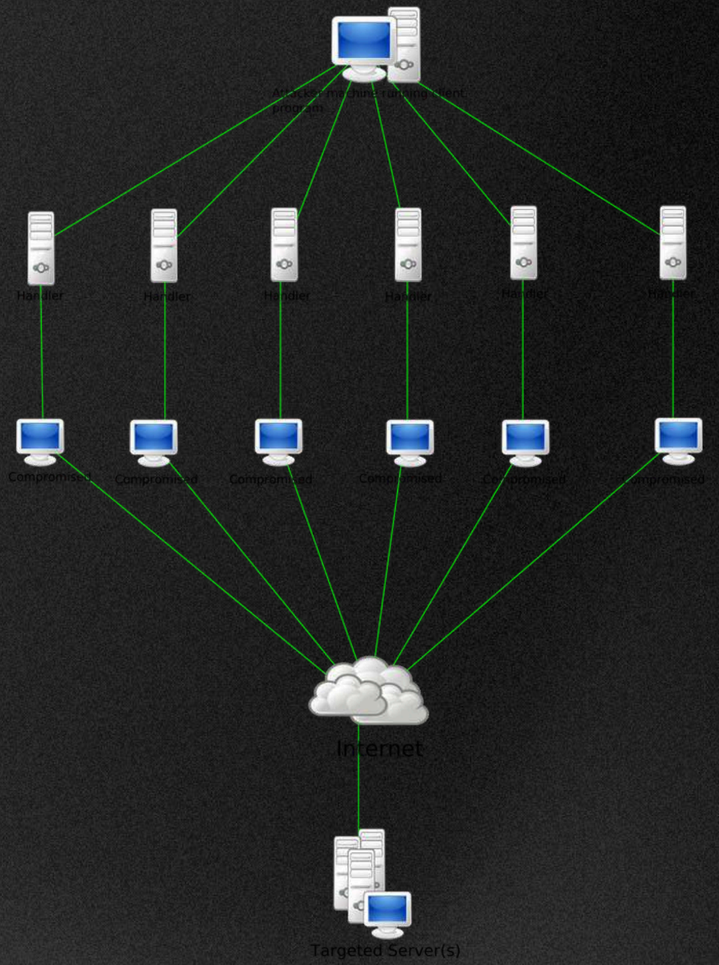

NET
REBELS
EPICODE

DDOS

Cos'è un attacco DDoS? Un attacco DDoS (Distributed Denial-of-Service) è una tipologia di attacco informatico che si caratterizza per il sovraccarico intenzionale di un sito web, server o risorsa di rete con traffico malevolo. Questo provoca un blocco o un malfunzionamento del sistema bersagliato, impedendo agli utenti legittimi di accedere al servizio e bloccando il traffico normale. A un livello generale, un attacco DDoS o DoS può essere paragonato a un ingorgo stradale creato da centinaia di richieste false ai servizi di "car sharing". Queste richieste appaiono legittime ai servizi di "car sharing", che inviano i loro autisti per prelevare i clienti, bloccando le strade e impedendo al traffico autentico di raggiungere la destinazione

Evoluzione degli attacchi Nonostante oggi richiedano un volume di traffico superiore rispetto a qualche anno fa, gli attacchi DDoS rimangono una minaccia concreta. Secondo i report di Kaspersky Labs, il numero complessivo di questo tipo di attacco è aumentato del 32% ogni anno. Un altro trend allarmante è rappresentato dalla disponibilità di piattaforme di lancio per attacchi DDoS come 0x-booter. In gergo tecnico, si parla di "DDos-as-a-service", ovvero attacchi DDoS su richiesta (o chiavi in mano), in grado di attivare circa 16.000 dispositivi IoT infettati dal malware Bushido. Questo evidenzia come la servitizzazione del cyber crimine sia ormai un fenomeno affermato. Come accennato in precedenza, è sempre più comune che gli attacchi vengano lanciati da botnet di terze parti, pagate per questo preciso scopo, e il trend sembra destinato a crescere.



