Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC CTI Report

Overview of hacktivist threats to Dutch organisations

Publication date: 9-10-2023 (Dutch version), 13-10-2023 (English translation)

TLP:GREEN

Authorised distribution for TLP:GREEN
(Traffic Light Protocol)

This NCSC CTI Report, which has been issued by the NCSC, bears the label TLP:GREEN. The NCSC uses the Traffic Light Protocol (TLP) to define clearly and unambiguously what may be done with the information it provides. A TLP designation associated with any kind of information tells you with whom you are allowed to share it. This is explained in the FIRST standard (www.first.org/tlp).

Your input is welcome at info@ncsc.nl.

Contents

Contents 2

Essence 3

Hacktivist groups 4

Hacktivist motivation 6

Digital attacks by hacktivists 8

Prognosis 11

Perspective for action 13

References 15

NCSC CTI Report

The NCSC CTI Report is a new product produced by the National Cyber Security Centre (NCSC) to provide more in-depth information on a current cyber threat that requires additional context, interpretation and perspective for action.

If you have any questions and/or comments regarding this product, or perhaps found it particularly useful, please get in touch with the NCSC through your point of contact or send us an email at info@ncsc.nl. We value your feedback!

Essence

- **In 2023, pro-Russian hacktivists targeted many Dutch organisations with DDoS attacks**. Other types of hacktivists, such as TurkHackTeam, also engaged in DDoS attacks on Dutch organisations.
- **We see fewer instances of other digital attacks by hacktivist groups, such as defacement and hack-and-leak operations, in the Netherlands.**
- **Most hacktivist attacks are not of an advanced level. Such digital attacks generally have a limited impact.**
- **Hacktivists undertake digital attacks for different reasons**. In this analysis, the NCSC discusses eight different hacktivists and their digital attacks.
- **In this publication, the NCSC identifies triggering events for different forms of hacktivism.** These are political or social events that may lead to a hacktivist response.
- **Upcoming events may serve as triggers for digital attacks by hacktivists**. Examples are the parliamentary elections in November 2023 and the 2025 NATO summit in the Netherlands.

Hacktivist groups

In 2023, Dutch organisations were targeted by digital attacks executed by hacktivist groups. In this publication, the NCSC describes different types of hacktivists and their digital attacks, as well as their claimed reasons for such attacks.

Hacktivist attacks usually have a **limited and symbolic impact**. Hacktivist groups generally use strong rhetoric to demand attention for their digital attack and social or political cause. Often, they spread their messages via social media.

- Most hacktivist attacks are not at an advanced level and are therefore mitigated successfully.
- In some cases, a digital attack by a hacktivist actor has a greater impact, for instance when they gain unauthorised access to very sensitive data and decide to publish it online.
- Also, a more advanced DDoS attack can have a serious impact if your organisation depends heavily on online services and inadequate mitigating measures have been implemented.

A great deal of attention for DDoS attacks, too little attention for other types of attack

Since early 2023, hacktivists have targeted many Dutch organisations through DDoS attacks. The media have reported extensively on these attacks, but other types of digital attack by hacktivists have received much less attention from the media. Examples are hack-and-leak operations and defacements.

- These other types of digital attack have been detected to a limited extent in the Netherlands. However, there are many instances of incidents in other countries in which hacktivists defaced a website or social media account or leaked confidential information.

Fluctuating composition of hacktivist groups

Hacktivists are often driven by political or social ideas. In some cases, they have an ad-hoc composition with changing members. Such a changing composition opens up opportunities for investigators.

- Hacktivist groups often use social media channels to coordinate digital attacks. On the other hand, many hacktivist groups have a hard core that remains associated with the group for a longer period of time and is responsible for coordinating digital attacks, for instance.

  The hacktivist group Killnet used Telegram channels to keep in contact with its supporters. These Telegram channels have tens of thousands of participants, not all of them hacktivists as cybersecurity investigators and journalists also follow these groups.

- Hacktivists may operate independently but states may also tolerate, support or even control (or partially control) hacktivist groups that execute digital attacks.[1]

The authenticity of hacktivist groups is often difficult to verify

Sometimes doubts arise as to the authenticity of a hacktivist group. Exercise restraint in trusting claims and statements made by entities who say they speak on behalf of a hacktivist group. Anonymous Sudan is an example of a hacktivist group that has been subjected to doubt regarding its authenticity.

