TD SYNNEX

Attacchi DDOS

Un’analisi delle tecniche, dei target e dei modi per proteggersi

7 Marzo 2025

Webinar

Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

7 tipi di Threat Actor

Cyber Crime Organizations

Hacktivists

Insider Threats

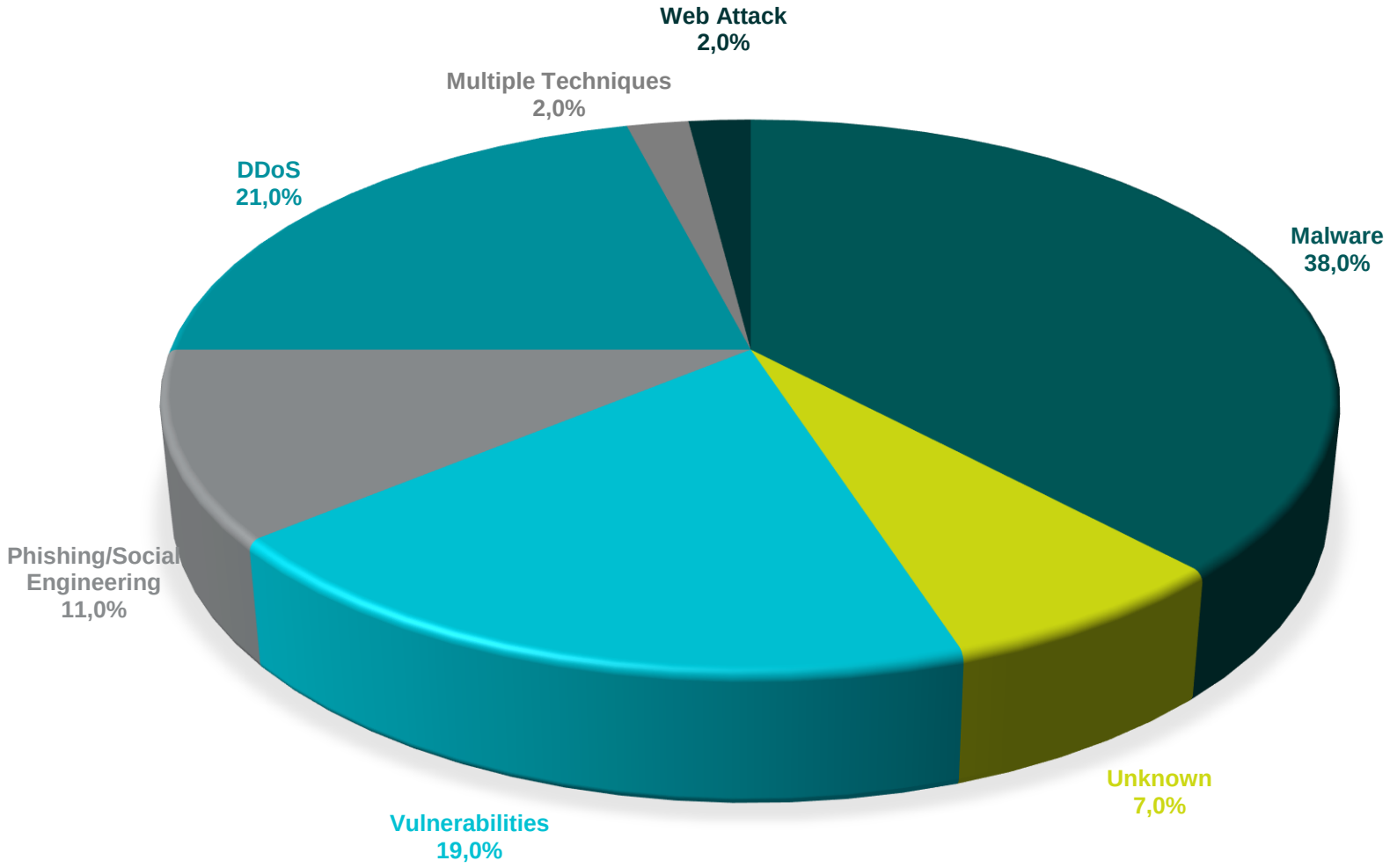
Cyber Extorsionist

Script Kiddies

State Sponsored Hackers

Cyberterrorists

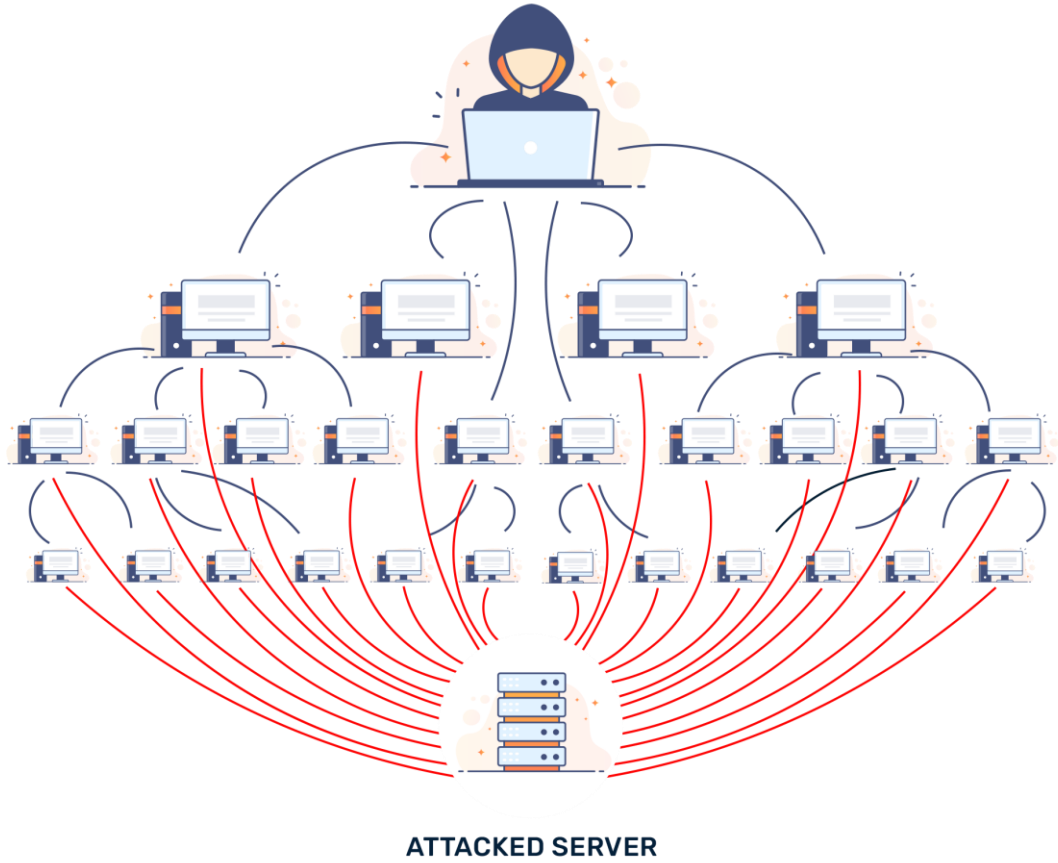
Tecniche di attacco 2024 (Italia)



Cos’è un attacco DDOS

Un attacco DDOS ha come obiettivo disattivare o eliminare un sito o un'applicazione Web, un servizio cloud o altre risorse online mediante il sovraccarico di richieste di connessione inutili, pacchetti falsi o altro traffico dannoso.