DDOS DIRITTI PENALI

Diritto Penale Informatico: Attacchi Denial of Service L'evoluzione dei sistemi informatici ha portato a comportamenti illeciti online, spingendo il legislatore a introdurre norme specifiche nel diritto penale informatico. Tra questi comportamenti, gli attacchi Denial of Service (DoS e DDoS) sono particolarmente rilevanti e sono regolati da specifici articoli del Codice Penale italiano

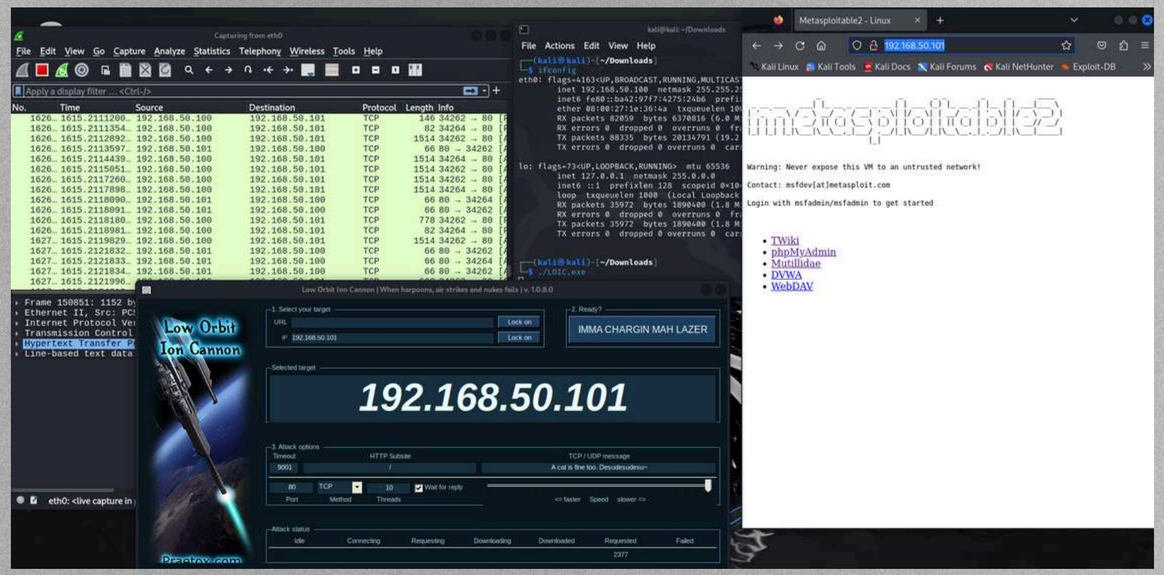
Articoli relativi agli attacchi DoS e DDoS Art. 635-quater L'articolo 635-quater del Codice Penale punisce chiunque danneggi o distrugga dati con il fine di rendere inservibili i sistemi informatici o telematici, o di ostacolarne il normale funzionamento. Le pene previste variano da 1 a 5 anni di reclusione. Questo articolo `e particolarmente applicabile in caso di attacchi Denial of Service (DoS e DDoS), che mirano a interrompere o bloccare il funzionamento dei servizi online. Esempi di tali attacchi includono: • Sovraccarico di un server con traffico eccessivo. • Utilizzo di botnet per eseguire attacchi distribuiti (DDoS). • Exploit di vulnerabilit`a nei sistemi per causare interruzioni.