- Early in 2023, Anonymous Sudan displayed behaviour that differed significantly from that of the group that operated under the same name in 2019. In that year, Anonymous Sudan periodically executed digital attacks in response to the ongoing political and economic situation in Sudan.[2] The group's activist operations focused heavily on social themes in this period, such as censorship and limitations to freedom of expression in Sudan.
- In 2023, Anonymous Sudan advocates a strong pro-Russian narrative in frequent DDoS attacks on organisations in nations that support Ukraine in its resistance against Russian occupying forces. This significantly changed behaviour and motivation gives rise to questions about the group's origin and authenticity. Moreover, the hacktivist group Anonymous denies having ties with Anonymous Sudan via its Telegram channel.[3]
- Groups like Anonymous are not homogeneous entities. Anonymous does not have formal leadership; it operates as a decentralised network of individuals. This hampers internal cohesion. There is also the risk of a third party hijacking the actor's name.

Hacktivist motivation

Hacktivist groups execute digital attacks for different reasons. To illustrate the diversity of hacktivist groups, we will describe eight different hacktivist groups relevant to Dutch organisations in greater detail.

These groups were selected on the basis of their attacks as detected, the impact of their digital attacks and the diversity of their motives. As such, the eight groups are illustrative of the hacktivist threat landscape in the Netherlands, but this does not constitute a total overview of all hacktivist groups that are active in the Netherlands. There are many more.

Hacktivism in relation to the war in Ukraine

An international conflict such as rising tensions in Europe following the Russian invasion of Ukraine may lead to hacktivist reactions.

- **Killnet** is an actor that recently executed countless digital attacks on organisations in countries that support Ukraine in its resistance against Russian occupying forces. Since 2023, Killnet has also executed DDoS attacks on Dutch organisations. An example would be the attacks on Dutch healthcare institutions in January 2023.[4]
- **NoName057(16)** is a hacktivist actor that, like Killnet, attacks organisations in countries that support Ukraine in its battle against the Russian occupation. NoName057(16) has been attacking Dutch organisations via DDoS attacks since 2023, often using the DDosia botnet.[5]
- **Anonymous Sudan** is an actor that has been active for several years now and is frequently associated with Killnet today.[6] In the past, this actor focused on influencing internal political affairs in Sudan. Recently, Anonymous Sudan has mainly adhered to a pro-Russian narrative in its digital attacks. The hacktivist actor Anonymous denies being associated with Anonymous Sudan.

Hacktivism after events considered injurious by an ideological or religious movement

Digital attacks can also be a response to developments or events that are considered injurious by ideological or religious movements.

- **TurkHackTeam** is a hacktivist movement that undertakes digital attacks in response to events with a political and religious background. For instance, TurkHackTeam executed digital attacks on Dutch organisations in 2017 following rising international tension concerning a Turkish referendum, amongst other things by targeting Dutch websites with defacement operations.[7]

  TurkHackTeam also initiated a digital campaign after the Quran was burned (Sweden, Denmark) and torn up (the Netherlands) early in 2023. A large number of hacktivist groups joined this campaign.

- **Mysterious Team Bangladesh** performs both DDoS and defacement attacks. The group has been operating internationally since 2020, primarily targeting India and Israel. [8]

  Early in 2023, Mysterious Team Bangladesh also undertook DDoS attacks on Dutch organisations in response to TurkHackTeam's aforementioned call for support in reaction to protesters tearing a Quran.[9] These attacks impacted several Dutch domains. A few weeks later, Mysterious Team Bangladesh's attention switched back to targets in other countries.

Other motives of hacktivist groups

Some hacktivists act as judge, jury and executioner where it concerns social themes, for instance **GhostSec** and **Anonymous**.

- **Anonymous** was recently involved in digital attacks on Iranian government institutions in response to surveillance operations[10] and growing censorship by the Iranian authorities.[11] Other recent themes were the Russian invasion of Ukraine [12] and abortion regulations in the US.[13]
- **GhostSec** takes part in a range of hacktivist campaigns, including one against the Iranian regime (OpIran) and one from a pro-Palestinian perspective against Israel (OpIsrael), the latter involving attacks against Israeli organisations in response to Israeli policy regarding Palestinian territories.[14]

  What is notable about GhostSec is that these hacktivists often claim that they have access to OT systems, although these claims are hard to verify. Earlier on, groups like Anonymous and GhostSec were also very active in response to the terrorist attack on Charlie Hebdo in Paris in 2015.[15]

Digital attacks by hacktivists

Hacktivists execute digital attacks to achieve a political or social objective. They generally rely on four different types of digital attack.

