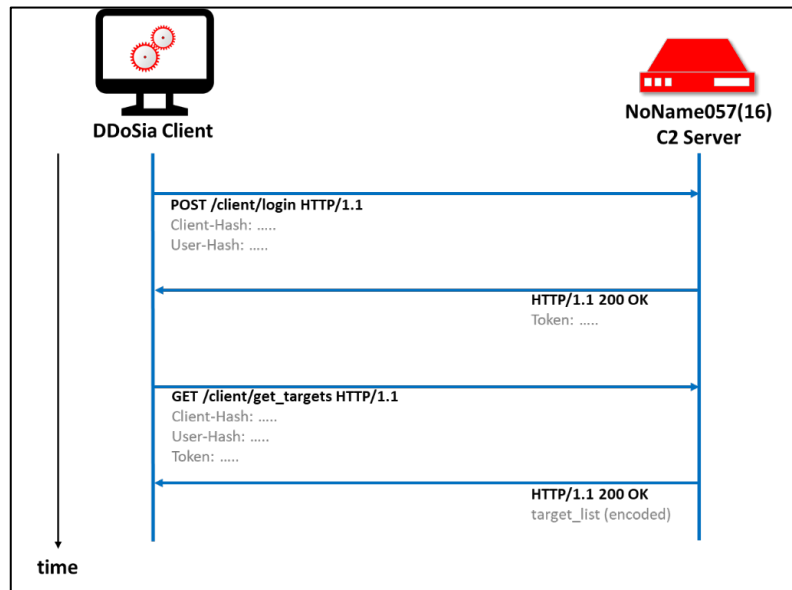


Figure 7: DDoSia-C2 communication

The communication between DDoSia clients and C2 servers is personalised by means of a user hash, which identifies the participant, and a client hash, which identifies the participant's computer. The user hash also serves to identify the respective user when making payments to the "heroes". Lastly, the DDoSia client receives the list of attack targets (`target_list (encoded)`).

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

Communication with the attack target

The DDoSia client generates the specific queries to the websites to be attacked based on instructions in the list of attack targets (retrieved from the C2 servers).

A template is used for this, supplemented by parameterised random character strings. When designing these templates and the randomly generated content, the actor takes particular care to ensure that the data traffic looks very similar to legitimate web queries in order to make automated detection of the DDoS attacks more difficult.

The diagram below shows how the DDoSia client imitates legitimate data traffic, thereby tricking protection mechanisms into not preventing the malicious traffic. As a result, this traffic usually cannot be automatically detected and blocked by protection mechanisms such as DDoS protection and firewalls:

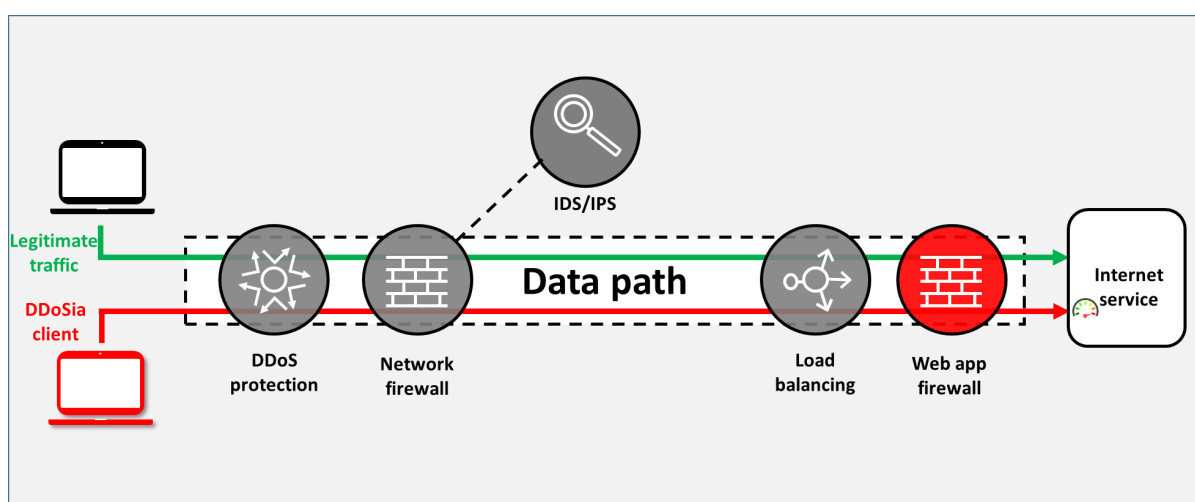


Figure 8: Malicious data traffic from the DDoSia client

The following examples show templates supplemented by parameterised random character strings:

Example 1:

