DDoS

Preparazione e risposta agli attacchi Denial of Service

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, anche attuando il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza, promuovendone azioni comuni.

L'Agenzia è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. In tale veste ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico del Paese promuovendo la realizzazione di azioni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese. A tal fine sviluppa anche capacità necessarie per proteggere dalle minacce informatiche reti, sistemi informativi e servizi informatici delle Pubbliche Amministrazioni e degli operatori di infrastrutture critiche nazionali, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Siti web: **Agenzia per la Cybersicurezza Nazionale** **CSIRT Italia**

Contatti: **info@acn.gov.it**

Seguici sui nostri canali social:

Esclusione di responsabilità

Il presente documento fornisce, a titolo esemplificativo e non esaustivo, indicazioni di mero ausilio alle attività di sicurezza dell'Organizzazione e non solleva la stessa dall'onere di porre in essere, nel rispetto della normativa vigente in materia di cybersicurezza, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici.

SOMMARIO

EXECUTIVE SUMMARY

Il Denial of Service (DoS) identifica gli eventi cyber in cui un attore malevolo effettua un attacco per compromettere la disponibilità di un bene informatico o di un servizio mediante l'esaurimento delle sue risorse di rete, di elaborazione o di memoria necessarie per accedervi. Una specifica tecnica di attacco, largamente utilizzata e conosciuta come **Distributed Denial of Service (DDoS),** prevede l'utilizzo di un elevato numero di sorgenti di traffico multiple e distribuite.

Modello semplificato

Per comprendere e prevenire meglio la minaccia, può essere utile un *modello semplificato* che rappresenta l'infrastruttura generica di un soggetto che intende:

- Fornire a utenti esterni l'accesso a servizi interni.
- Accedere a servizi di sistemi esterni tramite Internet .

Rischi

Ogni infrastruttura connessa a Internet è potenzialmente esposta ad attacchi DDoS e dunque a rischio di:

- Discontinuità/degradamento
- Isolamento inconsapevole

Coinvolgimento

Si può risultare coinvolti in un attacco DDoS tramite:

- Coinvolgimento diretto
- Coinvolgimento indiretto
- Ripercussione di eventi esterni

Tipologie di attacco

Sulla base delle risorse su cui si generano gli impatti, possono essere individuate le seguenti tipologie di attacco:

- Volumetrico
- Esaurimento di stato
- Applicativo
- *Malformed packet*

Raccomandazioni e contromisure

Proteggere i propri asset dalla minaccia DDoS richiede **l'adozione di misure preventive**. Le raccomandazioni e le contromisure proposte sono articolate in tre tipologie.

Processi e strategie

Raccomandazioni relative alla preparazione di piani di risposta, alla formazione del personale e alla selezione e collaborazione con i partner tecnologici.

Soluzioni di sicurezza

Raccomandazioni relative alle soluzioni tecnologiche da adottare per migliorare le capacità di prevenzione e gestione della minaccia.

Controlli di sicurezza

Raccomandazioni relative alla necessità di implementare strategie, processi e soluzioni tecnologiche per la prevenzione e reazione agli attacchi.

1 DDoS LANDSCAPE

Il presente capitolo fornisce una definizione della minaccia **Denial of Service** (DoS) e **Distributed Denial of Service** (DDoS), introducendo un'analisi degli asset coinvolti in tali attacchi: servizi di connettività, infrastruttura di rete e di sicurezza, e risorse applicative. Nel seguito viene fornito un **modello di riferimento** necessario a supportare le organizzazioni nel comprendere gli effetti della minaccia sugli asset impattati, poiché ogni soggetto che espone servizi su Internet o che utilizza per le proprie attività servizi esposti da altri, costituisce un potenziale target.

Sulla base di tale modello di riferimento, il capitolo si conclude con un'analisi approfondita delle **ripercussioni potenziali** derivanti dagli attacchi DoS/DDoS.

Le definizioni incluse in questo documento sono in linea con quelle fornite dalla Tassonomia Cyber dell'ACN. In caso di necessità, la Guida alla notifica degli incidenti al CSIRT Italia fornisce indicazioni relative alle modalità di notifica previste.

1.1 Introduzione e definizione

Il termine **Denial of Service (DoS)** identifica gli eventi cyber in cui un attore malevolo effettua un attacco per **compromettere la disponibilità di un bene informatico o di un servizio** mediante l'esaurimento delle sue risorse di rete, di elaborazione o di memoria necessarie per accedervi. Una specifica tecnica di attacco, largamente utilizzata e conosciuta come **Distributed Denial of Service (DDoS)**, prevede l'utilizzo di un elevato numero di **sorgenti di traffico multiple e distribuite**, tale da rendere più difficile la conseguente mitigazione manuale dell'evento.

Nel corso del documento, essendo la tipologia di attacco più ampiamente diffusa, il termine DDoS verrà utilizzato come sinonimo anche del più generico DoS.

Tutte le infrastrutture connesse a Internet possono essere oggetto di attacchi DDoS e il conseguente impatto sulla **disponibilità** dei servizi erogati sarà fortemente dipendente dalle soluzioni di mitigazione e dalle ottimizzazioni preventivamente adottate.

Le **motivazioni** associate agli attacchi DDoS variano a seconda dello scopo perseguito dagli attaccanti e possono essere tipicamente categorizzate come segue:

- **economiche**: rientrano in tale classe le azioni finalizzate all'ottenimento di guadagni finanziari attraverso, ad esempio, l'estorsione di denaro in cambio della cessazione di fermi prolungati nell'erogazione di servizi online, così come azioni volte a sabotare le operazioni di concorrenti;
- **ideologiche**: rientrano in tale categoria, ad esempio, attacchi volti a promuovere un'agenda politica o principi di connotazione sociale, azioni caratteristiche del ben noto fenomeno dell'"hackivismo". In questo caso, gli attori malevoli possono attaccare siti web per compromettere l'erogazione di servizi o alterare i contenuti (in inglese, 'defacement') di portali di rappresentanza o istituzionali, al fine amplificare la diffusione di messaggi di natura politica o ideologica nonché provocare ingenti **danni reputazionali** al soggetto attaccato. Di questa natura sono sovente anche gli attacchi DDoS utilizzati **nel contesto delle guerre asimmetriche e delle operazioni ibride** e finalizzati al danneggiamento o la compromissione di servizi essenziali della parte avversa;
- **personali**: vendetta, dimostrazione di abilità tecnica del singolo o di un gruppo e ricerca di notorietà, sono aspetti legati a questa categoria. Tali azioni sono solitamente finalizzate ad accreditarsi a comunità online o a consolidare il proprio status all'interno dell'ecosistema cybercriminale.

È importante rilevare che gli attacchi DDoS possono anche essere utilizzati come **diversivo per mascherare** ulteriori **azioni malevole di maggiore pericolosità e impatto**, distogliendo l'attenzione della vittima e facilitando intrusioni o accessi non autorizzati realizzati tramite altre tecniche. Infine, è utile richiamare l'attenzione sulla possibilità di poter diventare partecipanti inconsapevoli di un attacco DDoS lanciato verso una terza parte, ad esempio attraverso l'utilizzo di botnet, di cui si parlerà in seguito.

1.2 Modello di riferimento

Per chiarire su quali elementi può insistere un attacco DDoS e come prevenirne o mitigarne gli effetti, si fornisce di seguito un **modello semplificato di riferimento** che definisce gli **asset** maggiormente coinvolti da tali attacchi. Nel corso dell'intero documento, il modello rappresenterà un quadro concettuale in base al quale sistematizzare le informazioni illustrate.

Il modello di riferimento rappresenta i **moduli** da cui è composta un'infrastruttura generica di un soggetto che intende:

- fornire a utenti esterni l'accesso a **servizi interni** (es. sito Internet istituzionale ospitato all'interno della propria infrastruttura);
- accedere a servizi di **sistemi esterni** tramite Internet (es. accedere alla propria posta ospitata in cloud o a siti di altri soggetti).

In entrambi i casi si ha la necessità di garantire l'accessibilità di **servizi remoti** passando per sistemi che hanno **risorse limitate e condivise**. Il dimensionamento e l'ottimizzazione degli apparati deve tenere conto dell'utilizzo e della criticità del servizio al quale accedere, considerando l'impatto che potrebbe derivare dall'inaccessibilità anche parziale dei servizi.

In Figura 4 è raffigurato il modello di riferimento; esso risulta composto da **tre asset principali** per i quali vengono di seguito fornite le definizioni e delle indicazioni di carattere generale.

Figura 1: Asset "servizi di connettività"

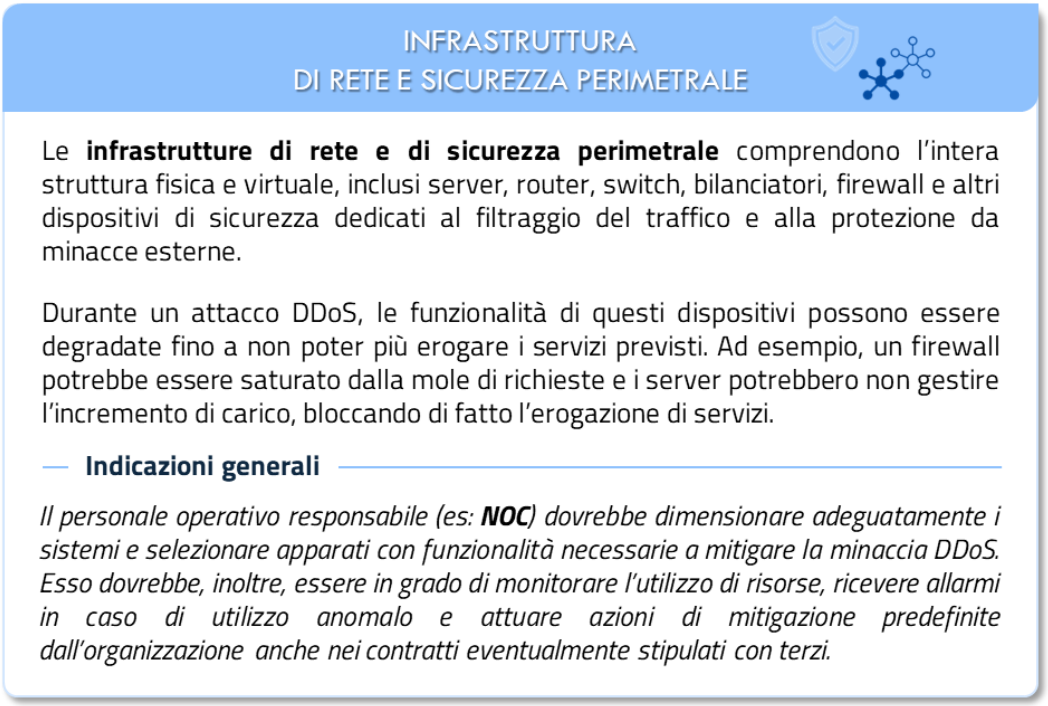

Figura 2: Asset "infrastrutture di rete e di sicurezza perimetrale"

Figura 3: Asset "risorse applicative"

Gli attacchi DDoS provocano un **sovraccarico eccessivo delle risorse sopra descritte** e rappresentate in Figura 4, superando la loro capacità operativa e compromettendo potenzialmente l'accessibilità e la disponibilità dei servizi erogati. Per ognuno degli asset identificati esistono tecniche di attacco DDoS che verranno analizzate nei successivi capitoli congiuntamente alle relative contromisure specifiche.

