

I'LL BLAST YOU, BABY!

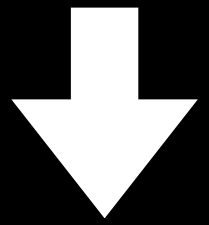
I segreti degli strumenti di DDoS: Ufonet, LOIC e HOIC.
Riflessione sugli aspetti etici e legali.



Simone La Porta,
Nicoló Callegaro, Gianluca Sansone,
Alessio Forlì, Grazia Cinzia Coco,
Alejandro Cristino, Simone Esposito

Attacco DDoS

Un attacco DDoS (Distributed Denial of Service) mira a rendere un servizio, una rete o una risorsa indisponibile per i suoi utenti legittimi, sovraccaricando il sistema con un'enorme quantità di traffico proveniente da molteplici fonti distribuite.



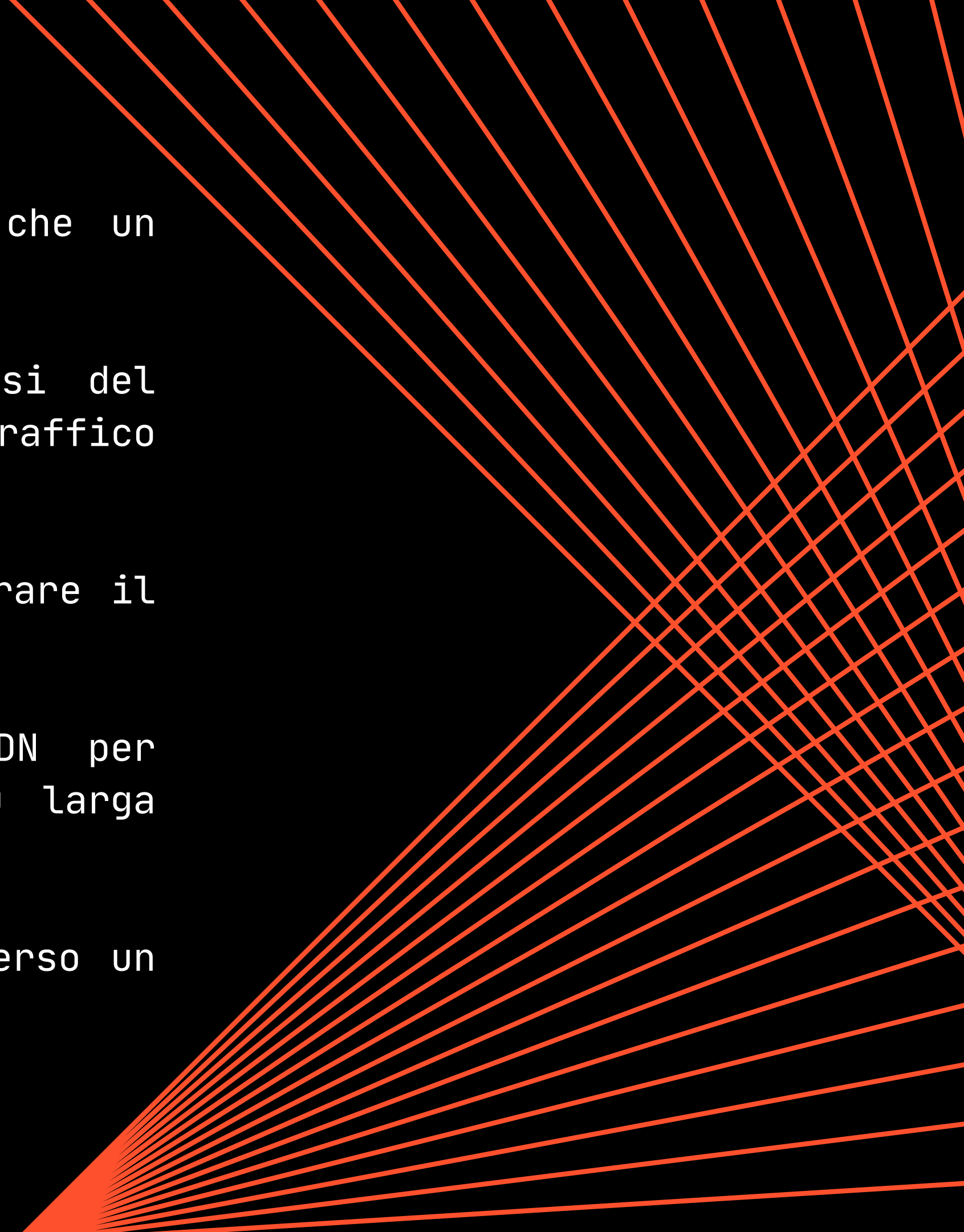
Componenti:

- **Attaccante:** entità che avvia l'attacco.
- **Handler:** server controllati dall'attaccante che coordinano l'attacco inviando comandi ai bot.
- **Bot/Zombie:** dispositivi compromessi che eseguono gli attacchi (computer, server, dispositivi IoT, ecc.)
- **Target:** sistema, server o rete bersaglio dell'attacco.

PRINCIPALI TECNICHE DI ATTACCO

- **Volume-Based Attacks:** sovraccaricano la larghezza di banda del target con un'enorme quantità di traffico.
 - **UDP Flood:** invio massivo di pacchetti UDP per saturare la larghezza di banda.
 - **ICMP Flood:** invio massivo di richieste ping (ICMP Echo Request) per consumare larghezza di banda e risorse di rete.
- **Protocol Attacks:** sfruttano le debolezze dei protocolli di rete per consumare risorse server.
 - **SYN Flood:** invia una raffica di richieste SYN (inizio di una connessione TCP) senza mai completare l'handshake, esaurendo le risorse del server.
 - **Ping of Death:** invia pacchetti ICMP di dimensioni maggiori di quelle permesse, causando errori nel sistema target.
- **Application Layer Attacks:** prendono di mira la layer applicativa (livello 7 del modello OSI) con richieste che sembrano legittime, ma sovraccaricano il server applicativo.
 - **HTTP Flood:** invia una quantità enorme di richieste HTTP GET o POST per sovraccaricare il server web.
 - **Slowloris:** apre connessioni HTTP incomplete, mantenendole aperte il più a lungo possibile per esaurire le risorse del server.

METODI DI MITIGAZIONE

- **Rate Limiting:** limitare il numero di richieste che un server può accettare in un dato periodo.
 - **Traffic Analysis:** utilizzare strumenti di analisi del traffico per identificare e bloccare il traffico sospetto.
 - **WAF (Web Application Firewall):** filtrare e monitorare il traffico HTTP per proteggere le applicazioni web.
 - **Content Delivery Networks (CDN):** utilizzare CDN per distribuire il traffico e assorbire attacchi su larga scala.
 - **Blackholing:** reindirizzare il traffico malevolo verso un "black hole" per prevenire che raggiunga il target.
- 
- A series of orange lines of varying lengths and angles radiate from the bottom right corner of the slide, creating a dynamic, abstract pattern against the black background.

STORIA DEGLI ATTACCHI DDoS pt.1

- **Anni '90 - Prime avvisaglie:**

- **1996:** il primo attacco DDoS noto è stato lanciato contro la rete ISP Panix, causando una significativa interruzione del servizio. Questo attacco ha segnato l'inizio dell'uso dei DDoS come arma cibernetica.
- **Fine anni '90:** con l'aumento della connettività Internet, i primi strumenti e script per eseguire attacchi DDoS iniziarono a circolare nei forum underground. L'attacco si basava principalmente su richieste ICMP e SYN flood per sovraccaricare le risorse dei server.