- Template: "hxxp[s]://www.webseite.ch/de/search/?term=\$_1"
- \$_1 is a random string of 6 to 12 characters (e.g. here: kenuab)

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

Example 2:

- Template: "hxxp[s]://www.webseite.ch/de/register/?name=\$_1.\$_1@\$_2.ch"
- \$_1 is a random string of 6 to 8 characters consisting of lower-case letters, \$_2 is a random string of 10 to 12 characters consisting of lower-case letters (e.g. here \$1: goenza.leurebe and \$2 pahelsnwmni)

Accessed URL:

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

The DDoSia client thus continuously generates web queries that differ in terms of parameters and cause a processing load in the downstream ICT infrastructure (e.g. databases used in business processes). The queries are therefore difficult to distinguish from legitimate data traffic due to their dynamic structure.

Technical response to the DDoS attack (mitigation)

By analysing the attack patterns (e.g. by filtering the log files for the user agent of the DDoSia client), a list of IP addresses of the "heroes" involved can be compiled. Using this list, the malicious network traffic can already be blocked at the level of the internet router (edge router) of the organisation concerned, or at the level of the internet service provider (ISP) itself (e.g. by means of null routing¹²).

During the DDoS attacks examined here, Swiss ISPs blocked DDoS data traffic in their backbone by placing blocks on IP ranges and autonomous systems (ASs). These blocks were continually updated during the attacks and were based on the comprehensive sharing of information made possible by the NCSC.

As the security and operational processes (incident response management, change management and release management) require manual work (e.g. definition of blocking rules), a certain time lag between the detection and the mitigation of such DDoS attacks is inevitable. The latest experiences and statements suggest that a response time of around two hours is to be expected.

Given that the actor cannot always determine the protective measures implemented at the affected organisations, the attacks are likely to continue unabated – but without causing any further downtime.

Quantification

During the DDoS attacks on the Federal Administration, approximately 20,000 IP addresses were detected. Statistics on these attacks show that 3% of the IP addresses were within the Swiss IP address range.

The data traffic of the DDoS attacks was relatively low, averaging 20,000 to 25,000pps (packets per second) and less than 200Mbit/s (megabits per second). These metrics are typical for application-layer DDoS attacks.

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

4 How the attacks unfolded

The DDoS attacks on Switzerland started at 8am on Wednesday, 7 June 2023, with the website <https://www.parlament.ch> appearing as the first target in the C2 target list.

The reasons for this new target were:

- discussions in the Swiss Parliament about weapons exports¹³
- the 5 June announcement regarding President Volodymyr Zelenskyy's video message to the Swiss Parliament on 15 June 2023¹⁴

The actor's followers were informed via its Telegram channel:

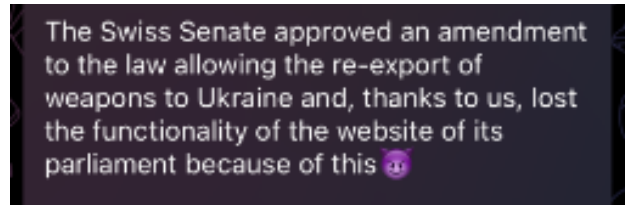


Figure 9: First message on the Telegram channel; source: Telegram

The announcement of President Zelenskyy's video message was also commented on in a Telegram message:

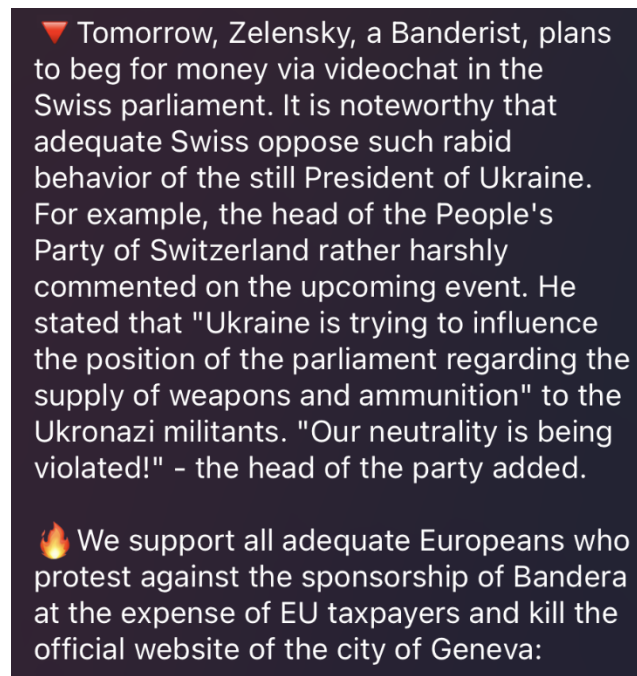


Figure 10: Second Telegram channel message; source: Telegram

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

Timeline of events

The DDoS attacks took place over a period of around two weeks. It is worth noting that the actor had previously launched attacks of a broadly similar scope (in terms of duration, technology used and nature of the attacks) on other countries and that such attacks are still ongoing.

