

Alchimia delle Cyberwarfare: (D)DoS e Botnet nell'odierno panorama dei conflitti digitali

Speaker:

Emanuele “*Sniper*” De Lucia



21^a EDIZIONE

// Whoami

>_ Emanuele De Lucia

>_ Security Researcher && Cyber Intelligence Specialist

>_ Chief Intelligence Officer at  Cluter25

>_ Blog personale: www.emanueledelucia.net

// Verticali

>_ Reverse && Detection Engineering

>_ Metodologie e Tecniche di Evasione e Persistenza

>_ Attribuzione e classificazione del malware

>_ Adversary Tracking // Threat Hunting // Cyber Intelligence



// Agenda

- Cyberwarfare:
 - Definizione e Panoramica
 - Contesto
 - Lesson Learned
- (D)DoS e Botnet:
 - Cosa sono
 - Tipologie
- Principali Infrastrutture Ostili:
 - (D)DoS-for-Hire
 - Жадность
 - DDoSia
 - KillNet
 - Toffan
 - MTB (Mysterious Team Bangladesh)
- Impatti:
 - Geopolitica e Motivazioni
 - Tendenze Emergenti
- Mitigazione



// Cyberwarfare

→ Definizione

- Uso deliberato ed orchestrato di risorse informatiche per condurre operazioni militari, di intelligence e/o attività di sabotaggio. Esse possono includere:
 - Attacchi (D)DoS
 - Infiltrazione di reti / spionaggio
 - Sabotaggio infrastrutture critiche
 - Manipolazione dell'informazione



// Cyberwarfare

→ Constesto

- 24 Febbraio 2022: Offensiva militare della Federazione Russa contro Ucraina.
 - 22 attacchi (D)DoS subiti dall'Ucraina di media giornaliera (spike > 40)
 - Elevatissimo aumento degli attacchi (D)DoS rivolti a Paesi NATO
- 7 Ottobre 2023: Offensiva militare di Hamas contro Israele
 - 20 attacchi (D)DoS subiti da Israele di media giornaliera (spike > 50)
 - Elevato numero di attacchi (D)DoS contro Paesi terzi

// Cyberwarfare

→ Lesson Learned:

- Attacchi (D)DoS diffusi e numerosi
- Esteso ventaglio di settori colpiti da attacchi (D)DoS (energia, trasporti, governo, aerospazio, tecnologia, difesa, ricerca, educazione, media etc.etc.)
- (D)DoS come principale strumento offensivo e di propaganda per molti gruppi attivisti
- Rapido sviluppo di capacità utili a condurre attacchi (D)DoS da parte di diversi gruppi di minaccia
- Attacchi (D)DoS provenienti sia da progetti collaborativi, da reti proprietarie e (D)DoS-for-Hire



// (D)DoS e Botnet

→ Cosa sono:

- (D)DoS: è un tipo di attacco informatico che vede generalmente un gran numero di sistemi inviare grosse quantità di traffico ad un server o ad un sito web, sovraccaricandolo e impedendo agli utenti legittimi di accedervi
- Botnet: Rete di sistemi (spesso infetti da malware o da software di controllo) utilizzata per eseguire attacchi informatici, tra cui gli attacchi (D)DoS

// (D)DoS e Botnet

→ Tipologie:

- (D)DoS-for-Hire:
 - Infrastruttura DDoS a noleggio. L'attaccante solitamente non ne ha il possesso.
- Reti proprietarie:
 - L'attaccante ha il pieno controllo della rete botnet utilizzata
- Reti collaborative:
 - L'attaccante basa la propria capacità di attacco su di una partecipazione «sociale»
- Reti ibride:
 - L'attaccante dispone sia di risorse proprietarie che di una partecipazione «sociale»



21^a EDIZIONE

// (D)DoS e Botnet

→ (D)DoS-for-Hire:

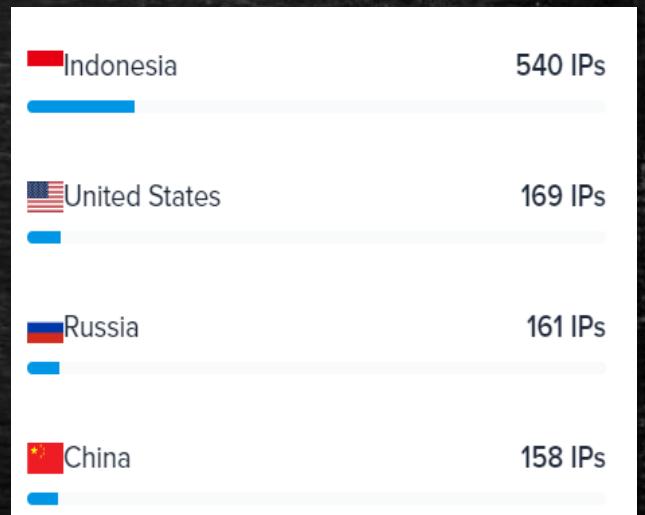
- Servizi commerciali diffusi almeno dal 2013. Vendite underground già dal 2007/2008.
- Consentono a chiunque di compiere facilmente attacchi (D)DoS efficaci.
- Nessuna particolare conoscenza tecnica richiesta.
- Utilizzo diffuso e largamente osservabile in diversi gruppi attivisti.
- Da 29 a 380 USD / mese per attacchi volumetrici da 15 fino a 510 Gbit/s
- Molteplici protocolli supportati L4 / L7
- Tendenza ottimizzazione attacchi L7