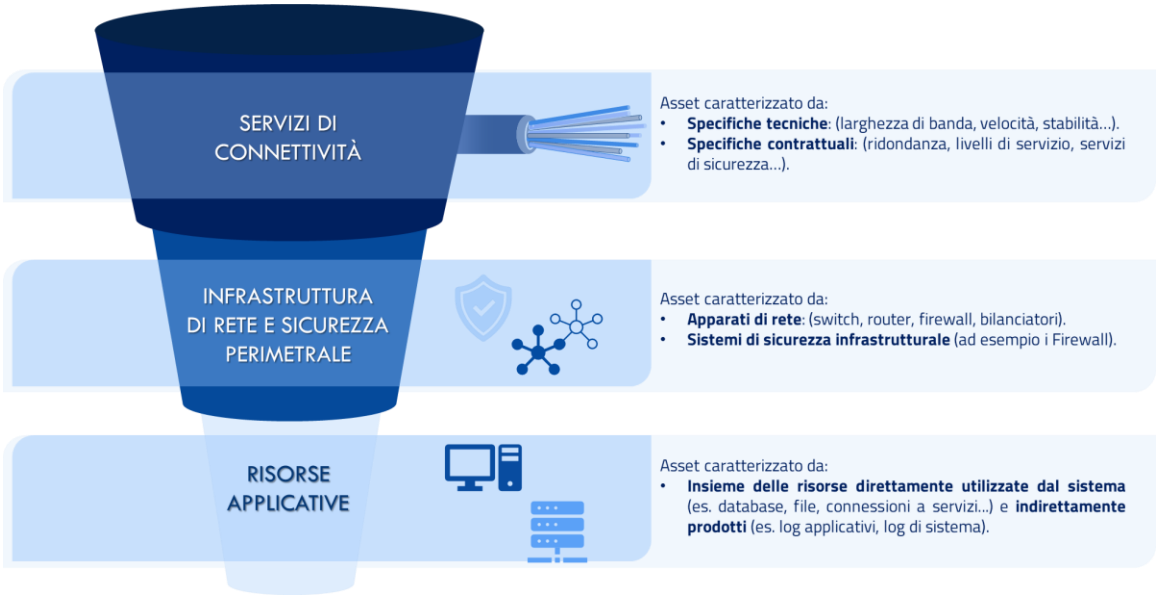

Figura 4: Modello semplificato di infrastruttura: asset di maggiore interesse

1.3 Rischi e ripercussioni dei DDoS

Ogni infrastruttura connessa a Internet è potenzialmente esposta ad attacchi DDoS e dunque principalmente esposta al rischio di:

Discontinuità/degradamento della fruizione dei servizi erogati e acceduti

L'uso eccessivo delle risorse indicate nel modello di riferimento, ovvero servizi di connettività, infrastrutture di rete e sicurezza perimetrale e risorse applicative, generalmente porta all'interruzione dei servizi (es. siti web) e all'impossibilità di accedere a servizi esterni (es. posta elettronica).

Isolamento inconsapevole da sistemi esterni

In molti casi, chi non dispone di adeguate soluzioni di sicurezza, blocca selettivamente il traffico dagli indirizzi che contribuiscono maggiormente a un attacco DDoS. Gli attaccanti, consapevoli di questa risposta, utilizzano tecniche di spoofing e riflessione per ingannare i team di sicurezza, portandoli a bloccare inconsapevolmente servizi esterni essenziali come DNS, posta elettronica, CDN e servizi cloud.

Il **coinvolgimento** delle vittime durante un attacco DDoS può variare a seconda del target identificato dagli attori malevoli, per cui si può distinguere tra un coinvolgimento diretto o indiretto del soggetto e ripercussioni di eventi esterni.

Per **coinvolgimento diretto** si intendono quei casi in cui l'infrastruttura di pertinenza di un'organizzazione è il vero e proprio target dell'attacco DDoS. In questo caso, si hanno precise evidenze, quali ad esempio rallentamento o allarmi dei sistemi Anti-DDoS.

Il soggetto è coinvolto direttamente perché è l'obiettivo dell'attacco (es: DDoS rivolto verso il soggetto).

Per **coinvolgimento indiretto** si intendono quei casi in cui alcuni servizi di un soggetto target vengono sfruttati da un attaccante al fine di convogliare traffico indesiderato verso l'infrastruttura di un secondo soggetto. In questo caso, sul primo soggetto si potrebbero non avere evidenze significative, quanto piuttosto implicazioni a livello reputazionale o legale.

Pur non essendo l'obiettivo principale dell'attacco, una risorsa di un soggetto viene coinvolta e sfruttata per colpire un altro bersaglio (es: reflection o generazione di traffico massiccio proveniente da sistemi coinvolti anche inconsapevolmente).

Per **ripercussione di eventi esterni** si intendono quei casi in cui l'attacco non riguarda direttamente o indirettamente l'infrastruttura di pertinenza di un soggetto, ma i suoi effetti si riflettono sulla stessa provocando isolamento o impedendo il traffico da e verso servizi e/o sistemi esterni.

Anche se né il soggetto né le sue risorse vengono direttamente attaccati o sfruttati, l'impatto dell'attacco si verifica su una risorsa esterna che, bloccandosi, provoca effetti collaterali sul soggetto stesso (es: interruzione di un provider di servizi).

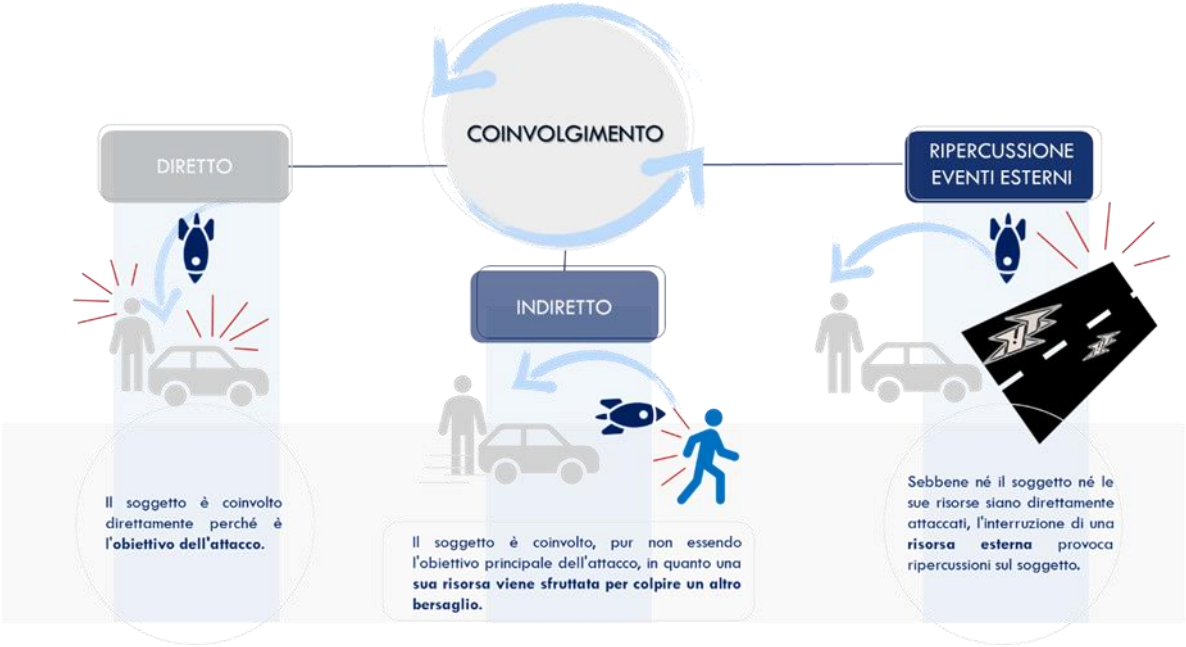

Figura 5: Tipi di coinvolgimento e la loro ripercussione sulle risorse

Viste le tipologie di coinvolgimento di un'organizzazione durante un attacco DDoS, è importante comprendere le sue **ripercussioni** sui soggetti nel caso in cui non vengano predisposte soluzioni adeguate alla gestione di tali attacchi. Per questo motivo, si fornisce di seguito una sintesi delle principali ripercussioni sulle organizzazioni derivanti dall'impossibilità di fornire servizi a utenti e sistemi esterni, così come di permettere agli utenti e servizi interni l'accesso a servizi esterni.

Ripercussioni derivanti dall'impossibilità di fornire servizi a utenti e sistemi esterni

- **Interruzione di pubblici servizi:**
  - *erogazione di servizi essenziali al cittadino*: come, ad esempio, Identità Digitale (SPID), Posta Elettronica Certificata (PEC), portali di servizi fiscali e previdenziali, servizi di e-government, servizi di emergenza, pagamento online e pubblica sicurezza.
- **Perdita di ricavi:**
  - *e-commerce e transazioni online*: i clienti non hanno la possibilità di completare acquisti o transazioni, comportando una perdita economica immediata;
  - *servizi in abbonamento*: l'inaccessibilità dei servizi può causare disdette o richieste di rimborsi, con conseguente perdita di ricavi.
- **Danni reputazionali:**
  - *fiducia dei cittadini/clienti*: i fruitori insoddisfatti potrebbero perdere fiducia nell'affidabilità del servizio e valutare azioni legali o il passaggio ad un competitor di settore;

- *recensioni negative*: gli utenti insoddisfatti possono lasciare recensioni negative online, influenzando negativamente l'immagine pubblica dell'organizzazione.

- **Impatto sulla fiducia degli investitori:**
  - *valore delle azioni*: gli investitori potrebbero percepire l'azienda come meno sicura e affidabile, portando a un calo del valore delle azioni;
  - *attrattività per investimenti futuri*: l'incapacità di garantire la continuità dei servizi può ridurre l'attrattività dell'azienda per futuri investimenti.

Ripercussioni derivanti dall'impossibilità di accesso a servizi esterni per utenti e servizi interni

- **Interruzione di pubblici servizi:**
  - *impossibilità di accesso*: le organizzazioni preposte all'erogazione di servizi pubblici non possono accedere agli strumenti e alle risorse online necessarie a fornire tali servizi alla collettività e per espletare le attività di competenza.
- **Interruzione delle operazioni aziendali:**
  - *servizi critici*: l'impossibilità di accedere a servizi esterni essenziali per l'operatività dell'azienda può interrompere le operazioni aziendali critiche, causando inefficienze e ritardi;
  - *collaborazione e comunicazione*: l'impossibilità di utilizzare strumenti di comunicazione e collaborazione esterni può rallentare i flussi di lavoro e la cooperazione tra i team.
- **Riduzione della produttività:**
  - *impossibilità di accesso*: i dipendenti non possono accedere agli strumenti e alle risorse online necessarie per il loro lavoro, riducendo la produttività complessiva;
  - *interruzioni nei processi aziendali*: le interruzioni nei servizi esterni possono causare ritardi significativi nei processi aziendali interni, con impatti a cascata su altre attività operative.

ATTACK STRATEGIES 2

Il presente capitolo esplora le strategie di attacco DDoS, focalizzandosi sulle **tipologie** e sulle **tecniche e tattiche** maggiormente utilizzate dagli attori malevoli. Attraverso un'analisi delle **metodologie** impiegate, il capitolo mira a fornire ai professionisti della sicurezza informatica conoscenze fondamentali al fine di sviluppare e implementare **strategie di difesa efficaci** contro una minaccia in continua evoluzione come quella DDoS. A tal fine, sulla base del modello di riferimento precedentemente illustrato, il capitolo si conclude con un'esposizione degli **effetti** di ciascuna tipologia di attacco in relazione agli asset coinvolti.

2.1 Tipologie di attacco

Un attacco DDoS può assumere diverse connotazioni sulla base delle risorse su cui si generano gli impatti. Per ognuna delle diverse **tipologie di attacco DDoS** qui identificate verranno fornite delle descrizioni e dei casi di esempio.

2.1.1 Attacco volumetrico

Volumetrico	Questo attacco mira al consumo della disponibilità di banda di rete dell'infrastruttura target.
Descrizione	Gli attacchi volumetrici puntano a consumare la banda di rete destinata alla fruizione di un servizio target (attacco frontale) o di uno dei servizi accessori essenziali al suo raggiungimento (attacco laterale). Essi, quindi, negano l'accesso al servizio target da parte degli utilizzatori legittimi generando traffico indesiderato di volume pari o superiore alla banda di rete a disposizione del servizio target.
Metriche	**bps** (bits per second): misura la quantità totale di dati inviati al bersaglio per saturare la larghezza di banda.
Esempi	**UDP Flood**: questo attacco consiste nell'inoltro di un'ingente quantità di pacchetti UDP verso il target. Tali richieste possono

	essere inviate a porte casuali; in tal caso, oltre a consumare banda (obiettivo primario di un attacco volumetrico), si obbliga il server ricevente, o gli apparati di sicurezza, a cercare un'applicazione in ascolto su quelle porte o la corretta destinazione del pacchetto, comportando così ulteriori danni a causa dell'incremento del consumo di risorse. **DNS Amplification Attack**: questo attacco consiste nell'invio di piccole richieste a un server DNS su protocollo UDP, falsificando l'indirizzo IP sorgente con quello della vittima (spoofing). I server DNS reagiscono con risposte molto più grandi, inviate direttamente al target, sovraccaricandolo con un enorme volume di traffico. **DNS Flood (open recursive resolver)**: questo attacco consiste nell'inoltro di una grande quantità di richieste DNS verso il target usando un DNS Server con opzione **open recursive resolver**. Questo particolare tipo di DNS Flood viene citato per porre l'attenzione sui rischi in cui incorrono le organizzazioni che espongono server DNS Open Resolver su Internet. L'attacco consiste nel richiedere a server DNS Open Resolver la risoluzione di query DNS complesse, questi le risolveranno ricorsivamente e inoltreranno verso il server DNS autoritativo (vero target dell'attacco) tutte le richieste necessarie. In questo contesto i proprietari dei server DNS Open Resolver prendono inconsapevolmente parte all'attacco. Una organizzazione che dovesse esporre su Internet server Open Resolver, oltre ad un consumo di risorse inutile e spesso al di sopra di quanto originariamente previsto, si espone a potenziali ripercussioni legali.