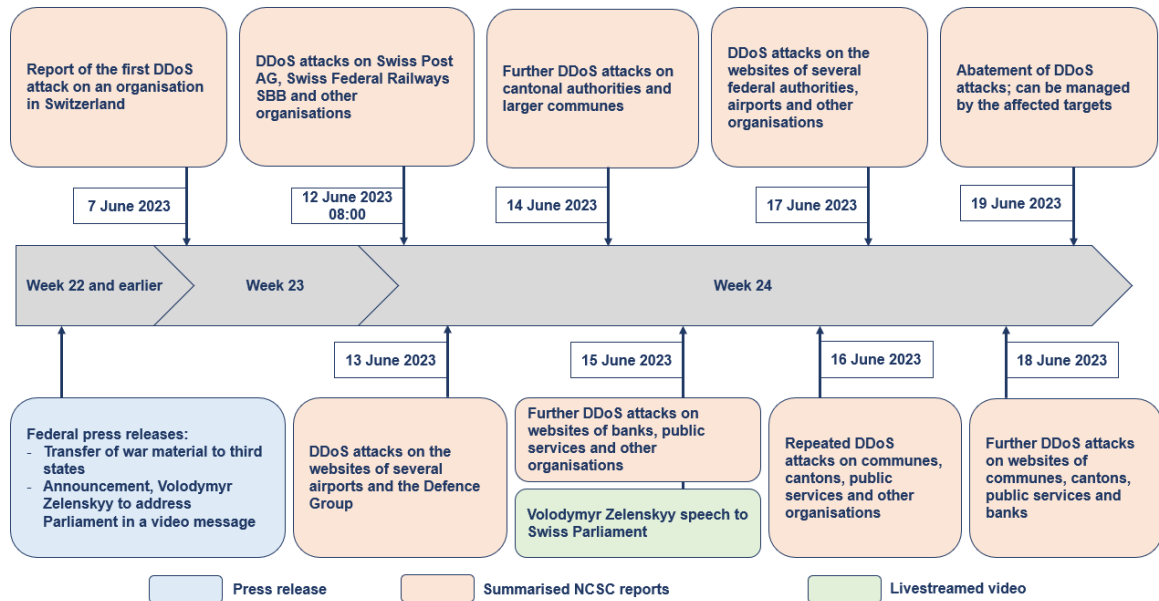


Figure 11: Timeline of events (summary)

The following table shows the successful DDoS attacks:

Targets	Date						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Federal Administration	4	1		1		2	
Cantons			2		3		
Cities			6				6
Public Service	2		1	1			1
Airports		8				6	
Financial sector				5		2	1
Other				1	3		
Defence Group				1			
Total 57	6	9	9	9	6	10	8

Table 3: Overview of successful DDoS attacks

It can be seen that there were around eight successful DDoS attacks per day on average. The websites of airports, financial sector organisations and city authorities were clearly the main targets. It is also evident that the focus was more on public authorities at the start of week 24, before switching to private-sector targets in the second half of the week.

Another table shows the attacks reported to the NCSC compared with the successful DDoS attacks reported by the actor (see Table 4: Reports to the NCSC compared with postings by the actor on Telegram):

Date	Sources	
	Attacks reported to the NCSC	DDoS attacks publicised as successful
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

Table 4: Reports to the NCSC compared with postings by the actor on Telegram

If we compare the total of 57 successful DDoS attacks according to Table 3: Overview of successful DDoS attacks(85 reports, see Table 4), there is clearly a discrepancy. This shows that some organisations and authorities were able to successfully mitigate the DDoS attacks or prevent noticeable outages.

The following table (see Table 5: List of websites attacked between 12 and 18 June 2023) supplements the timeline of events (websites are listed in chronological order of attack):

Date	Attacks on Swiss authorities and organisations reported to the NCSC	Comment
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 	On the first day of cyberattacks, public authorities and government-related organisations were the primary targets.
13.06.2023	<ul style="list-style-type: none"> • www.vtg.admin.ch • www.flughafen-zuerich.ch • www.gva.ch 	On the second day, the websites of the Defence Group (Armed Forces) within the Federal Department of Defence, Civil Protection and Sport (DDPS) and of various airports were attacked.
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 	On the third day, the actor focused mainly on city authorities.