// (D)DoS e Botnet

→ (D)DoS-for-Hire: Dettagli di un reale attacco

- 2907 indirizzi IPv4
- L7 HTTP GET /
- Random User Agents



HACKINBO®
Winter **2023** Edition

// (D)DoS e Botnet

→ (D)DoS-for-Hire: Facilità d'uso

Attack Panel

The network is **online** and operating fine

Max. boots per day **unlimited**

Step 1: Select attack method

Layer 4 / Layer 7

Boot power **100 Gbit/s**

UDP

VIP power **+60 Gbit/s**

Yes

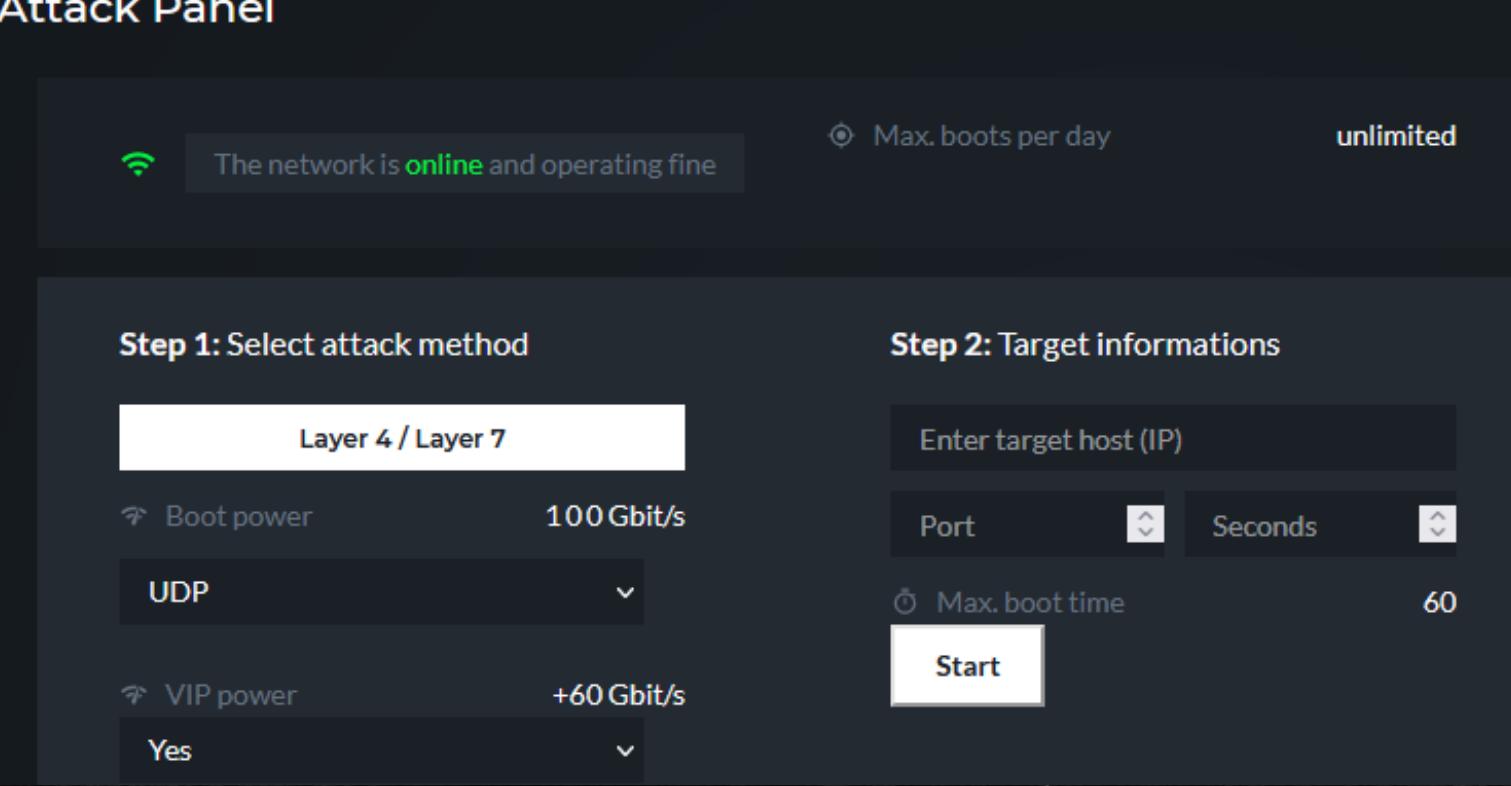
Step 2: Target informations

Enter target host (IP)

Port **Seconds**

Max. boot time **60**

Start



// (D)DoS e Botnet

→ (D)DoS-for-Hire: Facilità d'uso

Start Attack [Export API](#) [Create preset](#) [Load preset](#) [Schedule](#)