L’applicazione o l’appliance soggetta all’attacco tipicamente non riesce a gestire il traffico e va incontro a malfunzionamenti.



Motivazioni

Guadagni finanziari

Notorietà

Hacktivism

Sabotaggio e Danneggiamento

Vendetta

Riscatto

Attori Nazionali

Vantaggi Competitivi

Alcuni tipi di attacco

Volumetric Attack

Attaccano la rete target con un flusso di richieste misurabile in Gbps, andando a sovraccaricare il sistema di destinazione.

Es. UDP Flood

Protocol Attack

Misurabile in pacchetti al secondo, PPS, si uniscono alle richieste legittime e consumano le sessioni disponibili.

Es. SYN Flood, Ping of Death

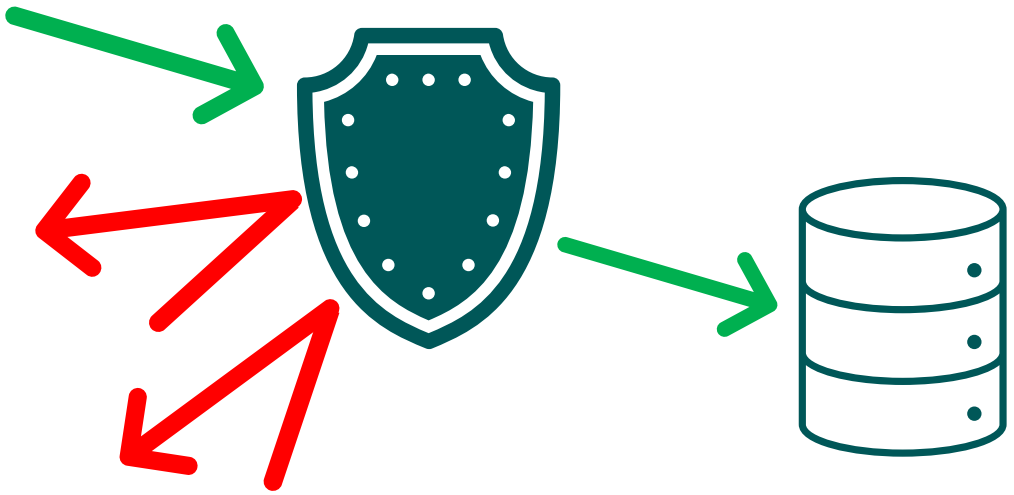
Application Layer Attack

Attacca specifiche applicazioni e ne consuma le sessioni. Tipico di applicazioni http o https.