Date	Attacks on Swiss authorities and organisations reported to the NCSC	Comment
	<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 	The fourth day of the wave saw more attacks on public authorities and 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 	On the fifth day, the actor primarily targeted public authorities in the canton of Nidwalden.
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 	On the sixth day, federal authorities were back in the line of fire.
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 	The last day of the wave saw further attacks on city authorities.

Table 5: List of websites attacked between 12 and 18 June 2023

5 Impact of the attacks

The posts on the actor's Russian-language Telegram channel were each read by around 5,500 participants and those on the English-language Telegram channel by around 1,000 to 1,500 participants. Compared with the media coverage in Switzerland (see section 5.1), the actor's reports of successful attacks were not widely relayed on social media channels such as Twitter during the period of the attacks.

Due to the nature of the attacks (target-specific, application-layer), websites that could not be secured by blocking entire address ranges (based on source IP addresses or the blocking of ASs¹⁵) were particularly at risk (e.g. government portals that need to be accessed by Swiss nationals living abroad). The reason for this is that the configuration of WAFs first has to be adapted to the specific attack. Until this has taken place, the target remains exposed. The NCSC estimates that such configuration adjustments require around two hours of work. The processes used (e.g. analysis, staging, rollout) are based on the security and operational processes of the respective organisation (incident response management, change management and release management) or the terms of the relevant service level agreement in the case of outsourced managed security services (process and response time).

For example, Basel Stadt's eKonto portal was overloaded by massive simultaneous login attempts on Wednesday, 14 June 2023. The canton of Nidwalden's eTax login was overwhelmed in the same way on Friday, 16 June. Following adjustments to the protective measures, the attacked websites were quickly accessible again from within Switzerland.

The actual damage incurred by the targets consisted of reputational damage and the effort and expense required to mitigate the DDoS attacks.

Many of the companies affected have subsequently reviewed their risk management and, in some cases, stepped up the involvement of their ISP¹⁶ in their internal protective measures (e.g. by subscribing to a DDoS protection mechanism).

5.1 Media impact

On 5 June 2023, the Swiss Parliament announced that Ukraine's President Volodymyr Zelenskyy would be addressing its members on 15 June. This announcement, together with the parliamentary decision to allow the transfer of war materiel, triggered the start of DDoS activities by NoName057(16). Parliament's website (parlament.ch) was one of the first to be attacked, as announced by Parliamentary Services on Twitter at 3.05pm on 7 June 2023. When other Federal Administration websites went down on Monday, 12 June 2023, the NCSC issued a press release about the DDoS attacks. This information was widely reported in the Swiss media, with the NCSC counting around 50 articles in the print media and over 370 online articles.

As a result of the coverage in the Swiss media, the DDoS attacks and their underlying political message increasingly came to the attention of the country's population at large. However, this led to uncertainty and questions among the public. In total, the NCSC press office received over 40 media enquiries. Federal Cybersecurity Delegate Florian Schütz was in the public spotlight in this period, giving interviews to various media organisations in which he explained DDoS in order to minimise the uncertainty among the population.

The intense media coverage tailed off after President Zelenskyy's speech on 15 June 2023,

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

¹⁶ https://en.wikipedia.org/wiki/Internet_service_provider

and by the time the DDoS attacks ended on 19 June 2023, there was almost no further mention of them.

Some media reporting lumped the attacks together with an unrelated ransomware attack on the company Xplain, which was publicised at the same time. The NCSC always stressed in its media activities that the attacks were the work of different groups. For example, the group Play was behind the attack on Xplain (one of the Federal Administration's IT suppliers), and the group NoName claimed responsibility for the DDoS attack on the Parliamentary Services website on Telegram. It also emphasised that the motives of the actors behind a ransomware attack (Xplain) and a politically motivated DDoS attack are fundamentally different.

5.2 Political impact

The DDoS attacks themselves did not elicit a strong reaction in the Federal Assembly. The President of the National Council, Martin Candinas, and the President of the Council of States, Brigitte Häberli-Koller, mentioned the attacks in their respective chambers.

On 15 June 2023, National Councillor Doris Fiala submitted a parliamentary procedural request (Ip. 23.3755 "Are we already at cyberwar, including in the Confederation?").¹⁷ In its response, the Federal Council emphasised that the DDoS attacks were to be classified as an act of vandalism and had caused only minor damage. As such, they should be clearly distinguished from serious cases. The Federal Council also explicitly warned against describing these attacks as "cyberwarfare". Such a label "exaggerates the threat they pose and so furthers the attackers' objective of spreading uncertainty".¹⁸

It can be assumed that Parliament will continue to take an active interest in the Confederation's action on cyberattacks in general and, in the aftermath of the recent attacks, specifically on protection against DDoS attacks. No further political impact from the attacks is expected.