2.1.2 Attacco esaurimento di stato

Esaurimento di stato	Questo attacco mira al consumo delle risorse di calcolo e/o di memoria dei dispositivi destinate alla gestione dello stato delle connessioni.
Descrizione	Alcuni dispositivi, come firewall, bilanciatori e Intrusion Protection System (IPS) impiegano, per erogare le loro funzionalità, tabelle in cui conservano lo stato delle connessioni

	che stanno gestendo. L'attacco, generando un volume eccessivo di connessioni incomplete o malformate, porta ad esaurire le risorse destinate a queste tabelle. L'impossibilità per il dispositivo di accettare nuove connessioni legittime causa un'interruzione del servizio.
Metriche	**rps** (requests per second): misura il numero di richieste al secondo inviate al target.
Esempi	**TCP SYN Flood:** questo attacco sfrutta il processo di handshake TCP[1] per sovraccaricare le tabelle di stato con richieste incompiute. Nello specifico, esso consiste nell'inoltro di molteplici richieste di "inizializzazione" della connessione TCP alle quali poi non verrà dato seguito; ogni richiesta TCP SYN occuperà uno spazio nelle tabelle di stato dei dispositivi coinvolti che non verrà cancellata fino allo scadere di un timeout. Se vengono inoltrate più richieste contemporanee il dispositivo potrebbe non avere sufficiente spazio per trattare le richieste di connessione lecite. **DNS Query/NXDOMAIN Flooding**: questo attacco sovraccarica un server DNS di richieste per domini inesistenti, in modo da consumare le risorse necessarie, durante l'espletamento della ricerca di ogni dominio richiesto per confermarne l'inesistenza, per mantenere lo stato. In entrambi i casi pur essendo spesso le connessioni dirette ad applicazione/servizio, gli stati sono mantenuti e gestiti da apparati posizionati, per protezione (es: firewall o IPS) o bilanciamento di carico, sul percorso della comunicazione; la saturazione di risorse per la conservazione degli stati si genera dunque su questi apparati.

[1] Processo in cui due computer si "presentano" e stabiliscono una connessione prima di scambiarsi dati. Avviene in tre fasi: il primo computer "dichiara di voler aprire una connessione" (SYNc), il secondo conferma di "aver ricevuto, di essere disponibile e pronto" (SYNc ACKnoledge) e il primo "conferma l'avvio della comunicazione" (ACKcnowledge).

2.1.3 Attacco applicativo

Applicativo	Mira al consumo delle risorse necessarie all'esecuzione dei software applicativi.
Descrizione	L'attacco è finalizzato a esaurire le risorse necessarie al corretto funzionamento delle **applicazioni software** o degli elementi dell'ambiente software (indicato anche come **service container**) su cui l'applicazione è in esecuzione (es: sistema operativo, web server, data base, sistemi di virtualizzazione, etc…). Il progressivo aumento delle risorse utilizzate causa generalmente prima un degrado del servizio e, infine, il blocco totale. Questa tipologia di attacco può essere realizzata, ad esempio, inviando richieste che per l'applicazione risultano particolarmente onerose da elaborare o aprendo più connessioni simultanee che operano e interagiscono con l'applicazione in maniera intenzionalmente estremamente lenta. È possibile che attacchi del genere possano generare un tale numero di log da renderne difficile l'analisi. Per questo motivo gli attaccanti potrebbero condurre attacchi DDoS applicativi al fine di mascherare e rendere più difficile il rilevamento di attacchi volti alla compromissione del servizio target attraverso altre tecniche.
Metriche	**rps** (*requests per second*): misura il numero di richieste al secondo inviate al bersaglio per sovraccaricare le risorse applicative. **ast** (*average session time*): misura la durata media di una sessione e cresce (o arriva al timeout massimo impostato) quando l'applicazione viene impegnata con sessioni intenzionalmente estremamente lente.
Esempi	**Slowloris:** questo attacco consiste nell'inizializzazione di connessioni HTTP che vengono tenute aperte per un periodo prolungato al fine di consumare gradualmente le risorse del web server fino ad esaurire tutte quelle disponibili per l'erogazione del servizio. **Slow POST:** questo attacco consiste nel lento invio di richieste

	HTTP POST al server, saturando così le risorse di memoria o di elaborazione, impedendo al server di gestire ulteriori richieste. **Slow Read:** questo attacco consiste nella lettura molto lenta delle risposte del server a richieste HTTP GET, sovraccaricando così le risorse di rete e di calcolo e causando rallentamenti o blocchi.

2.1.4 Attacco *malformed packet*

Malformed packet	Questo attacco mira allo sfruttamento di vulnerabilità dei sistemi necessari ad accedere a un servizio. Per raggiungere questo obiettivo, un singolo pacchetto IP o una breve sequenza, se appositamente artefatti, possono bloccare un sistema vulnerabile.
Descrizione	Gli attacchi *malformed packet* sfruttano la presenza di vulnerabilità software che, se non sanate, possono essere sfruttate dagli attaccanti per causare comportamenti imprevisti, come crash, riavvii o blocchi dei sistemi, delle applicazioni o dispositivi.
Metriche	***Non applicabile*** - le metriche di volume e frequenza del traffico non sono rilevanti per l'attacco *malformed packet*, poiché in questo tipo di attacco rientrano casistiche per cui anche un singolo pacchetto può causare danni al sistema target.
Esempi	**Ping of Death**: questo attacco consiste nell'invio di un pacchetto ICMP Echo Request (ping) con dimensioni superiori a quelle consentite dallo standard comportando la frammentazione in più pacchetti IP. Quando il sistema vulnerabile tenta di riassemblare il pacchetto frammentato esso può andare in crash o avere comportamenti imprevisti sul funzionamento del sistema. **Vulnerabilità specifica (CVE)**: questo attacco consiste nell'utilizzo di richieste artefatte al fine di sfruttare vulnerabilità e provocare comportamenti indesiderati quali risposte anomale da parte del dispositivo, rallentamenti, riavvi, blocchi o in alcuni casi lo spegnimento dello stesso.

2.2 Tecniche e tattiche di attacco

Per perpetrare attacchi DDoS, gli attori malevoli ricorrono a differenti tecniche volte ad assicurarsi un determinato vantaggio. Di seguito vengono elencate alcune delle **principali tecniche** utilizzate.

2.2.1 Dislocazione delle sorgenti di traffico

La tecnica più nota è quella della "**dislocazione**", il DDoS è in effetti un attacco DoS proveniente da sorgenti opportunamente dislocate, che consiste nel compiere un attacco coordinato a partire da **più punti della rete Internet,** possibilmente **distribuiti in più zone geografiche, più AS (Autonomous System)[2] e più ISP (Internet Service Provider)**. Questa tecnica, comunemente utilizzata dagli attaccanti, rende più difficile implementare una risposta agli incidenti in assenza di apparati dotati di specifiche funzionalità Anti-DDoS. Difatti, in questo caso, il traffico indesiderato proviene da un considerevole numero di sorgenti diverse che, in genere, cambiano durante l'attacco, rendendo difficile e spesso inutile, se non addirittura deleterio, effettuare un blocco selettivo.

Non è raro che il traffico sia solo **apparentemente** dislocato e che sia invece proveniente da un dispositivo (o da pochi dispositivi) che falsifica l'indirizzo IP sorgente (c.d. tecnica di spoofing). Questa eventualità risulta particolarmente insidiosa in quanto potrebbe indurre al blocco di sorgenti di traffico lecite assolutamente estranee all'attacco e potenzialmente necessarie ad espletare funzioni primarie.

Tra gli esempi di DDoS in cui è stata utilizzata la tecnica di dislocazione è certamente significativo quello gestito da Google[3] nel 2022, caratterizzato da traffico proveniente da più di 5.000 sorgenti diverse localizzate in 132 nazioni.

Una rappresentazione grafica della presente tecnica è illustrata in Figura 6.

[2] Un Autonomous System (AS) su Internet è una rete o un gruppo di reti gestite da un'unica organizzazione con un proprio set di regole per instradare il traffico dati.

[3] How Google Cloud blocked largest Layer 7 DDoS attack yet, 46 million rps - Google Cloud Blog, 2022

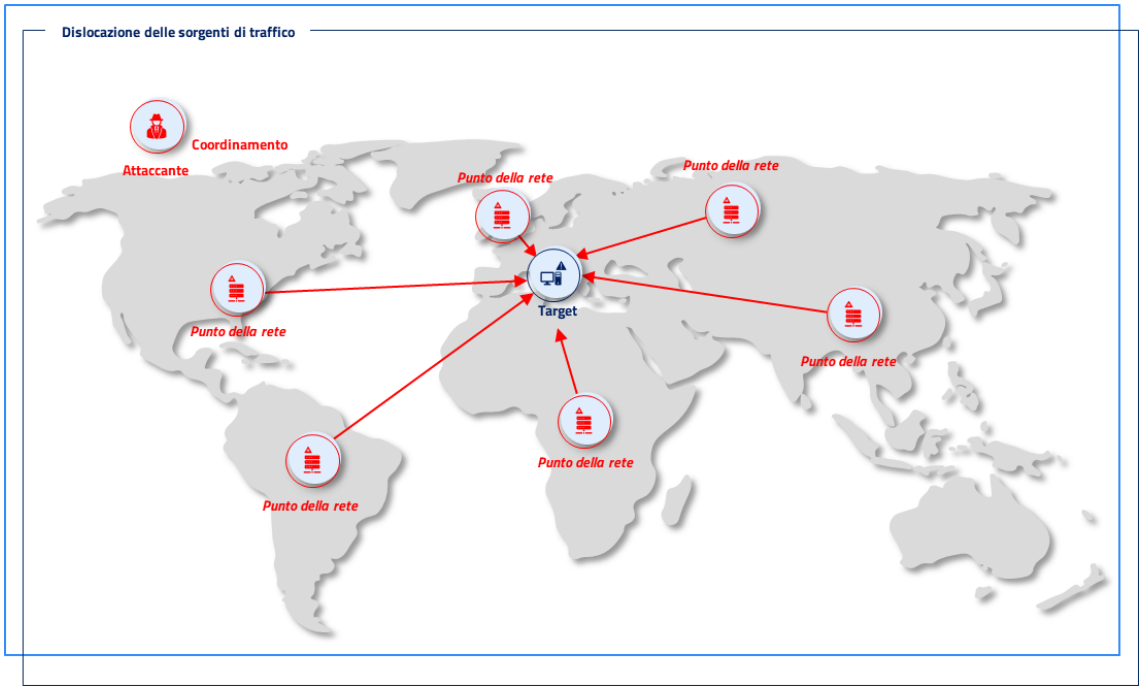

Figura 6: Rappresentazione schematica della tecnica "Dislocazione delle sorgenti di traffico"

2.2.2 Riflessione

La **riflessione** è una tecnica che consiste nello sfruttamento delle risorse di un server "terzo" per inoltrare traffico indesiderato a un target. Tale **obiettivo** può essere ottenuto, ad esempio tramite:

- tecniche di falsificazione dell'indirizzo mittente (spoofing) che inducono il servizio terzo a inoltrare una risposta al falso indirizzo (il target);
- utilizzo di servizi che richiedono l'accesso a risorse esterne (i target dell'attacco) al fine di completare la richiesta.

Tra gli esempi tipici di riflessione della prima tipologia (spoofing) ricadono quelli in cui l'attaccante, fingendosi la vittima, rivolge una richiesta ad un servizio esposto su Internet, come ad esempio server DNS (*Domain Name System*), NTP (*Network Time Protocol*) o SSDP (*Simple Service Discovery Protocol*). Si noti che queste tipologie di attacchi utilizzano spesso servizi "*session less*", basati su protocollo UDP. Questa tipologia di attacco può coinvolgere migliaia di dispositivi in contemporanea, che generano richieste verso server esposti su Internet e a cui segue un traffico di risposta verso il target. Gli effetti osservati sono quelli di attacchi DDoS con dimensioni significative in termini di bps e/o rps. Si noti che, tali esiti, vengono raggiunti senza utilizzare la tecnica di amplificazione, nonostante essa venga spesso utilizzata congiuntamente alla presente per perpetrare tali attacchi.

Un esempio di utilizzo della tecnica di riflessione realizzata senza spoofing è stato quello del 2013

che ha visto coinvolto **Spamhaus Project**[4], sito che raccoglie e diffonde informazioni per cercare di contrastare il fenomeno dello spam e di altre dinamiche malevole su Internet. In tale attacco, insieme ad altre tecniche, fu usata quella della riflessione.