Activity 1: DDoS attacks

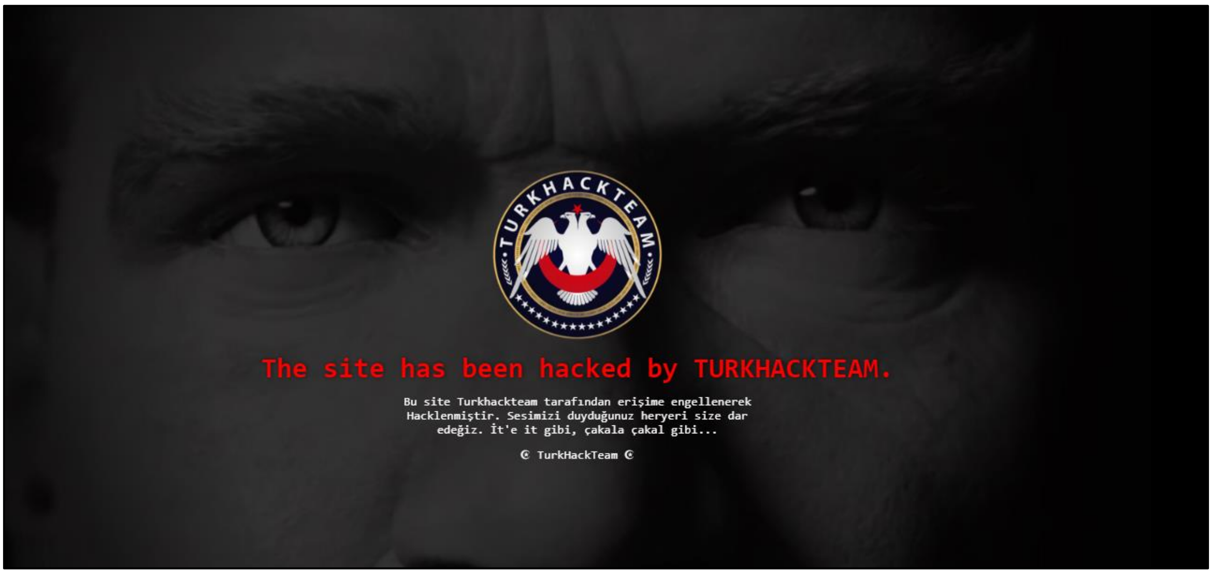
Hacktivists deploy DDoS attacks to achieve political (or other) objectives.[16] Such attacks are often undertaken in response to social or political developments. A DDoS attack has a temporary impact on the availability of a system connected to the internet, such as a website.

- DDoS attacks are relatively simple in execution. Systems that are connected to the internet can be targeted by DDoS attacks. Attackers do not have to gain access to the system.
- Hacktivists often use a large number of sympathisers that make a voluntary contribution to a botnet, thus supplying capacity for digital attacks. In the case of NoName057(16) and the DDosia botnet, sympathisers can download a tool via GitHub to make their system available for DDoS attacks.[17]

Activity 2: Defacement

In addition to DDoS attacks, some hacktivist groups also execute defacement attacks. This involves an attacker gaining unauthorised access to a digital media, such as a website or social media account.

- The attacker then uses this media to distribute activist texts, which are usually inflammatory, distressing and/or provocative. It is a way for the attacker to attempt damaging the victim’s reputation and cause upheaval amongst visitors of the targeted website.
- As such, defacement attacks enhance the fame of the hacktivist actor and their political or social cause, making them a common type of attack by hacktivists.
- The NCSC detected a manifestation of the event-source-polyfill protestware in the Netherlands in September 2023, a type of malicious code rolled out via a third-party software library that is used by multiple organisations. As a result, visitors from Russia were shown messages criticising the Russian invasion of Ukraine. This protestware was also detected abroad in the past.[18]



The site has been hacked by TURKHACKTEAM.

Bu site Turkhackteam tarafından erişime engellenerek
Hacklenmiştir. Sesimizi duyduğunuz heryeri size dar
edeğiz. İt'e it gibi, çakala çakal gibi...

