Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC
Settore Analisi

30 ottobre 2023

Analisi successiva dell'incidente

Attacchi DDoS NoName057(16), giugno 2023

Il presente rapporto analizza gli attacchi DDoS («distributed denial of service»), verificatisi nelle prime due settimane di giugno 2023 (settimane 23 e 24) ai danni di organizzazioni e autorità svizzere. Esso illustra nel dettaglio l'utilizzata variante di attacco DDoS a livello di applicazione.

La Svizzera ha superato senza danni duraturi gli attacchi DDoS del gruppo NoName057(16). Le organizzazioni e autorità svizzere prese di mira erano perlopiù preparate ad attacchi DDoS e hanno pertanto potuto reagire in modo adeguato. Si deduce che grazie all'implementazione, adeguata alle esigenze, dei meccanismi di sicurezza è possibile minimizzare in modo determinante i potenziali danni.

A causa degli svariati obiettivi colpiti dall'attore nonché della rilevanza politica del discorso al Parlamento di Volodymyr Zelensky, i media si sono occupati molto degli attacchi DDoS. Grazie a questa ampia divulgazione mediatica, il gruppo ha raggiunto il suo scopo, ovvero attirare su di sé l'attenzione della popolazione. Obiettivo del gruppo di hacker filorusso NoName057(16) era quello di diffondere i propri interessi politici, a seguito di diverse decisioni del Parlamento svizzero (p. es. consegna di materiale bellico a Paesi terzi, annuncio del discorso di Volodymyr Zelensky al Parlamento).

Gli attacchi DDoS miravano a compromettere la disponibilità dei siti web («resource exhaustion» o esaurimento delle risorse). Non vi è stata alcuna fuga di dati produttivi.

Indice

1 Sintesi

Durante le prime due settimane di giugno 2023 (settimane 23 e 24) si sono verificati attacchi DDoS («distributed denial of service)[1] contro organizzazioni e autorità svizzere. All'origine di questo ciberattivismo (hacktivismo) contro la Svizzera vi erano diverse decisioni del Parlamento svizzero in rapporto con la guerra in Ucraina (vedi capitolo 8 [1] e [2]). Tramite simili attacchi DDoS gli hacktivisti si aspettano un'ampia risonanza, al fine di rendere noti i propri interessi politici e raggiungere i propri scopi.

L'attore ha preso di mira in particolare organizzazioni o autorità vicine all'Amministrazione federale e che godono di una buona reputazione nell'opinione pubblica (p. es. Parlamento svizzero, Posta Svizzera SA, Ferrovie federali svizzere FFS). A causa degli attacchi DDoS singole pagine web non erano temporaneamente accessibili (per poche ore), mentre altre sono rimaste inaccessibili per alcuni giorni. Non vi sono stati danni permanenti all'infrastruttura TIC o altri danni economici. Questo non era neanche l'obiettivo principale dell'attore, il quale intendeva innanzitutto richiamare l'attenzione di media, popolazione e politica.

L'attore è il gruppo di hacktivisti filorussi NoName057(16), che da marzo 2022 compie attacchi DDoS contro diversi obiettivi in tutto il mondo (p. es. amministrazioni e autorità pubbliche, imprese e altre organizzazioni) ritenuti «nemici della Russia». Il successo degli attacchi viene comunicato dal gruppo sull'omonimo canale Telegram.

Per i propri attacchi NoName057(16) mobilita dei ciberattivisti («heroes»), che mettono a disposizione, dietro compenso, i propri computer per gli attacchi DDoS. Questi «heroes» possono inoltre proporre gli obiettivi da attaccare. L'attore mette a disposizione il client DDoS «DDoSia» e fornisce supporto tecnico agli «heroes» mediante il canale Telegram «DDoSia-Project».

Gli attacchi basati su Internet si sono concentrati a livello di applicazione (OSI Layer-7)[2]. NoName057(16) voleva provocare, in modo mirato, l'interruzione dei siti web mediante sovraccarico delle risorse disponibili sul sistema («resource exhaustion» o esaurimento delle risorse), affinché determinati servizi non fossero più accessibili al pubblico (p. es. acquisto online di biglietti FFS). L'ondata di attacchi è durata due settimane e dal punto di vista tecnico è rimasta sempre uguale. Ciò che è cambiato è stato il ritmo giornaliero con cui i vari obiettivi sono stati colpiti. Non tutti gli interessati erano ugualmente preparati a simili attacchi DDoS. Di conseguenza, alcuni hanno reagito più rapidamente di altri, riuscendo così a ridurre al minimo le ripercussioni.

Le conseguenze di un attacco DDoS possono essere minimizzate mediante misure tecniche (p. es. «web application firewall»: adeguamento a livello di configurazione delle regole del firewall affinché il client DDoS venga riconosciuto e bloccato; vedi capitolo 3.3) e organizzative (p. es. «business continuity management» [BCM] o gestione della continuità operativa[3]).

Il pericolo latente di questi attacchi implica la necessità di seguire in permanenza lo sviluppo specifico nel ciberspazio, di valutare i rischi e di adeguare all'occorrenza i dispositivi di sicurezza. Le interruzioni causate dagli attacchi e il successivo interessamento da parte dei media hanno fatto emergere il potenziale di miglioramento, presso singoli interessati, per quanto riguarda la risposta a simili attacchi. Alcuni di essi hanno già attuato apposite misure.

[1] https://it.wikipedia.org/wiki/Denial_of_service

[2] https://it.wikipedia.org/wiki/Modello_OSI

[3] https://it.wikipedia.org/wiki/Gestione_della_continuità operativa

2 Introduzione

2.1 Contesto geopolitico

A fine febbraio 2022 la Russia ha attaccato militarmente l'Ucraina. Nel quadro di questo conflitto gli attacchi avvengono anche nel ciberspazio, da parte sia di attori statali sia di ciberattivisti (hacktivismo). Dal canto suo, la Russia stessa è bersaglio di ciberattacchi condotti da diversi ciberattivisti e altre organizzazioni. Anche altri Paesi, in particolare gli Stati membri della NATO, sono vittime di ciberattacchi.

Finora sono state rilevate solo poche ciberattività di stampo attivistico contro la Svizzera e gli obiettivi svizzeri. Il numero e l'intensità di queste ciberattività corrisponde alla valutazione delle minacce da parte del Centro nazionale per la cibersicurezza (NCSC) e del Servizio delle attività informative della Confederazione (SIC). La realizzazione della minaccia non comporta alcun cambiamento della situazione di minaccia: anche in futuro la Svizzera può essere in parte toccata da ciberattività di stampo attivistico. Finora è stato possibile rispondere a simili attacchi mediante misure di sicurezza e di lotta convenzionali (mitigazione degli attacchi). Di conseguenza i danni per la Svizzera sono stati di lieve entità.

Nel rapporto sulla situazione «La sicurezza della Svizzera 2023»[4] il SIC illustra la situazione nel dettaglio. L'immagine seguente mostra i ciberattacchi condotti dai ciberattivisti nel primo anno di guerra (DDoS / attacchi alla disponibilità):

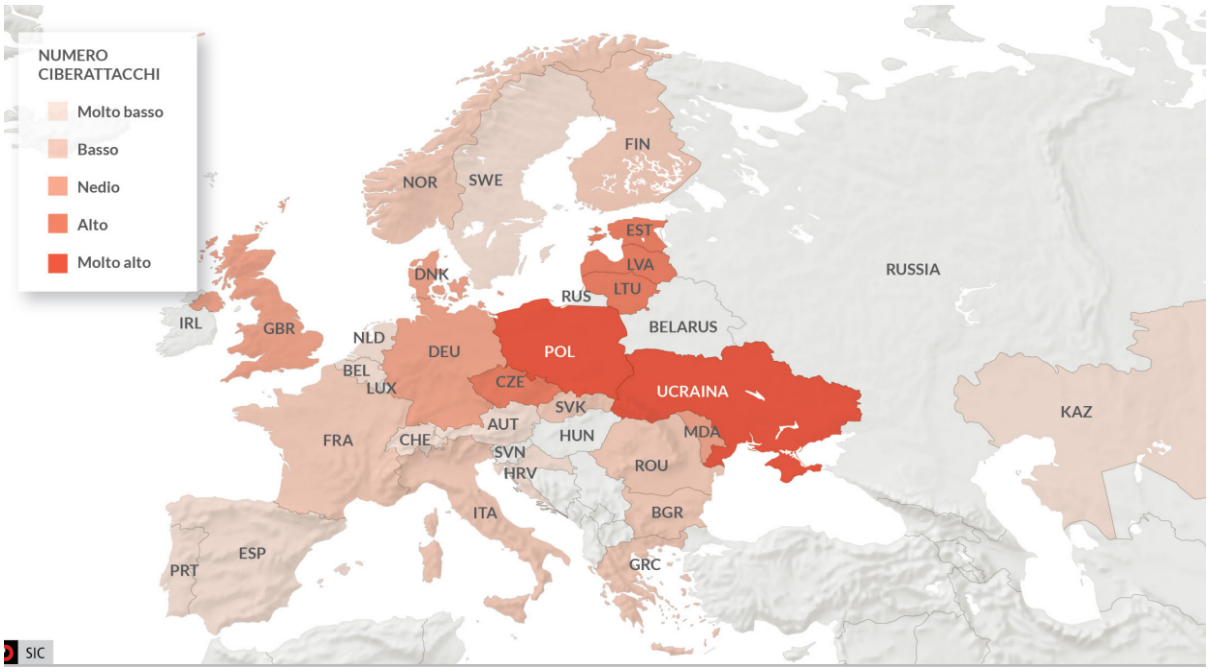

Figura 1: Attacchi DDoS da parte di ciberattivisti nel primo anno di guerra
(fonte: Rapporto sulla situazione 2023 del SIC)

Il termine ciberguerra[5] è composto dai termini **ciber**spazio e **guerra**. Designa un conflitto bellico (o militare) tra due Stati condotto per un certo periodo di tempo con i mezzi della tecnologia dell'informazione.

Gli attacchi DDoS («distributed denial of service») lanciati, limitatamente nel tempo, da

[4] https://www.vbs.admin.ch/it/ddps/organizzazione/unita-amministrative/servizio-attivita-informative.detail.document.html/vbs-internet/it/documents/serviziodelleattivitainformative/rapportisituazione/NDB-Lagebericht-2023-i.pdf.html

[5] https://it.wikipedia.org/wiki/Guerra_cibernetica

NoName057(16) lo scorso giugno contro diversi obiettivi in Svizzera non possono essere considerati eventi bellici e rientrare nella definizione di ciberguerra; si tratta piuttosto di atti di ciberattivismo (vedi capitolo 2.2).