Una rappresentazione grafica della presente tecnica è illustrata in Figura 7.

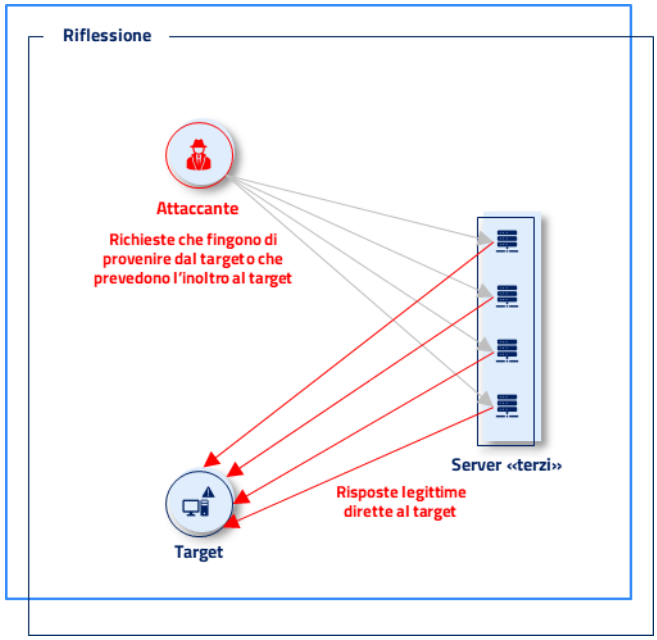

Figura 7: Rappresentazione schematica della tecnica "Riflessione"

2.2.3 Amplificazione

L'**amplificazione** è una tecnica che sfrutta la peculiarità di alcuni protocolli di rete capaci di originare una risposta più grande (in termini di byte) della richiesta. Il rapporto tra la dimensione della risposta e quello della richiesta è detto **fattore di amplificazione** e dà una misura del vantaggio dell'attaccante. Per il protocollo DNS un tipico fattore di amplificazione è pari a 60, ciò significa che un attaccante che dispone di una connettività pari a un sessantesimo di quella del target è teoricamente in grado di sopraffarlo.

Una rappresentazione grafica della presente tecnica è illustrata in Figura 8.

[4] The DDoS That Knocked Spamhaus Offline (And How We Mitigated It) – Cloudflare, 2013

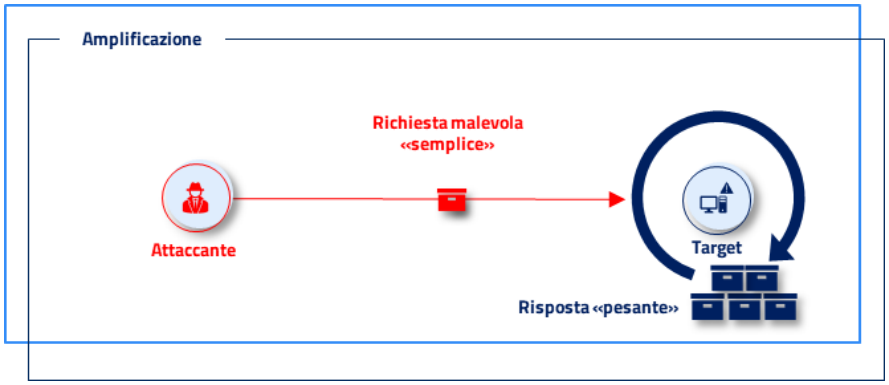

Figura 8: Rappresentazione schematica della tecnica "Amplificazione"

Un esempio significativo di attacchi in cui il ricorso a tale tecnica è stato determinante, risulta legato all'utilizzo del protocollo NTP con funzionalità **MONLIST**[5], che ha sfruttato un fattore di amplificazione di circa 200. In particolare, MONLIST consente di richiedere ad un server Network Time Protocol (NTP) la lista degli ultimi IP/dispositivi che hanno sincronizzato con esso i propri orologi.

A fronte di una semplice richiesta, la risposta può potenzialmente contenere un elevato numero di elementi a cui corrisponde un altrettanto elevato fattore di amplificazione. Si noti come, in questo caso, l'utilizzo congiunto con le tecniche di riflessione risulta essere molto efficace. Una rappresentazione grafica dell'utilizzo congiunto delle tecniche di amplificazione e riflessione è illustrata in Figura 9.

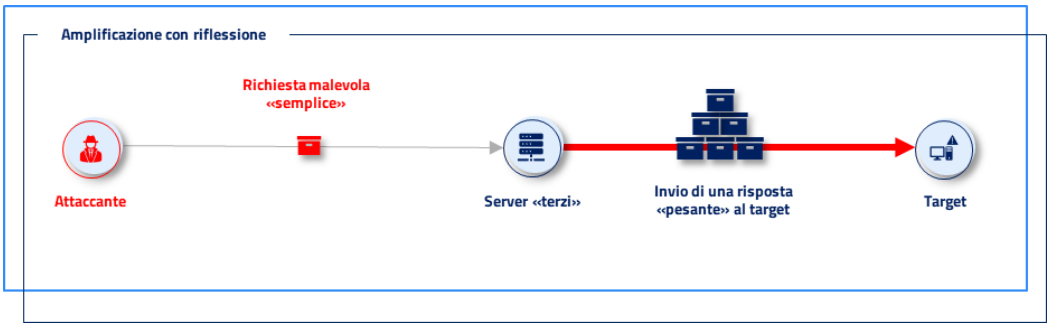

Figura 9: Rappresentazione schematica della tecnica "Amplificazione con riflessione"

Questa tipologia può anche essere rivolta verso specifiche applicazioni dove, sempre a fronte di semplici richieste, vengono innescate pesanti elaborazioni sia in fase di risposta sia nell'utilizzo di ulteriori risorse (es.: banda).

[5] Technical Details Behind a 400Gbps NTP Amplification DDoS Attack – Cloudflare, 2014

2.2.4 Utilizzo di botnet

Le cosiddette **botnet**[6] sono spesso sfruttate dagli attaccanti per condurre attacchi DDoS.

Attraverso il C&C, gli attaccanti possono scegliere i dispositivi da utilizzare per svolgere l'attacco, sfruttando la loro collocazione geografica e originando grandi flussi di traffico sfruttando le tecniche di riflessione e spoofing.

Uno dei primi esempi di botnet utilizzate per sferrare attacchi di dimensioni significative è stato **Mirai**[7]. La botnet Mirai, costituita da migliaia di dispositivi IoT vulnerabili compromessi, è stata coinvolta nel 2016 in attacchi di dimensione ed effetti significativi ed ha interessato uno dei fornitori di servizi DNS più importanti (Dyn)[8].

Una rappresentazione grafica della presente tecnica è illustrata in Figura 10.

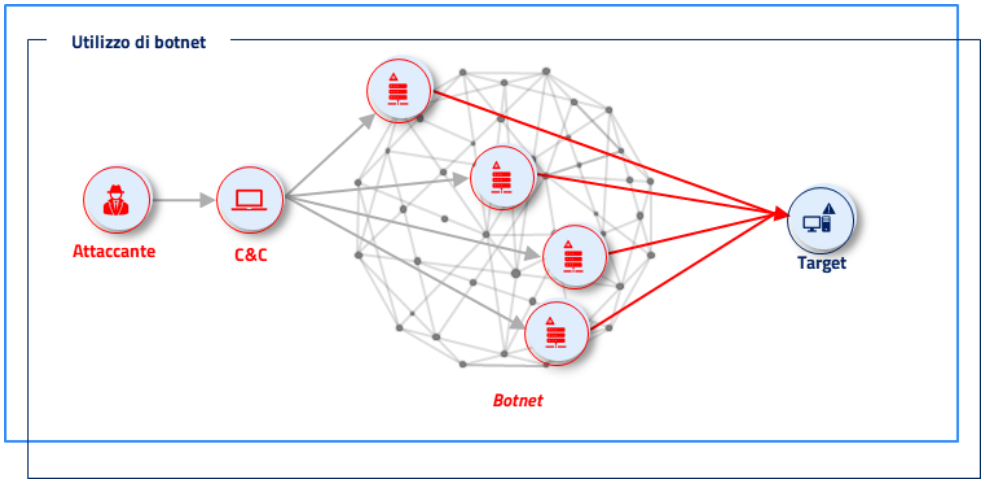

Figura 10: Rappresentazione schematica della tecnica "Utilizzo di Botnet"

Si noti che gli attaccanti ricorrono spesso a numerose tecniche di attacco simultaneamente. Una rappresentazione grafica di un attacco che prevede l'utilizzo congiunto delle tecniche qui

[6] Il termine botnet indica un insieme di dispositivi (modem, PC, etc.) sotto il controllo di un attaccante, pronti ad eseguire comandi (come fossero "roBOT"). Per controllare la botnet l'attaccante utilizza un elemento detto **Command & Control** (C&C), ovvero una infrastruttura remota in grado di impartire comandi, monitorare, ricevere e inviare dati dai dispositivi che la costituiscono. Una volta compromessi i dispositivi possono essere utilizzati dagli attaccanti per svolgere attività illecite, quali ad esempio attacchi DDoS, spam o mining di criptovalute.
Per creare una botnet sono tipicamente utilizzate varie tecniche con il comune obiettivo di **acquisire, in maniera persistente, il controllo del dispositivo**. La compromissione può avvenire utilizzando diversi vettori (es.: malware diffusi via phishing, sfruttamento di vulnerabilità, brute-forcing di password deboli o virus con capacità di auto-propagazione), attraverso cui i dispositivi coinvolti entrano a far parte in maniera inconsapevole della rete.

[7] Inside the infamous Mirai IoT Botnet: A Retrospective Analysis – Cloudflare, 2017

[8] I rallentamenti resero irraggiungibili una serie di popolari servizi come Twitter, Netflix, Reddit che utilizzavano Dyn come DNS autoritativo per i propri domini.

presentate è illustrata in Figura 11.

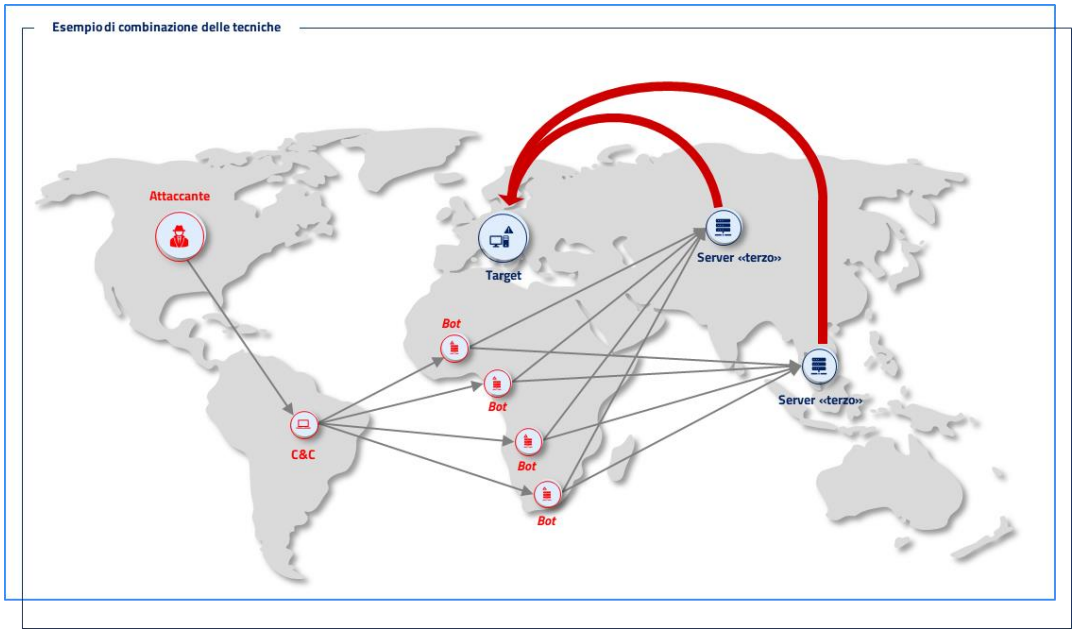

Figura 11: Rappresentazione schematica di un attacco che prevede l'utilizzo congiunto di più tecniche

Infine, può essere utile sottolineare che una serie di attacchi brevi e di caratteristiche variabili possono essere indicativi di azioni preparatorie rivolte a testare le capacità di reazione e le soglie oltre cui si è in grado di generare un impatto.

2.3 Asset principali, tipologie ed effetti correlati

Il presente paragrafo mette in relazione gli **asset principali** descritti nel modello di riferimento (§ capitolo 1.2) con le **tipologie di attacco** presentate precedentemente, evidenziandone gli **effetti** al fine di facilitare una **pianificazione mirata delle contromisure**.