- **Anni 2000 - Diffusione e raffinamento:**

- **2000:** il famoso attacco DDoS contro Yahoo! nel febbraio 2000, eseguito da un hacker adolescente noto come "Mafiaboy", ha reso evidente la potenza distruttiva degli attacchi DDoS. Questo attacco ha bloccato il sito per diverse ore.
- **Anni 2000:** Gli attacchi DDoS sono diventati più comuni e sofisticati. Gli hacker hanno iniziato a sfruttare botnet, reti di computer compromessi, per eseguire attacchi su larga scala. Strumenti come Trinoo, TFN (Tribe Flood Network) e Stacheldraht sono diventati noti.

STORIA DEGLI ATTACCHI DDoS pt.2

- **Anni 2010 - Aumento della complessità:**
 - **2012:** il gruppo hacktivista Anonymous ha eseguito numerosi attacchi DDoS contro siti web governativi e corporativi, utilizzando strumenti come LOIC (Low Orbit Ion Cannon). Questi attacchi sono stati coordinati attraverso campagne di social media e chat room IRC.
 - **2016:** l'attacco DDoS contro Dyn, un fornitore di servizi DNS, ha bloccato l'accesso a molti siti web popolari come Twitter, Netflix e Reddit. L'attacco è stato eseguito utilizzando la botnet Mirai, composta da dispositivi IoT compromessi.
- **Anni 2020 - L'era dei grandi attacchi:**
 - **2020:** gli attacchi DDoS hanno raggiunto nuovi livelli di intensità, con attacchi che hanno superato i 2 Tbps. L'uso di tecniche avanzate di amplificazione e riflessione ha aumentato notevolmente l'efficacia degli attacchi.
 - **Presente:** gli attacchi DDoS continuano a evolversi, diventando più sofisticati e difficili da mitigare. Gli attacchi multi-vettoriali, che combinano diverse tecniche di attacco, sono ora comuni.

REGOLAMENTAZIONE

Gli attacchi DDoS sono severamente regolamentati in Italia e in Europa da diverse normative e direttive che mirano a proteggere le reti e i sistemi informatici dalle minacce cibernetiche

- **Direttiva NIS 2016/1148 (Network and Information Security Directive)** mira a raggiungere un elevato livello comune di sicurezza delle reti e dell'informazione in tutta l'UE.
- **Regolamento (UE) 2019/881**, noto come Cybersecurity Act, rafforza l'ENISA (Agenzia dell'Unione europea per la cybersicurezza) e introduce un quadro europeo per la certificazione della sicurezza cibernetica dei prodotti ICT.
- **Italia:** Codice Penale (articoli 615-ter, 635-bis, 635-quater, 635-quinquies) prevede sanzioni per accesso abusivo a sistemi informatici e danneggiamento di informazioni e sistemi.

UFONET

Potente strumento DDoS open-source che sfrutta una vasta rete di botnet per lanciare attacchi DDoS. È scritto in Python e offre una varietà di metodi di attacco.

```
888      888 88888888888 .d88888b. 888b   888      888
888      888 888      d88PY888b 8888b 888      888
888      888 888      888      888 88888b 888      888
888      888 8888888 888      888 888Y88b 888 .d88b. 888888
888      888 888      888      888 888 Y88b888 d8P  Y8b 888
888      888 888      888      888 Y88888 888888888 888
Y88b. .d88P 888      Y88b. .d88P 888      Y8888 Y8b.      Y88b.
'Y88888P' 888      'Y88888P' 888      Y888 'Y8888 'Y8888

{(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

=====

▼ Version: 1.8 ▼ [DPh] DarK-PhAnT0m! ▼

-----

-> _BOTNET [DDoS]: [ 00000008 ] ▼ Bots (Available)
    _> ZOMBIES [ 00000001 ] * HTTP GET (simple)
    _> DROIDS [ 00000001 ] * HTTP GET (complex)
    _> UCAVs [ 00000001 ] * WebAbuse (multiple)
    _> ALIENS [ 00000001 ] * HTTP POST
    _> X-RPCs [ 00000001 ] * XML-RPC
    _> DNSs [ 00000001 ] * DNS
    _> NTPs [ 00000001 ] * NTP
    _> SNMPs [ 00000001 ] * SNMP

-> _DORKS: [ 00000110 ] ▼ Open Redirect (CWE-601) patterns
    _> ENGINES [ 00000003 ] * Dorking providers (Working)

-> _PEERS: [ 00000001 ] ▼ Blackholes (Community)
    _> WARPS [ 00000001 ] * Static W.A.R.P.S
    _> NODES [ 00000000 ] * Dynamic Radar Detector

-> _TOOLS: [ 00000016 ] ▼ Extra Tools (Misc)
    _> ABDUCTOR * Defensive Shield Detector
    _> AI.BOTNET * Intelligent Attack System
    _> AI.BROWSER * Private Sandbox Browser
    _> AI.EVASIVE * Automatic Evasion System
    _> AI.GAMES * Fun & Games Center
    _> AI.GEO * Geomapping System
    _> AI.GLOBAL_NET * Global UFONET Network
    _> AI.LIBRARY * Public (data.Links) Library
    _> AI.STATS * Live Stats Reporter
    _> AI.STREAMING * Video (data.Streams) Player
    _> AI.WEB * Graphical User Web-Interface
    _> BLACKHOLE * Warper (p2p.Botnet) Generator
    _> CRYPTER * Telegram (crypto.Community) System
    _> INSPECTOR * Objective Scanning Crawler
    _> AI.NETWORK * Network (MACs, IPs) Reporter
    _> XRAY * Ultra-Fast Ports Scanner
```

