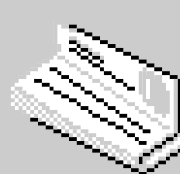
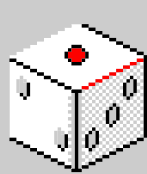
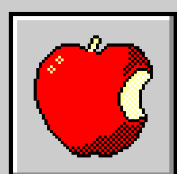


History of Dos and 000s



LOIC, HOIC,UFONET



11:11PM

What's a DDoS attack?



<https://it.wikipedia.org/wiki/DDoS>

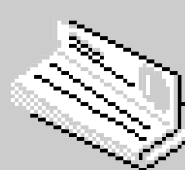
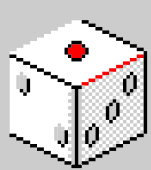
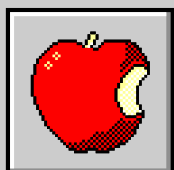


Gli attacchi **DDoS(Distributed Denial of Service)** hanno radici che risalgono agli anni '90: nel 1996, Panix subì SYN flood attack, mentre nel 1997 durante il DEF CON Khan C. Smith tolse l'accesso ad internet a tutta Las Vegas.

Il **primo grande attacco DDoS** documentato si è verificato nel **2000**, quando Michael Calce, noto come "Mafiaboy", ha lanciato una serie di attacchi contro grandi siti web come Yahoo!, eBay, Amazon, e CNN, causando interruzioni significative.

Questi attacchi si basano su una rete di computer infettati (**botnet**) che sovraccaricano i server bersaglio con un'enorme quantità di traffico, rendendo i servizi inaccessibili agli utenti legittimi.

Nel corso degli anni, la complessità e la frequenza degli attacchi **DDoS** sono aumentate, diventando uno strumento comune nelle cyber guerre e nelle proteste online. Oggi, la protezione contro i DDoS è una componente cruciale della sicurezza informatica per le organizzazioni di tutto il mondo.



[Indice](#)

What's a DoS attack?

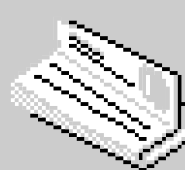
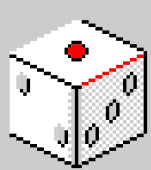
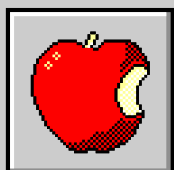


<https://it.wikipedia.org/wiki/DoS>



DoS è un tipo di attacco informatico in cui un singolo dispositivo (come un computer o un server) cerca di sovraccaricare la risorsa di destinazione (come un sito web o un server di rete) con un volume eccessivo di richieste. L'obiettivo principale di un attacco DoS è quello di **esaurire le risorse del sistema di destinazione**, come la larghezza di banda di rete o la capacità di elaborazione, rendendo così il servizio inaccessibile agli utenti legittimi.

- **Origine singola:** L'attacco proviene da una sola sorgente, che può essere un computer compromesso o un server controllato dall'attaccante.
- **Semplicità:** Poiché l'attacco viene eseguito da una singola fonte, può essere più semplice da individuare e mitigare rispetto a un attacco DDoS.
- **Tipologie:** Gli attacchi DoS possono includere il flooding della rete con pacchetti di dati, il consumo delle risorse del server con richieste valide ma onerose o il crash dei servizi attraverso vulnerabilità di sicurezza.



[Indice](#)

Hacktivismo

I criminali possono sferrare un attacco DDoS contro società o siti web di cui non condividono le **convinzioni filosofiche o ideologiche**.

Guerra cibernetica

I governi possono usare le minacce informatiche come gli attacchi DDoS per **indebolire l'infrastruttura** critica di uno stato nemico.

Estorsione

I criminali spesso si servono delle minacce DDoS per **estorcere denaro alle aziende**.

Intrattenimento

Molti attacchi vengono sferrati dagli hacker a puro scopo di divertimento per **creare scompiglio** o provare il crimine informatico.

Competizione

Un'azienda può sferrare un attacco DDoS contro un'altra società per **guadagnare un vantaggio** competitivo.

Diritto di accesso

Gli attacchi DoS e DDoS **impediscono agli utenti legittimi di accedere ai servizi online**, violando il loro diritto di accesso a informazioni e servizi. Particolarmente critico per servizi essenziali come quelli bancari, sanitari e governativi.

Danni economici

Possono causare gravi **perdite finanziarie per le aziende**, non solo per il tempo di inattività, ma anche per i costi associati alla mitigazione e riparazione dei danni.

Responsabilità civile e penale

I responsabili degli attacchi possono essere **perseguiti sia civilmente che penalmente**. Questo può comportare multe sostanziali, risarcimenti per danni e pene detentive.