ATTACCO VOLUMETRICO	ATTACCO ESAURIMENTO DI STATO	ATTACCO APPLICATIVO	ATTACCO MALFORMED PACKET
Saturazione delle risorse di banda fornita dall'ISP con annesso degradamento o interruzione della connettività e/o impossibilità di accesso ai servizi	-	-	-
Saturazione delle risorse di CPU e memoria a disposizione dei dispositivi direttamente esposti (router, firewall, bilanciatori etc)	Esaurimento delle risorse di CPU e memoria dei dispositivi esposti (router, firewall, bilanciatori, etc)	-	Blocco o continuo riavvio di dispositivi (firewall, bilanciatori, etc)
Esaurimento, degrado delle prestazioni, o eccessivo utilizzo delle risorse dedicate all'erogazione del servizio applicativo	-	Esaurimento, degrado delle prestazioni, o eccessivo utilizzo delle risorse dedicate all'erogazione del servizio applicativo	Blocco o continuo riavvio di elementi del service container o della vera e propria applicazione

Figura 12: Asset, tipi di attacco e rischi correlati

A partire da quanto illustrato nei capitoli precedenti, il successivo approfondirà il tema delle contromisure fornendo **raccomandazioni generali** utili per innalzare il livello di resilienza dei soggetti. L'allegato al presente documento presenterà, inoltre, **raccomandazioni specifiche** per la gestione di tutte le tipologie d'attacco presentate in questo capitolo.

3 RACCOMANDAZIONI GENERALI

Questo capitolo descrive **misure** e **contromisure** che le organizzazioni possono adottare per aumentare la propria **resilienza agli attacchi DDoS**. Queste indicazioni possono risultare utili a chi fornisce servizi digitali e deve garantirsi l'accesso a risorse esterne.

La valutazione **dell'esposizione della propria organizzazione agli attacchi DDoS** risulta essere un punto di estrema importanza e necessita, laddove possibile, di una **valutazione dei rischi** e dell'adozione di sistemi che possano permettere la mitigazione degli attacchi. Tale aspetto può essere caratterizzato mettendo in pratica opportune raccomandazioni che considerano l'adozione di:

- sistemi Anti-DDoS volumetrici (in cloud, on premise o ibridi);
- dispositivi di rete (es.: router, firewall, access point) con funzioni di protezione da attacchi DDoS infrastrutturali;
- sistemi Anti-DDoS applicativi specifici per i servizi esposti (es. WAF con funzioni Anti-DDos per i servizi HTTP/S);
- corretto dimensionamento degli apparati e sistemi;

nonché la scelta di:

- ISP e *carrier* che forniscono soluzioni Anti-DDoS e che possano supportare tecnicamente il soggetto in caso di attacco;
- partner tecnologici in grado di fornire chiare indicazioni in merito ai livelli di servizio e alle relative garanzie di continuità.

L'adozione e l'applicazione di **adeguati sistemi di sicurezza** è solitamente un forte deterrente nei confronti degli attaccanti: una volta riscontrata la presenza di sistemi Anti-DDoS, gli obiettivi o le modalità di attacco possono variare sensibilmente. Relativamente alle attività **operative di supporto e ripristino** che CSIRT Italia ha condotto nei confronti dei soggetti della Constituency, è stato spesso osservato che la presenza di sistemi Anti-DDoS volumetrici induce gli attaccanti a modificare le loro strategie iniziali optando, ad esempio, per attacchi applicativi. In funzione delle motivazioni dell'attaccante, l'adozione e l'applicazione di opportune contromisure da parte di un soggetto, potrebbe impedire il perpetrarsi degli attacchi.

In particolare, la **predisposizione di un piano di risposta** associato all'uso di specifiche tecnologie e al corretto coinvolgimento dei vari attori, migliora le capacità di prontezza di un'organizzazione ma non può prescindere dalla **corretta formazione del personale specializzato**. In caso di attacco, infatti, le scelte tecniche e/o le contromisure adottate in emergenza risultano essenziali per la resilienza delle infrastrutture coinvolte.

3.1 Raccomandazioni e contromisure

Per una difesa efficace contro gli attacchi DDoS, è essenziale adottare un **approccio integrato** che combini processi e strategie, soluzioni tecnologiche e controlli di sicurezza rigorosi. Di seguito viene presentata una panoramica delle ***best practice*** suddivise in **tre categorie principali**: processi e strategie, soluzioni di sicurezza e controlli di sicurezza.

Figura 13: Le tre tipologie di raccomandazioni generali

Queste *best practice* mirano a identificare interventi per **prevenire, rilevare e mitigare gli attacchi DDoS** in modo che le organizzazioni possano verificare e/o rafforzare significativamente la loro resilienza contro questa minaccia.

Processi e strategie

In tale dominio, relativamente al DDoS, le principali misure da adottare riguardano la preparazione di **piani di risposta,** la **formazione del personale**, le **simulazioni di attacco,** un corretto approccio alla **selezione dei partner tecnologici e l'opportuna collaborazione con gli stessi.**

- **Piani di risposta agli incidenti**

  La preparazione è cruciale per minimizzare l'impatto di un attacco DDoS. Un piano di risposta agli incidenti dettagliato dovrebbe chiarire le responsabilità del personale e le interazioni con gli altri attori coinvolti (es.: gli Internet Service Provider), i passaggi per identificare l'attacco, la scelta tra le possibili azioni per mitigarlo e le azioni per ripristinare i

servizi. Questo piano deve essere aggiornato regolarmente e testato attraverso simulazioni per garantirne l'efficacia.

- **Formazione e consapevolezza del personale**
  Riconoscere i primi segnali di un attacco DDoS, sapere come reagire, configurare correttamente le proprie infrastrutture e considerare correttamente i requisiti da sottoporre ai fornitori, sono fattori imprescindibili nelle attività di risposta a tale minaccia. La preparazione del personale risulta dunque un fattore di cruciale importanza.
- **Selezione e collaborazione con ISP, partner tecnologici e altri soggetti**
  Scegliere attentamente i fornitori di servizi Internet (ISP) e gli altri partner che forniscono apparati di rete e di sicurezza consente di selezionare gli opportuni prodotti e servizi (es.: supporto durante un attacco) da acquisire e contrattualizzare. Questi partner possono fornire assistenza immediata, risorse aggiuntive per la mitigazione e consigli strategici basati sulle loro esperienze e competenze.
- **Simulazioni di attacco**
  Eseguire esercitazioni periodiche e simulazioni di attacchi DDoS sulla propria infrastruttura consente di valutare l'efficacia del piano di risposta agli incidenti, di identificare eventuali punti deboli e di familiarizzare con specifici strumenti. Queste simulazioni aiutano a migliorare la coordinazione della squadra e a rafforzare le difese dell'organizzazione.

Soluzioni di sicurezza

Le raccomandazioni relative alle soluzioni di sicurezza forniscono indicazioni circa gli **strumenti e le soluzioni tecnologiche** da adottare ai fini di migliorare le capacità di prevenzione e gestione della minaccia DDoS.

- **Adozione di sistemi e servizi anti-DDoS volumetrici**
  Implementare sistemi Anti-DDoS volumetrici idonei a gestire e mitigare una quantità di traffico indesiderato superiore a quella gestibile dalla connettività adottata. Esistono tre tipologie di soluzioni, *on premise*, *in cloud* e *ibrida* in cui vengono coinvolti elementi interni/esterni alla rete dell'organizzazione per agire sul traffico e/o fornire protezione dagli attacchi a esaurimento di stato e applicativi.
- **Adozione di dispositivi di rete con funzionalità di protezione da attacchi DDoS**
  Adottare per le proprie infrastrutture sistemi che contengano nativamente funzionalità di protezione Anti-DDoS, anche in caso di presenza di sistemi Anti-DDoS volumetrici a monte. In questo modo è possibile ridurre i rischi derivanti da attacchi di esaurimento di stato oltre che da altre dinamiche non esplicitamente legate al DDoS.

- **Dispositivi aggiuntivi di rete DPI in grado di analizzare e filtrare il traffico**
  Valutare l'inserimento di apparati "in linea" nella rete per mitigare attacchi DDoS, specialmente lungo i flussi di traffico critici. Tali dispositivi sono in grado, attraverso la Deep Packet Inspection (DPI), di analizzare il traffico (spesso anche quello cifrato[9]), rilevare anomalie, inviare allarmi e attivare azioni di mitigazione.
- **Adozione di sistemi Anti-DDoS applicativi**
  Adottare sistemi di sicurezza applicativi in grado di analizzare approfonditamente il contenuto del traffico, rilevare o supportare l'analisi di anomalie e di bloccare le richieste che possono portare al degrado delle performance degli applicativi. I sistemi di sicurezza applicativa più comuni sono quelli pensati per i servizi web, ovvero i cosiddetti WAF (Web Application Firewall)[10].
- **Utilizzo di sistemi Content Delivery Network (CDN)**
  Utilizzare servizi CDN, per diminuire il carico sulla propria infrastruttura grazie alla distribuzione dei contenuti statici attraverso server del fornitore ubicati in diverse località geografiche. Molti fornitori di servizi di questo tipo offrono servizi di Anti-DDoS cloud, solitamente molto utili per la mitigazione di attacchi applicativi. In questo caso è necessario verificare sempre che il piano adottato comprenda la protezione Anti-DDoS (in alcuni casi venduta separatamente) e che siano state recepite le indicazioni del vendor in merito alle configurazioni del server e alla sua pubblicazione sul web.
- **Spostamento in cloud di propri servizi con soluzioni SaaS, IaaS, PaaS**
  In alcuni casi è possibile decidere di spostare parte delle proprie applicazioni acquisendo risorse in modalità *Software as a Service* (SaaS), *Infrastructure as a Service* (IaaS) o *Platform as a Service* (PaaS) da un Cloud Service Provider. In questi casi tipicamente è possibile, senza l'acquisto di HW/SW e configurando alcuni servizi in funzione del loro utilizzo, attivare soluzioni Anti-DDoS volumetriche, di protezione delle risorse di stato e applicative. Rimane, tuttavia, cruciale la scrupolosa selezione dei propri partner tecnologici e l'attenta valutazione delle eventuali responsabilità derivanti dalla configurazione delle soluzioni.

[9] Consentendo di configurare su di loro la terminazione del canale SSL di cifratura, per l'accesso ai dati in chiaro.
[10] Si noti che non in tutti i casi sono presenti funzionalità Anti-DDoS per questi sistemi. Inoltre, non è raro che attacchi applicativi possano comportare disservizi dovuti a configurazioni errate di questi sistemi di sicurezza.

Controlli di sicurezza

Le raccomandazioni relative ai controlli di sicurezza riguardano la necessità di implementare strategie, processi e le soluzioni tecnologiche per:

- **Prevenire gli effetti di un attacco DDoS**
  La prevenzione richiede una attenta selezione di strumenti e servizi, una progettazione adeguata delle proprie infrastrutture, l'attivazione di tutte le funzionalità tecnologiche a disposizione e l'attivazione dei piani predisposti.
- **Riconoscere prontamente l'insorgenza di un attacco**
  Riconoscere l'insorgenza di un attacco richiede l'utilizzo di piattaforme e servizi, nonché la loro integrazione nei processi di monitoraggio ICT aziendale.
- **Reagire a fronte di attacchi DDoS**
  La reazione ad un attacco DDoS richiede l'attivazione di opportuni processi e il corretto coinvolgimento di attori esterni ed interni all'organizzazione, nonché l'utilizzo degli strumenti acquisiti.

ALLEGATO

AZIONI DI MITIGAZIONE PER TIPOLOGIA DI ATTACCO

Implementare sistemi di risposta e predisporre **piani di azione** relativi a ciascuna tipologia di attacco DDoS costituiscono attività preventive che richiedono un'attenta pianificazione.

In questo allegato, verranno esaminate le contromisure che possono essere implementate in risposta alle diverse tipologie di attacchi DDoS: volumetrici, di esaurimento di stato, applicativi e *malformed packet*.

Figura 14: Tipologie di attacco DDoS

Attacco volumetrico

Come già approfondito nel capitolo 2.1, gli attacchi **volumetrici** mirano al consumo della disponibilità di banda di rete dell'infrastruttura target.

Una soluzione che può garantire la veloce implementazione delle contromisure necessarie a garantire la continuità del servizio è quella **di installare e configurare adeguatamente un sistema Anti-DDoS Volumetrico,** facendo in modo che esso sia in grado di bloccare il traffico indesiderato prima che questo possa occupare la banda a disposizione.

I **principali attori** che concorrono alla gestione proattiva e reattiva di un attacco volumetrico sono illustrati in Figura 15.

