IT

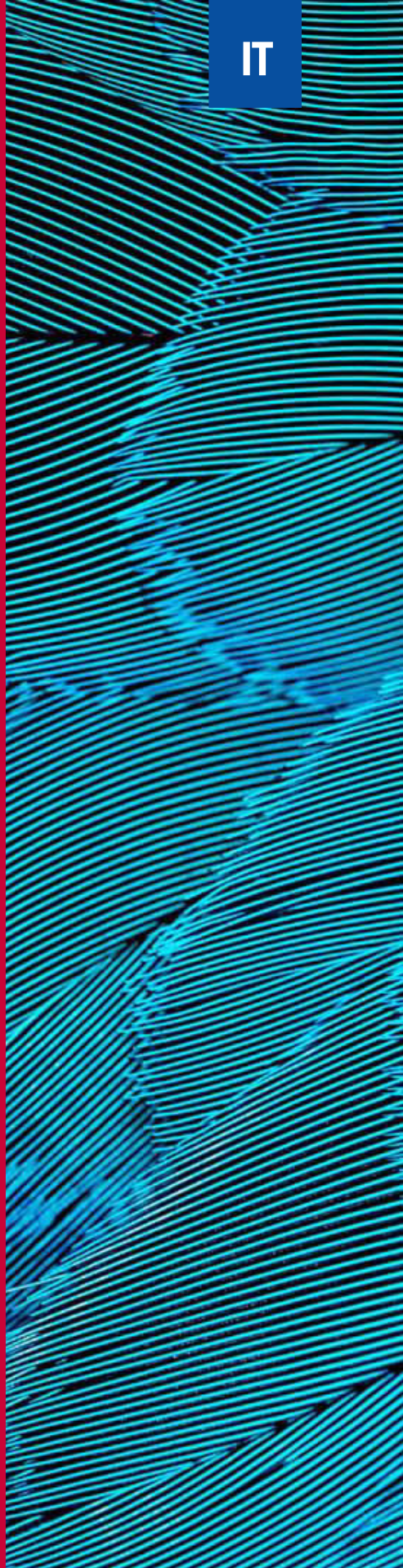
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Da gennaio 2019 ad aprile 2020

Attacco distribuito di negazione del servizio

Panorama delle minacce analizzato dall'ENISA



Quadro generale

È noto che gli attacchi distribuiti di negazione del servizio (Distributed Denial of Service, DDoS) si verificano quando gli utenti di un sistema o di un servizio non sono in grado di accedere alle informazioni, ai servizi o ad altre risorse pertinenti. Questa fase può essere realizzata facendo esaurire le risorse del servizio o sovraccaricando il componente dell'infrastruttura di rete.[1] Gli attori malintenzionati hanno incrementato il numero di attacchi, prendendo di mira più settori con motivazioni diverse. Se da un lato i meccanismi e le strategie di difesa stanno diventando più robusti, dall'altro anche gli attori malintenzionati mostrano competenze tecniche più avanzate. I rapporti[3,4,5] suggeriscono un incremento dell'uso di tecniche di attacco di riflessione e amplificazione che impiegano vettori nuovi, diversi da quelli comunemente noti (amplificazione basata su UDP ecc.).[6] Si osserva anche un miglioramento delle tattiche commerciali degli attori malintenzionati, che iniziano a pubblicizzare i loro servizi sul web. Storicamente i servizi DDoS venivano pubblicizzati nei forum sul dark web, mentre ora gli autori si servono dei comuni canali dei social media, come YouTube e Redit, per promuovere i loro servizi.[2]

Nel 2019 si sono osservati nuovi ingressi nella lista dei primi 10 Paesi di origine del traffico DDoS (Hong Kong, Sudafrica, ecc.).[7] È stato anche l'anno che ha visto un aumento dell'attività DDoS da parte delle botnet. I dispositivi IoT costituiscono un «focolaio» per le botnet DDoS, e la Cina (24%), il Brasile (9%) e l'Iran (6%) sono stati ritenuti i paesi maggiormente infettati dagli agenti di una botnet.[3] Secondo le previsioni di ricercatore della sicurezza, l'implementazione e la distribuzione delle reti 5G aumenteranno in modo esponenziale il numero di dispositivi connessi, e quindi l'espansione delle botnet.[3]