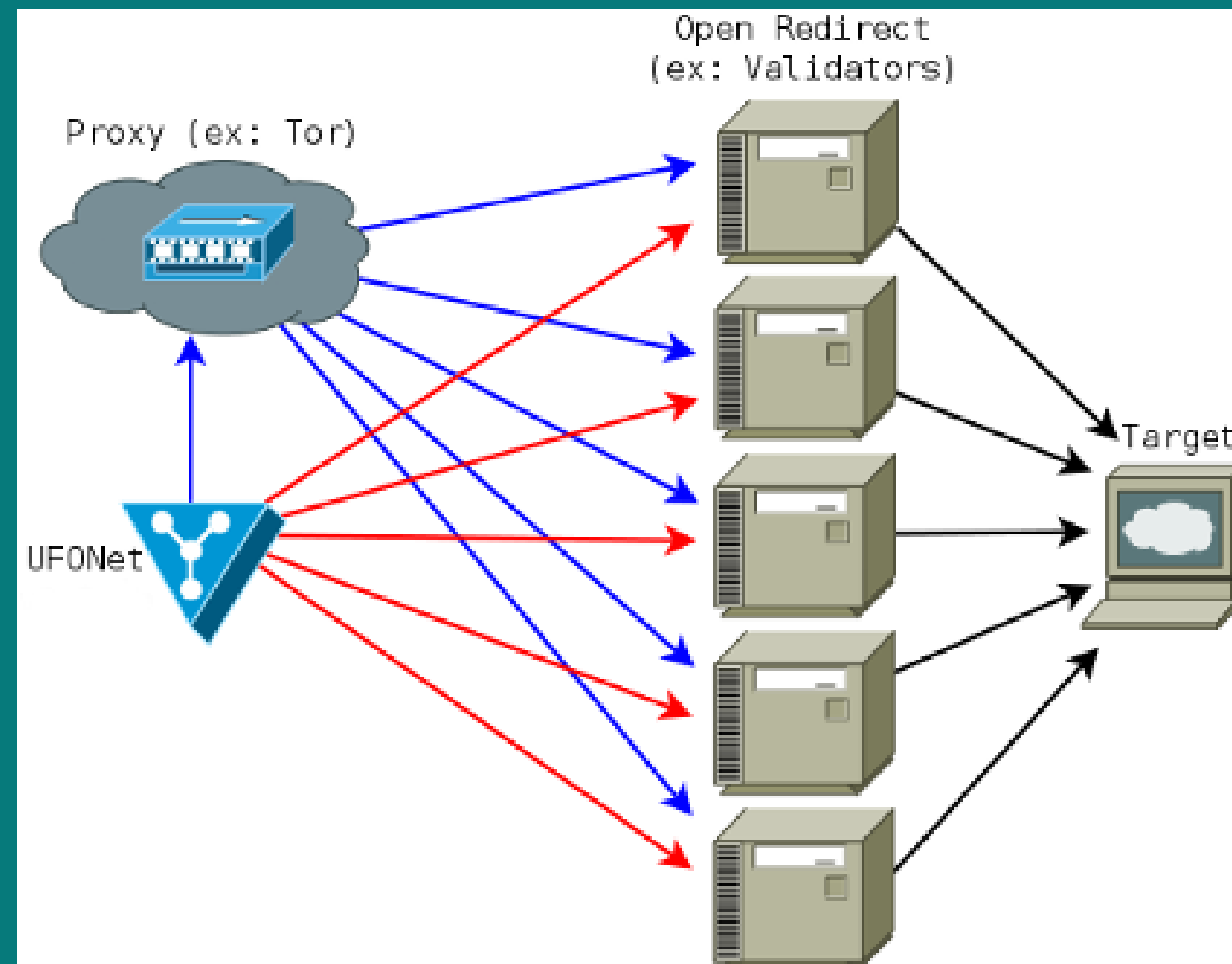
Uso di botnet

L'uso di botnet per attacchi DDoS comporta ulteriori implicazioni legali. Compromettere computer di terze parti per creare una botnet è un **reato grave**, con pene che possono includere lunghe condanne detentive.

Responsabilità degli intermediari

I provider di servizi internet (ISP) e altre entità intermedie possono essere tenuti a implementare misure di sicurezza per prevenire attacchi DDoS. La **mancata adozione di tali misure** può comportare responsabilità legali.