2.2 Categorizzazione

Gli attacchi DDoS contro la Svizzera sono stati condotti da hacktivisti animati da motivi politici, che hanno in tal modo fatto opera di propaganda filorussa. Tramite questi attacchi l'attore è riuscito a limitare in parte i siti web presi di mira (vedi capitolo 3.2). Per questo motivo a giugno l'NCSC ha classificato gli attacchi come atti di **ciberattivismo**[6]:

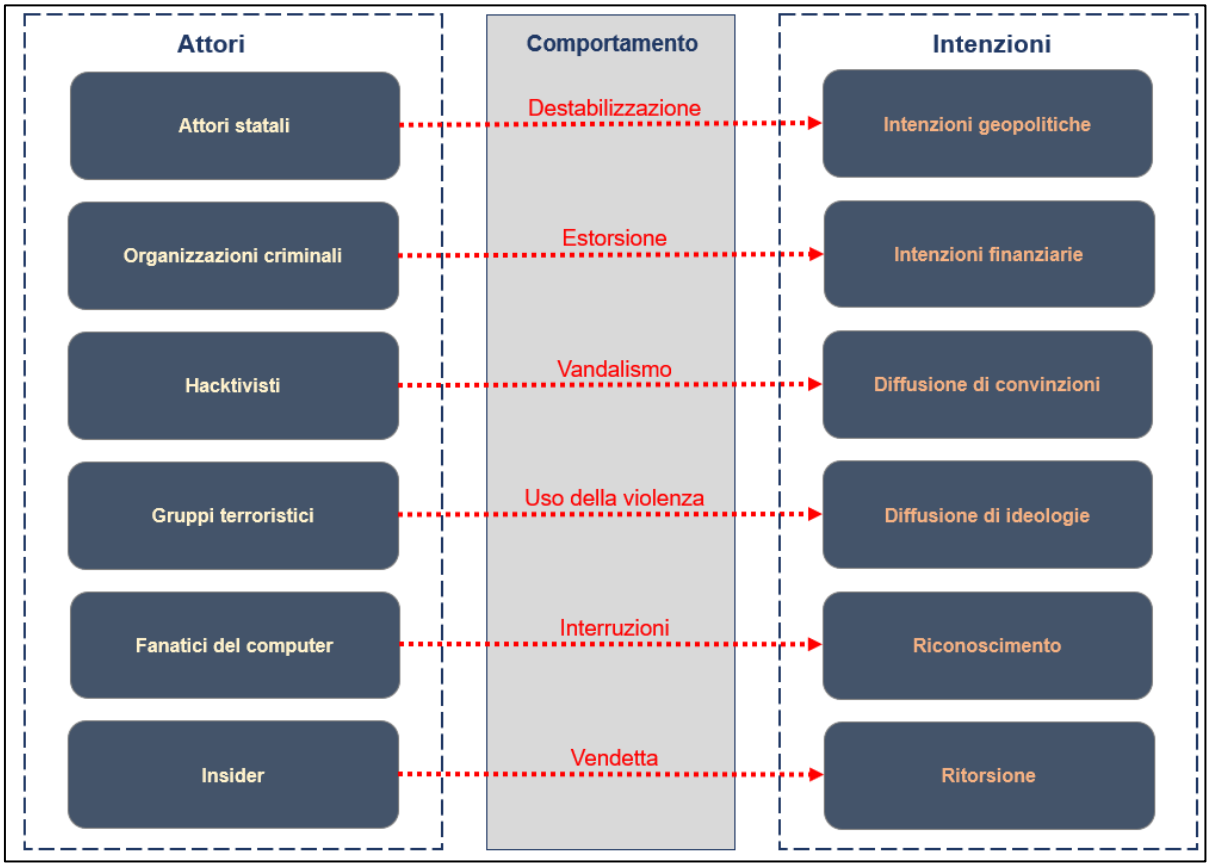

Figura 2: Attori, il loro comportamento e le loro intenzioni

L'attore NoName057(16) diffonde i suoi potenziali successi sempre attraverso il servizio di messaggistica istantanea Telegram. In questo modo vuole richiamare la massima attenzione sulle sue attività di natura politica. La diffusione mediatica dei successi e l'attenzione politica e sociale destata nello Stato preso di mira vanno, di fatto, attribuite alle operazioni d'informazione (info Ops).

[6] https://it.wikipedia.org/wiki/Attivismo

3 Descrizione dell’attacco

3.1 Tipo di attacco DDoS

Esistono diverse possibilità per esaurire le risorse dei sistemi tramite gli attacchi DDoS. Gli attacchi miravano a imitare il legittimo comportamento d’uso degli utenti sui siti web. A tale proposito sono stati aperti in modo automatizzato servizi web, come moduli di ricerca o di registrazione, che hanno un determinato impatto sulla logica di business successiva. Dato che la logica di business e i componenti di rete a monte, ad esempio i server di applicazioni, i «load balancer» o le «web application firewall» (WAF), vengono dimensionati per motivi economici in base al numero di utenti atteso, gli accessi artificiali possono sovraccaricare i limiti prestazionali previsti, con la conseguenza che gli utenti effettivi non possono più usufruire dei servizi abituali e i siti web non sono più utilizzabili come di consueto o non sono accessibili.

Il capitolo 3.3 si sofferma sui dettagli tecnici.

3.2 Attore NoName057(16)

Il gruppo NoName057(16) ha rivendicato pubblicamente su Telegram gli attacchi DDoS. Questo gruppo filorusso, attivo da marzo 2022, è apparso per la prima volta durante i disordini bellici legati all’invasione russa dell’Ucraina (febbraio 2022), dichiarando la ciberguerra nei confronti della guerra informativa contro la Russia. Il gruppo comunica principalmente tramite il canale Telegram, attraverso il quale annuncia anche i suoi obiettivi. Inoltre, su Telegram i follower possono esprimere le proprie preferenze riguardo al prossimo obiettivo da attaccare.

Procedura generale

Il seguente grafico illustra la procedura generale dell'attore in tre fasi (vedi la descrizione tecnica al capitolo 3.3):

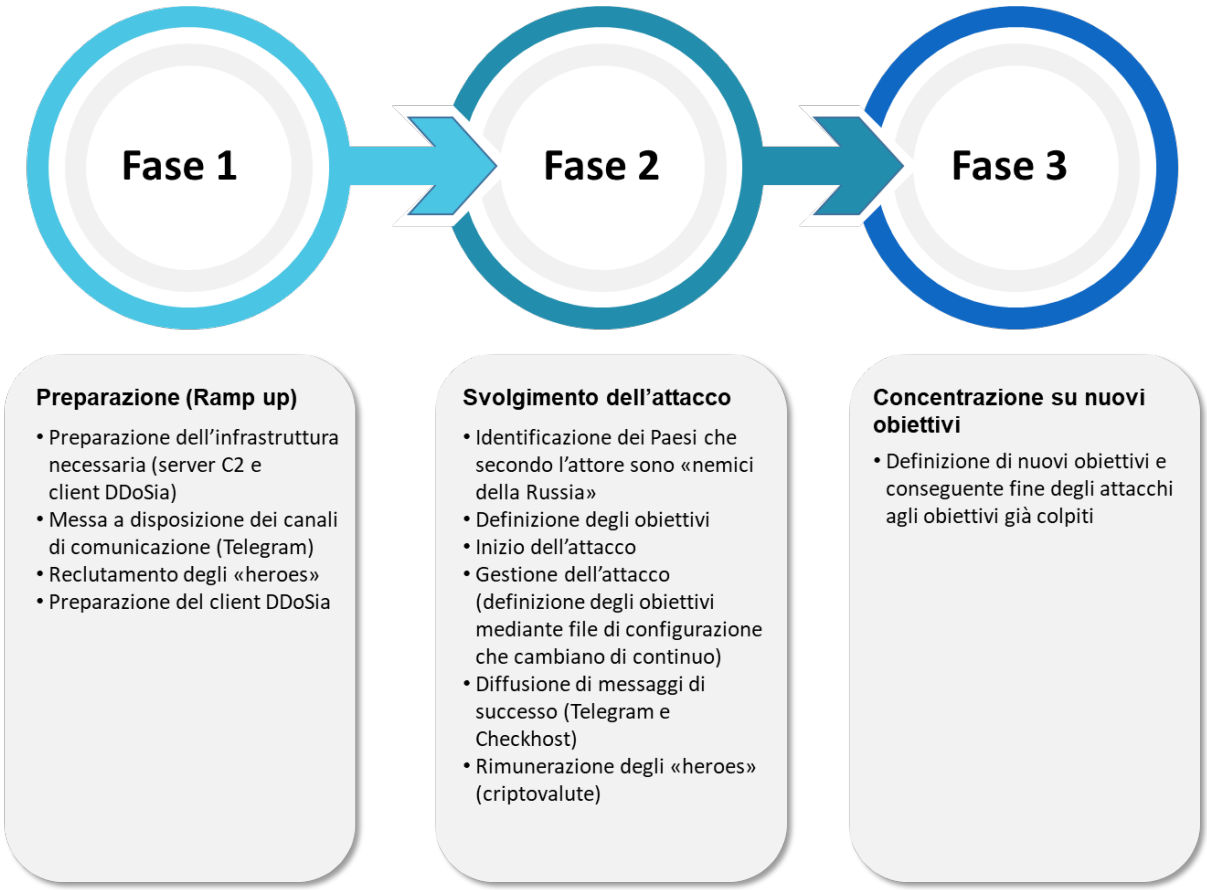

Figura 3: Procedura generale

Obiettivi attaccati

Gli obiettivi principali del gruppo di hacktivisti erano i siti web dell'Ucraina nonché quelli degli Stati membri della NATO e dei Paesi dell'UE. Nel mirino degli hacker vi erano anche i Paesi sostenitori dell'Ucraina o che hanno imposto sanzioni contro la Russia. A causa delle due decisioni del Parlamento a presunto vantaggio dell'Ucraina (vedi capitoli 8, [1] e [2]), per un breve periodo di tempo anche la Svizzera è diventata bersaglio degli attacchi. Gli attacchi DDoS alla Svizzera, durati una settimana, non sono avvenuti né per motivi economici né per via del benessere del Paese. È prevedibile che anche in futuro l'attore continuerà ad attaccare vari Stati a scopo propagandistico.