☪ TurkHackTeam ☪

Illustration 1: TurkHackTeam uses standard templates such as shown above. These are offered to group members to execute defacements.[19]

Activity 3: Hack-and-leak

Hack-and-leak operations aim to publish confidential information that was obtained illegally in order to damage the victim's reputation. Hacktivists may threaten to leak confidential data aiming to force the victim to make different choices.

- Hack-and-leak attacks can have a major impact. In addition to threatening data confidentiality, they may also threaten data integrity. This makes it difficult to establish the integrity of the leaked data. For instance, a malicious party may intentionally add incorrect information to a stolen dataset before leaking it.

Activity 4: OT attacks

Sometimes, hacktivists claim that they have attacked operational technology (OT).[20] A digital attack on operational technology may cause significant disruptions since it is used to control operational processes in the physical world, including controlling and monitoring machinery.[21]

- The NCSC observes rising hacktivist claims concerning OT in other countries. For now, they seem to have limited impact and the outcomes of the attacks appears uncertain. Claims are often difficult to verify, mainly serving a symbolic purpose. Moreover, few actors possess the actual knowledge and capacity to have a deliberate effect.[22]

		Activity type			
		DDoS	Defacement	Hack-and-leak	OT attacks
Group	Killnet	🟥	🟨	🟨	
	NoName057(16)	🟥	🟨		
	Anonymous Sudan	🟥	🟨	🟥	
	TurkHackTeam	🟥	🟥	🟨	
	Mysterious Team Bangladesh	🟥	🟨	🟨	
	GhostSec	🟨	🟨	🟨	▨
	Anonymous	🟨	🟨	🟨	

🟥	Activity detected in the Netherlands	🟨	Type of activity detected abroad	▨	Claimed type of activity

Illustration 2: Different hacktivist groups and their activities

Hacktivists and ransomware

In some cases, they also show an interest in ransomware. The Killnet and Anonymous Sudan groups, for instance, claimed that they started collaborating with the infamous criminal actor called REvil.[23] REvil is known for its ransomware attacks but has been much less prominent since a series of arrests in January 2022.[24]

- Ransomware attacks are generally undertaken by criminal actors because they have a clear business model. Cybercriminals encrypt an organisation’s systems and/or files and ask for a random so the organisation can regain access to its systems and files. This is often combined with data exfiltration and threats to leak the data. A similar business case for pressuring an organisation to achieve a political or social objective can be made for hacktivists.
- Even so, the NCSC has not detected any significant hacktivist activity involving ransomware attacks. In many cases, it appears that ransomware attacks are not opportune for hacktivists because they do not have the capacity or resources to undertake such an attack, for instance, or because other types of digital attack are better suited for their objective.
- As such, the NCSC deems it **unlikely** that hacktivists will undertake ransomware attacks on Dutch organisations in the short and medium term. Nor has the NCSC detected any activities in line with the ransomware claims of groups like Killnet, Anonymous Sudan and REvil.

Prognosis

We can identify different triggering events by analysing the behaviour of the various hacktivists. This will help us gain an understanding of what events may lead to a hacktivist response.

Triggering events are events that may lead to a hacktivist response in the form of digital attacks. The list shared in this analysis is not exhaustive but covers aspects observed by the NCSC in the course of hacktivist attacks on Dutch organisations. By including triggering events in the analysis, we achieve insight into cause and effect with respect to events that may lead to digital attacks.

		Actor				
		Killnet	NoName057(16)	Anonymous Sudan	Turk Hack Team	Mysterious Team Bangladesh
Triggering event	Further political positioning and sanctions in the context of the Russian invasion of Ukraine	√	√	√		
	Pro-Ukrainian political symbolism *(e.g. visit from high government officials)*	√	√	√		
	Arms supply to Ukraine	√	√	√		
	Events that a religious group considers to be injurious (e.g. tearing up of the Quran in March 2023)			√	√	√
	Rising diplomatic tension *(e.g. Turkish referendum situation in 2017)*				√	

Table 1: Identified triggering events for hacktivist attacks on Dutch organisations

Triggering events do not explain all digital attacks

Not all hacktivist attacks are the result of a triggering event. Some hacktivist attacks are undertaken without a specific cause. An NCSC analysis of recent DDoS attacks by NoName057(16) shows that this group frequently executes DDoS attacks without any direct cause. The DDoS attacks are more generally targeted against organisations in countries that support Ukraine in its battle against the Russian invasion.