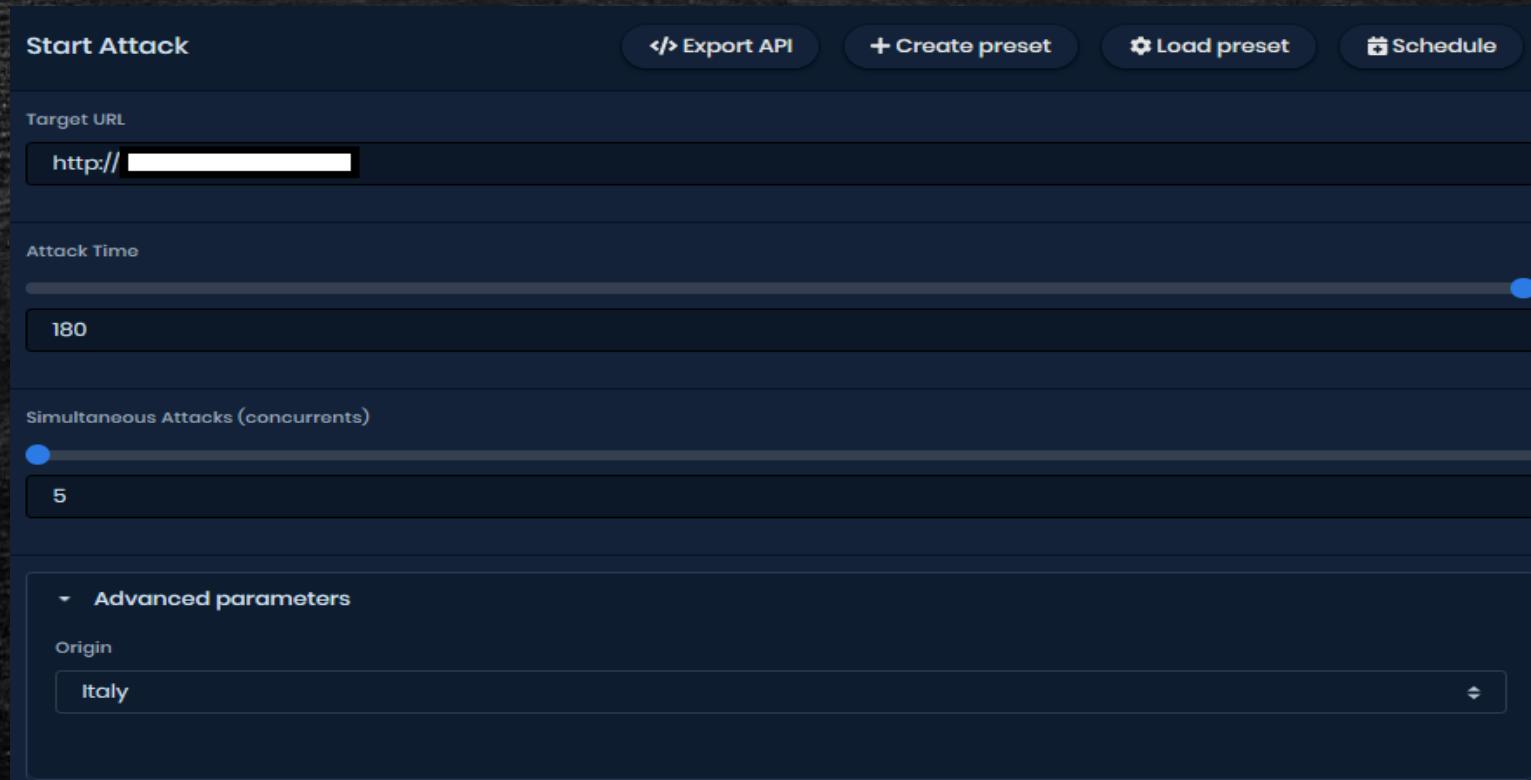
Target URL
http:// [REDACTED]

Attack Time
180

Simultaneous Attacks (concurrents)
5

Advanced parameters

Origin
Italy



// (D)DoS e Botnet

→ (D)DoS-for-Hire: Architetture comuni



HACKINBO®
Winter 2023 Edition

// Principali Botnet

→ ЖадНОСТЬ: Informazioni Generali

- Rete proprietaria su architettura multilivello
- Utilizzata probabilmente da attori State-Sponsored
- Indirizzi IPv4 di uscita su periferiche MikroTik
- Hunting Conditions:

Connection signature == « \x01\x00\x00\x00 » &&

DNS Recursion on TCP/UDP 53 &&

«MikroTik Test Server» on TCP 2000 &&

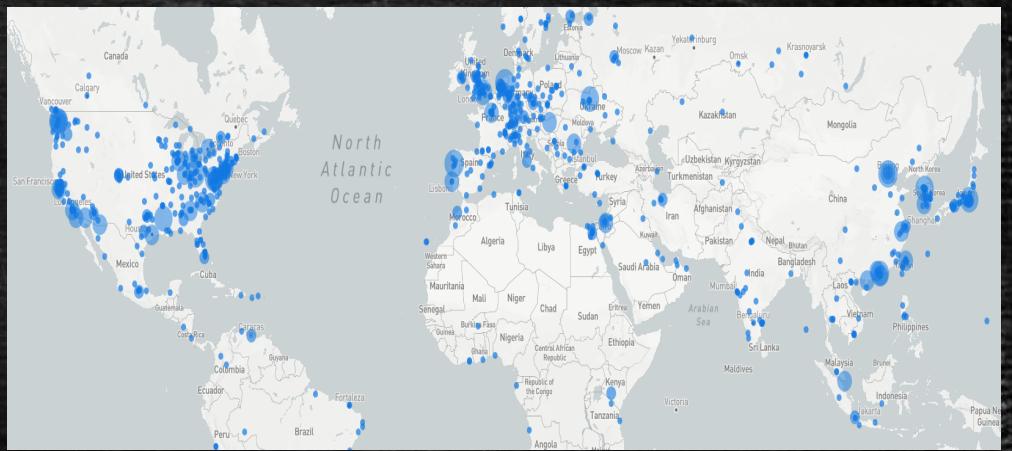
HTTP Proxy on TCP 8080 (L7 HTTP Attacks)

 146.110 LinkCom Ukraine, Lviv	\x01\x00\x00\x00
 34.237 Cypking Network & Communication Ltd Cyprus, Famagusta	\x01\x00\x00\x00
 142.241 eCourier Limited Bangladesh, Comilla	\x01\x00\x00\x00
 154.12 GK TELECOMUNICACIONES SA DE CV Mexico, Guadalajara	\x01\x00\x00\x00
 19.199 NORT TELECOM Brazil, Ibirapuera	\x01\x00\x00\x00