Nel seguente diagramma sono riassunti gli Stati attaccati dall'attore nel periodo compreso tra il 1° aprile 2023 e il 24 giugno 2023:

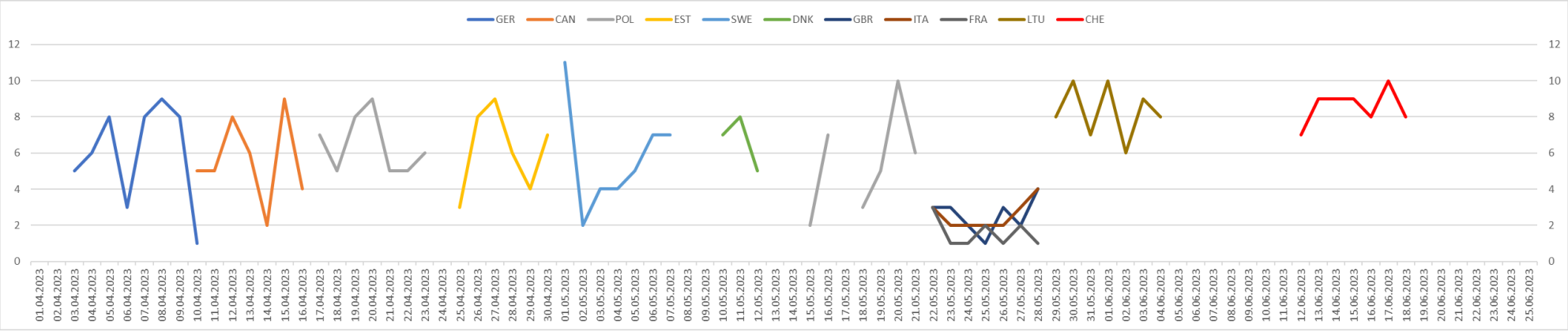

Figura 4: Attacchi DDoS ad altri Stati prima, durante e dopo l'attacco alla Svizzera (elenco non esaustivo)

Dal diagramma emerge che la Svizzera (designazione CHE secondo lo standard ISO) è uno dei molti Paesi attaccati dall'attore. Inoltre, si può notare che l'attore era già attivo contro altri Stati prima degli attacchi DDoS contro la Svizzera, avvenuti tra il 12 giugno e il 18 giugno 2023.

Analisi delle minacce («threat assessment») sull’attore

Il seguente grafico visualizza l’analisi delle minacce dell’NCSC sull’attore NoName057(16). Dall’analisi emerge, ad esempio, che la complessità («threat level», ovvero il livello di minaccia) dell’ondata di attacchi è stata piuttosto ridotta, ma che gli attacchi DDoS sono stati condotti con un’intensità elevata («attack frequency»):

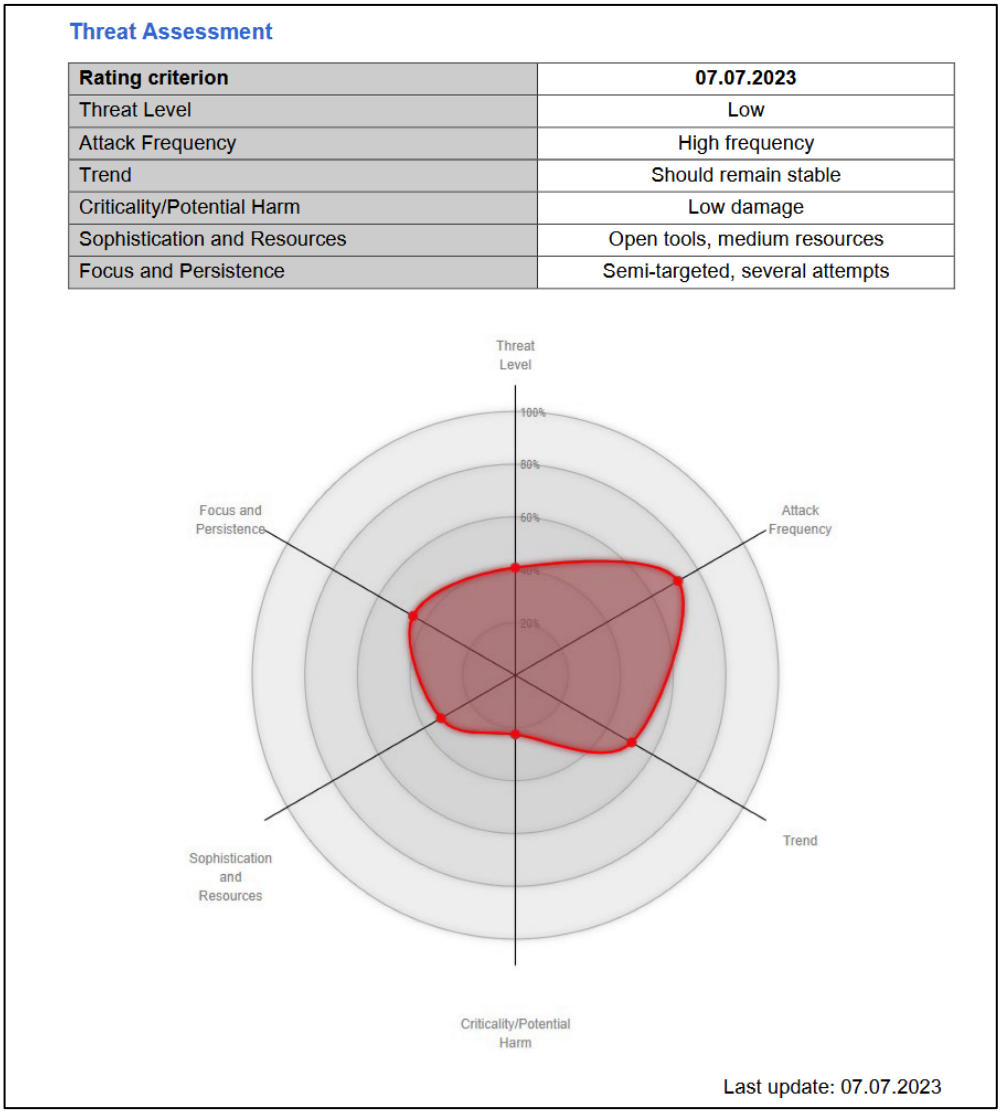

Figura 5: Analisi delle minacce dell’NCSC sull’attore «NoName057(16)»

Motivazione dell’attore

L’11 marzo 2022, l’attore ha pubblicato su Telegram la seguente linea guida sulle attività del gruppo di hacktivisti:

Figura 6: Post su Telegram tradotto in inglese

Per realizzare i suoi interessi politici e le sue intenzioni, l’attore avvia e coordina gli attacchi DDoS per ottenere la massima attenzione possibile.

In un altro post su Telegram, l'attore ha motivato come segue la scelta di questa metodologia di attacco:

Motivazione formulata dall'attore	Classificazione della motivazione da parte dell'NCSC	Raggiungimento della motivazione dal punto di vista dell'NCSC
«Se i server aziendali vengono eseguiti nel cloud, l'aumento del traffico di rete comporta un aumento dei costi».	L'attore vuole causare un danno economico.	Parzialmente raggiunto. Non sono stati causati danni economici significativi.
«Se un sito web rimane offline per più di due giorni, la sua visibilità nei motori di ricerca si riduce sensibilmente».	L'attore intende limitare la reperibilità dei siti web.	Non raggiunto. La visibilità nei motori di ricerca non è stata compromessa.
«Anche se il sito web è nuovamente disponibile, la reputazione dell'operatore è stata danneggiata».	L'attore vuole compromettere la reputazione dei siti web oggetto dei suoi attacchi.	Non raggiunto. La reputazione delle vittime degli attacchi è stata indebolita solo durante il periodo dell'attacco.
«I sistemi attaccati possono rivelare informazioni all'esterno in seguito ai messaggi di errore generati automaticamente (p. es. informazioni interne sulle banche dati)».	L'attore vuole provocare un flusso in uscita di informazioni tecniche.	Parzialmente raggiunto. L'NCSC non può escludere che simili informazioni siano state divulgate durante l'ora dell'attacco.

Tabella 1: Motivazione dell'attore e valutazione dell'NCSC

Gli attacchi riusciti vengono pubblicati sul canale Telegram **@noname05716** come prova, con un messaggio che indica il sito web attaccato, la bandiera del Paese in questione e un link a un rapporto sul sito web check-host.net.

Dal sito web check-host.net è desumibile se i siti web di diversi Paesi sono accessibili (online). Anche a posteriori è possibile generare istantanee che consentono di verificare se determinati siti web erano accessibili in un determinato momento. Il messaggio che l'obiettivo attaccato non era disponibile in un determinato momento viene presentato dall'attore come prova del successo dell'attacco (come un trofeo). Al messaggio di Telegram vengono aggiunti vari saluti e inviti a seguire e sostenere il gruppo.

Canali di comunicazione dell'attore

L'attore comunica principalmente tramite due canali di Telegram:

- **@noname05716:** canale di chat generale (di solito screenshot di attacchi DDoS avvenuti con successo) in russo
- **@noname05716eng:** traduzioni in inglese di molti post del canale di chat principale

La restante comunicazione avviene attraverso canali supplementari:

Nome del canale compreso testo originale	Traduzione
DDoSia - мануалы + актуальное ПО	DDoSia – manuali + software attuali
DDoSia - поддержка	DDoSia – supporto
Полезные материалы	Materiale utile
Общий чат	Chat generale
English support	Supporto in inglese
Предложение целей	Proposte di obiettivi da attaccare
Ваши видео и скриншоты работы с клиентом DDosia	Video e screenshot del lavoro con il client DDoSia

Tabella 2: Elenco e traduzione dei canali di Telegram

Modello aziendale dell'attore

L'attore non utilizza una classica rete botnet[7], ma conta sul supporto di volontari, i cosiddetti «heroes». Questi «heroes» installano sui loro computer il client DDoSia (vedi in basso), utilizzato per eseguire l'attacco.

Gli «heroes» si registrano tramite un bot di Telegram. Dopo la registrazione, il bot di Telegram invia un indirizzo URL per scaricare i file DDoSia eseguibili e un file di testo con un ID univoco per identificare gli «heroes» registrati.