Funzionamento:

- Utilizza principalmente attacchi HTTP flood, ma supporta anche altre tecniche come attacchi DNS e UDP flood.
- Sfrutta una rete di “zombie” (bot compromessi) per distribuire il traffico dell’attacco su molti IP, rendendo l’attacco più difficile da mitigare.
- Ha sia una GUI che un’interfaccia a riga di comando (CLI), offrendo flessibilità agli utenti.
- Include vari metodi di attacco come GET, POST e CONNECT flood. Può anche utilizzare tecniche di spoofing per mascherare l’origine del traffico.


```
888      888 88888888888 .d88888b. 888b   888      888
888      888 888      d88PY888b 8888b 888      888
888      888 888      888      888 88888b 888      888
888      888 8888888 888      888 888Y88b 888 .d88b. 888888
888      888 888      888      888 888Y88b888 d8P  Y8b 888
888      888 888      888      888 888888 888888888 888
Y88b. .d88P 888      Y88b. .d88P 888      Y8888 Y8b.      Y88b.
'Y88888P' 888      'Y88888P' 888      Y888 'Y8888 'Y8888

{(D)enial(OFF)ensive(S)ervice[ToolKit]}-{by_(io=psy+/03c8.net)}

=====

▼ Version: 1.8 ▼ [DPh] DarK-PhAnT0m! ▼

-----

-> _BOTNET [DDoS]: [ 00000008 ] ▼ Bots (Available)
    |_> ZOMBIES [ 00000001 ] * HTTP GET (simple)
    |_> DROIDS [ 00000001 ] * HTTP GET (complex)
    |_> UCAVs [ 00000001 ] * WebAbuse (multiple)
    |_> ALIENS [ 00000001 ] * HTTP POST
    |_> X-RPCs [ 00000001 ] * XML-RPC
    |_> DNSs [ 00000001 ] * DNS
    |_> NTPs [ 00000001 ] * NTP
    |_> SNMPs [ 00000001 ] * SNMP

-> _DORKS: [ 00000110 ] ▼ Open Redirect (CWE-601) patterns
    |_> ENGINES [ 00000003 ] * Dorking providers (Working)

-> _PEERS: [ 00000001 ] ▼ Blackholes (Community)
    |_> WARPS [ 00000001 ] * Static W.A.R.P.S
    |_> NODES [ 00000000 ] * Dynamic Radar Detector

-> _TOOLS: [ 00000016 ] ▼ Extra Tools (Misc)
    |_> ABDUCTOR * Defensive Shield Detector
    |_> AI.BOTNET * Intelligent Attack System
    |_> AI.BROWSER * Private Sandbox Browser
    |_> AI.EVASIVE * Automatic Evasion System
    |_> AI.GAMES * Fun & Games Center
    |_> AI.GEO * Geomapping System
    |_> AI.GLOBAL_NET * Global UFONET Network
    |_> AI.LIBRARY * Public (data.Links) Library
    |_> AI.STATS * Live Stats Reporter
    |_> AI.STREAMING * Video (data.Streams) Player
    |_> AI.WEB * Graphical User Web-Interface
    |_> BLACKHOLE * Warper (p2p.Botnet) Generator
    |_> CRYPTER * Telegram (crypto.Community) System
    |_> INSPECTOR * Objective Scanning Crawler
    |_> AI.NETWORK * Network (MACs, IPs) Reporter
    |_> XRAY * Ultra-Fast Ports Scanner
```