// Principali Botnet

→ ЖадНОСТЬ: Dettagli Tecnici

- Numero potenziali egress-IPv4: > 4k
(in Italia > 175)
- Diffusione Globale: Alta
- Tracciabilità potenziali egress-IPv4: Alta
- Tracciabilità tecnica targets: Medio-Bassa
- Ottimizzazione: L4 DNS Amplification (1:179)
- Overlap con botnet Mēris
- CVE-2018-14847 probabilmente usato per
abilitare l'HTTP Proxy Server sui dispositivi
(ca 500 attivi ad Ottobre 2023)
- Difficoltà Gestione: Media



HACKINBO®
Winter 2023 Edition

// Principali Botnet

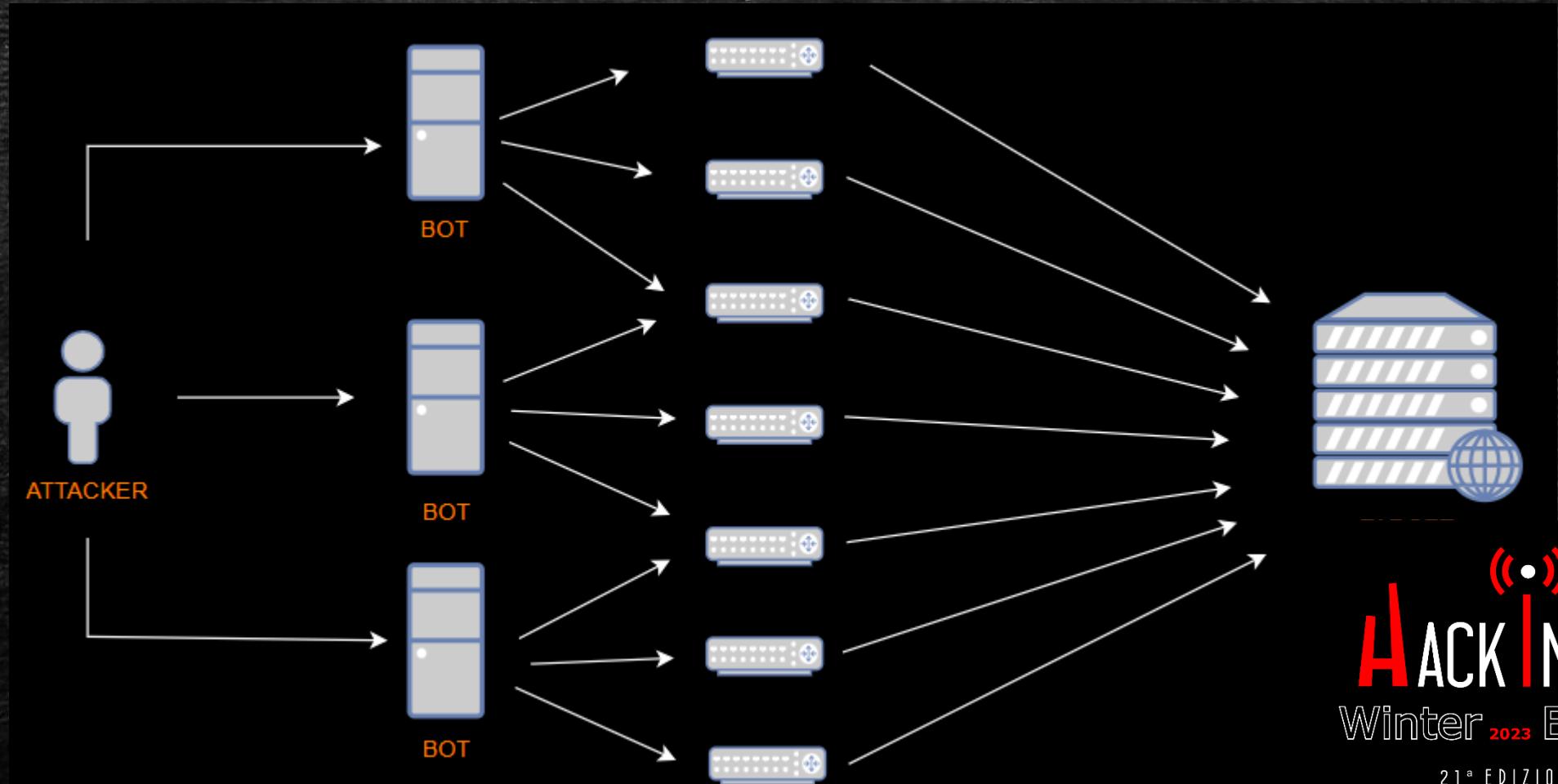
→ Жадность: Utilizzo

- Utilizzata come «vendetta» contro Ukrposhta (servizi postale Ucraino) per la stampa del francobollo commemorativo dell'affondamento della nave da guerra Moskva
- Largamente utilizzata nel contesto del conflitto Russo – Ucraino contro vari bersagli, fra quali: mfa.gov.ua, mil.gov.ua, msv.gov.ua, kmu.gov.ua etc. etc.