Upcoming parliamentary elections

Elections are frequent triggers for different actors to undertake digital attacks for a political or social reason. Early parliamentary elections will be held in the Netherlands on 22 November 2023.

- Hacktivists may use hack-and-leak operations or defacement attacks to influence public opinion in relation to elections. They can try to disrupt information provision for elections by means of DDoS attacks.
- Google Cloud has published a report on DDoS attacks executed during the midterm elections in the US in 2022.[25] A strong increase in DDoS attacks against the websites of political candidates was detected just before and during the elections. Their number dropped quickly after the midterm elections.
- At present, we have not found any indication of upcoming hacktivist attacks related to the Netherlands elections. However, we do consider it **possible** that this may occur in the near future. Our assessment is based on an analysis of hacktivist activities during elections in other countries.

In the longer term: 2025 NATO summit

A NATO summit draws the attention of different types of actors, including hacktivists. In the period leading up to and after the NATO summit in Vilnius in June 2023 several confidential documents were claimed to have been leaked. The actor *From Russia with Love* posted 29 documents on Telegram that were claimed to contain information about the summit, such as participant lists and protocol-related information.[26]

- The research agency Graphika also stated that the NATO summit was targeted by a disinformation campaign.[27] It was said to have used falsified online identities and documents to spread misleading information. The campaign aimed to cause unrest amongst NATO members and undermine NATO support to the Ukraine in its battle against Russian occupying forces.
- The Netherlands is to organise the 2025 NATO summit. With an eye to previous hacktivist activities around similar international political events, the NCSC considers it **likely** that this NATO summit will be the target of hacktivist attacks.

Other triggering events

Triggering events may be announced shortly before they occur. The Netherlands visit of the Ukrainian President Zelensky was not made public until the day on which it occurred.[28] Triggering events may also occur in the short term that may lead to a hacktivist response in the upcoming period. The examples mentioned in this document are not limitative.

Perspective for action

This perspective for action provides you with starting points for dealing with different hacktivist threats.

Dealing with DDoS attacks by hacktivist groups

Hacktivist groups execute DDoS attacks on a regular basis, affecting the availability of an online service.

On 2 February 2023, the NCSC issued the factsheet 'Omgaan met DDoS-aanvallen van hacktivistische groeperingen' [Dealing with DDoS attacks by hacktivist groups]. This scope for action offers recommendations to prevent that online services become unavailable due to a DDoS attack. [🖱] It also contains further references to additional publications and recommendations.

Defacement

In a defacement attack, an attacker gains unauthorised access to a digital media, such as a website or social media account, defacing it with disruptive texts.

- In many of the cases investigated by the NCSC, hacktivists gained access to websites by leveraging vulnerabilities, in some cases at vendors like hosting parties, or for instance in the Content Management System (CMS) and additional plug-ins used by the website.
- Access to social media accounts is generally obtained by abusing weak authentication methods (such as vulnerable passwords and a lack of multifactor authentication).

Include the CMS and plug-ins of your website in your **patching policy**. Please refer to the NCSC's basic measure 'Richt patchmanagement in' [Organise patch management]. [🖱]

Gain insight into and a grip on vendors interfaced with your communication platforms. The NCSC publication 'Omgaan met risico's in de toeleveringsketen' [Dealing with risks in the supply chain] helps you do this. [🖱]

Implement **strong authentication** for social media accounts. Communicate this clearly to your employees who use such accounts. Please refer to the basic measure 'Pas sterke authenticatie toe' [Implement strong authentication]. [🖱]

Hack-and-leak

Hack-and-leak operations allow hacktivists to gain access to confidential information and post it online to damage the victim’s reputation.

Implement the **basic measures** to prevent attackers from gaining unauthorised access to confidential information. [👆]

Additionally, you should develop and do a trial run with a **crisis communication plan** to be used in case your organisation is targeted by a hack-and-leak operation. The NCSC guide ‘Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten’ [Key points for crisis management and communication during digital incidents] provides starting points. [👆]

Incorporate hacktivist threats in your risk analyses

Incorporate the various hacktivist threats as described in this publication in your risk analyses. Look at confidential data and processes that may be interesting to different types of hacktivist groups.

- You could do this by considering your organisation from the perspective of a hacktivist group. Ask yourself what data and/or processes you would want to target, why and when you would do so, and what attack method would be suitable. You can then incorporate these insights into your risk analysis.