Gli «heroes» possono registrarsi nel bot di Telegram con il proprio numero ID e un wallet di criptovalute. L'attore promette loro di pagarli in criptovalute in base al numero di attacchi portati a termine. Questi ultimi vengono determinati sulla base del numero complessivo di attacchi effettuati dai volontari attivi in un determinato giorno.
In un post di Telegram del mese di marzo 2023, l'attore descrive lo schema di pagamento come segue:

- 80 000 rubli per il primo posto
- 50 000 rubli per il secondo posto
- 20 000 rubli per il terzo posto

Un importo di 50 000 rubli è stato suddiviso tra il quarto e il decimo posto.

I pagamenti avvengono in criptovalute come Ethereum, Bitcoin e Tether. Nel canale DDoSia di Telegram, gli «heroes» possono consultare informazioni sulle loro statistiche complessive (elenco dei primi dieci classificati).

Non è chiaro chi sia lo sponsor di questi mezzi finanziari. A differenza di altri ciberattivisti, l'attore finora non ha lanciato una richiesta di donazioni, ad esempio attraverso i social media.

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

3.3 Descrizione tecnica

All'inizio del conflitto in Ucraina, l'NCSC ha constatato un aumento delle attività DDoS che utilizzavano il malware «Bobik»[8]. Le vittime degli attacchi non sapevano che i loro computer fossero stati infettati da questo malware e utilizzati per effettuare attacchi DDoS. Nel frattempo NoName057(16) ha cambiato tipo di approccio e invita pubblicamente gli «heroes» nei social media a utilizzare il client DDoS speciale denominato «DDoSia».

Il passaggio di Bobik al client DDoS speciale consente di ridurre notevolmente l'onere operativo dell'attore, che così non deve procurarsi dispositivi infetti. Il cambiamento è quindi avvenuto per motivi economici.
Per effettuare gli attacchi DDoS, l'attore ricorre al progetto DDoSia[9], composto da server «command and control» (C2) e client DDoSia. DDoSia è stato sviluppato a settembre 2022 per consentire ai cosiddetti «heroes» di mettere a disposizione (tramite Telegram) a titolo volontario i loro computer e le loro connessioni Internet per eseguire gli attacchi.

Descrizione del client DDoSia

Il client DDoSia è in continuo sviluppo, è programmato nel linguaggio di programmazione «Go» ed è eseguibile sulle piattaforme Linux, Windows, MacOS e Android.

Il client DDoSia utilizza per default lo user agent «Go-http-client/1.1» del linguaggio di programmazione «Go». Durante gli attacchi DDoS, l'identificativo HTTP «Go-http-client/1.1» dello user agent è rimasto invariato. L'identificazione univoca dello user agent ha semplificato la mitigazione tramite WAF. Nelle WAF è stato possibile bloccare questo user agent adeguando la configurazione.

Non è stato constatato alcun camuffamento tramite «spoofing»[10] dell'indirizzo IP del client DDoSia. Di conseguenza, gli «heroes» sono potenzialmente identificabili attraverso il loro indirizzo IP. Nei suoi canali di supporto di Telegram, l'attore raccomanda di utilizzare la rete VPN, in modo da rendere più difficile l'identificazione degli «heroes».
Informazioni dettagliate sul client DDoSia, compreso il «reverse engineering», sono disponibili sul blog del fornitore di servizi di sicurezza Sekoia (vedi capitolo 8, [4]).

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

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

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

Descrizione della comunicazione «command and control»

La seguente illustrazione mostra il flusso di comunicazione dei client DDoSia con i server «command and control» (C2)[11]:

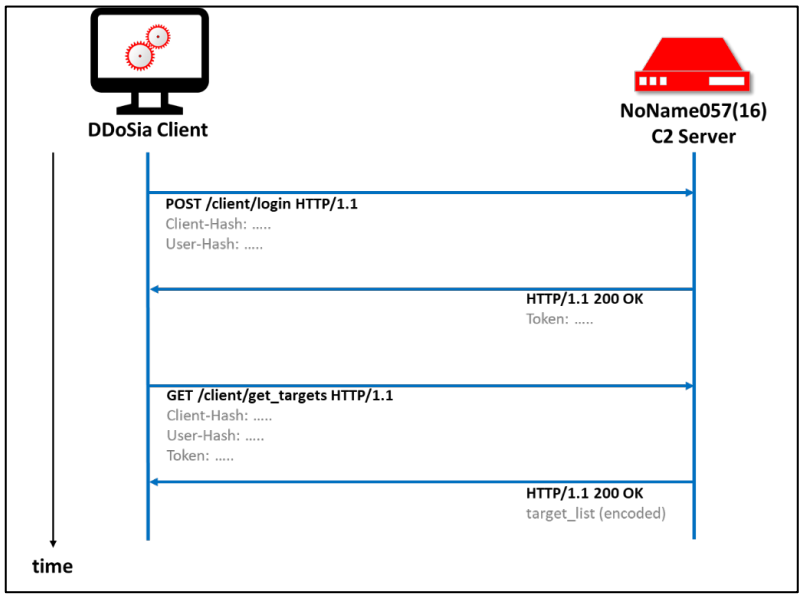

Figura 7: Comunicazione tra DDoSia e C2

La comunicazione tra i client DDoSia e i server C2 è personalizzata tramite un «user-hash», che identifica il partecipante, e un «hash-client», che identifica il computer del partecipante. Inoltre, l'«user-hash» è utilizzato per identificare il rispettivo utente, al fine di effettuare il pagamento degli «heroes». Il client DDoSia riceve infine l'elenco degli obiettivi da attaccare `(target_list(encoded))`.

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

Comunicazione con l’obiettivo dell’attacco

Sulla base delle istruzioni nell’elenco degli obiettivi da attaccare (scaricato da server C2), il client DDoSia genera i compiti concreti che devono essere eseguiti nei siti web da attaccare.

A tale proposito viene utilizzato un modello («template») completato con sequenze parametrate di caratteri casuali. Nell’ambito della progettazione di questi modelli nonché dei contenuti generati casualmente, l’attore presta particolare a rendere questo traffico di dati il più verosimile possibile alle ricerche che avvengono in modo legittimo nel web. In tal modo diventa più difficile identificare in maniera automatizzata gli attacchi DDoS.

L’illustrazione qui di seguito mostra come il client DDoSia imita il traffico di dati legittimo, ingannando così i meccanismi di protezione, senza quindi impedire il traffico di dati dannoso. Per tale motivo, questo traffico di dati solitamente non viene identificato e bloccato automaticamente da meccanismi di protezione come DDoS protection e firewall:

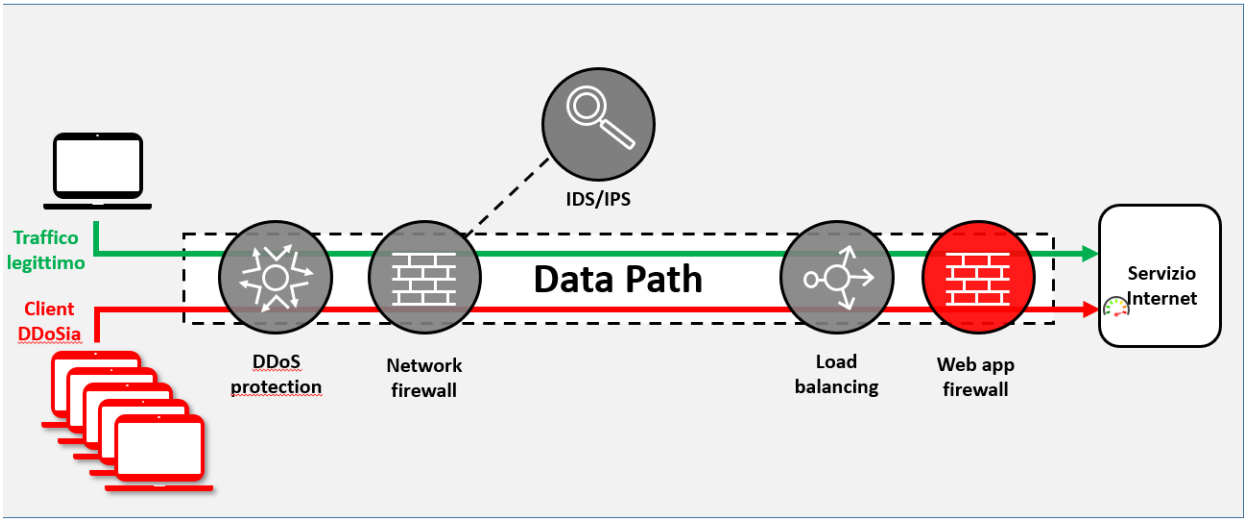

Figura 8: Traffico di dati dannoso del client DDoSIA

I seguenti esempi mostrano modelli che vengono completati con sequenze parametrate di caratteri casuali:

Esempio 1:

- Template: `"hxxp[s]://www.webseite.ch/de/search/?term=$_1"`
- $_1 è una sequenza casuale di 6–12 caratteri (p. es. in questo caso: kenuab)

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

Esempio 2:

- Template: `"hxxp[s]://www.webseite.ch/de/register/?name=$_1.$_1@$_2.ch"`
- $_1 è una sequenza casuale di 6–8 caratteri composta da lettere minuscole, $_2 è una sequenza casuale di 10–12 caratteri (p. es. in questo caso $1: goenza.leurebe e $2 pahelsnwmni)

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

In questo modo il client DDoSia genera continuamente richieste web con parametri differenti, il cui carico di processo viene generato nelle infrastrutture TIC a valle (p. es. nelle banche

dati utilizzate nei processi aziendali). Le richieste sono quindi difficili da distinguere dal traffico di dati legittimo, a causa della loro struttura dinamica.

Reazione tecnica all'attacco DDoS (mitigation)

Analizzando i modelli di attacco (p. es. filtrando i file di log sullo user agent del client DDoSia) è possibile creare un elenco degli indirizzi IP degli «heroes» interessati. Questo elenco può essere utilizzato per bloccare il traffico di rete dannoso già nel router Internet (router edge) dell'organizzazione interessata o del fornitore di servizi Internet («Internet Service Provider», ISP), ad esempio mediante «zero-routing»[12].

Nel quadro degli attacchi DDoS analizzati, gli ISP svizzeri hanno interrotto il traffico di dati DDoS nel loro servizio «backbone», bloccando gli intervalli IP («IP ranges») e i sistemi autonomi («autonomous systems», AS). I blocchi sono stati continuamente adeguati durante gli attacchi. L'intenso scambio di informazioni, reso possibile dall'NCSC, ha costituito la base di tali blocchi.