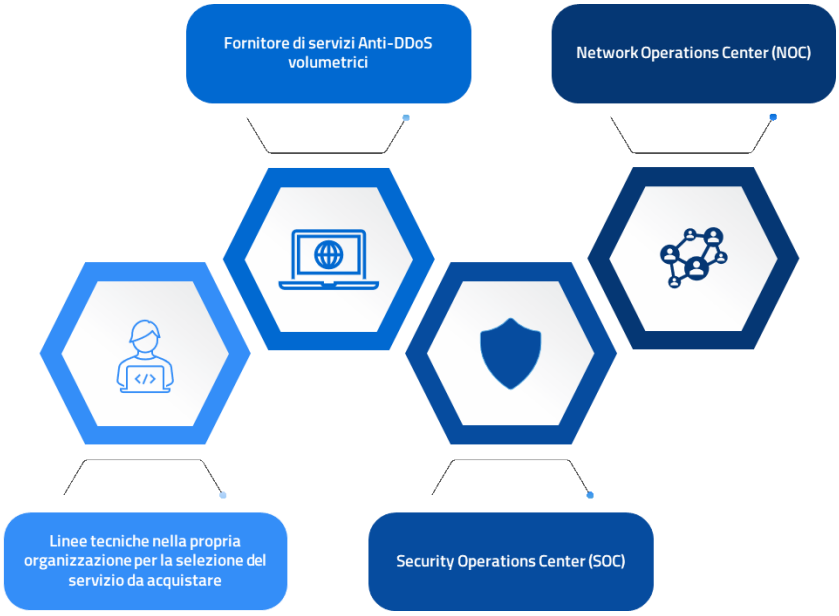

Figura 15: I principali attori della gestione proattiva e reattiva di un attacco volumetrico

Contromisure specifiche per la gestione:

- selezionare e acquisire **servizi e soluzioni Anti-DDoS volumetrico** da ISP o altri "DDoS *mitigation providers*". Queste soluzioni, tipicamente "*in Cloud*", in alcuni casi possono anche prevedere una componente posizionata presso la propria rete – apparati che vengono definiti "on premise" – che identifica il traffico indesiderato e istruisce i sistemi cloud circa il come ripulire il traffico indesiderato. Vista la loro natura duale, queste soluzioni vengono spesso indicate come "ibride".

  Nella componente "***in Cloud"***, realizzate attraverso "*Cleaning Farm*" dotate di grande capacità di banda e posizionate all'interno delle infrastrutture del Service Provider, le operazioni sul traffico indesiderato vengono effettuate tramite le cosiddette "lavatrici di traffico" – in inglese *washing machine* – che costruiscono nel tempo una "baseline" del traffico "atteso" e intervengono nel caso in cui si presenti traffico inatteso o corrispondente a note tipologie di attacco.

  La velocità del processo di mitigazione dipende in parte delle scelte effettuate in fase di installazione. In alcuni casi, infatti, si potrebbe preferire incorrere nel rischio di brevi periodi di congestione del traffico per evitare di abilitare troppo spesso la mitigazione e affrontare gli eventuali costi che questa richiede, in altri casi – ove si avesse maggiore contezza della tipologia di traffico atteso ed esigenze di continuità di servizi stringenti – si potrebbero preferire interventi più tempestivi.

  La soluzione "*in Cloud*" è altamente scalabile e sicura, ma tende a essere più costosa e può richiedere modifiche ai propri processi, compresi quelli di pubblicazione dei servizi. Inoltre, non è raro che le lavatrici di traffico vengano azionate manualmente quando necessario,

una configurazione che permette certamente un risparmio in termini economici ma espone a potenziali rischi, come ad esempio quello di subire un impatto che determini lunghi tempi di inattività dei servizi prima ancora di poter intervenire.

Le soluzioni "ibride", invece, risultano essere più versatili ed economicamente convenienti, ma richiedono una gestione "in casa" degli apparati.

Non esiste una soluzione ottimale in tutti i contesti di utilizzo. Ogni organizzazione, in base alle proprie valutazioni e necessità dovrebbe identificare la soluzione più adatta;

- sottoporre a revisione i propri processi e il **piano di risposta** per assicurarsi un **utilizzo efficace delle soluzioni e dei servizi di monitoraggio e supporto** acquistati. A tal proposito, è particolarmente importante analizzare i servizi acquistati e le relative procedure che li descrivono al fine di renderli compatibili con i propri processi interni;
- **integrare** le soluzioni acquistate nei propri strumenti e nei **processi per il monitoraggio e gestione di incidenti di sicurezza informatica;**
- **predisporre**, prima che ne sia necessario l'utilizzo, delle **azioni e opzioni di "*ultima ratio*"** , nonché i processi interni per la loro valutazione e attivazione (es: restrizione della raggiungibilità dei propri servizi esposti al solo insieme di nazioni che risultano più critiche per il proprio business/missione; insieme di servizi che si ritiene meno critici e sacrificabili durante l'attacco; ridondanze sacrificabili per rendere più efficaci le azioni di contrasto durante l'attacco);
- **studiare e verificare i dimensionamenti** in termini di capacità di banda residua in assenza di attacchi, ma in momenti di alto traffico, nella connettività acquistata dal proprio ISP e negli apparati che compongono l'infrastruttura interna alla propria azienda o, in caso di IaaS, acquistata dal proprio Cloud Service Provider. Tale azione permette di identificare eventuali colli di bottiglia e apparati sottodimensionati, nonché di prevedere una catena di possibili effetti e segnali da monitorare;
- valutare **possibili ridondanze e diversificazioni di ISP per la propria connettività Internet** (es: contratto di connettività con due Internet Service Provider differenti);
- **innalzare la ridondanza e l'affidabilità degli elementi** e dei servizi **esterni** alla propria rete il cui corretto funzionamento è **critico per la propria continuità di business/mission**. Un esempio particolarmente ricorrente collegato ai DDoS è quello dei DNS Autoritativi, ovvero i DNS responsabili di conservare le associazioni corrette per tutti i propri "sotto domini"[11]. In tale contesto, un esempio tipico di attacco "DDoS laterale" è quello in cui, per rendere

[11] Es: nomeservizio1.nomedominiosoggetto.it, nomeservizio2.nomedominiosoggetto.it

non raggiungibili i servizi di un certo soggetto, vengono attaccati i relativi server DNS autoritativi, senza i quali quindi chi vuole accedere al servizio non riesce a ritrovare traccia della sua localizzazione su Internet. È quindi molto importante scegliere attentamente a chi affidare questo ruolo, diversificando tra più di un fornitore o almeno su due infrastrutture separate e verificando attentamente le garanzie di servizio e le misure di protezione che il fornitore ha introdotto;

- **identificare i servizi esterni** alla propria rete **la cui raggiungibilità risulta critica** per lo svolgimento del proprio business/mission. In questo modo, a fronte di una saturazione della connettività Internet che porterebbe impatto sulla continuità dei propri processi, è possibile studiare modalità alternative per supportare e svolgere quelle attività (es: in caso di impatti sulla connettività Internet della sede, alcuni dipendenti potrebbero essere messi in grado di connettere il proprio PC ad Internet attraverso una connessione cellulare);
- inserire una serie di **"filtri statici",** sebbene non possano risolvere da soli un attacco volumetrico ben strutturato, può contribuire a ridurre significativamente alcune componenti dell'attacco bloccando, quanto prima possibile, flussi che non sono coerenti con i servizi che si espongono (es: bloccare qualunque flusso si diriga ad un server web che non sia coerente con le relative porte protocolli; configurare un rate-limiting con cui, in caso di sovrautilizzo, si evita che flussi che si ritiene secondari occupino la totalità della risorsa di connettività). Oltre che valutarne l'attivazione per la durata degli attacchi, in alcuni casi è possibile richiedere al proprio ISP un servizio per cui questi filtri sono inseriti in forma stabile e direttamente sulle sue infrastrutture, consentendo di filtrare preliminarmente eventuali attività malevole;
- utilizzare sistemi **Content Delivery Network (CDN)**[12] che consentono di distribuire i contenuti statici dei propri siti web attraverso server del fornitore, diminuendo così il carico che invece corrisponde a flussi dati verso la componente residua del sito web ospitata presso la propria infrastruttura.

[12] Si noti che eventuali servizi e funzionalità aggiuntive Anti-DDoS, anche nel caso siano offerti dal fornitore di CDN possono dover essere acquisite e/o configurate a parte,.

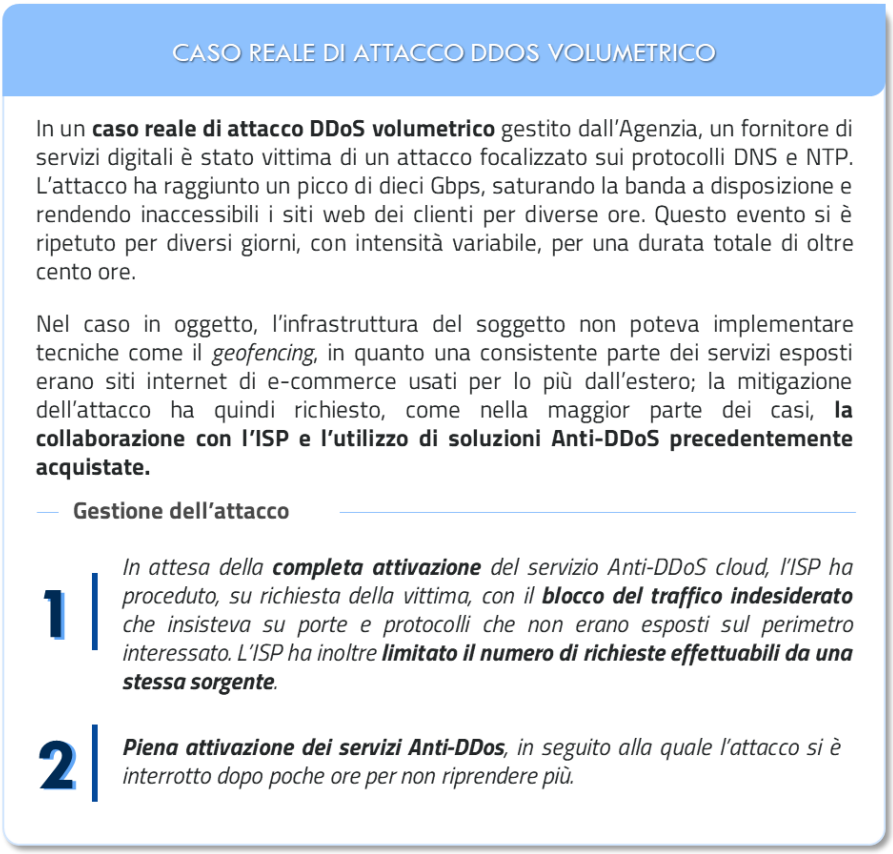

Figura 16: Caso reale di attacco DDoS volumetrico

Attacco esaurimento di stato

Come già approfondito nel capitolo 2.1, gli attacchi di **esaurimento di stato** mirano ad esaurire le risorse di calcolo e memoria dei dispositivi di rete, come i firewall e i load balancer, esaurendo le loro tabelle di stato.

Nel caso di DDoS con esaurimento di stato, l'elemento determinante per la resilienza agli attacchi risulta essere la corretta progettazione e il corretto utilizzo di apparati dotati delle giuste caratteristiche e funzionalità.

Si ritiene utile far notare che, purtroppo, una volta arrivati a saturazione, anche a fronte di picchi molto brevi, non è raro che un apparato rimanga "in blocco" anche se l'attacco è cessato o è stato gestito da altre soluzioni. In questi casi, dunque, è particolarmente utile monitorare i parametri degli apparati, identificare se ve ne sono "in blocco", ed essere pronti ad operazioni di riavvio e ripristino delle funzionalità.

I **principali attori** che concorrono alla gestione proattiva e reattiva di un attacco di esaurimento di stato sono illustrati in Figura 17.