Sebbene gli attacchi DoS non siano una novità per chi si occupa di cibersicurezza e difesa delle reti, il loro livello di complessità è in aumento e si osserva che gli attori malintenzionati eseguono più attività di ricognizione rispetto a prima.[3,8]

Risultati

241%_ **di aumento del numero totale di attacchi durante il terzo trimestre del 2019, rispetto allo stesso periodo del 2018[3]**

Il 79,7%_ **di tutti gli attacchi DDoS era di tipo SYN flood[7]**

L'86%_ **degli attacchi mitigati nel terzo trimestre del 2019 utilizzava più di due vettori[9]**

L'84%_ **degli attacchi DDoS è durato meno di 10 minuti[10,11]**

509_ **ore è stata la durata dell'attacco DDoS più lungo nel secondo trimestre del 2019[3]**

Kill chain

Negazione del servizio (denial of service)

Reconnaissance (Ricognizione)	Weaponisation (Armamento)	Delivery (Consegna)	Exploitation (Sfruttamento)

Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Il modello Cyber Kill Chain® è stato sviluppato da Lockheed Martin, che lo ha adattato da un concetto militare legato alla struttura di un attacco. Per studiare un particolare vettore di attacco, si può utilizzare questo modello per mappare ogni fase del processo e fare riferimento agli strumenti, alle tecniche e alle procedure impiegate dall'aggressore.

MAGGIORI INFORMAZIONI

I primi cinque attacchi DDoS

SYN FLOOD DA 500-580 MILIONI DI PACCHETTI AL SECONDO. Tra tutte le tecniche utilizzate da attori malintenzionati, SYN flood è ancora considerata difficile da mitigare a causa delle sue caratteristiche, dell'infrastruttura presa di mira e del fatto che è richiesto più hardware per gestire un elevato volume di pacchetti. Nel gennaio 2019, un ricercatore della sicurezza ha osservato un record di attività di SYN flood, che ha distribuito 500 milioni di pacchetti al secondo (mpps) prendendo di mira uno dei suoi clienti e, successivamente, nell'aprile 2019, il volume è salito a 580 mpps.[12]

WS-DISCOVERY. Web services dynamic discovery[13] (WS-Discovery) è protocollo di discovery basato su multicast. Ne è stato osservato l'impiego principalmente da parte dei dispositivi IoT per rilevare automaticamente ogni nodo sulle reti locali (LAN), ma, come per altri protocolli, può essere utilizzato anche per scopi diversi da quello a cui è destinato, soprattutto nel settore IoT.[5] Gli attori malintenzionati l'hanno trovato un valido strumento per l'amplificazione degli attacchi. Un ricercatore della sicurezza ha riferito[3] un fattore di amplificazione di 95 volte, mentre un altro ricercatore ha riferito un aumento del 15 000% rispetto alle dimensioni in byte originali.[14]

ATTACCHI DI RIFLESSIONE E DI AMPLIFICAZIONE Questi tipi di attacchi sono ampiamente e storicamente noti per essere caratterizzati da una piccola richiesta di consegna di un payload di maggiori dimensioni. In sintesi, l'attore malintenzionato falsifica l'indirizzo IP del mittente (vittima) e successivamente l'host destinatario invia alla vittima tutte le risposte correlate.[9] Questa metodologia è efficace soprattutto sui protocolli basati su UDP per via della loro natura priva di connessione (connectionless) e del fattore di amplificazione (il protocollo CLDAP ha un fattore di amplificazione di 50-70 volte). Tuttavia, il protocollo TCP non è soggetto a questo tipo di attacco.[15]

Un buon esempio di questi tentativi sono gli attacchi di flooding SYN-ACK a riflessione e amplificazione: questo tipo di flood non deve essere necessariamente di larghezza di banda elevata per produrre un impatto. Al contrario, avere un'elevata velocità di pacchetti al secondo può consentire all'attacco di non dare nell'occhio e risultare così più efficace.[3]