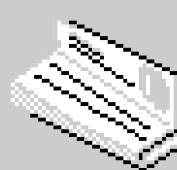
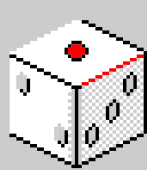
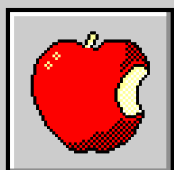
UFONet



<https://it.wikipedia.org/wiki/UFONet>

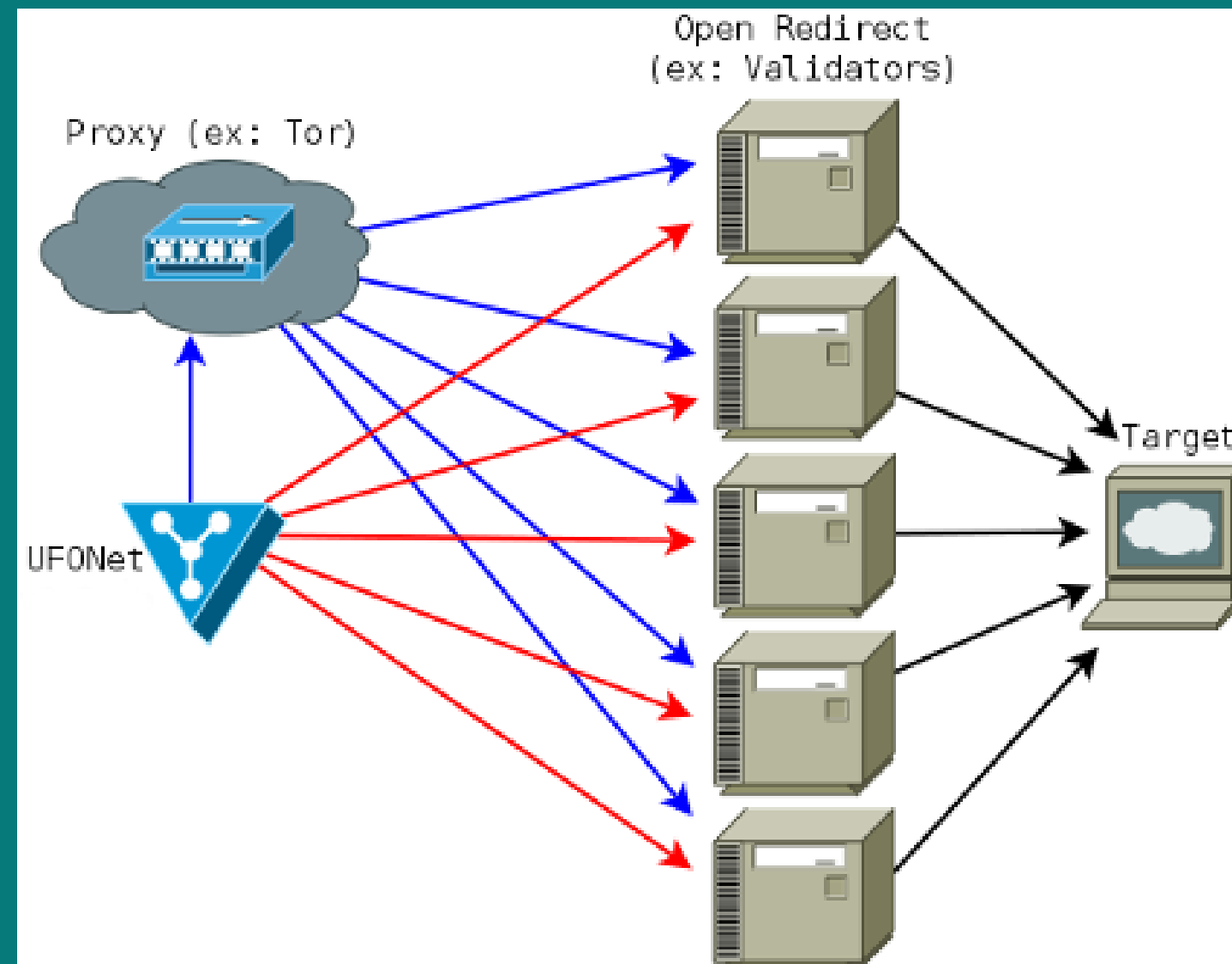
UFONet (User Friendly Open Network) è un **toolkit** di tipo DDoS (Distributed Denial of Service) open-source, creato da un gruppo di sviluppatori anonimi nel **2016**.

E' stato progettato per lanciare **attacchi DDoS contro siti web e servizi online**, con lo scopo di renderli inaccessibili o rallentare notevolmente le loro prestazioni. Ciò viene fatto inviando un grande numero di richieste HTTP verso il bersaglio, in modo da **sovraccaricare il server** e renderlo impossibilitato a rispondere alle richieste legittime degli utenti. Utilizza una tecnica chiamata "**amplification attack**", che consiste nell'utilizzare server di terze parti (ad esempio, server DNS o NTP) per amplificare il traffico verso il bersaglio. Ciò consente di **aumentare la potenza** dell'attacco e rendere **più difficile l'identificazione** delle fonti dell'attacco.