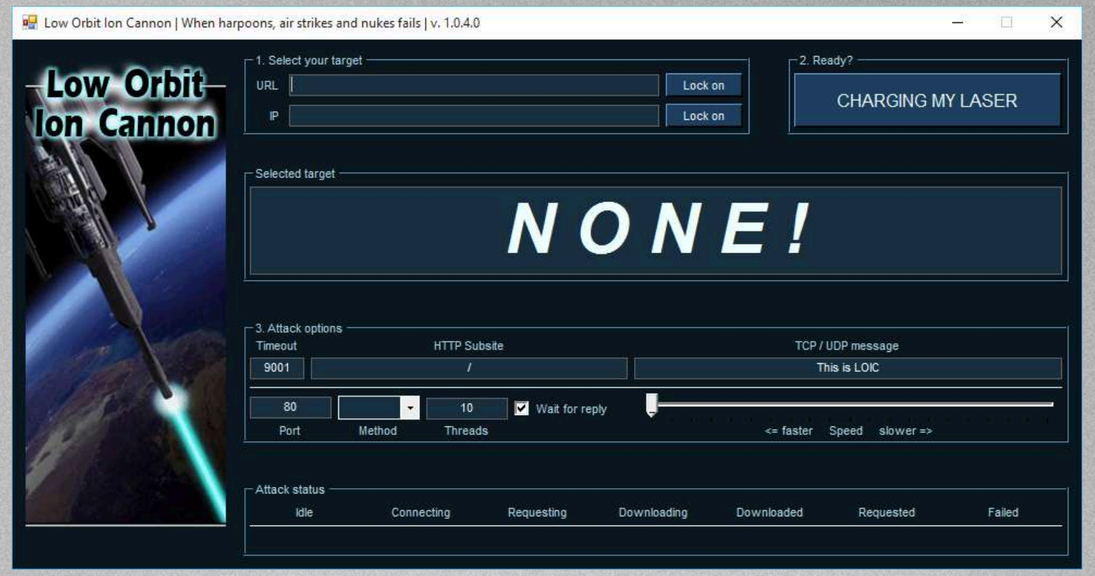
Conclusione L'unica ragione legittima per un attacco DoS sarebbe quella di aumentare la sicurezza della propria rete. Questo pu`o essere fatto assumendo qualcuno per penetrare nel proprio sistema o per attaccarlo con un DoS.

LOIC

LOIC

LOIC, acronimo di "Low Orbit Ion Cannon", è uno strumento di attacco di tipo denial-of-service (DoS) o distributed denial-of-service (DDoS). È un software open source originariamente creato per testare la sicurezza delle reti, ma è diventato noto per il suo utilizzo da parte di gruppi di hacktivisti come Anonymous per condurre attacchi contro vari siti web e servizi online.





LOIC

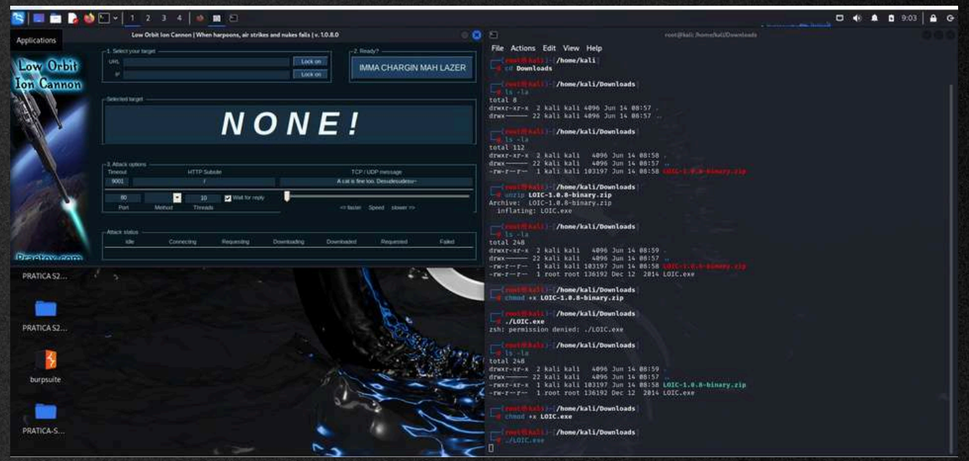
Fasi di attacco LOIC Un tipico attacco LOIC procede attraverso diverse fasi:

1. Selezione del bersaglio L'aggressore seleziona un sito Web, un server o una rete da interrompere. Gli obiettivi comuni sono siti aziendali, infrastrutture critiche e reti governative.

2. Armi LOIC viene scaricato e configurato per l'attacco. Le impostazioni vengono ottimizzate, tra cui: durata dell'attacco, limiti di velocità e parametri di spoofing.