DDoS BIT-AND-PIECE/CARPET BOMBING. Questo tipo di attacco di negazione del servizio distribuito e a riflessione (Distributed and Reflective Denial of Service Denial of Service, DRDoS) è noto per colpire soprattutto i settori delle telecomunicazioni e dei fornitori di servizi.[17] In un esempio[18] di questo attacco è stata presa di mira una selezione casuale di indirizzi IP di un fornitore di servizi Internet (Internet Service Provider) per riflettere il traffico verso i router perimetrali del provider. In tal modo, la vittima non è stata in grado di identificare il DDoS fino a quando il suo servizio non è stato sopraffatto dalla propria serie di indirizzi IP selezionati.[19]

ATTACCHI DDOS MULTI-VETTORE Gli attori malintenzionati spesso eseguono molteplici vettori di attacchi DoS per aggiungere complessità e varietà al loro tentativo. Ciò significa che, attraverso la semplice automatizzazione di diversi tipi di attacchi a livello applicativo (HTTP Flood, DNS Flood, ecc.) e a livello di rete (riflessione/amplificazione su UDP/TCP, ecc.), essi cercano di massimizzarne l'impatto saturando la larghezza di banda nonché le risorse o i servizi nell'ambiente bersaglio.[16]

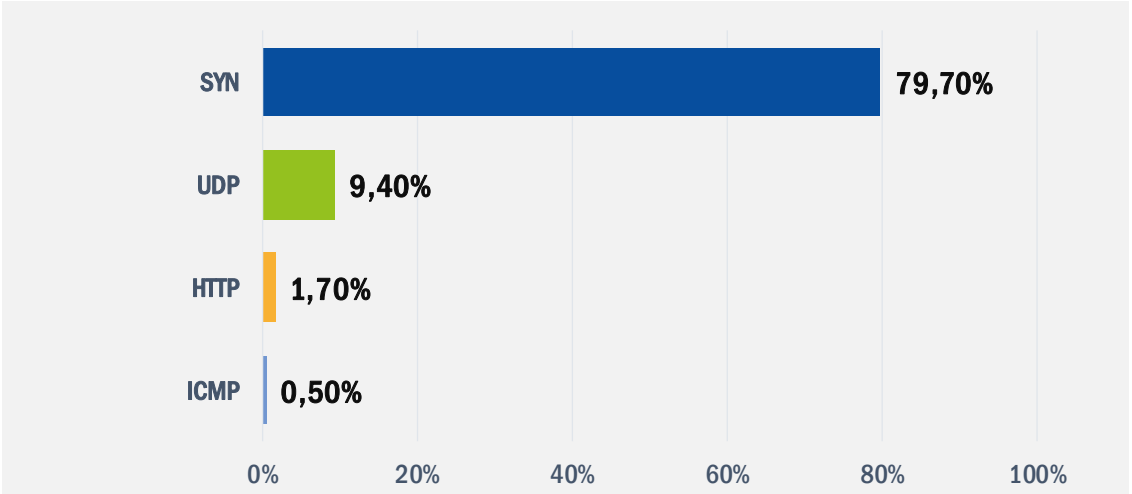


Figura 1. Distribuzione degli attacchi DDoS per tipo. Fonte: Kapersky[16]

Vettori di attacco

_ Come

Analogamente agli anni precedenti, il 2019 non ha costituito un'eccezione in termini di UDP flood. Secondo un ricercatore in materia di sicurezza, l'UDP flood è stato il vettore di attacco più diffuso e il team ritiene che possa essere legato all'adozione predominante di questo protocollo in settori ad alto rischio, come quello dei giochi. SYN flood, simulazione di risposte del DNS e attacchi basati su TCP seguono gli UDP flood nella lista dei principali vettori di attacco.