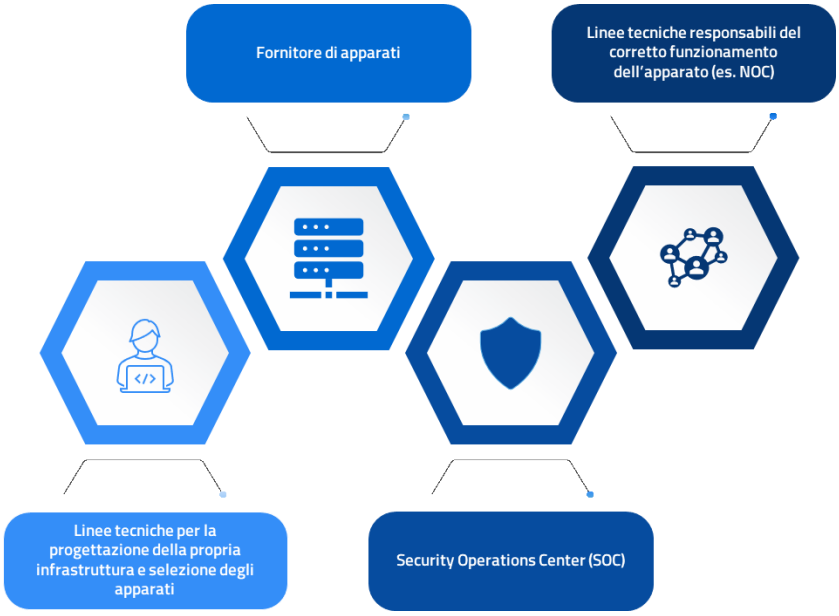

Figura 17: I principali attori della gestione proattiva e reattiva di un attacco di esaurimento di stato

Contromisure specifiche per la gestione:

- **scegliere e configurare apparati** per la propria infrastruttura (es.: router, firewall, bilanciatori, access point) **che abbiano funzionalità anti-DDoS** per esaurimento di stato. In tal senso, analizzare le funzionalità e i dati di performance comunicati da un produttore è molto importante. Nello specifico, la presenza di funzionalità mirate a proteggere l'apparato dalle dinamiche che portano all'esaurimento delle risorse per gestire gli stati delle connessioni e la possibilità di variare alcuni parametri è determinante per la capacità di resistere ad un DDoS infrastrutturale;
- valutare l'**aggiunta di apparati "in linea"** nella propria rete per attivare **funzionalità per la mitigazione di DDoS**. In alcuni casi può essere utile inserire, lungo la direttrice di flussi di traffico particolarmente critici che incontrano apparati non in grado di proteggersi da DDoS, degli apparati ad-hoc. Spesso in questi apparati "aggiuntivi" coesistono funzionalità per la protezione da esaurimento di stato e da DDoS applicativi. In alcuni casi possono anche essere presenti componenti "on premise" per la gestione dei DDoS volumetrici. Oltre alle funzionalità di protezione infrastrutturale specifiche (per le principali si veda a seguire), questi apparati sono in grado di analizzare flussi di traffico anche non in chiaro[13] tramite **Deep Packet Inspection (DPI)**, ovvero analisi che arrivano fino al livello di contenuti applicativi, nonché di identificare una serie di dinamiche anomale, inviare allarmi, realizzare una serie di azioni sui flussi e attivarne altre a valle di analisi;

[13] fungendo da terminatore del canale di cifratura SSL

- **raccogliere allarmi e integrarli** nei propri strumenti e processi **per il monitoraggio e la gestione di incidenti di sicurezza informatica.**

Di seguito le **principali funzionalità** con cui tipicamente si mitigano gli effetti di un DDoS con esaurimento di stato:

1. **SYN Cookies**: è una tecnica che consente di gestire richieste SYN senza allocare risorse di stato fino a quando la connessione non è completamente stabilita.
2. **Tuning dei Timeout sessioni in attesa o inattive (*half-open time*)**: permette di configurare valori mirati per i tempi di timeout per le connessioni in attesa (ovvero per cui non si è completata la procedura TCP Handshake di apertura della comunicazione) o inattive (ovvero aperte ma a lungo lasciate inutilizzate), consentendo di liberare risorse più rapidamente.
3. **Connection Limiting (limitazione del numero di connessioni)**: questa tecnica impone un limite al numero massimo di connessioni che un singolo IP, o un gruppo di IP, può mantenere contemporaneamente. Se l'IP tenta di aprire più connessioni di quelle consentite, il traffico aggiuntivo viene rifiutato, bloccato o sottoposto ad altri vincoli (es: rate limiting).
4. **Rate Limiting (limitazione del tasso di utilizzo della singola connessione)**: consente di imporre una soglia massima al numero di connessioni o richieste che possono essere fatte in un breve periodo (es. 10 connessioni al secondo) da un singolo IP o gruppo di IP. Se un IP supera questo limite, il traffico successivo viene bloccato o limitato fino alla fine dell'intervallo temporale.

Con molte di queste tecniche è **necessario cercare un trade-off** tra protezione e rischio di impattare connessioni legittime. Si tenga presente, comunque, che con un ***tuning* corretto**, si può riuscire a fare in modo che gli effetti negativi possano manifestarsi solo durante gli attacchi ed essere meno significativi del degrado o blocco completo delle funzionalità dell'apparato. Una possibile ulteriore strategia può consistere nell'essere più stringenti su servizi meno critici (e dunque limitando particolarmente i *timeout* o il numero di sessioni di flussi che li interessano) e leggermente meno stringenti su quelli più critici.

In alcuni casi è possibile utilizzare queste funzionalità congiuntamente a tecniche di ***white listing*** (ovvero esclusione da restrizioni più stringenti di un elenco di indirizzi che si ritiene affidabili e a cui si vogliono dedicare più risorse) o ***black listing*** (ovvero utilizzo di liste di IP corrispondenti a botnet o altri IP segnalati come sospetti e su cui si vogliono operare blocchi o comunque applicare in maniera più stringente le limitazioni di risorse).

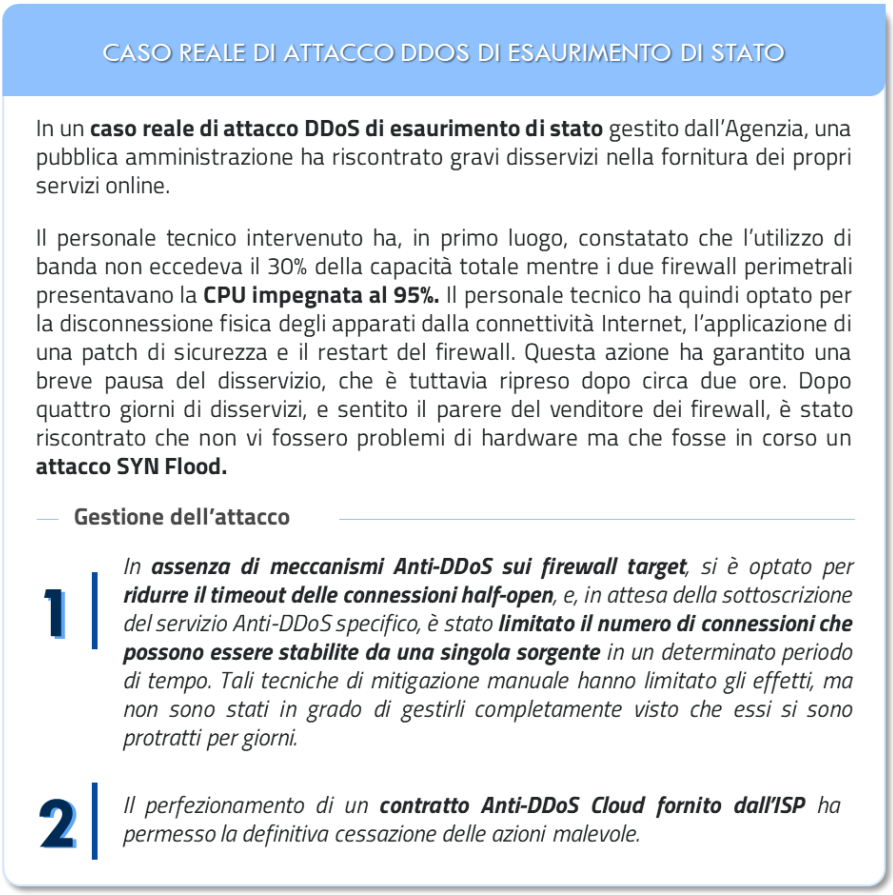

Figura 18: Caso reale di attacco DDoS di esaurimento di stato

Attacco applicativo

Come già approfondito nel capitolo 2.1, gli attacchi **applicativi** sono diretti ai servizi di livello applicativo, come HTTP/HTTPS, DNS e SMTP, mirando a esaurire le risorse computazionali e di memoria del server applicativo.

Nella protezione applicativa il legame con l'applicazione stessa, le sue funzionalità e le sue evoluzioni è strettissimo ed è dunque determinante tenerne conto nelle relative contromisure.

I **principali attori** che concorrono alla gestione proattiva e reattiva di un attacco applicativo sono illustrati in Figura 19.

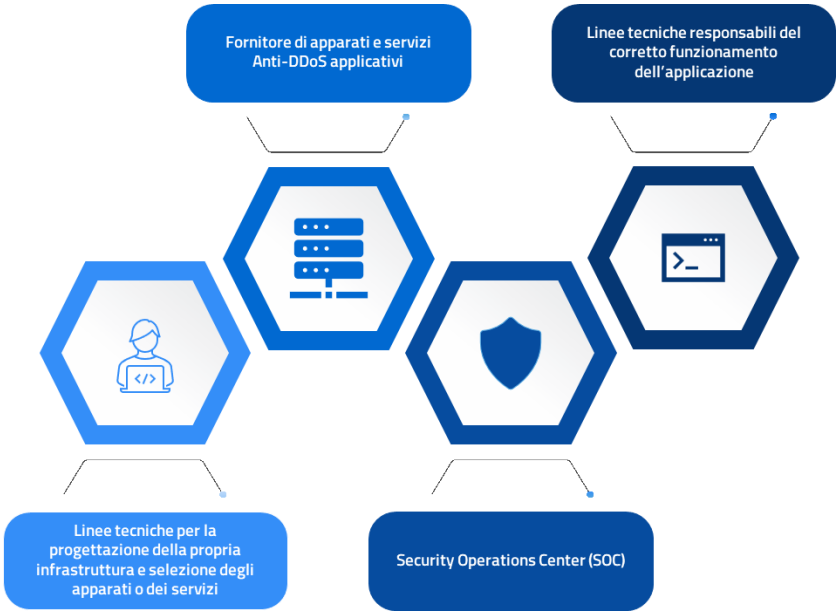

Figura 19: I principali attori della gestione proattiva e reattiva di un attacco applicativo

Contromisure specifiche per la gestione:

- selezionare e acquisire **servizi e soluzioni Anti-DDoS applicativo**. Esistono soluzioni "*in Cloud*" o anche "*On Premise*", con funzionalità Deep Packet Inspection (come, ad esempio, Intrusion Detection Prevention System, Next Generation Firewall) che possono essere rivolte alla protezione non soggetta a tipologia specifica[14], o specializzata, come ad esempio i Web Application Firewall (WAF) o infine a protezione specifica delle API;
- **integrare i processi di rilascio** in campo delle applicazioni, con le **procedure di aggiornamento delle configurazioni degli strumenti di protezione.** Oltre ad una serie di meccanismi che sono spesso applicabili in maniera indistinta alle applicazioni di un certo tipo (es: applicazione con un front-end web), la protezione applicativa ha delle componenti particolarmente legate alla specificità dell'applicazione stessa e delle modalità di interazione degli utenti. L'aggiunta di un nuovo pannello di autenticazione o di una nuova funzionalità che prevede interazione con l'utenza, potrebbe dover essere esplicitamente integrata nei meccanismi di protezione. Risulta dunque determinante anche un adeguamento dei processi;

[14] In questo caso con protezione da attacchi più semplici ed abbastanza indipendenti dall'applicazione stessa (spesso in questo caso parliamo di funzionalità integrate in dispositivi rivolti alla protezione infrastrutturale e che consentono di configurare anche, ad esempio, restrizioni al numero o alla intensità di utilizzo di connessioni verso l'applicazione).

- **raccogliere allarmi ed integrarli** nei propri strumenti e processi per il **monitoraggio e la gestione di incidenti di sicurezza informatica.**

Di seguito le **principali funzionalità** con cui tipicamente si mitigano gli effetti di un DDoS applicativo:

1. **Captcha**[15]: è un meccanismo che richiede agli utenti di risolvere "test" (es. immagini o lettere distorte) in modo da distinguere gli umani dai bot. Tale meccanismo protegge da richieste automatizzate malevole e contribuisce a prevenire l'abuso di moduli online, proteggere procedure di login, e dunque a interrompere "sul nascere" alcune delle dinamiche che poi portano a sovraccaricare l'applicazione.
2. **Behavioral Analytics**: analizza i comportamenti del traffico e degli utenti per rilevare anomalie o comportamenti sospetti che potrebbero indicare un attacco, come schemi di richieste insoliti o interazioni con l'applicazione da parte degli utenti che deviano dai comportamenti usuali. Consente poi di applicare blocchi o altre tecniche per "rallentare l'attaccante".
3. **Bot Management**: funzionalità per impedire o rallentare l'accesso all'applicativo da parte di sistemi automatizzati e da botnet. Queste funzionalità lavorano attraverso soluzioni che riconoscono quando un dialogo appare originato da un bot (es: device fingerprinting, captcha, cookie/javascript analysis), classificano il bot in modo da riconoscere quelli legati ad attività lecite (es: da parte di motori di ricerca o sistemi che monitorano il corretto funzionamento) e supportano l'applicazione di tecniche come quelle indicate in seguito per bloccare l'impatto applicativo.
4. **Rate Limiting:** limita il numero di richieste che un client può fare a un'applicazione o API in un certo periodo di tempo. Questa funzionalità è comunemente implementata nei server web, WAF, API gateway, e load balancer per mitigare DDoS.
5. **Traffic Shaping/Throttling**: regola la velocità con cui le richieste sono accettate o elaborate. Utilizzato per bilanciare il carico e rallentare il traffico malevolo.
6. **Challenge-Response Mechanisms**: meccanismi che presentano sfide agli utenti (come ulteriori CAPTCHA o richieste di autenticazione) quando vengono rilevati comportamenti sospetti o volumi di traffico anomali.
7. **Session Management & Tokenization**: limita il numero di sessioni attive per utente e utilizza token di autenticazione unici per garantire la sicurezza delle sessioni. Questa

[15] *Completely Automated Public Turing-test-to-tell Computers and Humans Apart.*

funzionalità permette di prevenire fenomeni di session hijacking o abuso di sessioni con riutilizzo di sessioni precedentemente aperte.