Dato che i processi di sicurezza e quelli operativi («incident response management», «change management» e «release management») richiedono impostazioni manuali (p. es. definizione di regole di blocco) è necessario prevedere un determinato lasso di tempo tra il rilevamento e la mitigazione di simili attacchi DDoS. Sulla base di esperienze e affermazioni attuali, il tempo di reazione medio può ammontare a circa due ore.
Poiché l'attore non è in grado di rilevare le misure di protezione implementate presso le organizzazioni colpite, si deve partire in ogni caso dal presupposto che gli attacchi continuino senza sosta, ma senza causare più interruzioni.

Quantificazione

Durante gli attacchi DDoS all'Amministrazione federale sono stati constatati circa 20 000 indirizzi IP. Le statistiche sugli attacchi all'Amministrazione federale mostrano una quota del 3 per cento di indirizzi IP appartenenti all'ambito degli indirizzi IP svizzeri.

Con una media tra 20 000 pps e 25 000 pps (pacchetti per secondo) e meno di 200 Mbit/s (megabit per secondo), il traffico di dati relativo agli attacchi DDoS è risultato piuttosto esiguo. Si tratta di indicatori tipici degli attacchi DDoS a livello di applicazioni.

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

4 Fasi dell'attacco

Gli attacchi DDoS contro la Svizzera sono iniziati mercoledì 7 giugno 2023 alle ore 08.00. Il sito web https://www.parlament.ch compare come primo obiettivo nell'elenco dei bersagli C2.

I motivi per questo nuovo obiettivo sono i seguenti:

- discussioni nel Parlamento svizzero sulle esportazioni di armi[13];
- l'annuncio del 5 giugno 2023 relativo al videomessaggio di Volodymyr Zelensky al Parlamento svizzero il 15 giugno 2023[14].

I follower sono stati informati tramite il canale Telegram dell'attore:

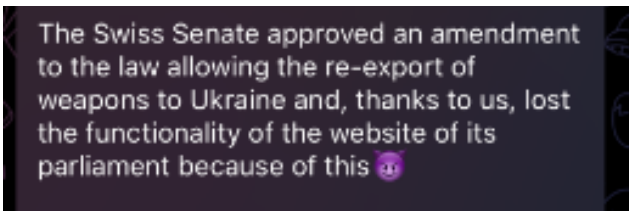

Figura 9: Primo messaggio nel canale Telegram (fonte: Telegram)

Anche l'annuncio del videomessaggio di Volodymyr Zelensky è stato commentato con un messaggio in Telegram:

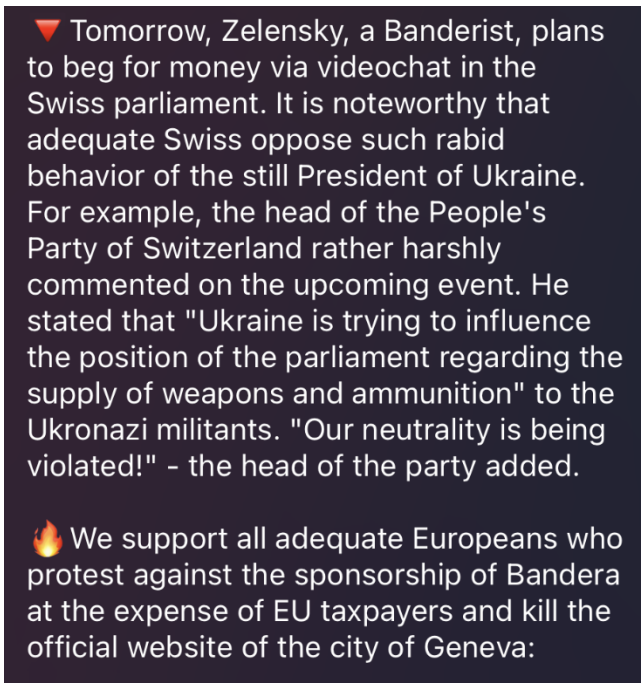

Figura 10: Secondo messaggio nel canale Telegram (fonte: Telegram)

[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

Cronologia degli attacchi

Gli attacchi DDoS si sono verificati durante circa due settimane. Va ricordato che l'attore aveva attaccato già in precedenza altri Stati più o meno nella stessa misura (dal punto di vista temporale, tecnologico e del contenuto) e che gli attacchi persistono.

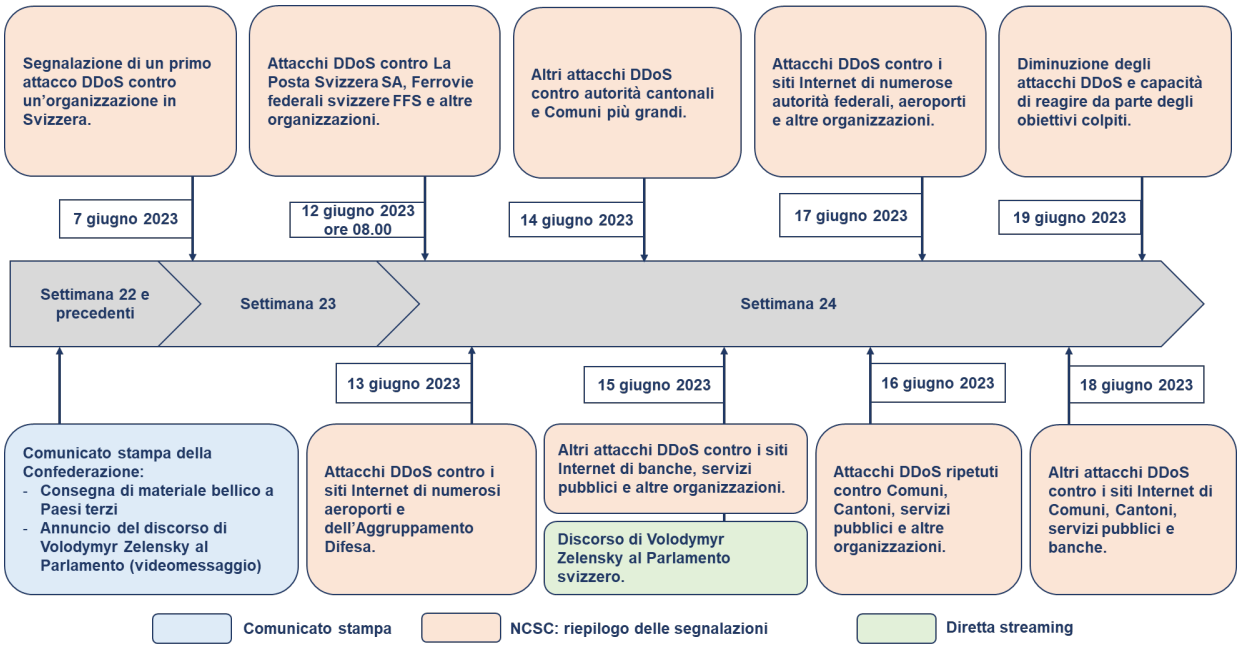

Figura 11: Cronologia degli eventi (riassunto)

Nella seguente tabella sono riassunti gli attacchi DDoS di successo:

Obiettivi	Data						
	12.6.2023	13.6.2023	14.6.2023	15.6.2023	16.6.2023	17.6.2023	18.6.2023
Amministrazione federale	4	1		1		2	
Cantoni			2		3		
Città			6				6
Servizi pubblici	2		1	1			1
Aeroporti		8				6	
Settore finanziario				5		2	1
Altro				1	3		
Armamento				1			
Totale 57	**6**	**9**	**9**	**9**	**6**	**10**	**8**

Tabella 3: Illustrazione degli attacchi DDoS di successo

La tabella mostra che in media al giorno sono andati a buon fine circa otto attacchi DDoS. È evidente la concentrazione degli attacchi ai siti web di aeroporti, di organizzazioni del settore finanziario e di città. Dalla tabella si desume, inoltre, che all'inizio della settimana 24 sono state attaccate soprattutto le autorità e soltanto nella seconda parte della settimana organizzazioni dell'economia privata.

Un’altra tabella mostra gli attacchi segnalati all’NCSC in rapporto agli attacchi DDoS pubblicati come riusciti (vedi Tabella 4):

Data	Fonti	
	Attacchi segnalati all’NCSC	Attacchi DDoS pubblicati come riusciti
12.6.2023	11	6
13.6.2023	11	9
14.6.2023	10	9
15.6.2023	11	9
16.6.2023	10	6
17.6.2023	16	10
18.6.2023	16	8
Totale	**85**	**57**

Tabella 4: Segnalazioni all’NCSC in rapporto alle comunicazioni pubblicate dall’attore su Telegram

Confrontando i 57 attacchi DDoS riusciti secondo la Tabella 3 con il totale degli attacchi DDoS segnalati all’NCSC (85 segnalazioni, vedi Tabella 4), si riscontra una differenza. Alcune organizzazioni e autorità, infatti, sono riuscite a mitigare con successo gli attacchi DDoS o a prevenire importanti interruzioni.

La seguente tabella (vedi Tabella 5) funge da precisazione della cronologia (in ordine crescente):

Data	Attacchi contro autorità e organizzazioni svizzere segnalati all’NCSC	Osservazione
12 giugno 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	Il primo giorno dei ciberattacchi sono state attaccate soprattutto autorità e organizzazioni parastatali.
13 giugno 2023	• www.vtg.admin.ch • www.flughafen-zuerich.ch • www.gva.ch	Il secondo giorno sono stati attaccati i siti web dell’Aggruppamento Difesa del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e di numerosi aeroporti.
14 giugno 2023	• www.geneve.com • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch • www.stadt.sg.ch	Gli obiettivi del terzo giorno sono stati in particolare i siti web delle città.

Data	Attacchi contro autorità e organizzazioni svizzere segnalati all'NCSC	Osservazione
	• www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch	
15 giugno 2023	• www.ncsc.admin.ch • www.ruag.com • www.postauto.ch • www.zvv.ch • www.swissid.ch	Il quarto giorno sono stati nuovamente attaccati i siti web di autorità e organizzazioni.
16 giugno 2023	• www.nw.ch • www.steuern-nw.ch • etax-login.nw.ch • www.stans.ch • www.buochs.ch • www.snb.ch	Il quinto giorno, l'attore si è concentrato soprattutto sulle autorità del Cantone di Nidvaldo.
17 giugno 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	Il sesto giorno erano nuovamente le autorità federali ad essere nel mirino degli attacchi.
18 giugno 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	L'ultimo giorno dell'ondata di attacchi sono stati ancora una volta presi di mira i siti web delle città.