Punti di Forza:

- Distribuzione del traffico: utilizza una botnet per distribuire il traffico dell’attacco, aumentando l’efficacia.
- Flessibilità: supporta vari metodi di attacco e tecniche di spoofing.
- Anonymity: l’uso di botnet può rendere più difficile rintracciare l’attaccante.

Debolezze:

- Complessità: più complesso da configurare e utilizzare rispetto a LOIC e HOIC.
- Legalità: Come per altri strumenti DDoS, il suo uso non autorizzato è illegale e comporta gravi conseguenze legali.

LOIC

Low Orbit Ion Cannon

LOIC è uno strumento di attacco DDoS open-source molto noto. Sviluppato originariamente da Praetox Technologies e successivamente reso popolare da gruppi hacktivistici come Anonymous.



Funzionamento:

- Esegue attacchi DoS principalmente inviando grandi quantità di pacchetti TCP, UDP o HTTP a un singolo indirizzo IP, con l'intento di sovraccaricare il server di destinazione e renderlo inaccessibile.
- GUI semplice e intuitiva, che permette agli utenti di inserire l'URL o l'indirizzo IP del target e avviare l'attacco con pochi clic.
- Diverse modalità di attacco, come HTTP flood, TCP flood e UDP flood.
- Possibilità di configurare la velocità e il numero di richieste per secondo da inviare al target.

Punti di Forza:

- Facilità d'uso: grazie alla sua interfaccia semplice, anche utenti con poca esperienza tecnica possono utilizzarlo.
- Open source: essendo open source, è facilmente accessibile e modificabile.