3. Lancio dell'attacco L'aggressore lancia lo strumento LOIC contro il bersaglio. Per attacchi più grandi, vengono coordinate più istanze LOIC e botnet. Impatto dell'attacco Il target sperimenta la negazione del servizio, l'indisponibilità di risorse e servizi per gli utenti finali. Possono verificarsi danni finanziari, operativi e di reputazione.

4. Arresto dell'attacco L'attacco viene fermato arrestando lo strumento LOIC. I server di backup possono essere distribuiti per ripristinare i servizi. Vengono effettuate indagini forensi per rintracciare le fonti dell'attacco.

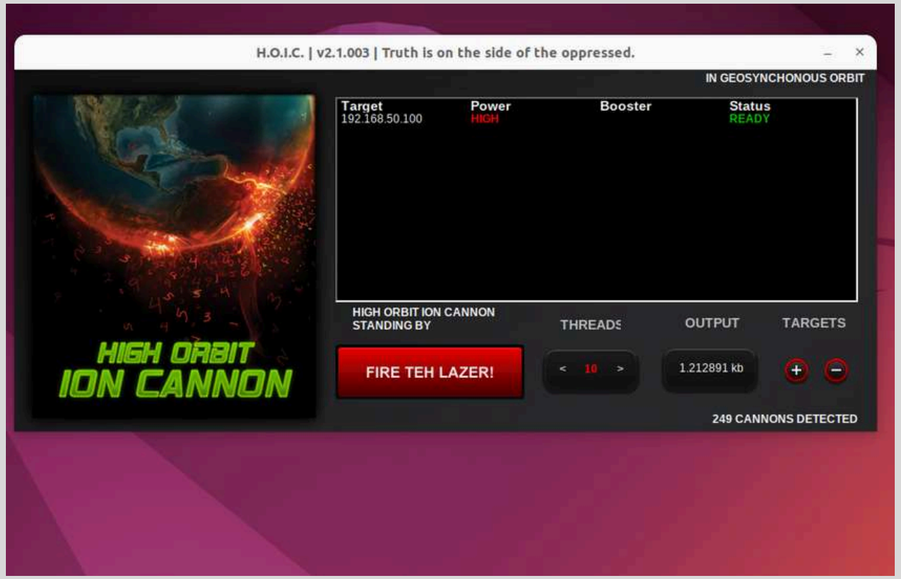


HOIC

HOIC

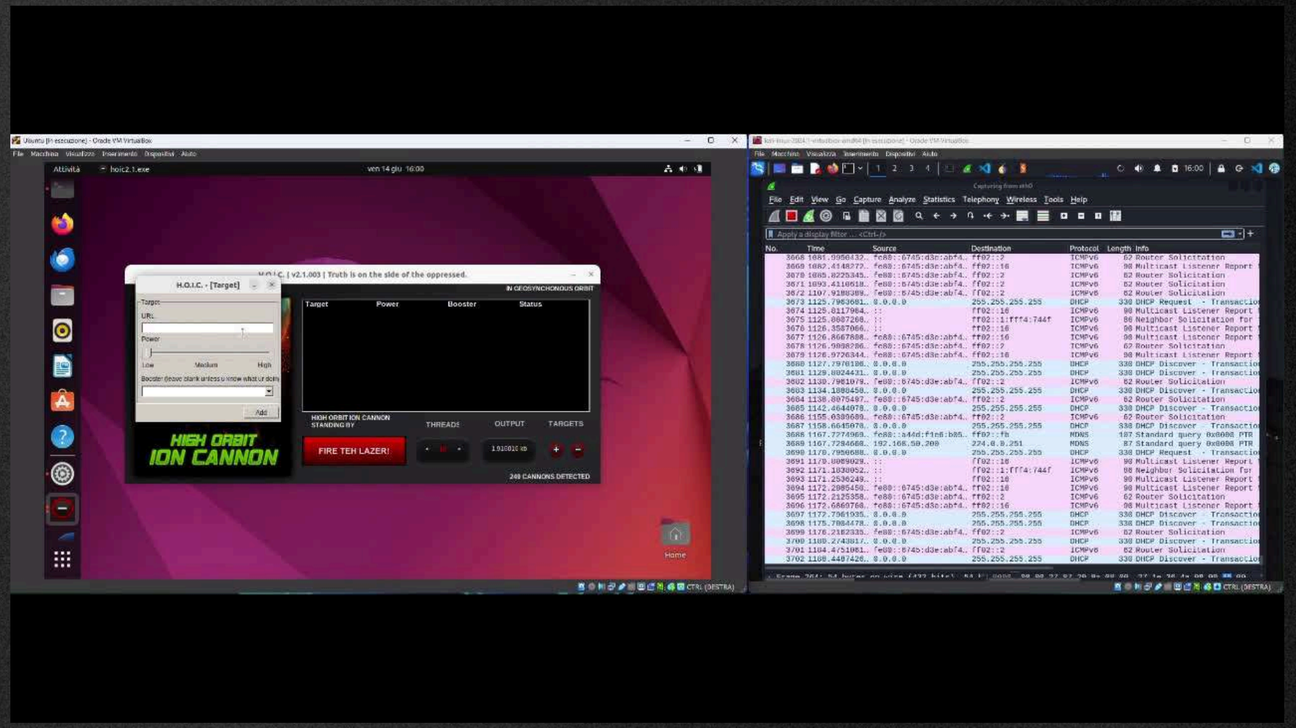
(HOIC) High Orbit Ion Cann HOIC è una piattaforma open-source progettata per valutare la resistenza delle reti e per eseguire attacchi di tipo DoS, capaci di colpire simultaneamente fino a 256 URL. È stato creato per sostituire il Low Orbit Ion Cannon (LOIC).