[Indice](#)

UFONet



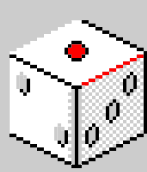
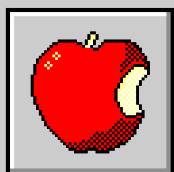
<https://it.wikipedia.org/wiki/UFONet>

Il **toolkit** è stato creato con l'**obiettivo di dimostrare la vulnerabilità dei sistemi di sicurezza online** e di sensibilizzare gli sviluppatori e gli amministratori di sistema sulla **necessità di implementare misure di sicurezza** adeguate per proteggere i loro siti web e servizi.

Clonando il sito web di UFONet, esso è un toolkit distruttivo, P2P e crittografico che permette di eseguire attacchi DoS e DDoS sul Layer 7 (APP/HTTP) attraverso l'exploit di vettori Open Redirect su siti web di terze parti per agire come una botnet, e sul Layer3 (Network) abusando del protocollo.

Funziona anche come **DarkNET criptata** per pubblicare e ricevere contenuti creando una rete globale client/server basata su un'architettura P2P a connessione diretta.

Bisogna sottolineare che chiunque esegua questo tipo di attività senza avere una conoscenza approfondita delle tecnologie coinvolte e delle conseguenze legali, è considerato un "lamer", un aspirante cracker con conoscenze informatiche limitate e basilari.



Simulazione di attacchi realistici

UFONet può simulare attacchi realistici (inclusi di tipo TCP SYN flood, UDP flood, ICMP flood) permettendo di **valutare la resistenza del sistema o della rete bersaglio.**

Personalizzazione degli attacchi

UFONet consente di personalizzare gli attacchi DDoS in base alle **esigenze specifiche** (tipo di attacco, frequenza e durata).

Analisi dei risultati

Fornisce una serie di metriche e **rapporti sull'attacco** (velocità di trasferimento dei dati, numero di pacchetti inviati e ricevuti, risposta del sistema o della rete bersaglio).

Accessibilità

Essendo un toolkit **open-source e gratuito** risulta accessibile a tutti.

Facile da utilizzare

Interfaccia utente **user-friendly**, anche per gli utenti non esperti in sicurezza informatica

Utilizzandolo per lanciare
attacchi DDoS illegali
contro sistemi o reti
senza autorizzazione, può
comportare conseguenze
serie.

Può non essere in grado di simulare tutti i tipi di attacchi DDoS, il che può **limitare** la sua **efficacia** come strumento di test di **sicurezza**.

Talvolta segnala attacchi DDoS che non sono realmente in corso, portando a **falsi allarmi** e perdite di tempo.

Richiede costante
manutenzione e
aggiornamento per
rimanere efficace.

Essendo user-friendly,
permette di lanciare
attacchi anche a **utenti
inesperti** con conoscenze
informatiche limitate che
non sono consapevoli
delle loro azioni.