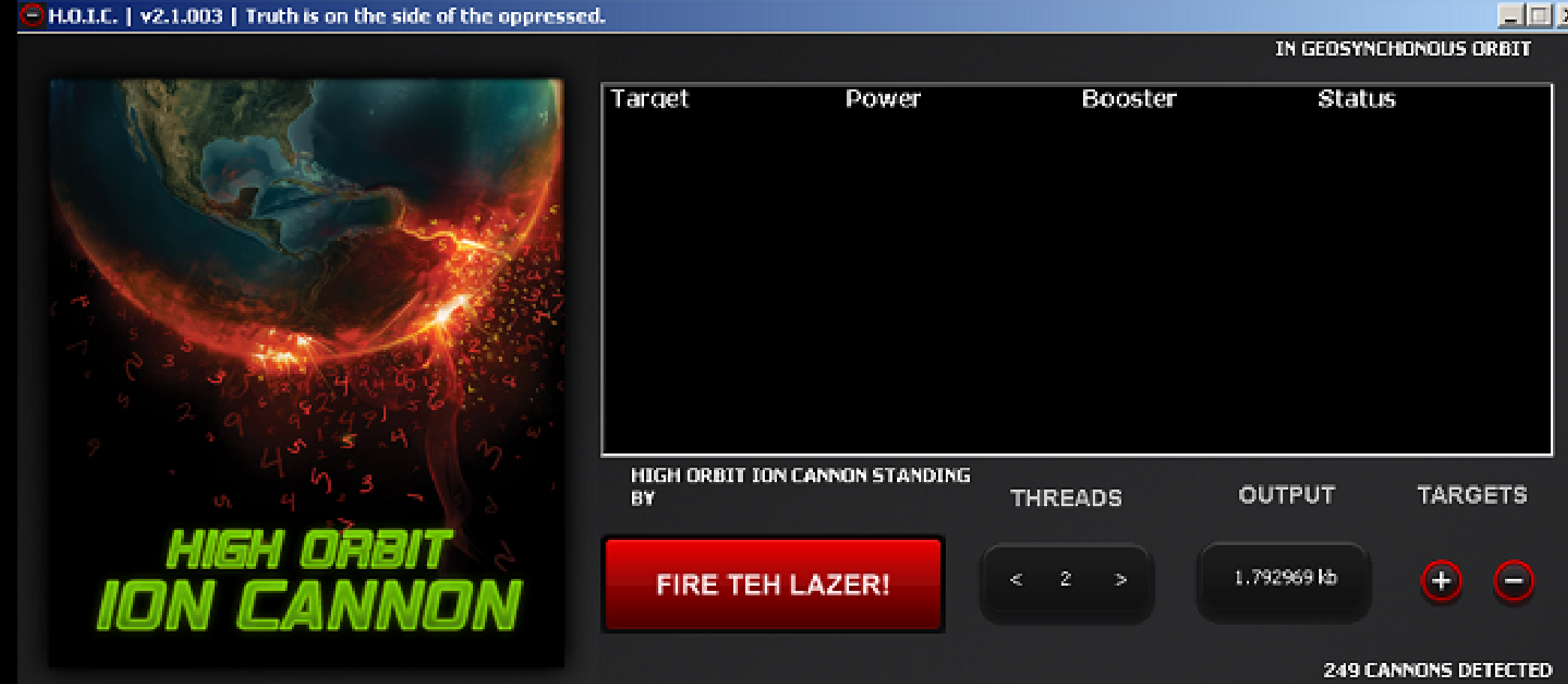
Debolezze:

- Tracciabilità: LOIC non nasconde l'IP dell'attaccante, rendendo facile per le autorità rintracciare chi esegue l'attacco.
- Efficacia limitata: l'efficacia di LOIC dipende dalla banda disponibile all'attaccante. È meno efficace contro obiettivi con larghezza di banda elevata e misure di difesa avanzate.

HOIC

High Orbit Ion Cannon

HOIC è un altro strumento di attacco DDoS, sviluppato per superare alcune delle limitazioni di LOIC. È stato creato per lanciare attacchi più potenti e sofisticati.