// Principali Botnet

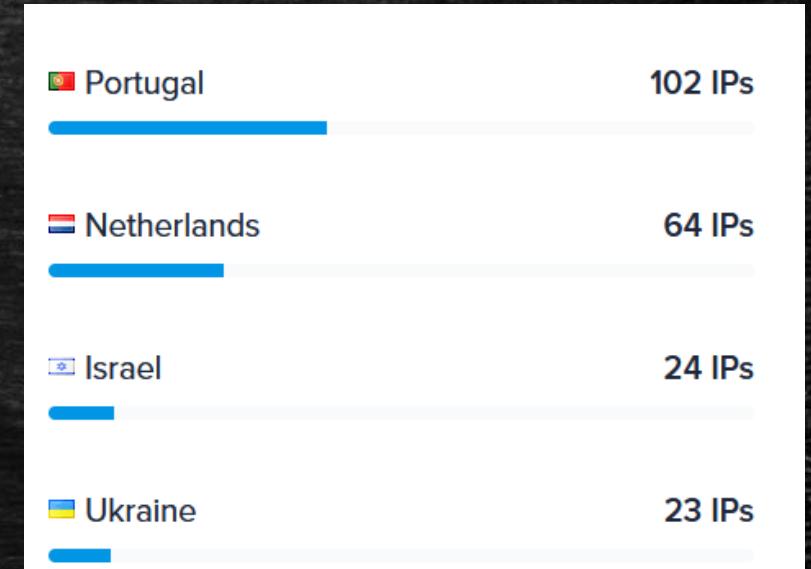
→ Жадность: Infrastruttura



// Principali Botnet

→ DDoSia: Informazioni Generali

- Rete ibrida su architettura multilivello
- Utilizzata in campagne attiviste vs Paesi NATO
- Comunità Telegram di > 40k account
- Python -> Go client per attacchi comunitari
- Alta variabilità degli indirizzamenti di uscita per la parte comunitaria. Bassa variabilità per la parte proprietaria.
- Medio – Alta complessità dell'infrastruttura. Presenta nodi mirati all'acquisizione di statistiche.



HACKINBO®
Winter 2023 Edition

// Principali Botnet

→ DDoSia: Dettagli Tecnici

- **Numero potenziali egress-IPv4:** ^_(ツ)_/^-
- **Diffusione Globale:** Bassa (per parte proprietaria)
- **Tracciabilità potenziali egress-IPv4:** Alta
(per parte proprietaria)
- **Tracciabilità tecnica targets:** Molto Alta
- **Ottimizzazione:** L7 HTTP/HTTPS FLOOD
- **Difficoltà di Gestione:** Medio-Alta