Computer infetti trovati

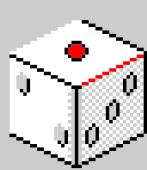
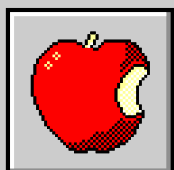
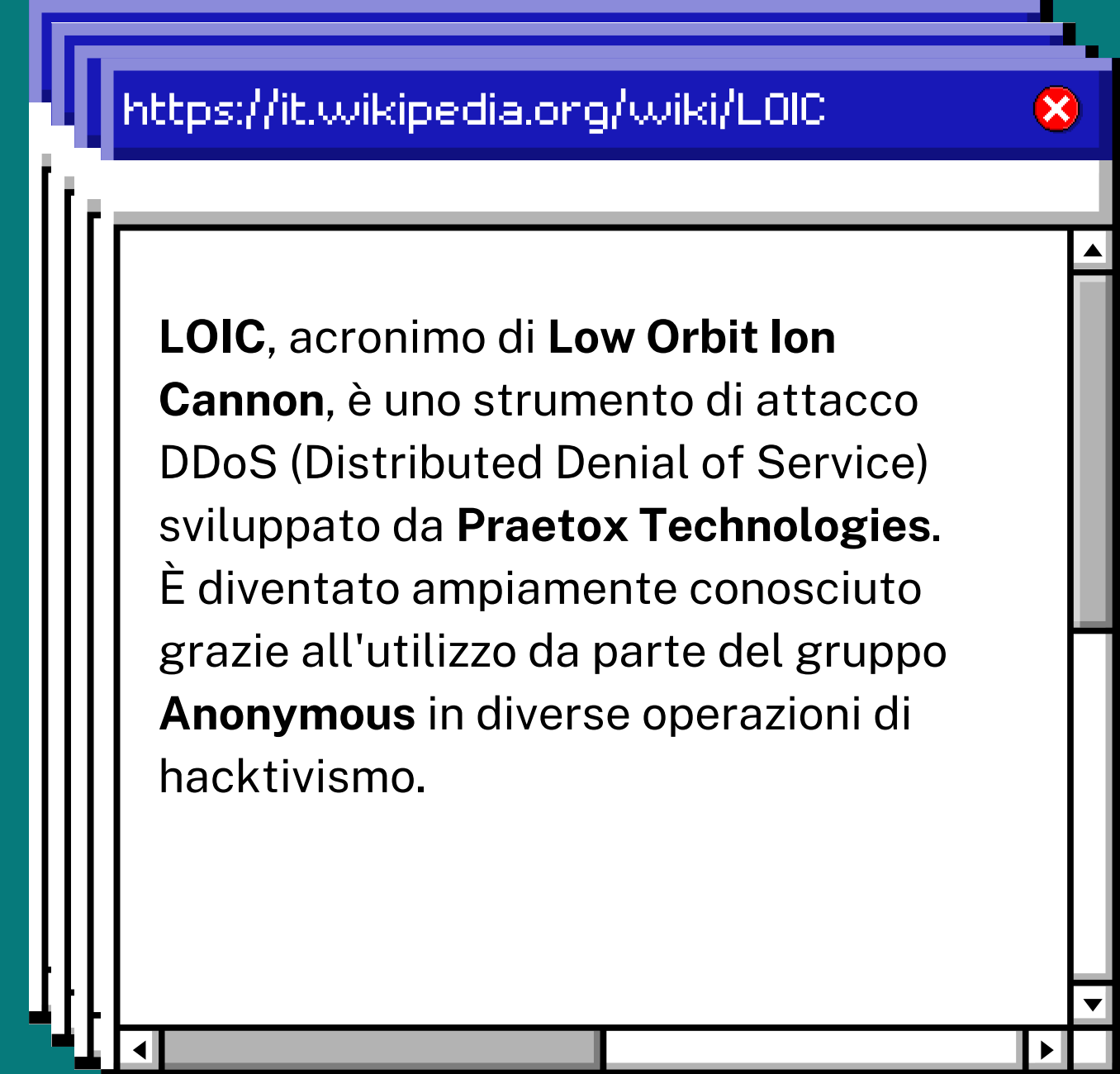
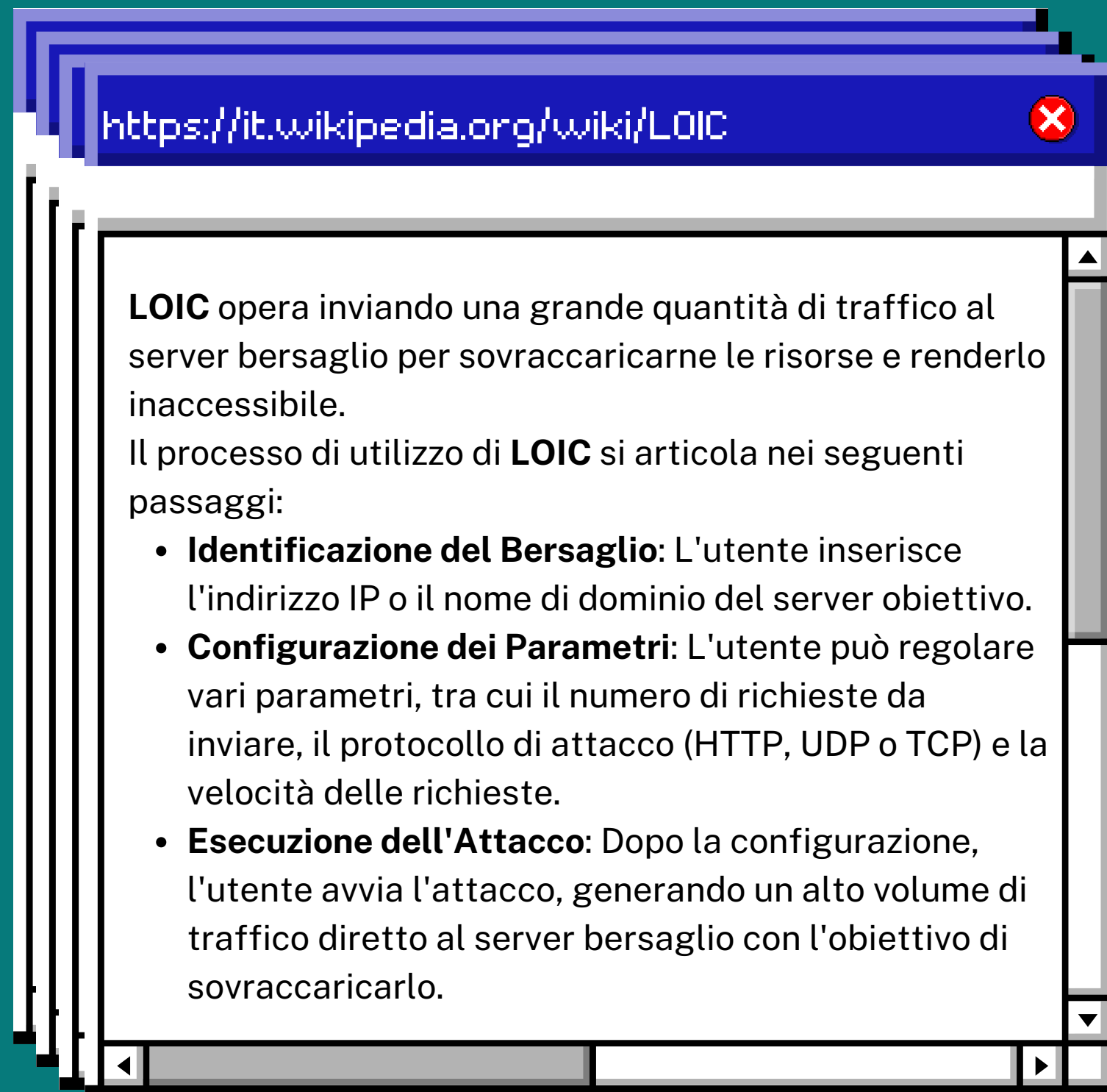
```
[Info] [AI] NOT any NEW victim(s) found for this query!
```

```
[Info] [AI] NOT any NEW victim(s) found for this query!
```

```
[Info] [AI] NOT any NEW victim(s) found for this query!
```

```
+Victim found: https://www.bankwindhoek.com.na/Lists/Contact%20Form/NewForm.aspx?Source=
+Victim found: https://www.capricorn.com.na/Lists/Contact%20Form/NewForm.aspx?Source=
+Victim found: https://servicesforemployers.floridarevenue.com/Lists/ContactUsList/NewForm.aspx?Source=
+Victim found: https://www.epcc.edu/Admissions/FinancialAid/Scholarships/Lists/GeneralScholarshipApplication/NewForm.aspx?Source=
+Victim found: https://cnrs.hcmc.gr/Lists/YPOBOLH/NewForm.aspx?Source=
```