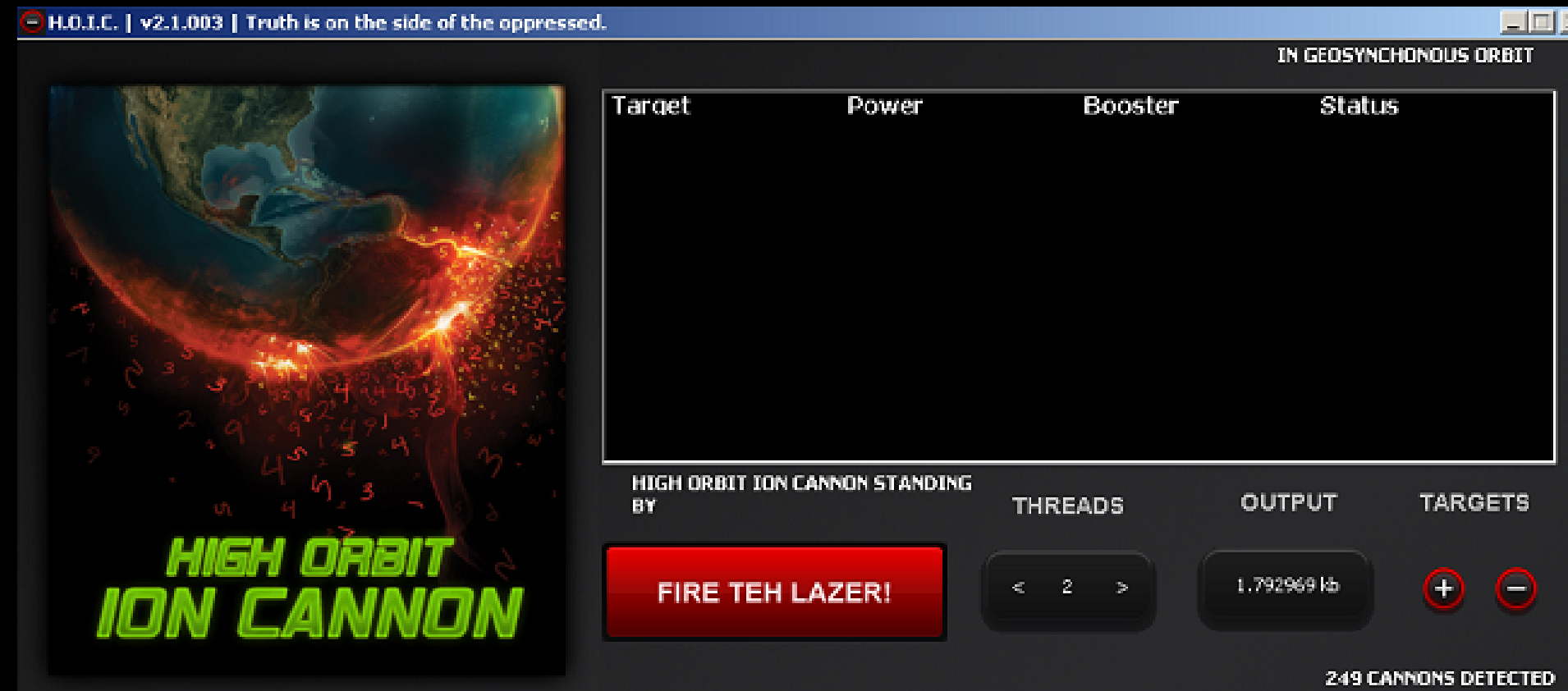


Funzionamento:

- HOIC utilizza attacchi HTTP flood, generando un volume enorme di richieste HTTP per saturare la banda del server target e causare un'interruzione del servizio.
- Una delle caratteristiche principali di HOIC è la capacità di utilizzare script chiamati "boosters", che aumentano significativamente la potenza dell'attacco modificando le richieste HTTP.
- Simile a LOIC, HOIC ha una GUI user-friendly che permette agli utenti di configurare e lanciare attacchi con facilità.

Punti di Forza:

- Potenza maggiore: grazie ai booster scripts, H0IC può generare un volume di traffico molto più elevato rispetto a LOIC.
- Scalabilità: può coordinare attacchi da più macchine, aumentando l'efficacia complessiva dell'attacco DDoS.