HOIC è utilizzato per lanciare attacchi di tipo DoS e DDoS, coordinati da diversi individui. L'attacco consiste nell'inondare un URL con traffico eccessivo al fine di renderlo inaccessibile. La sua interfaccia grafica semplice facilita il controllo e l'avvio degli attacchi mediante l'uso di "booster file", che consentono la personalizzazione degli attributi delle richieste. I "booster file" sono moduli configurabili che randomizzano gli header HTTP dei computer che partecipano all'attacco.



HOIC

Le principali limitazioni di HOIC sono che richiede un gruppo di utenti coordinati per essere efficace, con almeno 50 utenti necessari per lanciare un attacco e un numero maggiore per mantenerlo nel tempo se il sito target è protetto. Inoltre, manca di capacità sufficienti di anonimizzazione e randomizzazione per proteggere gli attaccanti. Sebbene HOIC sia stato originariamente sviluppato come strumento per il testing di resistenza, il suo uso per scopi illegali ha portato a una considerazione molto negativa. Gli Anonymous furono il primo gruppo a utilizzare HOIC pubblicamente in due diverse occasioni. La prima nel 2011 quando il gruppo hacktivista Anonymous l'ha utilizzato per lanciare attacchi DDoS di natura politica contro organizzazioni come PayPal, MasterCard e Sony, durante l'Operazione Payback. La seconda 19 gennaio 2012, in risposta alla chiusura di Megaupload, sempre da parte del gruppo Anonymous. Gli attacchi hanno preso di mira vari siti web, tra cui quelli del Dipartimento di Giustizia degli Stati Uniti e dell'FBI