Durante questo periodo sono stati osservati anche attacchi multi-vettore. Un ricercatore della sicurezza ritiene tuttavia che alcuni degli attacchi multi-vettore siano una conseguenza involontaria di un tentativo di DoS.[11]

Un rapporto sulla cibersicurezza[17] ha indicato che attacchi di amplificazione del DNS sono stati osservati dal team come il principale vettore di attacco DDoS, seguito da attacchi HTTP Flood e TCP SYN. Le osservazioni dei vettori di attacco nel terzo trimestre del 2019 sono risultate simili, con SYN flood in cima alla classifica, seguito da attacchi UDP, TCP e HTTP.

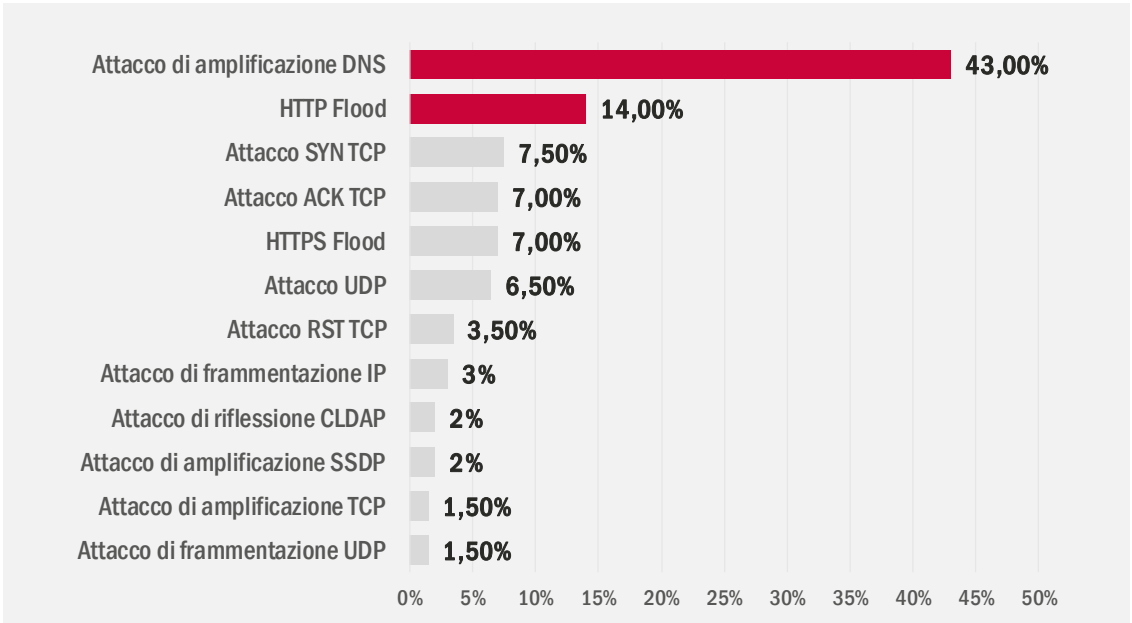


Figura 2. Distribuzione dei vettori di attacco DDoS. Fonte: NexusGuard[17]