// Principali Botnet

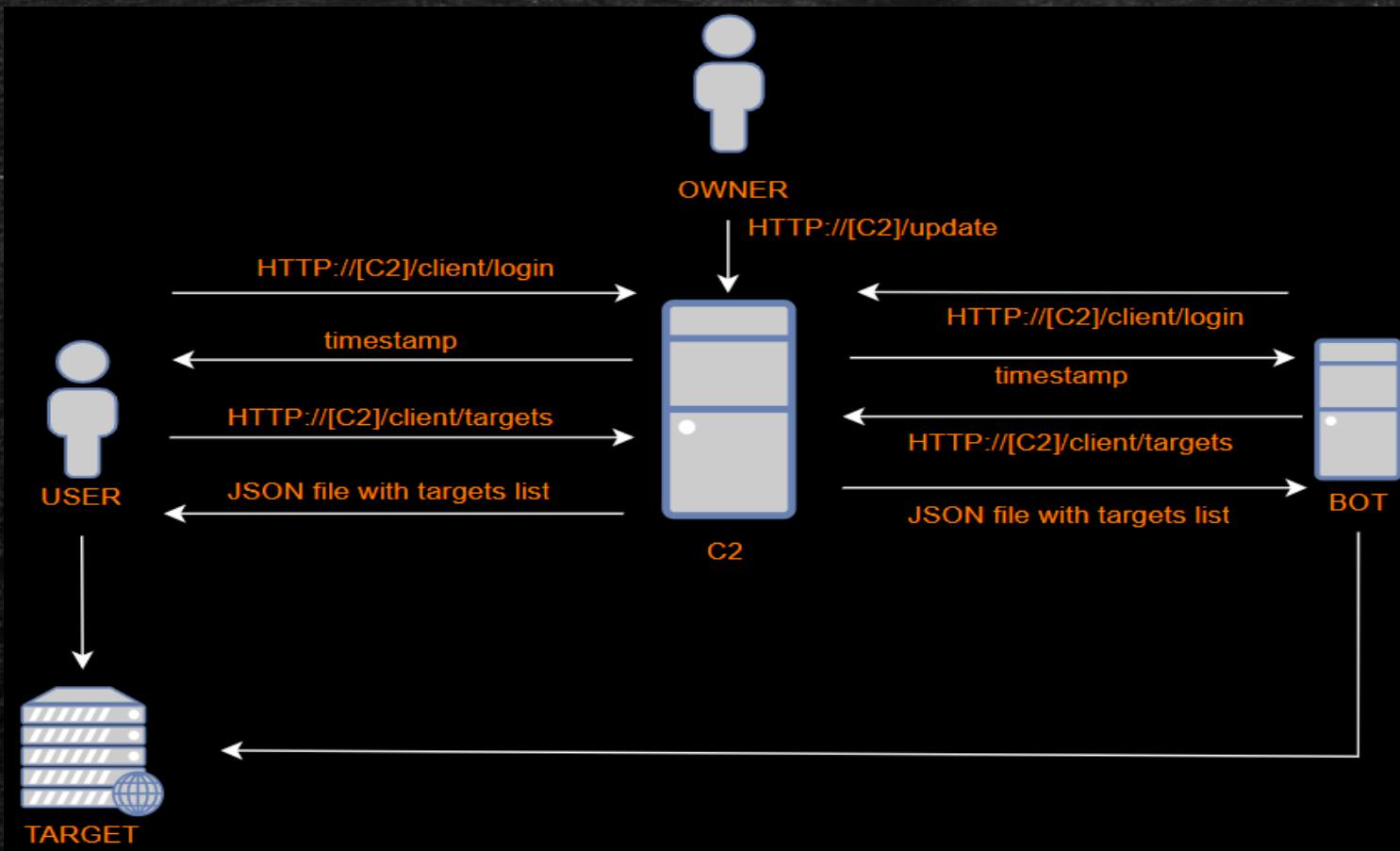
→ DDoSia: Utilizzo

- Attacchi osservati nel contesto del progetto attivista NoName057(16) contro Ucraina, Italia, Stati Uniti, Danimarca, Germania, Norvegia, Polonia, Finlandia etc. etc.
- Si caratterizza per la persistenza e la continua ciclicità con la quale gli attacchi vengono effettuati.
- Aggiorna di media le liste di attacco 3 / 4 volte per un numero di target che solitamente oscilla fra le 5 e le 20 al giorno



// Principali Botnet

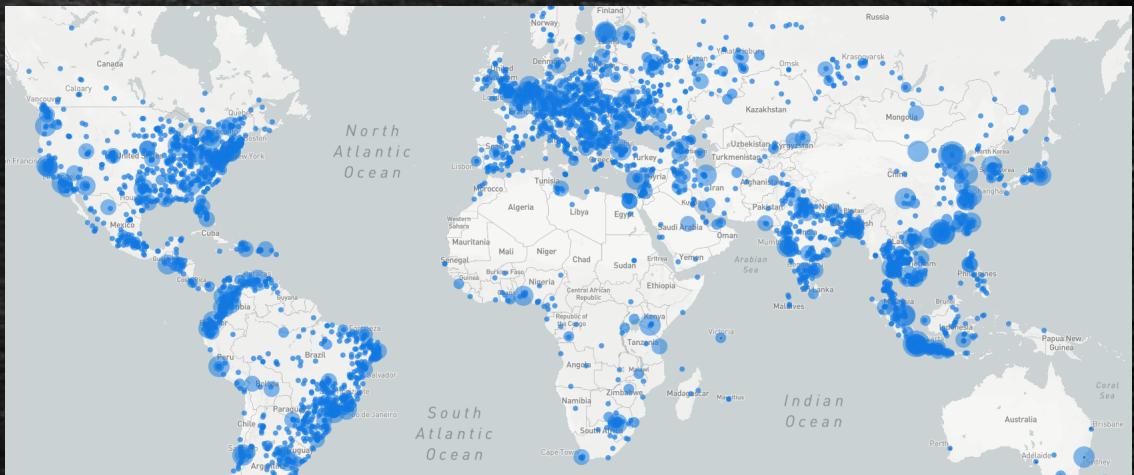
→ DDoSia: Infrastruttura



// Principali Botnet

→ KillNet: Infomazioni Generali

- Rete proprietaria /collaborativa
- CCAttack-based
- Diffusione globale egress-IPv4: Alta
- Tracciabilità potenziali egress-IPv4: Alta
- Sfrutta Sock4/5 e Open Proxy
- Ottimizzazione: L7 HTTP/HTTPS FLOOD
- Difficoltà di Gestione: Molto Bassa
- Egress-IPv4 potenziali > 15k nodi