LOIC



Facilità d'Uso:

LOIC è dotato di un'interfaccia utente semplice e intuitiva, che lo rende **accessibile** anche a chi ha poca esperienza tecnica.

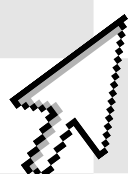
Progetto Open Source

Essendo open source, LOIC è disponibile **gratuitamente** e può essere **personalizzato** dagli utenti per specifiche necessità.

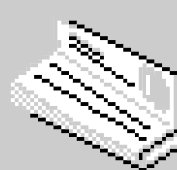
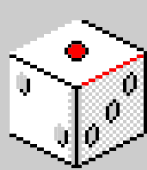
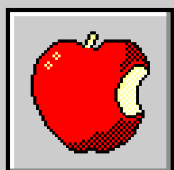
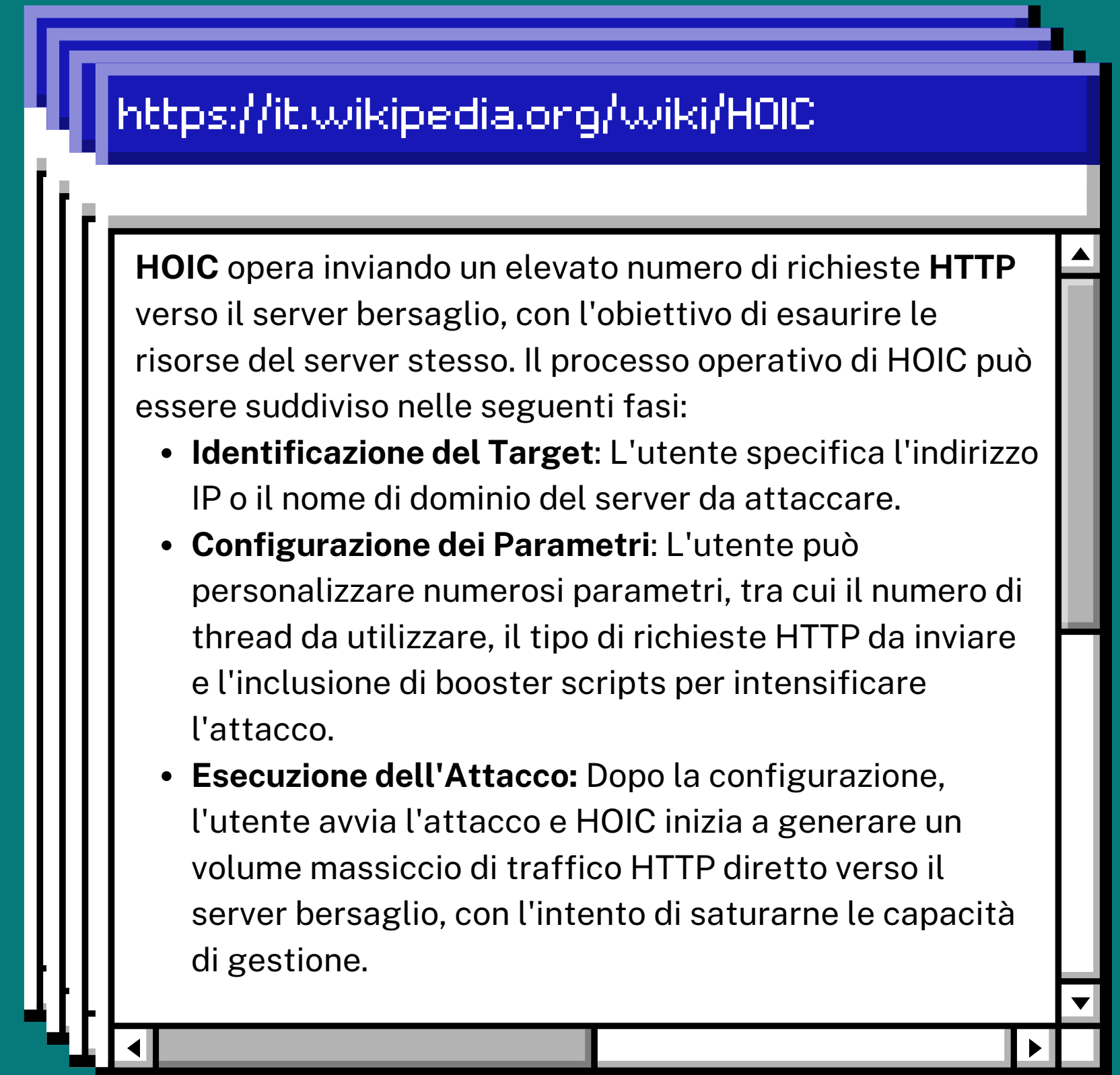
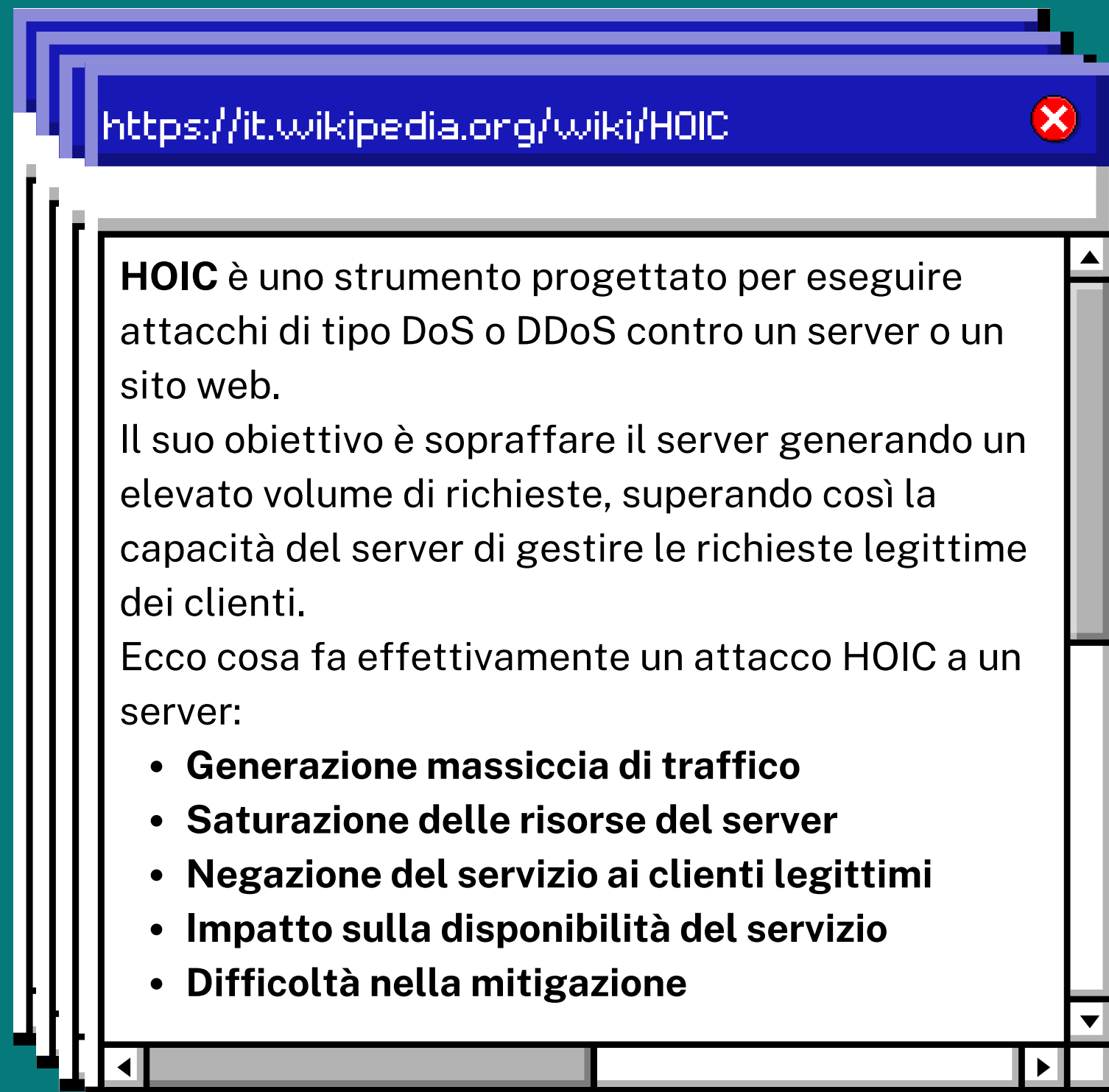
Efficacia in Attacchi Volumetrici:

LOIC è in grado di generare un **elevato volume di traffico**, che può mettere in difficoltà server non adeguatamente protetti.

L'utilizzo di LOIC per condurre attacchi DDoS è illegale nella maggior parte dei paesi e può comportare severe **ripercussioni** legali per gli autori degli attacchi.

[illegible]

HOIC



Molti server moderni sono equipaggiati con avanzati sistemi di difesa DDoS che possono attenuare l'impatto degli attacchi condotti con HOIC.

[illegible]

BONUS:

MIRAI



<https://it.wikipedia.org/wiki/MIRAI>

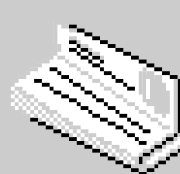
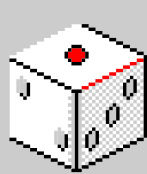
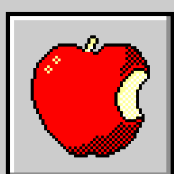


Mirai (dal giapponese 未来, “futuro”) è un malware progettato per operare su dispositivi connessi a Internet, specialmente dispositivi **IoT**, ed è stato utilizzato in svariati attacchi DDoS.

Il **codice sorgente** di **Mirai** è stato sottoposto a **reverse engineering**, e da **C** è stato riscritto in **Python** e poi pubblicato su **GitHub in open source**.

Il Command and Control implementato da Mirai supporta una semplice interfaccia a riga di comando, che permette all'attaccante di specificare un vettore di attacco, ossia uno o più indirizzi IP vittima e la durata dell'attacco.

Per quanto riguarda le funzioni di attacco, può lanciare varie tipologie di attacchi DDoS. A livello applicazione può lanciare attacchi di tipo HTTP floods, mentre a livello di rete e trasporto è capace di lanciare attacchi di tipo GRE IP and GRE ETH floods, SYN and ACK floods, STOMP floods, DNS floods e UDP flood. Inoltre, il CnC è sempre in attesa che i BOT comunichino i nuovi dispositivi infettati e le loro credenziali, le quali vengono usate per copiare il codice del virus e ampliare la Botnet.



[Indice](#)

MIRAI

```

util_itoa = util_c.util_itoa
util_memsearch = util_c.util_memsearch
util_stristr = util_c.util_stristr
util_fdgets = util_c.util_fdgets
util_isupper = util_c.util_isupper
util_isalpha = util_c.util_isalpha
util_isspace = util_c.util_isspace
util_isdigit = util_c.util_isdigit
# static ipv4_t get_dns_resolver(void)
ipv4_t(get_dns_resolver)

# def attack_udp_generic(targs_len, attack_target *targs, opts_len, attack_option
n *opts):
def attack_udp_generic(targs_len, attack_target(targs, opts_len), attack_option(
opts)):
    pkts = calloc(targs_len; sizeof ())
    ip_tos = attack_get_opt_int(opts_len; 0)
    ip_ident = attack_get_opt_int(opts_len; 0xffff)
    ip_ttl = attack_get_opt_int(opts_len; 64)
    BOOL dont_frag = attack_get_opt_int(opts_len, opts, ATK_OPT_IP_DF, False)
    port_t sport = attack_get_opt_int(opts_len, opts, ATK_OPT_SPORT, 0xffff)
    port_t dport = attack_get_opt_int(opts_len, opts, ATK_OPT_DPORT, 0xffff)
    data_len = attack_get_opt_int(opts_len; 512)
    BOOL data_rand = attack_get_opt_int(opts_len, opts, ATK_OPT_PAYLOAD_RAND, Tr
ue)
    source_ip = attack_get_opt_int(opts_len; LOCAL_ADDR)

    if data_len > 1460:
        data_len = 1460

    if (fd = socket(AF_INET, SOCK_RAW, IPPROTO_UDP)) == -1:
#ifdef DEBUG
    printf("Failed to create raw socket. Aborting attack\n")
attack_udp_c.py

```

attack_udp_c.py	89,1	11%
-----------------	------	-----