8. **Geo-blocking**: restringe l'accesso a risorse di rete o applicazioni in base alla provenienza geografica delle richieste, bloccando il traffico sospetto proveniente da regioni ad alto rischio. Efficace per ridurre il rischio di attacchi provenienti da aree geografiche note per attività malevole e a bassa probabilità di interazione con le proprie applicazioni.
9. **IP Reputation Filtering**: filtra il traffico in base alla reputazione dell'indirizzo IP, bloccando o rallentando automaticamente richieste provenienti da IP associati ad attività malevole (es. botnet).

Analogamente al caso della protezione da DDoS infrastrutturali, l'utilizzo di tecniche per la protezione applicative necessita di trade-off tra la protezione e il rischio di impattare connessioni legittime. È dunque necessario limitare quanto più possibile le connessioni malevole, ma monitorare gli effetti e allentare i controlli dove necessario.

Anche per la protezione applicativa è possibile utilizzare queste funzionalità insieme a tecniche di ***white listing*** (ovvero esclusione da restrizioni più stringenti di un elenco di indirizzi che si ritiene affidabili e a cui si vogliono dedicare più risorse) o ***black listing*** (ovvero utilizzo di liste di IP corrispondenti a botnet o altri IP segnalati come sospetti e su cui si vogliono operare blocchi o comunque applicare in maniera più stringente le limitazioni di risorse).

Nella protezione applicativa è inoltre particolarmente importante configurare e sfruttare appieno le funzionalità in grado di restringere le interazioni possibili con l'applicazione a quelle previste e necessarie. Ad esempio, servizi applicativi come DNS, NTP, SNMP, SSH, oltre che attraverso white listing, possono essere protetti efficacemente, attraverso un **hardening applicativo**, spegnendo o restringendo alcune delle funzionalità disponibili, ma non utilizzate.

CASO REALE DI ATTACCO DDOS APPLICATIVO

In un **caso reale di attacco DDoS applicativo** gestito dall'Agenzia, un sito web di e-commerce, dotato di un servizio di mitigazione DDoS Cloud e di funzionalità WAF (Web Application Firewall), ha subito un primo attacco DDoS applicativo di breve durata, rimanendo inattivo per pochi minuti. Le iniziali attività di approfondimento hanno di fatto attribuito l'evento a **generici rallentamenti del web server** che, secondo le informazioni presenti sul SIEM, non risultavano associati a picchi di richieste effettuati verso lo specifico FQDN. Nei giorni successivi, tuttavia, lo stesso sito ha sperimentato un periodo di inattività pari a circa 4 ore, causando consistenti perdite economiche. Le analisi condotte hanno appurato che il servizio Anti-DDoS Cloud non aveva rilevato l'attacco, mentre i firewall locali avevano registrato un consistente aumento del traffico.

A seguito di ulteriori approfondimenti è stato possibile associare all'evento un **attacco di tipo Slowloris effettuato verso il c.d. "default site" del Web Server**, che ha raggiunto i firewall locali senza passare per il bilanciatore di carico. In particolare, diverse sono state le problematiche riscontrate:

- **esposizione diretta su Internet dei Web Server** nonostante la presenza di un bilanciatore di carico;
- **abilitazione del "default site" su tutti i Web Server** e mancato inoltro al SIEM dei relativi eventi;
- **mancata implementazione delle indicazioni del vendor** del servizio Anti-DDoS Cloud relative, ad esempio, al blocco tramite regole firewall puntuali di tutto il traffico che non pervenisse dai propri IP tramite specifica whitelist.

Gestione dell'attacco

1. *Le attività di mitigazione proposte hanno previsto **l'applicazione delle regole indicate dal vendor del servizio Anti-DDoS e il blocco dell'accesso diretto.***
2. *A seguito di quanto implementato, l'attacco è proseguito per altre 18 ore ma **senza far registrare ulteriori impatti.***

Figura 20: Caso reale di attacco DDoS Applicativo

Attacco malformed packet

Come già approfondito nel capitolo 2.1, gli attacchi DoS basati su pacchetti malformati mirano a sfruttare vulnerabilità specifiche nelle applicazioni, nei dispositivi di rete o nelle infrastrutture di connettività, con l'intento di causare un'interruzione del servizio.

I **principali attori** che concorrono alla gestione proattiva e reattiva di un attacco *malformed packet* sono illustrati in Figura 21.

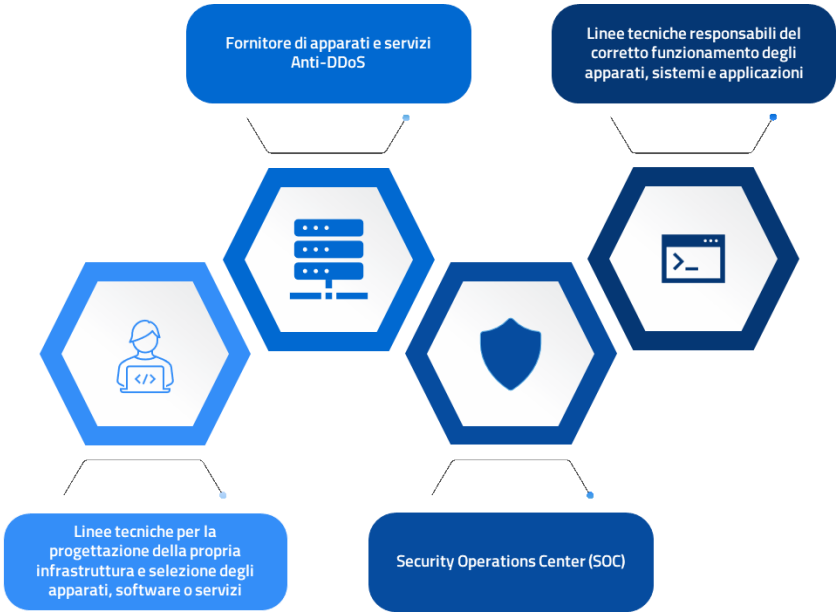

Figura 21: I principali attori della gestione proattiva e reattiva di un attacco malformed packet

Contromisure specifiche per la gestione:

- **implementare processi di Vulnerability Management:** assicurarsi che le applicazioni, i server e i dispositivi di rete siano inseriti nei processi di identificazione e gestione di aggiornamenti (Vulnerability Management) e di avere modalità per gestire prioritariamente (Critical Vulnerability Management) quelle che insistono su sistemi esposti ad Internet, che svolgono ruoli critici e relative a vulnerabilità che potrebbero essere sfruttate per causare malfunzionamenti o crash;
- **studiare e implementare possibili "*work around*"**: nel caso in cui l'elemento oggetto della vulnerabilità non risulti aggiornabile in tempi rapidi, verificare la possibilità di applicare una qualche forma di mitigazione / *work around* riducendo per esempio la possibilità che il pacchetto malformato possa raggiungere l'elemento interessato (es: per apparati di rete restringendo la raggiungibilità di alcuni servizi di gestione dell'apparato agli indirizzamenti strettamente necessari);
- **valutare l'aggiunta di apparati "in linea" nella propria rete, o di software a bordo dei sistemi, per attivare funzionalità di filtraggio pacchetti anomali.** Nel caso in cui non sia possibile procedere con aggiornamenti e patch, esistono soluzioni che consentono di applicare una "patch" virtuale a livello di rete o applicazione per bloccare attacchi che sfruttano specifiche vulnerabilità, mentre si pianifica o si esegue la patch ufficiale o l'aggiornamento del sistema. Queste funzionalità, che consentono di riconoscere e bloccare *malformed packet*, in alcuni casi coesistono con apparati rivolti alla protezione da attacchi di esaurimento di stato (es: firewall, *Intrusion Prevention System*) e/o da DDoS applicativi (es: WAF). Sulle stesse piattaforme sono spesso disponibili funzionalità per riconoscere e

filtrare attacchi *malformed packet* che, anche se non sfruttando una specifica CVE, fanno leva su caratteristiche dei protocolli di comunicazione e su alcune specifiche implementazioni da parte di vendor che innescano eccezioni o gestioni non corrette fino a portare a degradi o blocchi (es: TCP Flag Abuse, Ping of Death, Teardrop Attack, etc). In altri casi sono soluzioni software che vanno ad installarsi sui sistemi stessi da proteggere. L'aggiornamento costante delle soluzioni (e relative "firme" per riconoscere nuovi attacchi) è naturalmente determinante;

- **integrare** le soluzioni acquisite nei propri strumenti e nei **processi per il monitoraggio e gestione di incidenti di sicurezza informatica.**

Anche per la protezione da *malformed packet* è possibile ridurre l'esposizione al rischio attraverso tecniche di white listing, black listing e application hardening.

CASO REALE DI ATTACCO *MALFORMED PACKET*

In un **caso reale di attacco DDoS *malformed packet*** *gestito dall'Agenzia*, un fornitore di servizi informatici ha registrato l'indisponibilità di tutti i servizi esposti da uno stesso firewall nonché l'impossibilità di accedere al pannello di amministrazione. A fronte di un primo reset fisico dell'apparato e alle successive analisi tecniche, sono state **escluse problematiche hardware.** Il firewall risultava aggiornato all'ultimo firmware e opportunamente dimensionato rispetto al traffico medio. Di particolare interesse risultava il fatto che, durante i malfunzionamenti, la maggior parte del traffico veniva registrato in uscita e non in ingresso dal server. Sono state quindi avviate le opportune collaborazioni con l'ISP, che hanno permesso di accertare l'evidenza di un attacco DDoS. Difatti, le richieste TCP analizzate contenevano elementi di norma non presenti in regolari richieste, vale a dire:

- **flag SYN attivato**, solitamente utilizzato per inizializzare la sessione;
- payload (di solito vuoto o contenente un cookie) al cui interno veniva rilevata una **richiesta HTTP per un sito internet non presente all'interno dell'infrastruttura analizzata** (es: "GET / HTTP/1.1\r\nHost:torproject.com").

Il firewall avrebbe dovuto rilevare l'anomalia e scartare di conseguenza il pacchetto, ciononostante, per quel particolare modello, tali richieste risultavano in un'attivazione del servizio di "web filtering" destinato di norma agli utenti interni della rete. Veniva quindi restituita al mittente una pagina con un messaggio di cortesia, in cui si comunicava l'impossibilità di proseguire la navigazione per aspetti di policy. A fronte di piccole richieste effettuate dall'attaccante, plausibilmente realizzate con IP sorgente falsificato, corrispondevano **risposte amplificate da parte del firewall tali da saturare processi e banda a disposizione**.

Gestione dell'attacco

1. *Sono stati applicati **specifici workaround** necessari a bloccare tutte le richieste SYN con payload contenente la stringa "GET". L'attacco è stato così reso inefficace, nonostante le elaborazioni aggiuntive richieste al firewall.*
2. *L'attacco si è definitivamente concluso con **l'implementazione, da parte del vendor, delle opportune soluzioni.***

Figura 22: Caso reale di attacco DDoS Malformed Packet

TLP:CLEAR

IN CASO DI INCIDENTE

CONTATTA CSIRT ITALIA

Il **CSIRT Italia** si occupa delle attività di natura reattiva e proattiva nei confronti della minaccia cibernetica; è hub nazionale per la ricezione delle segnalazioni e notifiche di incidenti ed eventi e fornisce supporto ai soggetti impattati. Indirizza, altresì, i prodotti di allertamento preventivo sulle minacce e relative attività di mitigazione attraverso i suoi canali pubblici quali la sua pagina web, l'account Twitter e il canale Telegram.

In caso di incidente, compilare il modulo disponibile

https://segnalazioni.acn.gov.it/