// Principali Botnet

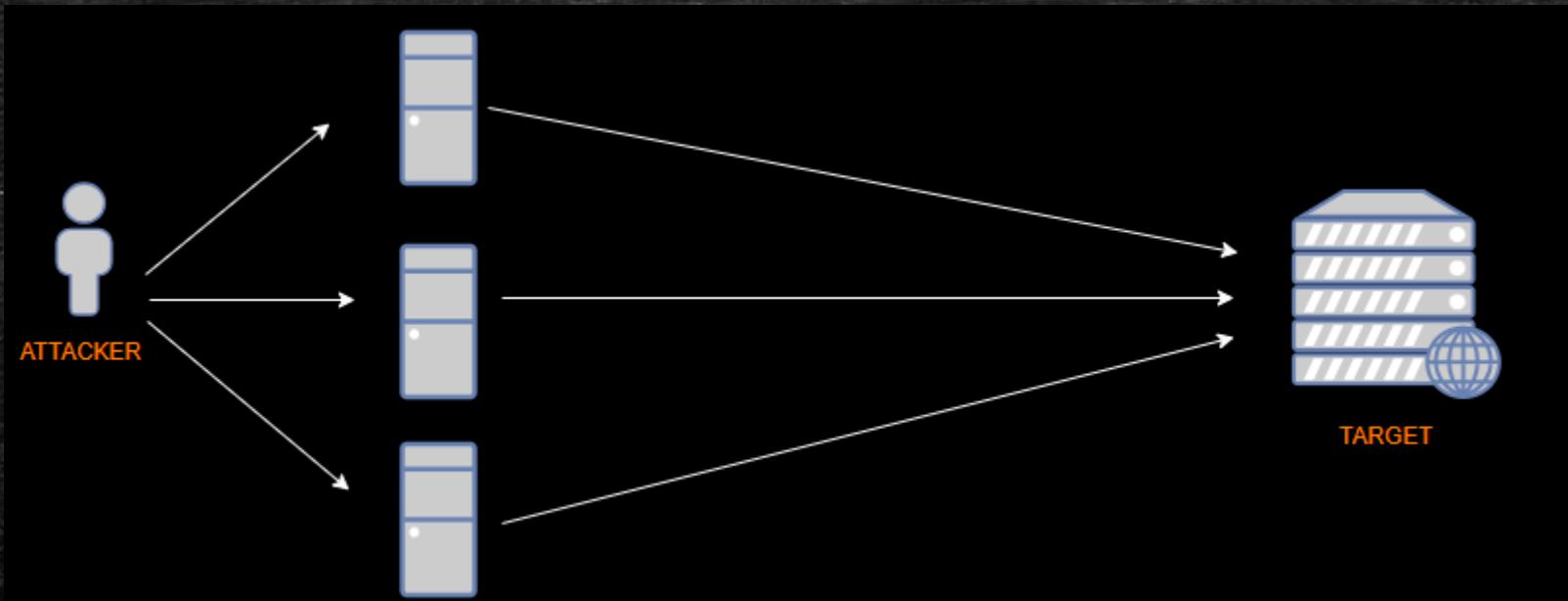
→ KillNet: Utilizzo

- Attacchi DDoS osservati nel progetto attivista KillNet contro Estonia, Italia, Lituania, Stati Uniti, Romania, Polonia, Romania etc.etc.
- Consistente ecosistema dei metodi e degli strumenti DDoS. Collaborazioni con servizi DDoS-for-Hire (principalmente Mirai-based, come Passion, Tesla, Panda e SkyNet)
- Progetto KillNet «Tesla» DDoS-for-Hire (50 bots per 100\$).
- Attacchi DDoS come principale topic della KillNet CYBER WAR «DARK» School



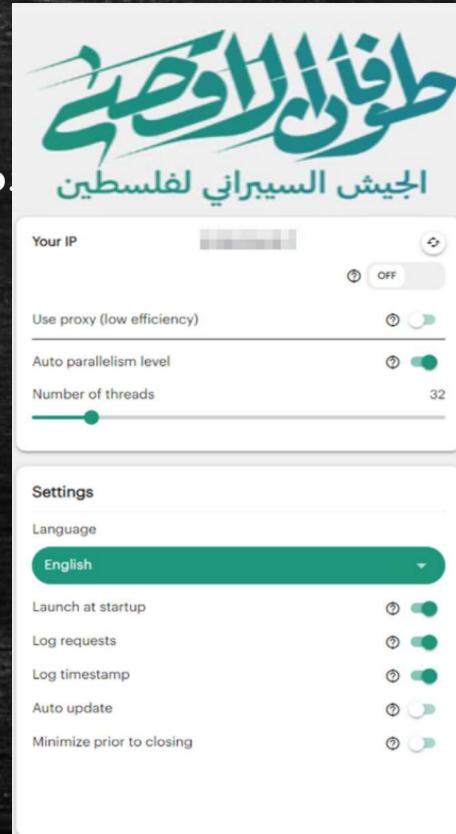
// Principali Botnet

→ KillNet: Infrastruttura



// Principali Botnet

- Toffan: Infomazioni Generali
- Rete collaborativa con agent Windows / Android
- Diffusione globale egress-IPv4: -_(ツ)_/-
- Esegue attacchi L7 HTTP/HTTPS
- Difficoltà di Gestione: Bassa
- Sfrutta GitHub per condividere l'elenco dei targets



HACKINBO®
Winter 2023 Edition

21ª EDIZIONE

// Principali Botnet

→ Toffan: Utilizzo

- Attacchi DDoS osservati nel progetto attivista Cyber Army of Palestine contro Israele, Stati Uniti, Emirati Arabi Uniti nel contesto del conflitto Hamas-Israele
- Facilità d'uso ed interfaccia grafica molto curata.
- Forte richiamo ad un progetto collettivo che si rivolge a «tutte le persone nei Paesi arabi».
- Orientato a massimizzarne la diffusione.
- Client scritto in Electron.



// Principali Botnet

→ Toffan: Infrastruttura



// Principali Botnet

→ Mysterious Team Bangladesh: Informazioni Generali

- Rete collaborativa basata su Raven Storm
- Diffusione globale egress-IPv4: -_(ツ)_/-
- Osservata principalmente in attacchi

L7 HTTP/HTTPS

- Difficoltà di Gestione: Medio / Bassa



Stress-Testing-Toolkit by Taguar258 (c) | MIT 2020
Based on the CLIF Framework by Taguar258 (c) | MIT 2020

The creators of Raven-Storm are not responsible
for any of your activitys or issues caused by Raven-Storm!
It is strictly illegal to exploit servers
which are not owned by you.