UFONET

UFONET

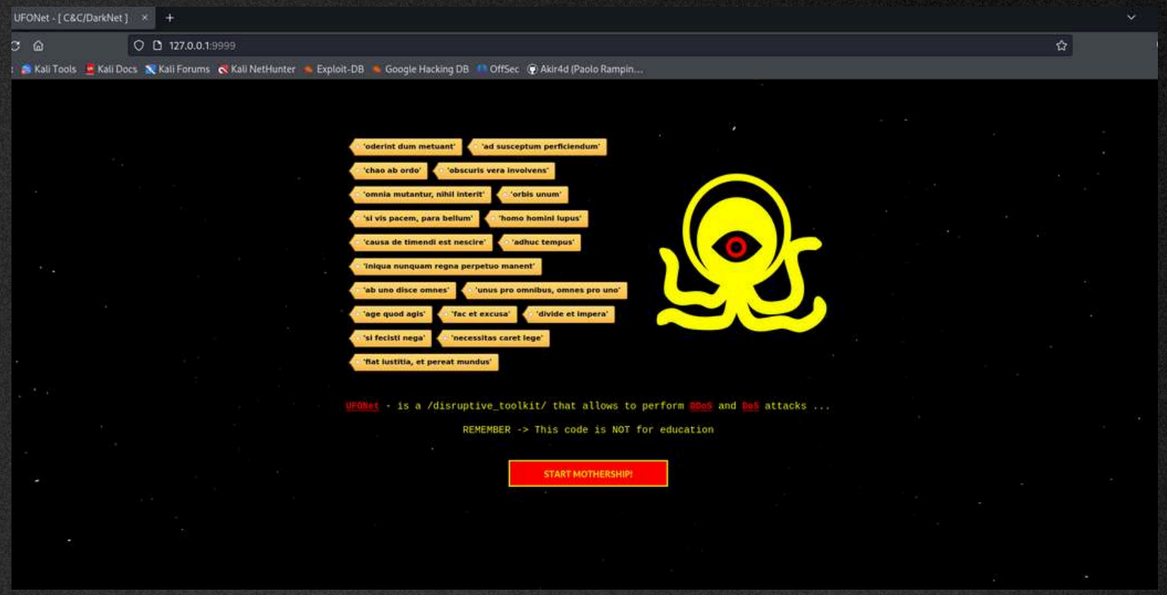
Ufonet è un toolkit gratuito P2P e criptografico che permette di eseguire attacchi DoS e DDoS

Ufonet sfrutta dei vettori di Open Redirect, ovvero la possibilità di ridirigere una chiamata verso un altro URL. Un attaccante può sfruttare delle vulnerabilità di una macchina per installarvi software RAT permettendogli di controllarla da remoto. A queto punto si parla di macchina “zombie”, ovvero una macchina pronta ad attaccare. Un insieme di questi “zombie costituisce una botnet capace di effettuare vari tipi di attacchi come il DDoS.
Vantaggi

·Ufonet ha una buona capacità di nascondere le proprie tracce;

·Offre fari tool per trovare vittime da infettar;

· È un P2P/darkent che gli permette di connettersi con altre macchine per eseguire complessi schemi d’attacco potendo, ad esempio, condividere i propri “zombie”;
·È gratuito e opensource.



Botnet

Globalnet | Wormhole | Explore

Attack

Welcome to: UFONet [C&C/DarkNET]

| HELP - F.A.Q. | AUTHOR |

Version: 1.8 ▼ [DPh] DarK-PhAnT0m! ▼

- Rel: Wen Mar 2 22:22:22 2022
- Dep: Fri Jun 14 07:33:01 2024

| LOG | CODE - MIRROR - SEED | UPDATE! |

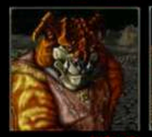
Mothership ID: **CYLON RAIDER**

- Stats: ViPR404+/(model:1^4)
- Ranking: Rookie
- Proxy: CHECK-TOR!
- Chargo: 12149
- Nodes: 2
- Jobs: 0


SHIP.BROWSER


SHIP.NEWS


SHIP.MISSIONS


SHIP.TV


GLOBAL.LINKS


GLOBAL.STREAMS


GLOBAL.BOARD


GLOBAL.GRID


GLOBAL.WARGAMES

Botnet

Configure requests

Search Botnet:

* Search automatically (may take time!)

SEARCH!

Download Botnet:

LIST NODES | TAKE ALL! | 46.163.118.220 TAKE IT!

Test Botnet:

Offline | ALL | Zombies | XML-RPCs | Attack Me!

View Botnet: Generate map!

Total Botnet = 12149

Zombies: 451
Aliens: 10
Droids: 13
UCAVs: 10
XML-RPCs: 64
NTPs: 29
DNSs: 11562
SNMPs: 10

GLOBAL.RADAR (nodes) = 0

SHIP.WARPS (nodes) = 2