Please refer to the basic measure ‘Richt **risicomanagement** in’ [Implement **risk management**]. [👆] The NCSC factsheet ‘Risico’s beheersen: de waarde van informatie als uitgangspunt’ [Controlling risks: the value of information as a starting point] provides additional starting points for implementing risk management. [👆]

Contact the NCSC in the event of a digital attack

The NCSC wants to talk to organisations that have been targeted by a hacktivist attack. By reporting a digital attack, you are contributing to the cybersecurity of Dutch organisations.

Please contact the NCSC via cert@ncsc.nl and include any technical details with your report.

References

[1] On 26 February 2022, the Ukrainian Minister of Digital Transformation called upon hackers all over the world to enlist with an Ukrainian IT army of volunteers and attack Russian targets.

[2] https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf

[3] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/

[4] https://www.rtvnoord.nl/nieuws/993786/pro-russische-hackersgroep-killnet-zit-achter-cyberaanval-umcg-update

[5] 'NoName057(16) voert DDoS-aanvallen uit op Nederlandse organisaties' [NoName057(16) carries out DDoS attacks on Dutch organisations], NCSC CTI Report, 17 March 2023

[6] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/

[7] https://www.reliaquest.com/blog/turk-hack-team-and-the-netherlands-operation/

[8] https://www.group-ib.com/blog/mysterious-team-bangladesh/

[9] In the past Mysterious Team Bangladesh's messages could be followed via the following account, which has been taken down since;
https://twitter.com/MysteriousTeam0/status/1626558530231877633

[10] https://www.techworm.net/2023/08/ghostsec-breaches-iranian-surveillance-system.html

[11] https://www.cnbc.com/2022/10/05/how-anonymous-and-other-hacking-groups-are-aiding-protests-in-iran.html

[12] https://www.businessinsider.in/tech/news/russia-ukraine-war-anonymous-hackers-launch-cyberwar-against-russia-taking-down-government-websites/articleshow/89817168.cms

[13] https://www.dailydot.com/debug/anonymous-hacks-texas-gop-website-floods-it-with-memes/

[14] https://thehackernews.com/2022/09/palestinian-hacktivist-group-ghostsec.html

[15] https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/

[16] A DDoS attack affects the capacity of online services or underlying servers and network equipment. For details, please visit the NCSC website at https://www.ncsc.nl/onderwerpen/ddos.

[17] 'NoName057(16) voert DDoS-aanvallen uit op Nederlandse organisaties' [NoName057(16) carries out DDoS attacks on Dutch organisations], NCSC CTI Report, 17 March 2023

[18] https://www.bleepingcomputer.com/news/security/third-npm-protestware-event-source-polyfill-calls-russia-out/

[19] This image was obtained from forums associated with TurkHackTeam.

[20] https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems

[21] https://www.digitaltrustcenter.nl/informatie-advies/operational-technology

[22] 'Cybersecuritybeeld Nederland 2023: Verwacht het onverwachte' [Cyber Security Assessment Netherlands 2023: Expect the unexpected), NCTV and NCSC, 2023

[23] On 14 June 2023, Anonymous Sudan announced on its Russian Telegram channel that it would undertake a massive joint attack with Revil and Killnet on European financial institutions.

https://flashpoint.io/blog/anonymous-sudan-ddos-timeline/

[24] https://www.bbc.com/news/technology-59998925

[25] ‘How Project Shield helped protect U.S. midterm elections from DDoS attacks’, Google Cloud, 23 March 2023; https://cloud.google.com/blog/products/identity-security/ddos-attack-trends-during-us-midterm-elections

[26] https://www.15min.lt/naujiena/aktualu/lietuva/nato-virsuniu-susitikimo-vilniuje-finisas-gresminga-programisiu-ataka-nutekinti-esa-slapti-duomenys-56-2082506

[27] ‘Summit Old, Summit New’, Graphika, August 2023; https://graphika.com/reports/summit-old-summit-new

[28] ‘Oekraïense president Zelensky in Nederland, speecht in Den Haag’ [Ukrainian President Zelensky in the Netherlands, gives speech in The Hague], NOS, 3 May 2023; https://nos.nl/artikel/2473745-oekraiense-president-zelensky-in-nederland-speecht-in-den-haag

Publication
National Cyber Security Centre (NCSC-NL)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

oktober 2023

TLP:GREEN