Es. Http Flood

Contromisure

- Riconoscere il traffico
- Riduzione Attack Surface
- WAF e NGFW
- Segregazione dei servizi



Cos’è una Botnet

Una **botnet** è un insieme di dispositivi controllati dai cybercriminali per attaccare un bersaglio. Il termine *“botnet”* deriva dalla fusione delle parole “robot” e “network” a rappresentare la natura di un *cyberattacco tramite botnet*.

Per ottenere il controllo di tanti dispositivi, i cybercriminali devono prima spingere gli utenti ad installare malware nei propri sistemi, spesso con firmware obsoleti e non aggiornati.

Proteggersi

Al momento i dispositivi più vulnerabili sono quelli IoT.

E’ necessario aggiornare firmware alle versioni più recenti e considerare questi prodotti nel ciclo di patching.

Segmentazione della rete. Tenere separati i dispositivi IoT dai dati sensibili, un dispositivo Zombie per una BotNet può essere la porta per altri tipi di attacchi

Hacktivism e il caso NoName057(16)

**Dieci Giorni di DDoS!
NoName057(16) colpisce il Comune di Milano e la Regione Abruzzo**

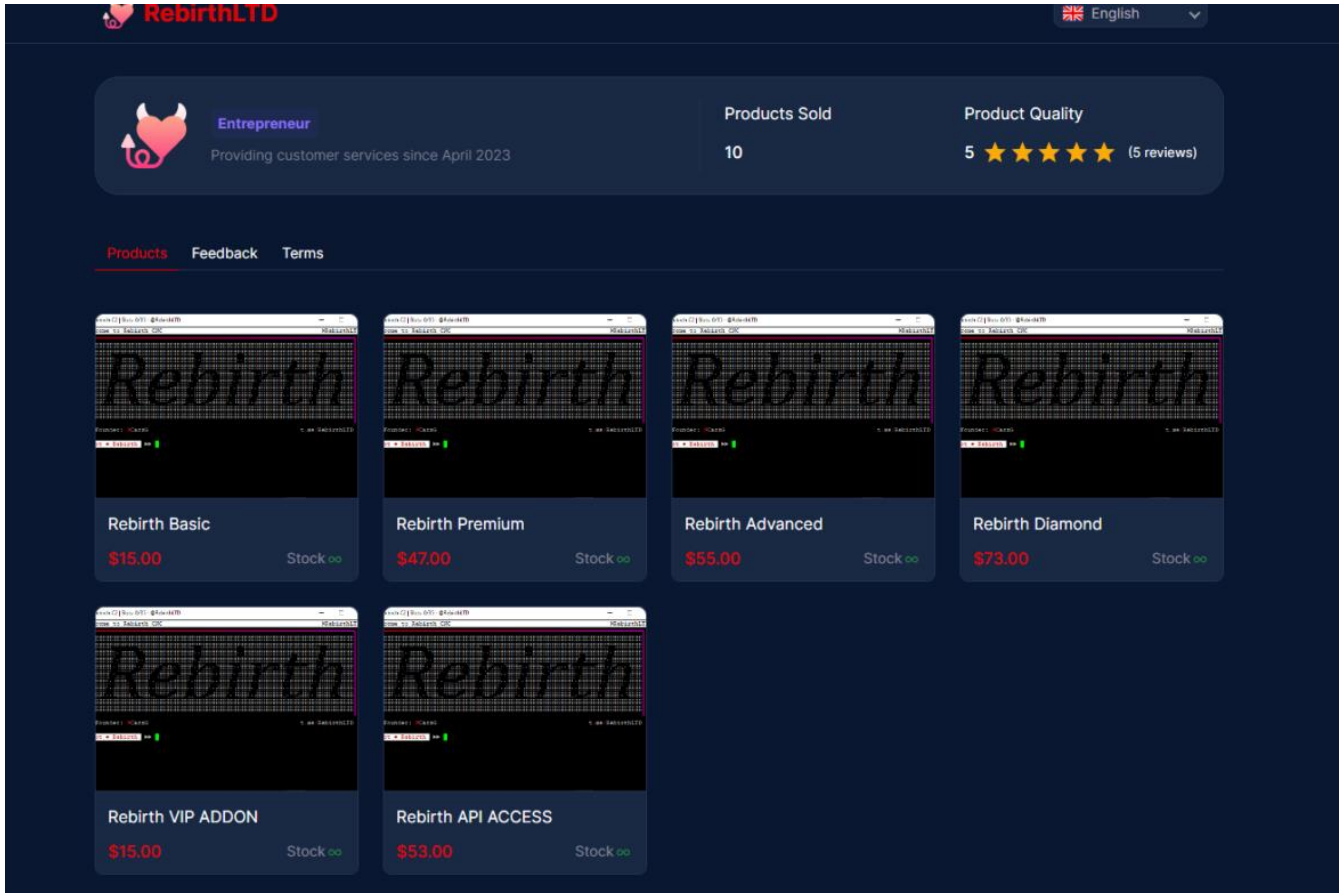
Attacchi mirati in alcuni momenti specifici, ultimo in ordine di tempo, la Lectio Magistralis di Mattarella all'Università Aix-Marseille del 5 Febbraio 2025