// Principali Botnet

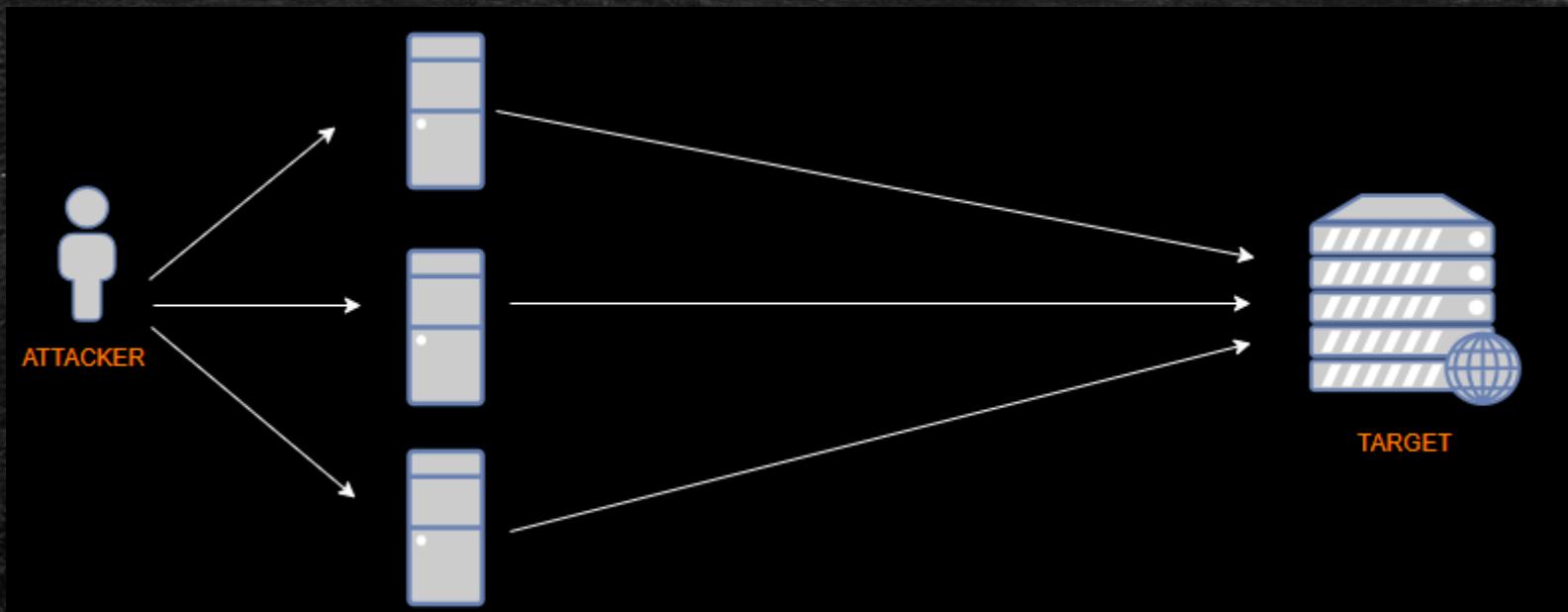
- Mysterious Team Bangladesh: Utilizzo
 - Attacchi DDoS osservati nel progetto attivista MTB contro India, Italia, Israele, Spagna, Estonia, Portogallo, Bulgaria, Turchia, Israele, Belgio, Regno Unito etc.etc.
 - Progetto MTB basato fortemente sull'utilizzo di tool open-source per attacchi DDoS.
 - Osservati principalmente attacchi L7 HTTP/HTTPS Flood vs bersagli che, almeno in apparenza, potessero garantire una buona probabilità di successo.
 - Collettivo che appare molto orientato all'auto-celebrazione, osservare ingaggi brevi con rivendicazione al minimo dissesto.
 - Spesso termine dell'ingaggio + cambio target all'attivazione di misure anti-DDoS



21^a EDIZIONE

// Principali Botnet

→ Mysterious Team Bangladesh: Infrastruttura



HACKINBO®
Winter 2023 Edition

// Geopolitica e Motivazioni

→ Key Points:

- Gli attacchi (D)DoS devono essere necessariamente considerati e valutati oltre la sfera tecnica.
- Essi influiscono attivamente sulla percezione comune riguardo le supposte capacità di difesa di un Paese e sull'opinione pubblica riguardo la resilienza delle infrastrutture colpite.
- Largamente presenti ed utilizzati nel contesto di entrambi i conflitti in essere. Probabile punto fermo nelle guerre moderne.
- Ampio ventaglio di motivazioni per effettuare un attacco (D)DoS:
i.e.: dissenso politico, attivismo, competizione, ritorsione, diversione, estorsione, conflitto, soddisfazione personale, terrorismo...



// Tendenze Emergenti

→ Key Points:

- **Aumento della Frequenza:** La frequenza degli attacchi (D)DoS risulta estremamente aumentata negli ultimi due anni.
- **Nuovi vettori:** HTTP/2 RRA (Rapid Reset Attack) sfrutta una vulnerabilità nel protocollo HTTP/2.
- **VM-based Botnet:** VPS invece che IoT. Si punta alla potenza del singolo nodo piuttosto che al numero. Sfruttamento di server non patchati o accesso mediante credenziali trapelate.
- **(D)DoS-for-Hire:** Sempre più gruppi di minaccia fanno affidamento su servizi (D)DoS-for-Hire per acquisire rapidamente capacità di condurre attacchi (D)DoS efficaci.



21^a EDIZIONE

// Mitigazione Veloce

→ Key Points:

- Identificare pattern comuni dell'attacco (*user-agent / URL Path*).
- Identificare sorgenti comuni dell'attacco (i.e. provider / ASN maggiormente frequenti).
- Identificare caratteristiche comuni degli egress-IPv4 e proattivamente bloccare il traffico proveniente da essi.

// Mitigazione meno-Veloce

→ Key Points:

- Riduzione superficie d'attacco. Isolare le risorse ed i servizi non strettamente necessari.
- Ottimizzare le architetture: ridondanza, bilanciamento dei carichi, auto-scaling... etc.etc.
- Incrementare il “costo degli attacchi”: Hardening OS e Software. Limite banda, limite numero connessioni simultanee, limiti ratei di trasmissione etc.etc.
- Sviluppo piano d'azione: Preparare e testare un piano per le emergenze che comprenda attacchi (D)DoS. Monitoraggio, Allerta I livello, Escalation, Gestione etc.etc.
- Contrastio Tecnico: Adozione WAF, Mitigazione Cloud-based etc.etc.

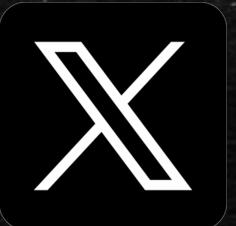


// Grazie !

→ Contact Points:



<https://www.linkedin.com/in/emanuele-de-lucia/>



https://twitter.com/Manu_De_Lucia

HACKINBO®
Winter 2023 Edition

21ª EDIZIONE