Tabella 5: Elenco dei siti web attaccati tra il 12 giugno 2023 e il 18 giugno 2023

5 Effetti dell'attacco

I messaggi sul canale Telegram in lingua russa sono stati letti da circa 5500 partecipanti, mentre quelli sul canale in inglese da circa 1000–1500 partecipanti. Rispetto alla copertura mediatica in Svizzera (vedi capitolo **Fehler! Verweisquelle konnte nicht gefunden werden.**), nei canali dei social media (p. es. Twitter) i messaggi di successo da parte dell'attore non sono stati riportati in maniera significativa durante l'intera durata dell'attacco.
Per via degli attacchi specifici a livello di applicazione, i siti web che non possono essere protetti tramite il blocco di interi intervalli di indirizzi (mediante indirizzi IP di origine o bloccando sistemi autonomi[15]) sono particolarmente a rischio (p. es. cittadini svizzeri all'estero che devono accedere ai portali delle autorità). Il motivo risiede nel fatto che la configurazione delle WAF deve essere dapprima adeguata all'attacco specifico. Fin quando le configurazioni non sono concluse, l'obiettivo rimane esposto a un attacco. L'NCSC parte dal presupposto che gli adeguamenti della configurazione richiedano circa due ore di lavoro. I processi applicati (p. es. analisi – configurazione [«staging»] – roll-out) si basano sui processi di sicurezza e su quelli operativi («incident response management», «change management» e «release management») della rispettiva organizzazione o sugli accordi di «service level agreement» (SLA), nel caso dei servizi di sicurezza esternalizzati (processo e tempo di reazione).

Un esempio è il conto elettronico della città di Basilea, che mercoledì 14 giugno 2023 è stato sovraccaricato da numerosi tentativi di accesso simultanei. Allo stesso modo, venerdì 16 giugno 2023 è stato sovraccaricato il sito per la dichiarazione elettronica delle imposte del Cantone di Nidvaldo. Poco dopo l'adeguamento delle misure di protezione, i siti web attaccati in Svizzera erano nuovamente accessibili.

Il danno effettivo per gli obiettivi attaccati consisteva nei danni alla reputazione e nell'onere per la mitigazione degli attacchi DDoS.

In seguito, molte aziende colpite dagli attacchi hanno esaminato la propria gestione dei rischi rafforzando, in alcuni casi, l'integrazione dell'ISP[16] nel proprio dispositivo di protezione (p. es. mediante un abbonamento a un meccanismo di protezione DDoS).

5.1 Effetto mediatico

Il 5 giugno 2023 è stato annunciato il discorso di Volodymyr Zelensky al Parlamento svizzero il 15 giugno 2023. Questo annuncio e la decisione del Parlamento di consegnare materiale bellico ha dato il via alle attività DDoS di NoName057(16). Uno dei primi siti web attaccati è stato quello del Parlamento (parlament.ch), come segnalato il 7 giugno 2023 alle ore 15.05 dai Servizi del Parlamento tramite Twitter. Poiché lunedì 12 giugno 2023 anche altri siti web dell'Amministrazione federale non erano più accessibili, l'NCSC ha pubblicato un comunicato stampa sugli attacchi DDoS. Tale comunicazione ha avuto un ampio riscontro tra i media svizzeri. L'NCSC ha contato 50 articoli nella stampa scritta e oltre 370 articoli online.

Grazie alla vasta copertura mediatica in Svizzera, gli attacchi DDoS e il loro messaggio politico di fondo hanno raggiunto gran parte della popolazione svizzera, generando, tuttavia, anche dubbi e insicurezza tra la popolazione. In totale, il Servizio stampa dell'NCSC ha ricevuto oltre 40 richieste dai media. In questo periodo, il delegato federale alla cibersicurezza Florian Schütz è stato sotto i riflettori dei media, poiché ha rilasciato varie interviste in cui ha spiegato il significato degli attacchi DDos al fine di ridurre l'insicurezza tra la popolazione.

L'intenso interesse mediatico si è man mano affievolito dopo il videomessaggio di Volodymyr Zelensky il 15 giugno 2023, per finire praticamente nel dimenticatoio dopo gli ultimi attacchi il

[15] https://it.wikipedia.org/wiki/Sistema_autonomo

[16] https://it.wikipedia.org/wiki/Internet_service_provider

19 giugno 2023.

In vari articoli, alcuni media hanno però confuso questi attacchi con l'attacco ransomware avvenuto contemporaneamente, ma in modo indipendente, nei confronti della società Xplain. Nell'ambito della sua attività mediatica, l'NCSC ha sempre sottolineato il fatto che gli autori degli attacchi erano due raggruppamenti diversi. L'attacco alla società Xplain (un fornitore di software dell'Amministrazione federale) è stato opera del gruppo «Play», mentre l'attacco DDoS contro i Servizi del Parlamento è stato rivendicato tramite Telegram dal gruppo «NoName». Inoltre è stato sottolineato che le motivazioni degli attori dietro a un attacco ransomware (Xplain) sono fondamentalmente diverse rispetto a quelle di un attacco DDoS a sfondo politico.

5.2 **Effetto politico**

Gli attacchi DDoS non hanno provocato particolari reazioni all'interno delle Camere federali. All'interno delle rispettive Camere, il presidente del Consiglio nazionale Martin Candinas nonché la presidente del Consiglio degli Stati Brigitte Häberli-Koller, hanno menzionato gli attacchi.
Il 15 giugno 2023, la consigliera nazionale Doris Fiala ha depositato un intervento (Ip. 23.3755 «Siamo già in ciberguerra, anche a livello federale?»)[17]. Nella sua risposta, il Consiglio federale ha sottolineato il fatto che gli attacchi DDoS devono essere considerati atti di vandalismo e che hanno causato soltanto danni di lieve entità. Pertanto, devono essere chiaramente contraddistinti dai casi gravi. Inoltre, il Consiglio federale ha messo esplicitamente in guardia dal classificare tali attacchi come ciberguerra. «Classificare questi attacchi come ciberguerra risulta eccessivo rispetto ai rischi connessi e di conseguenza asseconda l'intenzione degli aggressori di diffondere insicurezza»[18].

Si parte del presupposto che il Parlamento continuerà a informarsi attivamente sulle misure della Confederazione contro i ciberattacchi in generale e, in seguito agli attacchi avvenuti, in particolare sul tema della protezione contro gli attacchi DDoS. Non si prevedono ulteriori ripercussioni politiche degli attacchi.

5.3 **Effetto giuridico**

In seguito agli attacchi DDoS al sito web del Parlamento svizzero, il Ministero pubblico della Confederazione ha aperto un procedimento.[19] L'NCSC rimanda al procedimento in corso.

5.4 **Danni effettivi**

Dopo gli attacchi DDoS, l'NCSC ha svolto un sondaggio tra le aziende prese di mira. Dai riscontri ricevuti è emerso che l'insoddisfazione dei clienti è stato il danno maggiore, poiché i siti web erano temporaneamente indisponibili. Nella maggior parte dei casi le interruzioni sono durate alcune ore, in un solo caso tre giorni, accompagnati da momenti di instabilità. Non è possibile quantificare l'eventuale danno economico. È stato confermato che l'infrastruttura TIC non ha subito danni permanenti.

Le autorità e le organizzazioni vittime degli attacchi DDoS non hanno dovuto aumentare le risorse umane, tuttavia i collaboratori hanno prestato ore supplementari.

[17] https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233755

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

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

L’NCSC non è a conoscenza di organizzazioni (p. es. una PMI) costrette a cessare l’attività a causa degli attacchi DDoS.

Gli attacchi DDoS hanno confermato che attacchi di questo genere possono colpire qualsiasi obiettivo, causando almeno brevi interruzioni. Per tale ragione, l’NCSC raccomanda di gestire un dispositivo di protezione proattivo (vedi misure di protezione al capitolo **Fehler! Verweisquelle konnte nicht gefunden werden.**).

6 Raccomandazioni

Rispetto ad attacchi complessi (p. es. «advanced persistent threat» o minacce persistenti avanzate) che mirano all'intrusione in sistemi informatici, gli attacchi DDoS risultano meno complicati dal punto di vista tecnico. Le sfide per proteggersi dagli attacchi DDoS risiedono nella scalabilità degli attacchi e nello sviluppo di nuove tecniche per aggirare i meccanismi di protezione DDoS. Misure di sicurezza solide e un approccio proattivo sono pertanto fondamentali al fine di proteggersi dalle ripercussioni degli attacchi DDoS.

L'NCSC formula diverse raccomandazioni attuabili sotto forma di misure proattive per proteggersi dagli attacchi DDoS o come misure reattive dopo il verificarsi di simili attacchi.

Misure proattive

Le seguenti misure (elenco non esaustivo) vanno implementate a seconda delle necessità come preparazione a un eventuale attacco DDoS:

Misure proattive	Descrizione / utilità	Effetto nel caso degli attacchi DDoS in questione
Verificare la rilevanza degli attacchi DDoS nella propria gestione dei rischi informatici e dell'«IT service continuity management».	Gli attacchi DDoS vengono verificati dal punto di vista della loro rilevanza nel processo di gestione dei rischi e, se necessario, inclusi come rischio.	Contro tale rischio, prima dell'attacco vengono attuate misure tecniche e organizzative adeguate.
Identificare i propri siti web potenzialmente minacciati, nel quadro di un'analisi dell'impatto sull'attività operativa («business impact analysis», BIA).	Da una BIA emergono i requisiti per la disponibilità dei siti web.	I siti web critici per l'azienda sono noti e possono essere protetti in base ai requisiti aziendali.
Coordinarsi con il proprio ISP o con il fornitore di servizi di sicurezza gestiti («managed security service provider», MSSP) in merito alle misure di protezione, al fine di garantire la disponibilità.	Le misure per il rispetto dei requisiti di disponibilità dei siti web sono concordate con il rispettivo ISP e verificate periodicamente per garantirne l'attualità.	Le misure di protezione sono concordate contrattualmente e sono disponibili in caso di un potenziale attacco.
Prendere in considerazione le misure di protezione contro gli attacchi nella propria architettura di sicurezza («security by design»).	Le misure di protezione contro gli attacchi DDoS vengono implementate già durante la progettazione dei siti web. Ad esempio, una rete di distribuzione dei contenuti («content delivery network», CDN) può contribuire a limitare le ripercussioni degli attacchi DDoS, distribuendo il traffico su vari server dislocati in tutto mondo.	Tenendo conto dei requisiti di sicurezza nell'architettura di sicurezza, si riduce al minimo la probabilità che il traffico di dati DDoS raggiunga e sovraccarichi i siti web.
Utilizzare le WAF per i siti web potenzialmente minacciati.	Le WAF sorvegliano il traffico di dati a livello di applicazione e bloccano tutte le richieste dannose prima che raggiungano il sito	Solo grazie all'esistenza di una WAF è possibile proteggere rapidamente i siti web contro gli attacchi DDoS. La configurazione delle WAF può

Misure proattive	Descrizione / utilità	Effetto nel caso degli attacchi DDoS in questione
	web.	essere adeguata a un attacco DDoS specifico.
Elaborare e testare un piano d'emergenza.	Un piano d'emergenza contiene istruzioni strutturate da applicare in caso di un attacco DDoS. Inoltre, comprende l'«IT service continuity management» e il «business continuity management», (BCM).	Un piano d'emergenza consente di reagire in modo pianificato e strutturato in caso di un attacco DDoS.