5.3 Legal impact

The Office of the Attorney General of Switzerland has initiated proceedings in relation to the DDoS attack on the website of the Swiss Parliament.¹⁹ For the legal impact, the NCSC refers to the ongoing proceedings.

5.4 Actual damage

The NCSC conducted a survey of affected companies following the DDoS attacks. According to the feedback received, the greatest damage was customer dissatisfaction due to the targeted websites being temporarily unavailable. Most of these outages lasted a few hours, but in one case services were down for as long as three days, accompanied by instability. Any monetary damage cannot be further quantified. The respondents confirmed that there was no lasting damage to ICT infrastructure.

The authorities and organisations concerned did not have to deploy additional human resources to counter the DDoS attacks, although staff did work additional hours.

The NCSC is not aware of any organisation (e.g. an SME) being forced out of business as a

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

¹⁸ <https://www.parlament.ch/de/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>

result of the DDoS attacks.

The DDoS attacks confirmed that such incidents can hit any target and disrupt its operations, at least in the short term. The NCSC therefore recommends maintaining proactive protection (see protective measures in section 6).

6 Recommendations

Compared with complex attacks (e.g. advanced persistent threats) that aim to penetrate computer systems, DDoS attacks represent a lower level of technical complexity. The challenges in protecting against DDoS attacks lie in the scalability of the attacks and the development of new techniques to bypass DDoS protection mechanisms. Consequently, robust security measures and a proactive approach are crucial to protect against the impact of DDoS attacks.

Below, the NCSC sets out various recommendations that can be implemented in the form of proactive measures to protect against DDoS attacks or as reactive measures in the wake of such attacks.

Proactive measures

The following measures (not exhaustive) should be implemented as required to prepare for a potential DDoS attack:

Proactive measures	Description/purpose	Impact in the context of these DDoS attacks
Assess the relevance of DDoS attacks in your IT risk management and IT service continuity management.	DDoS attacks are assessed for relevance in the IT risk management process and, if necessary, included as a risk.	To counter this risk, appropriate technical and organisational measures are implemented before the attack.
Identify which of your websites are potentially at risk by means of a business impact analysis (BIA).	A BIA pinpoints the requirements for website availability.	Business-critical websites are known and can be protected in line with business requirements.
Consult your ISP or managed security service provider (MSSP) about protective measures to ensure availability.	Measures to ensure compliance with website availability requirements are agreed with the relevant service provider and checked periodically to ensure that they are up to date.	The protective measures are contractually agreed and are available in the event of a potential attack.
Incorporate protective measures against DDoS attacks into your security architecture (security by design).	Measures to protect against DDoS attacks are already implemented at the website design stage. For example, a content delivery network (CDN) can help mitigate the impact of DDoS attacks by distributing traffic across a variety of servers worldwide.	Incorporating security requirements into the security architecture minimises the likelihood of DDoS traffic reaching and overloading websites.
Use a web application firewall (WAF) for websites that are potentially at risk.	WAFs monitor traffic at the application level and block malicious requests before they can reach the website.	Only the presence of a WAF can quickly protect websites against DDoS attacks. The configuration of WAFs can be adjusted to deal with the specific DDoS attack.

Proactive measures	Description/purpose	Impact in the context of these DDoS attacks
Develop and test a contingency plan.	A contingency plan provides structured instructions in the event of a DDoS attack. It includes IT service continuity management and business continuity management (BCM).	A contingency plan allows a planned and structured response to the DDoS attack.

Table 6: Proactive measures

Reactive measures

The NCSC recommends implementing the following measures as appropriate to respond to a potential DDoS attack:

Measures in response to DDoS attacks	Description/Purpose	Impact in the context of these DDoS attacks
Monitor exposed websites and set up automated anomaly detection.	Monitoring data traffic helps to detect unusual patterns or increased network traffic.	This measure supports the early detection of and defence against DDoS attacks.
Ensure that you can react swiftly to DDoS attacks, both technically and organisationally.	Technical protective measures primarily serve to detect and defend against DDoS attacks. The security processes cover organisational aspects (e.g. security incident management, escalation, media relations).	DDoS attacks can be mitigated promptly by the rapid implementation of protective measures (e.g. blocking of IP addresses, configuration adjustments to security mechanisms by the on-call service).
Make sure that your websites are protected against automated attacks upstream in the security architecture (defence in depth).	Implementation of CAPTCHA ²⁰ technologies can ensure that a website form cannot be filled out automatically, for example.	Upstream protective measures prevent the automated DDoS attack from reaching the websites.
Block IP ranges and autonomous systems (ASs) based on indicators of compromise (IOCs).	Such blocks are based on the IOCs available at the NCSC's Cybersecurity Hub. The above-mentioned anomaly detection allows the IOCs to be identified on an organisation-by-organisation basis.	Malicious traffic can thus be prevented.
Block specific application-layer attacks.	Based on information from multiple sources (e.g. security incident and event management (SIEM) and various log files), the security mechanisms (e.g. WAF) can be specifically	By blocking the DDoS client (user agent), the DDoS attack can be repelled at WAF level.