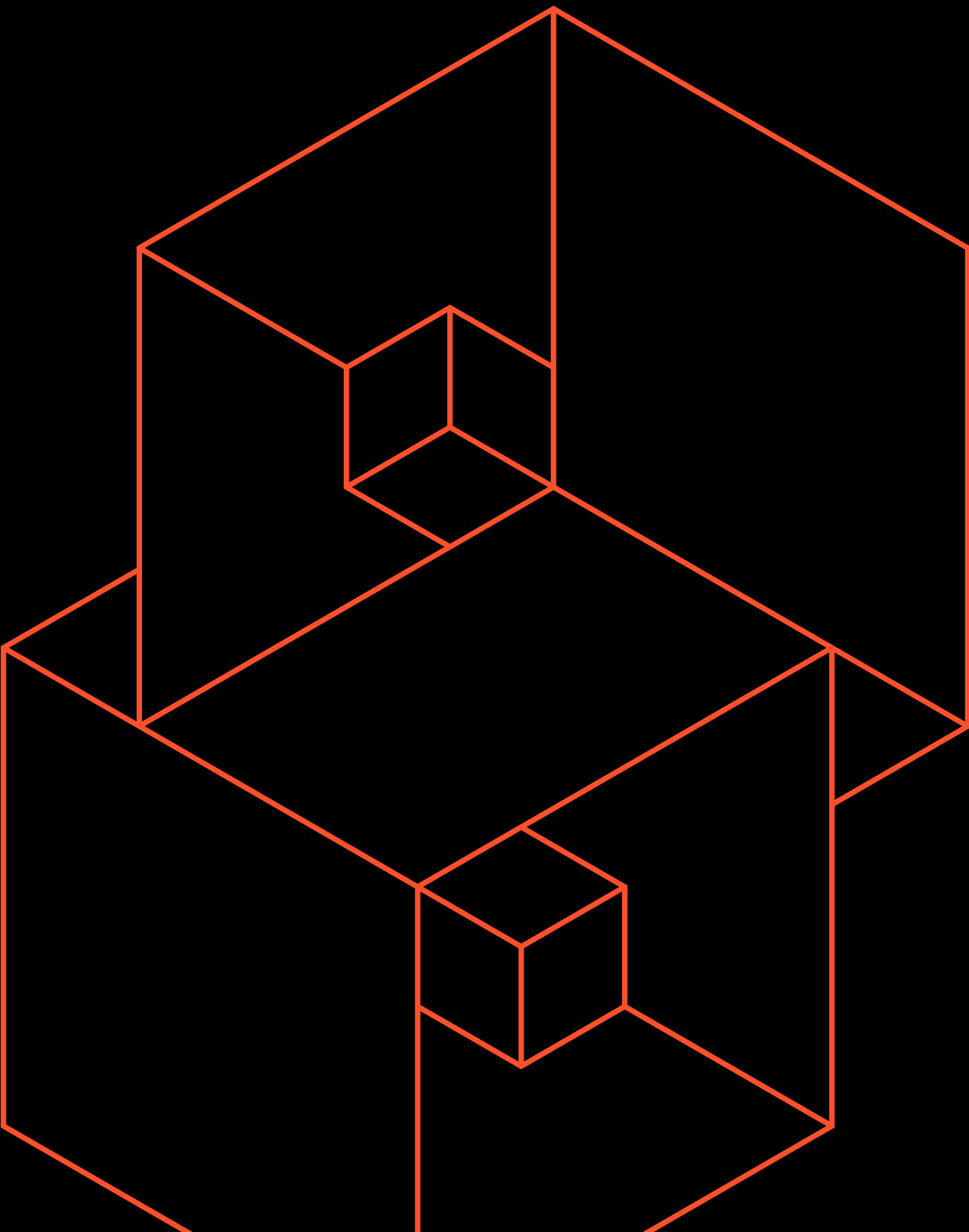


Debolezze:

- Tracciabilità: come LOIC, H0IC non nasconde l'IP dell'attaccante, rendendolo vulnerabile alla tracciabilità.
- Rischio legale: l'uso di H0IC per attacchi non autorizzati è illegale e può comportare gravi conseguenze legali.

SCHEMA RIASSUNTIVO

CARATTERISTICA	UFONET	LOIC	HOIC
Tipo di attacco	HTTP flood, DNS, UDP flood	TCP, UDP, HTTP flood	HTTP flood
Botnet	Sì, utilizza una rete di zombie	No	No
Interfaccia	GUI e CLI	GUI	GUI
Configurabilità	Molto flessibile (diversi metodi e spoofing)	Limitata	Elevata (grazie ai booster scripts)
Potenza	Elevata (grazie alla botnet)	Moderata	Elevata
Tracciabilità	Difficile da tracciare (uso di botnet)	Facile da tracciare	Facile da tracciare
Rischio legale	Alto	Alto	Alto
Efficienza	Molto efficiente grazie alla distribuzione	Dipende dalla banda dell'attaccante	Maggiore efficienza grazie alla scalabilità



GRAZIE