Tabella 6: Misure proattive

Misure reattive

L'NCSC raccomanda di attuare le seguenti misure a seconda delle necessità come reazione a un eventuale attacco DDoS:

Misure reattive ad attacchi DDoS	Descrizione / utilità	Effetto nel caso degli attacchi DDoS in questione
Sorvegliare i siti web esposti a un eventuale attacco DDoS e impostare un riconoscimento automatico di anomalie.	La sorveglianza del traffico di dati aiuta a riconoscere attività anomale o un aumento del traffico di rete.	Tali misure aiutano a individuare tempestivamente attacchi DDoS e a respingerli.
Garantire una reazione rapida dal punto di vista tecnico e organizzativo, in caso di un attacco DDoS.	Le misure di protezione tecniche servono in particolare per identificare e difendersi dagli attacchi DDoS. I processi di sicurezza regolano gli aspetti organizzativi (p. es. «security incident management», escalation, attività mediatica).	Una rapida implementazione di misure di protezione (p. es. blocco di indirizzi IP, adeguamenti configurativi ai meccanismi di sicurezza da parte del servizio di picchetto) consente di mitigare tempestivamente gli attacchi DDoS.
Garantire che i propri siti web siano protetti già a monte da attacchi automatizzati all'architettura di sicurezza (protezione avanzata).	L'implementazione della tecnologia CAPTCHA[20] garantisce che, ad esempio un modulo online, non possa essere compilato automaticamente.	Le misure di protezione preliminari impediscono all'attacco DDoS di accedere automaticamente ai siti web.
Bloccare gli intervalli IP e i sistemi autonomi sulla base degli indicatori di compromissione («indicators of compromise», IoC).	La base per un simile blocco è costituita dagli IoC, disponibili sul «Cyber Security Hub» dell'NCSC. Mediante il riconoscimento delle anomalie menzionato in precedenza, gli IoC possono essere identificati in modo specifico in base all'organizzazione.	In tal modo si può interrompere il traffico di dati dannoso.
Bloccare gli attacchi specifici a livello di applicazione.	Sulla base delle informazioni provenienti da più	Bloccando il client DDoSia (user agent), l'attacco DDoS può essere

[20] https://it.wikipedia.org/wiki/CAPTCHA

Misure reattive ad attacchi DDoS	Descrizione / utilità	Effetto nel caso degli attacchi DDoS in questione
	fonti (p. es. «security incident» ed «event management» [SIEM] e diversi file di log) è possibile adeguare in maniera mirata i meccanismi di sicurezza (p. es. WAF) per prevenire gli attacchi.	bloccato già con le WAF.

Tabella 7: Misure di reazione in caso di un attacco DDoS

Sul sito web dell'NCSC sono pubblicate ulteriori raccomandazioni e misure preventive da applicare (vedi capitolo 8, [3]).

7 Conclusione

Le classiche strategie di sicurezza anti DDoS, tradizionalmente orientate in particolare a contrastare gli attacchi DDoS[21] volumetrici, non sono sufficienti per proteggersi dall'attuale attore degli attacchi a livello di applicazione.

Nel presente caso, molti dei sistemi di attacco dei ciberattivisti erano identificabili tramite intervalli IP e sistemi autonomi. Per questo motivo, la maggior parte è stato possibile bloccarla in in modo mirato. Già poco tempo dopo i siti web attaccati erano quindi nuovamente disponibili. Sono state un importante meccanismo di sicurezza supplementare le WAF (se disponibili), configurate a posteriori specificatamente in base al modello di attacco.
Se in un futuro attacco DDoS i ciberattivisti partecipanti dovessero agire da punti geografici ancora più numerosi, si deve partire dal presupposto che l'entità del danno sarà maggiore. Diventerebbe più difficile identificare e bloccare tutti gli intervalli IP e/o i sistemi autonomi. Per questa ragione, in un caso simile, è probabile che i siti web subirebbero interruzioni prolungate.

Insegnamenti tratti

Dal punto di vista dell'NCSC vanno menzionati gli insegnamenti qui appresso:

- Nonostante i diffusi meccanismi di sicurezza DDoS implementati, vari attacchi dell'attore hanno avuto successo per un determinato periodo di tempo. Di conseguenza occorre verificare i dispositivi di sicurezza e adeguarli in base alle necessità.
- Gli attacchi DDoS possono avere ripercussioni anche sull'attività di terzi se viene attaccato con successo un sito web necessario per il corretto funzionamento di un altro sito web o di un processo aziendale. Una BIA funge da base per individuare tali dipendenze e per tenerne conto nella gestione della continuità operativa («business continuity management», BCM).
- Le ripercussioni di un blocco (p. es. tramite intervalli IP) sull'attività commerciale della rispettiva azienda (p. es. compromissione dell'accesso per gli utenti legittimi, siti web disciplinati per legge), vanno esaminate nel quadro di una BIA.
- Il coordinamento e lo scambio dettagliato di informazioni tra l'NCSC e le parti interessate sono stati molto importanti.
- Per la diffusione di informazioni specifiche sull'attacco (p. es. nome dell'attore) bisogna tenere conto dell'insieme dei vantaggi e degli svantaggi.
- Gli effetti di un attacco DDoS possono essere minimizzati in tempi relativamente brevi con gli abituali meccanismi di sicurezza (p. es. blocco di intervalli IP, blocchi geografici, WEF, limitazione dell'accesso), non appena i modelli di attacco sono conosciuti in maniera sufficientemente dettagliata.
- Se si possono stabilire livelli di riservatezza tra reti isolate che comunicano via Internet, è possibile utilizzare anche tecnologie più recenti come SCiON[22]. Questa tecnologia dispone di una protezione integrata da attacchi DDoS.
- L'intenso interesse mediatico ha sensibilizzato le autorità e le organizzazioni svizzere al tema degli attacchi DDoS.
- Dalle risposte al sondaggio dell'NCSC emerge che le aziende interessate rivaluteranno i rischi degli attacchi DDoS ed esamineranno le rispettive misure da adottare.

Osservazioni finali

Le organizzazioni di grandi dimensioni che dispongono, ad esempio, di un centro operativo di sicurezza («security operation center», SOC) hanno potuto reagire piuttosto rapidamente dopo

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

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

aver riconosciuto i modelli di attacco. A posteriori non è più possibile determinare in maniera definitiva se i problemi tecnici o la mancanza di processi di sicurezza abbiano provocato interruzioni prolungate (p. es. interruzione di siti web per diversi giorni).

Le rispettive aziende sono responsabili di effettuare gli adeguamenti necessari nell'ambito del processo di miglioramento continuo. L'NCSC consiglia di esaminare le misure raccomandate nel presente rapporto e di verificare gli insegnamenti tratti, al fine di attuarli sotto la propria responsabilità.

8 Allegati

Informazioni e spiegazioni sugli attacchi DDoS

L'NCSC pubblica sul proprio sito web spiegazioni e informazioni generali sugli attacchi DDoS[23].

I vari tipi di attacchi DDoS (p. es. volumetrici o di livello 7) sono illustrati nel dettaglio in un documento del Multi State Information Sharing & Analysis Center (MS-ISAC[24], in cooperazione con la US Cybersecurity & Infrastructure Security Agency CISA[25] e il Center for Internet Security CIS[26]).

Fonti informative di riferimento

Numero	Spiegazione e indirizzo URL
[1]	Il presidente ucraino Zelensky si rivolgerà ai parlamentari federali il 15 giugno, https://www.parlament.ch/press-releases/Pages/mm-info-2023-05-31.aspx
[2]	Il Consiglio degli Stati intende semplificare il trasferimento di materiale bellico svizzero, https://www.parlament.ch/de/services/news/Seiten/2023/20230607124254254194158159038_bsd093.aspx
[3]	Raccomandazioni dell'NCSC contro gli attacchi DDoS, https://www.ncsc.admin.ch/ncsc/it/home/cyberbedrohungen/ddos.html
[4]	Sekoia – informazioni dettagliate sul client DDoSia, https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

Tabella 8: Fonti informative di riferimento

Categorizzazione degli attori delle minacce e rispettive motivazioni

Per poter valutare le ripercussioni dei ciberattacchi, è innanzitutto importante determinare quali attori delle minacce eseguono gli attacchi. A loro volta, gli attori possono essere differenziati in base alla loro motivazione e classificati nelle seguenti categorie:

Attori delle minacce (threat actor)	Motivazioni
Attori statali	Gli attori statali hanno solitamente motivazioni geopolitiche. In simili casi vengono attaccate infrastrutture di rilevanza sistemica della controparte. L'obiettivo è destabilizzare la controparte e annetterla.
Organizzazioni criminali	Di solito, le organizzazioni criminali hanno intenzioni di natura finanziaria. Attraverso le loro attività fraudolente intendono estorcere denaro alle loro vittime, richiedendo un riscatto.
Hacktivisti	Gli hacktivisti vogliono attirare l'attenzione e diffondere le loro idee politiche o religiose. Attraverso mirati atti di vandalismo e operazioni d'informazione (info Ops)[27] mirano a

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

	destabilizzare le vittime e a convincerle della loro ideologia. L'obiettivo è attirare l'attenzione dell'opinione pubblica sulla loro ideologia.
Gruppi terroristici	I gruppi terroristici vogliono suscitare paura e terrore.
Fanatici del computer	I fanatici del computer vogliono ottenere un senso di potere per soddisfazione personale o per confermare le proprie competenze. Generalmente, sono anche interessati ad ottenere un certo riconoscimento in determinate cerchie.
Insider	Gli insider sono attori che, a differenza degli outsider, hanno un accesso privilegiato alla vittima (p. es. dipendenti, incaricati). Utilizzano questo accesso per causare danni o per arricchirsi indebitamente.