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

Measures in response to DDoS attacks	Description/Purpose	Impact in the context of these DDoS attacks
	adjusted to defend against the attack.	

Table 7: Measures in response to DDoS attacks

Further preventive measures and recommendations for action are published on the NCSC's website (see section 8, [3]).

7 Conclusion

Conventional anti-DDoS security strategies, which are traditionally geared more towards volumetric DDoS attacks,²¹ are not sufficient to protect against the application-layer attacks perpetrated by NoName057(16).

In the case at hand, the attacking systems deployed by the cyberactivists were mostly identifiable from IP ranges and autonomous systems (ASs) and could therefore largely be blocked in a targeted way. This ensured that the attacked websites were available again relatively quickly. An important additional security mechanism was provided by web application firewalls (WAFs), which, where available, could be specifically reconfigured to the attack pattern.

If the cyberactivists participating in a future DDoS attack are even more geographically widespread, the extent of the damage can be expected to be greater. It will be harder to identify and block all IP ranges and/or ASs, and therefore more prolonged disruptions to the attacked websites are to be expected in such a scenario.

Lessons learned

From the NCSC's perspective, the following lessons learned are worth noting:

- Despite widespread implementation of DDoS security mechanisms, the actor was able to perpetrate attacks successfully, at least to some extent and over a certain period. Consequently, security measures need to be reviewed and adapted as appropriate.
- DDoS attacks can also affect the business of third parties if a website that is needed for the correct functioning of another website or business process is successfully attacked. A business impact analysis (BIA) serves as the basis for identifying such dependencies and taking them into account in business continuity management (BCM).
- The impact of (e.g. IP range) blocks on the business activity of the company concerned (e.g. impaired access for legitimate users, legally regulated websites) needs to be examined within the scope of a BIA.
- The NCSC's coordination and detailed information sharing with the affected parties was very important.
- Before attack-specific information is disseminated (e.g. the actor's name), all of the pros and cons must be considered.
- The impact of a DDoS attack can be minimised relatively quickly using common security mechanisms (e.g. IP range blocking, geoblocking, WAFs, rate limiting) as soon as the attack patterns are known in sufficient depth.
- Where trust relationships can be established between isolated networks communicating via the internet, newer technologies such as SCION²² can also be used. SCION technology has built-in protection against DDoS attacks.
- The extensive media coverage has led to increased awareness of the issue of DDoS among Swiss authorities and organisations.
- Responses to the NCSC survey suggest that the affected companies will reassess their risk of DDoS attacks and review the relevant measures.

Closing remarks

Larger organisations, such as those with a security operations centre (SOC), were able to respond relatively quickly as soon as the attack patterns were known. Whether technical issues or a lack of security processes led to some more prolonged disruptions (e.g. website outages

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

²² <https://scion-architecture.net/>

lasting several days) can no longer be conclusively determined retrospectively.

The companies concerned are responsible for making the necessary adjustments as part of the continuous improvement process. The NCSC suggests that the measures recommended in this report and the lessons learned be examined and implemented as appropriate, on organisations' own responsibility.

8 Appendices

Information and explanations about DDoS attacks

The NCSC provides general information and explanations about DDoS attacks on its website.²³

The different types of DDoS attacks (e.g. volumetric attacks, layer 7 attacks) are explained in detail in a document by the Multi-State Information Sharing and Analysis Center (MS-ISAC),²⁴ in cooperation with the US Cybersecurity & Infrastructure Security Agency CISA²⁵ and the Center for Internet Security CIS²⁶).

Referenced information sources

Number	Explanation and URL
[1]	President Zelenskyy to address Swiss parliamentarians on 15 June (link in German), https://www.parlament.ch/press-releases/Pages/mm-info-2023-05-31.aspx
[2]	Council of States wants to make it easier to transfer Swiss war materiel (link in German), https://www.parlament.ch/de/services/news/Seiten/2023/20230607124254254194158159038_bsd093.aspx
[3]	NCSC recommendations for countering DDoS attacks, https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ddos.html
[4]	Sekoia – More detailed information about the DDoSia client, https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

Table 8: Referenced information sources

Categorisation of actors and their motivations

To assess the impact of cyberattacks, it is first important to determine which threat actors are carrying out the attacks. Threat actors can be divided into the following categories based on their motivations:

Threat actors	Motivations
State actors	State actors (or nation-state actors) usually have geopolitical objectives. They tend to attack systemically important infrastructures of the opposing party, with a view to destabilising and annexing that party.
Criminal organisations	Criminal organisations generally have financial motives. Their fraudulent activities are aimed at gaining control over their victims in order to extort ransom payments.
Hacktivists	Hacktivists want to generate attention and spread their political or religious views. Through targeted vandalism and information operations (Info Ops) ²⁷ they seek to destabilise their victims and win them over to their ideology. Their goal is to gain public attention for their beliefs.