Da Telegram:
Il Presidente italiano Sergio Mattarella ha paragonato la Russia al Terzo Reich, provocando una dura reazione da parte del Ministero degli Esteri russo. Mosca ha già promesso che tali dichiarazioni non resteranno senza conseguenze
L'Italia riceve da noi missili DDoS verso i suoi siti web per tali paragoni del russofobo Mattarella

NoName057(16) è un gruppo Hacker noto per i suoi attacchi nei confronti di obiettivi Ucraini, Europei e Americani, soprattutto siti di agenzie governative e media.

E' dichiaratamente un'organizzazione filo-russa e ha iniziato le sue operazioni a Marzo 2022 dopo lo scoppio della guerra in Ucraina

DDOS As A Service



BotNet as a Service consente di acquistare i servizi di una BotNet a prezzi che partono dalle poche decine di Euro.

Con un listino prezzi in base ai servizi acquistati, l'esempio di Rebirth è uno dei tanti servizi che offrono questo tipo di funzionalità e, come un vero e proprio abbonamento, a prezzo diverso corrispondono funzionalità diverse, come API o tool di settaggio dell'attacco.

DDOS e Defacing

Attività di Hacking volte a colpire siti di organizzazioni per modificarne l'aspetto e, nella maggioranza dei casi, introdurre rivendicazioni o messaggi specifici.

Fanno parte degli attacchi di Hacktivism

Hanno come obiettivi:

- Visibilità
- Danno Reputazionale
- Simbolismo del messaggio

La bufala degli spazzolini

THE U.S. Sun News Sport TV Entertainment Money Tech

Tech

TOOTH BE TOLD Over 3 million toothbrushes could be 'hacked' and 'turned into secret army for criminals,' experts claim

Read on for important tips on how to stay safe

Jona Jaupi, Technology and Science Reporter

Published: 9:32 ET, Feb 7 2024 | **Updated**: 8:13 ET, Feb 8 2024

Android TV BotNet

Circa 1,6 Milioni di TV Android attualmente infette con una nuova variante del Malware Vo1d, già noto in passato per aver infettato numerosi dispositivi IoT.

I dispositivi vengono utilizzati in attacchi di tipo Flood.
Sono gestiti tramite dei server Command and Control con aggiornamento P2P.

Al momento i paesi più infetti sono Argentina, Brasile, Cina, Indonesia, Sud Africa e Tailandia

TD SYNNEX

“There's no such thing as a 'attack'... A DDoS is a protest, it's a digital sit it. It is no different than physically occupying a space. It's not a crime, it's speech.”

Jay Liederman

https://www.ibm.com/it-it/topics/ddos
https://bunny.net/academy/security/what-are-distributed-denial-of-service-ddos-attacks/
https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/
https://www.proofpoint.com/it/threat-reference/botnet
https://www.servicenow.com/uk/products/field-service-management/what-is-iot.html
https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/
https://www.redhotcyber.com/post/dieci-giorni-di-ddos-noname05716-colpisce-il-comune-di-milano-e-la-regione-abruzzo/
https://www.kaspersky.it/about/press-releases/kaspersky-botnet-a-partire-da-100-dollari-sul-dark-web
https://cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/
https://sysdig.com/blog/ddos-as-a-service-the-rebirth-botnet/
https://www.the-sun.com/tech/10316172/three-million-toothbrushes-hacked-secret-army-criminals/
https://www.pcworld.com/article/2623327/new-botnet-malware-infects-1-6-million-android-tv-devices-worldwide.html

Q&A

PROSSIMI APPUNTAMENTI

14 MARZO: Windows AI e Security
21 MARZO: Stuxnet e gli attacchi iOT
28 MARZO: Il rapporto Clusit 2025

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com