Tabella 9: Categorizzazione degli attori delle minacce e rispettive motivazioni

Dettagli degli attacchi DDoS a ritmo giornaliero

Data del rapporto	Titolo	Descrizione	Osservazioni
12.6.2023	Attacchi DDoS del 12 giugno 2023 da parte di NoName057(16) contro siti web svizzeri, inclusa l'Amministrazione federale	Lunedì 12 giugno 2023 alle ore 08.20, hanno avuto luogo degli attacchi DDoS da parte di NoName057(16) contro alcuni siti web dell'Amministrazione (UDSC e DFGP). L'elenco dei siti web presi di mira è stato pubblicato qualche minuto più tardi ed è il seguente: • 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 Alle ore 10.03, NoName057(16) ha rivendicato sul suo canale Telegram attacchi contro la Svizzera, indicando il sito web del Parlamento [1] con un rapporto di check-host.net datato 12 giugno 2023, ore 09.28 (UTC 07.28) [2]. Il rapporto indica che la connessione funziona solo dalla Svizzera (protezione DDoS via geofencing). NoName057(16) giustifica la sua azione con i ringraziamenti di Zelensky alla Svizzera per l'adesione al decimo pacchetto di sanzioni contro la Russia,	• Tipo di attacco: attacco di livello 7 (HTTP POST e GET flood). • Origine del traffico degli attacchi DDoS: il traffico ha origine dallo spazio IP russo e da MIRhosting (AS206932, AS52000) nonché da Stark Industries (AS44477). • Altre raccomandazioni: la mitigazione può includere anche la ricerca di anomalie nel header HTTP nonché la protezione di funzioni ad alta intensità di risorse, utilizzando un captcha. Sul suo canale Telegram, NoName ha rivendicato gli attacchi contro il DFGP (11.23), l'UDSC (12.35), fedpol (13.47), il DFI (15.00), SOB (16.04) e La Posta (17.11). I rapporti di check-host [3] sono stati generati intorno alle ore 09.30 (UTC 07.31), ad eccezione di quello di La Posta, generato alle ore 13.47 (UTC 11.47). [3] https://check-host.net/check-report/103a5159k82c https://check-host.net/check-report/103a4fdakb51 https://check-host.net/check-report/103a4edck891 https://check-host.net/check-

Data del rapporto	Titolo	Descrizione	Osservazioni
		comunicata dalla Svizzera il 29 marzo 2023. [1] www.parlament.ch [2] https://check-host.net/check-report/103a4c6aka29	report/103a53afk272 https://check-host.net/check-report/103a523fk4ec https://check-host.net/check-report/103af460ka6b
13.6.2023	Attacchi DDoS del 13 giugno 2023 da parte di NoName057(16) contro siti web svizzeri inclusa l'Amministrazione federale	Martedì 13 giugno 2023 alle ore 09.20, un nuovo elenco di obiettivi viene usato da NoName057(16) per attacchi DDoS. L'elenco è il seguente: • flyedelweiss.com • www.vtg.admin.ch • www.flughafen-zuerich.ch • peoples.ch • engadin-airport.ch • www.bernairport.ch • airport-grenchen.ch • www.gva.ch L'elenco è stato aggiornato alle ore 11.10, con l'aggiunta dei seguenti nuovi obiettivi: • www.swisshelicopter.ch • zimex.com • www.pc7-team.ch	Sul suo canale Telegram, NoName ha rivendicato gli attacchi contro vtg.admin.ch (10.03), bernairport.ch (11.12), airport-grenchen.ch (12.27), gva.ch (13.34), engadin-airport.ch (14.47), peoples.ch (aérodrome St-Gall, 15.58), www.swisshelicopter.ch (16.19), zimex.com (17.27), www.pc7-team.ch (18.01). I rapporti di check-host [1] sono stati generati verso le ore 09.30 (UTC 07.30), ad eccezione di quelli di www.swisshelicopter.ch, zimex.com e www.pc7-team.ch che sono stati generati verso le ore 11.10 (UTC 09.10) Un'analisi del canale Telegram di NoName057(16) ha rivelato che alcuni commenti pubblicati da follower dopo gli attacchi del 12 giugno 2023, sono legati alla Svizzera e quindi aumentano il rischio per le organizzazioni menzionate di essere l'obiettivo di attacchi futuri: I Cantoni interessati sono stati avvisati attraverso questi commenti (ore 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-report/103d87c3k56c https://check-host.net/check-report/103dc68ek21e

Data del rapporto	Titolo	Descrizione	Osservazioni
			https://check-host.net/check-report/103dc78ak788 https://check-host.net/check-report/103dc833k3f3
14.6.2023	Attacchi DDoS del 14 giugno 2023 da parte di NoName057(16) contro siti web svizzeri	Mercoledì 14 giugno 2023 alle ore 08.00, NoName057(16) utilizza un nuovo elenco di obiettivi per attacchi DDoS. L'elenco è il seguente: • www.geneve.com L'elenco è stato aggiornato alle ore 8.20, con l'aggiunta dei seguenti nuovi obiettivi: • www.stadt-zuerich.ch • www.bs.ch • ekonto.egov.bs.ch • www.lausanne.ch • www.stadt.sg.ch E alle ore 11.15, con i seguenti obiettivi: • www.stadt.sg.ch • www.montreux.ch • www.bellinzona.ch • www.stadt-schaffhausen.ch Va notato che il sito web www.geneve.com corrisponde al sito turistico di Ginevra e non al sito web ufficiale della Città/Repubblica di Ginevra che invece è www.ge.ch	Sul suo canale Telegram, NoName ha rivendicato gli attacchi contro 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) e www.bellinzona.ch (16.02). I rapporti di check-host [1] sono stati generati verso le ore 09.30 (UTC 07.30), ad eccezione di quelli dei siti web www.stadt-schaffhausen.ch, www.lausanne.ch, www.montreux.ch, www.stadt.sg.ch e www.bellinzona.ch, generati verso le ore 10.50 (UTC: 08.50) Nella sua pubblicazione sull'attacco contro www.geneve.com, NoName057(16) fa riferimento al discorso del Presidente Zelensky all'Assemblea federale in videoconferenza, previsto per il 15 giugno 2023. [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-report/1040e788k29 https://check-host.net/check-

Data del rapporto	Titolo	Descrizione	Osservazioni
			report/1040e84ck7ed
15.6.2023	Attacchi DDoS del 15 giugno 2023 da parte di NoName057(16) contro siti web svizzeri	Giovedì 15 giugno 2023 alle ore 08.00, NoName057(16) utilizza un nuovo elenco di obiettivi per attacchi DDoS. L'elenco è il seguente: • 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	Sul suo canale Telegram, NoName ha rivendicato gli attacchi contro 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). I rapporti di check-host [1] sono stati generati verso le ore 09.15 (UTC 07.15). [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
16.6.2023	Attacchi DDoS del 16 giugno 2023 da parte di NoName057(16) contro siti web svizzeri	Venerdì 16 giugno 2023 alle ore 09.20, NoName057(16) utilizza un nuovo elenco di obiettivi per attacchi DDoS. L'elenco è il seguente: • 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 Alle ore 10.00 è stato aggiunto un sito web all'elenco:	Sul suo canale Telegram, NoName ha rivendicato gli attacchi contro 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). Il sito www.autofaehre.ch non figura nell'elenco degli obiettivi attaccati da BotNet di NoName057(16) e il sito web attualmente è accessibile (ore 15.00). È piuttosto probabile che si tratti di un errore di comunicazione di

Data del rapporto	Titolo	Descrizione	Osservazioni
		• www.vsz.ch	NoName05716. I rapporti di check-host sono stati generati verso le ore 09.15 (UTC 07.15).
18.6.2023	Attacchi DDoS del 17–18 giugno 2023 da parte di NoName057(16) contro siti web svizzeri	Sabato 17 giugno 2023 alle ore 09.20, NoName057(16) utilizza un nuovo elenco di obiettivi per attacchi DDoS. L'elenco è il seguente: • 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 Alle ore 10.30 è stato aggiunto un sito web all'elenco: • www.edi.admin.ch Alle ore 14.00 sono stati aggiunti i seguenti siti web all'elenco: • www.vtg.admin.ch • www.swisshelicopter.ch • www.zimex.com • www.heliswissinternational.com • www.pc7-team.ch Domenica 18 giugno 2023 alle ore 10.45, NoName057(16) utilizza un nuovo elenco di obiettivi per attacchi DDoS. L'elenco è il seguente: • 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 Alle ore 15.15 sono stati aggiunti i seguenti siti web all'elenco:	La maggior parte dei siti web presi di mira sabato e domenica erano già stati attaccati la settimana precedente. Sul suo canale Telegram, sabato 17 giugno 2023 NoName057(16) ha rivendicato gli attacchi contro 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) e www.pc7-team.ch (19.47). I rapporti di check-host sono stati generati tra le ore 09.30–10.00 (UTC 07.30-08.00), ad eccezione di quelli di gva.ch, vtg.admin.ch, www.swissprivatebankers.com, www.swisshelicopter.ch, www.zimex.com e www.pc7-team.ch generati verso le ore 14.00 (UTC 12.00). Sul suo canale Telegram, domenica 18 giugno 2023 NoName057(16) ha rivendicato gli attacchi contro 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) e www.zvv.ch (18.34) I rapporti di check-host sono stati generati tra le ore 09.30–10.00 (UTC 07.30-08.00), ad eccezione di quelli di www.swissprivatebankers.com e www.zvv.ch verso le 14.30 (12.30 UTC).

Data del rapporto	Titolo	Descrizione	Osservazioni
		• www.juliusbaer.com • sasd.ch • www.swissprivateban-kers.com • www.zvv.ch • www.myswitzer-land.com	

Tabella 10: Segnalazioni DDoS giornaliere con aggiunte dal 12 giugno 2023 fino al 18 giugno 2023