²³ <https://www.ncsc.admin.ch/ncsc/en/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 [Informationsoperationen: Trends und Kontroversen \(ethz.ch\)](https://www.ethz.ch/informationsoperationen-trends-und-kontroversen)

Terrorist groups	Terrorist groups aim to spread fear and terror.
Thrill seekers/script kiddies	Thrill seekers, including "script kiddies", want to make themselves feel powerful for their own personal satisfaction or to seek confirmation of their prowess. They are also often concerned with gaining recognition in certain circles.
Insiders	Insiders (as opposed to outsiders) are actors who have privileged access to the victim (e.g. employees, agents). They exploit this access to cause harm or to enrich themselves illegitimately.

Table 9: Categorisation of threat actors and their motivations

Details of DDoS attacks day by day

Report date	Title	Description	Comments
12.06.2023	NoName057(16) DDoS attacks of 12.06.2023 on Swiss websites, including Federal Administration	<p>At 08:20 on Monday, 12.06.2023, DDoS attacks were carried out by NoName057(16) on Federal Administration websites (FOCBS and FDJP). The list of websites targeted was posted a few minutes later and included the following:</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>At 10:03, NoName057(16) claimed responsibility on its Telegram channel for the attacks targeting Switzerland, indicating the Parliament website [1] with a Check-Host.net report of 12.06.2023 at 09:28 (UTC: 07:28) [2]. The report stated that the connection worked only from Switzerland (DDoS protection via geofencing). NoName057(16) said its action was motivated by Zelenskyy thanking Switzerland for agreeing to the 10th package of sanctions against Russia, which Switzerland announced on 29.03.2023.</p> <p>[1] www.parlament.ch [2] https://check-host.net/check-</p>	<ul style="list-style-type: none"> • Type of attack: layer 7 attacks (HTTP POST and GET flood). • Origin of DDoS attack traffic: traffic originating from Russian IP space and MIRhosting (AS206932, AS52000) as well as Stark Industries (AS44477). • Other recommendations: mitigation can also include searching for anomalies in the HTTP Header, as well as protecting resource-intensive functions using a captcha. <p>NoName057(16) claimed responsibility on its Telegram channel for the attacks on the FDJP (11:23), the FOCBS (12:35), fedpol (13:47), the FDHA (15:00), SOB (16:04) and Swiss Post (17:11). The Check-Host reports [3] were produced at around 09:30 (UTC: 07:31), with the exception of the Swiss Post report, which was produced at around 13:47 (UTC 11:47).</p> <p>[3] https://check-host.net/check-report/103a5159k82c https://check-host.net/check-report/103a4fdakb51</p>

Report date	Title	Description	Comments
		report/103a4c6aka29	https://check-host.net/check-report/103a4edck891 https://check-host.net/check-report/103a53afk272 https://check-host.net/check-report/103a523fk4ec https://check-host.net/check-report/103af460ka6b
13.06.2023	NoName057(16) DDoS attacks of 13.06.2023 on Swiss websites, including Federal Administration	<p>At 09:20 on Tuesday, 13.06.2023, a new list of targets was used by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</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>This list was updated at 11:10, and the following targets were added:</p> <ul style="list-style-type: none"> • www.swisshelicopter.ch • zimex.com • www.pc7-team.ch 	<p>NoName057(16) claimed responsibility on its Telegram channel for the attacks on vtg.admin.ch (10:03), bernairport.ch (11:12), airportgrenchen.ch (12:27), gva.ch (13:34), engadin-airport.ch (14:47), peoples.ch (St Galler aerodrome; 15:58), www.swisshelicopter.ch (16:19), zimex.com (17:27), www.pc7-team.ch (18:01).</p> <p>The Check-Host reports [1] were produced at around 09:30 (UTC 07:30), with the exception of those concerning www.swisshelicopter.ch, zimex.com and www.pc7-team.ch, which were produced at around 11:10 (UTC 09:10).</p> <p>An analysis of NoName057(16)'s Telegram channel revealed that comments posted by followers in the wake of the attacks on 12.06.2023 concerned Switzerland, increasing the likelihood of the organisations cited being the target of future attacks:</p> <p>The cantons in question were notified of these comments (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</p>

Report date	Title	Description	Comments
			https://check-host.net/check-report/103d8603k4c6 https://check-host.net/check-report/103d86f8kbb2 https://check-host.net/check-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	NoName057(16) DDoS attacks of 14.06.2023 on Swiss websites	<p>At 08:00 on Wednesday, 14.06.2023, a new list of targets was used by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</p> <ul style="list-style-type: none"> • www.geneve.com <p>This list was updated at 08:20, and the following targets were added:</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>And again at 11:15, when the following targets were added:</p> <ul style="list-style-type: none"> • www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch <p>It should be noted that the website www.geneve.com is the Geneva tourism website and not the official website of the city/Republic of Geneva, which is www.ge.ch.</p>	<p>NoName057(16) claimed responsibility on its Telegram channel for the attacks on 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) and www.bellinzona.ch (16:02). The Check-Host reports [1] were produced at around 09:30 (UTC: 07:30), with the exception of those concerning www.stadt-schaffhausen.ch, www.lausanne.ch, www.montreux.ch, www.stadt.sg.ch and www.bellinzona.ch, which were produced at around 10:50 (UTC: 08:50).</p> <p>In its publication concerning the attack on www.geneve.com, NoName057(16) mentioned President Zelenskyy's videoconference address to the Federal Assembly scheduled for 15.06.2023.</p> <p>[1] https://check-host.net/check-report/1040acf6k148 https://check-host.net/check-report/1040e8e8k532</p>

Report date	Title	Description	Comments
			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-report/1040e788k29 https://check-host.net/check-report/1040e84ck7ed
15.06.2023	NoName057(16) DDoS attacks of 15.06.2023 on Swiss websites	<p>At 08:00 on Thursday, 15.06.2023, a new list of targets was used by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</p> <ul style="list-style-type: none"> • ncsd.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>NoName057(16) claimed responsibility on its Telegram channel for the attacks on 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>The Check-Host reports [1] were produced at around 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/10440aadh1ad https://check-host.net/check-report/10440b9ak78e https://check-host.net/check-report/10440c2fkb4c</p>
16.06.2023	NoName057(16) DDoS attacks of	At 09:20 on Friday, 16.06.2023, a new list of targets was used	NoName057(16) claimed responsibility on its Telegram

Report date	Title	Description	Comments
	16.06.2023 on Swiss websites	<p>by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</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 • www.zentralbahn.ch • www.lakelucerne.ch <p>Another website was added to the list at 10:00:</p> <ul style="list-style-type: none"> • www.vsz.ch 	<p>channel for the attacks on 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>The website www.autofaehre.ch was not on the list of targets attacked by NoName057(16)'s BotNet and the site was accessible at 15:00. This was probably a communication error by NoName057(16). The Check-Host reports were produced at around 09:15 (UTC 07:15).</p>
18.06.2023	NoName057(16) DDoS attacks of 17.-18.06.2023 on Swiss websites	<p>At 09:20 on Saturday, 17.06.2023, a new list of targets was used by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</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>Another website was added to the list at 10:30:</p> <ul style="list-style-type: none"> • www.edi.admin.ch <p>Further websites were added to the list at 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>At 10:45 on Sunday, 18.06.2023, a new list of targets was used by NoName057(16) for DDoS attacks.</p> <p>The list was as follows:</p>	<p>The vast majority of the sites targeted on Saturday and Sunday had already been targeted during the preceding week.</p> <p>On Saturday, 17.06.2023, NoName057(16) claimed responsibility on its Telegram channel for the attacks on 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) and www.pc7-team.ch (19:47).</p> <p>The Check-Host reports were produced at around 09:30-10:00 (UTC 07:30-08:00), with the exception of those concerning gva.ch, vtg.admin.ch, www.swissprivatebankers.com, www.swisshelicopter.ch, www.zimex.com and www.pc7-team.ch, which were produced at around 14:00 (UTC 12:00).</p> <p>On Sunday, 18.06.2023,</p>

Report date	Title	Description	Comments
		<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>Further websites were added to the list at 15:15:</p> <ul style="list-style-type: none"> • www.juliusbaer.com • sasd.ch • www.swissprivatebankers.com • www.zvv.ch • www.myswitzerland.com 	<p>NoName057(16) claimed responsibility on its Telegram channel for the attacks on 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) and www.zvv.ch (18:34).</p> <p>The Check-Host reports were produced at around 09:30-10:00 (UTC 07:30-08:00), with the exception of those concerning www.swissprivatebankers.com and www.zvv.ch, which were produced at around 14:30 (12:30 UTC).</p>

Table 10: Daily DDoS reports between 12 and 18 June 2023, with additional information