Durata degli attacchi

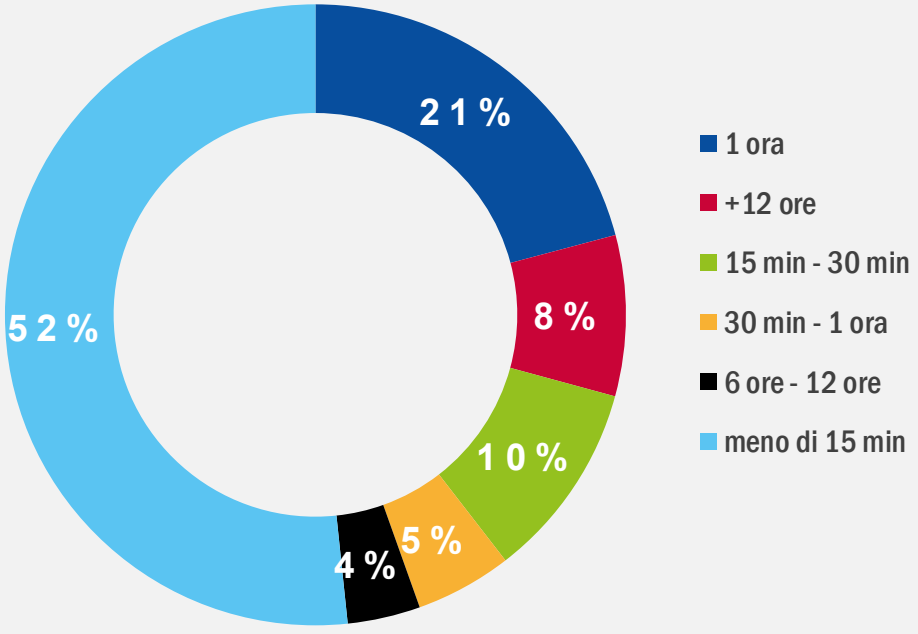


Figura 3 - Fonte: Imperva[11]

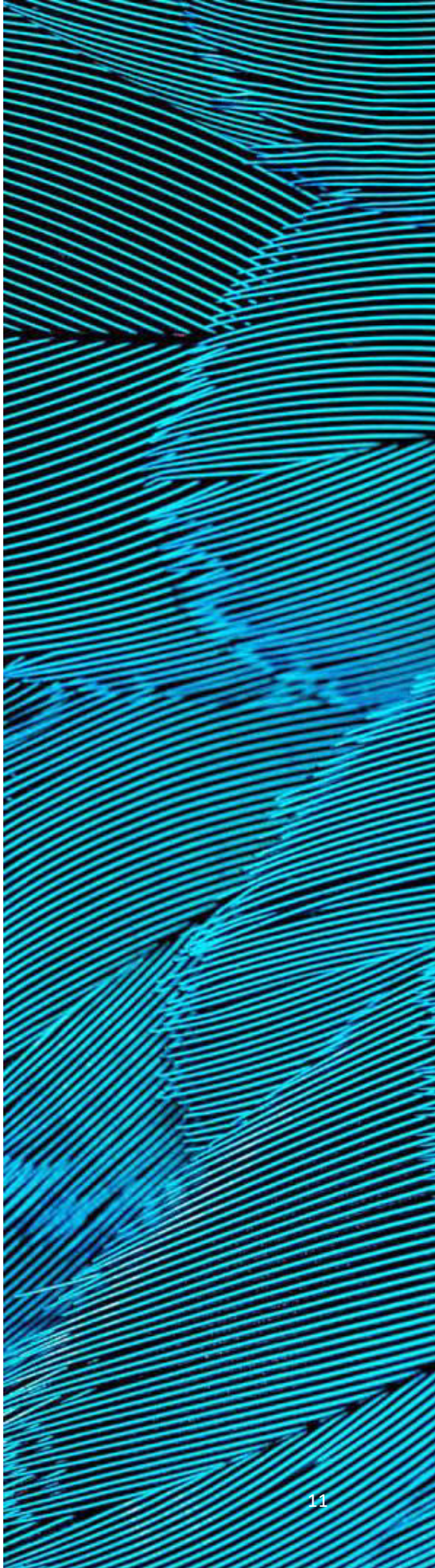
Mitigazione

_Azioni proposte

- Comprendere i servizi e le risorse critiche e dare priorità alla difesa, laddove questi possano essere sovraccaricati. Garantire che sia in atto un piano di risposta per tali scenari.[20]
- A seconda dei requisiti, considerare un servizio di protezione DDoS o un fornitore di servizi gestiti DDoS. Utilizzare metodi come il monitoraggio per una rapida identificazione delle infezioni.[1]
- Analogamente al punto precedente, la pubblicazione dei servizi attraverso reti per la distribuzione di contenuti (Content Delivery Network) può essere un modo efficace per assorbire i tentativi di attacco volumetrico (richiede l'impiego di altre tecniche in caso di attacchi più sofisticati).[21]
- I fornitori di servizi Internet e di cloud rivestono un ruolo essenziale nella difesa dagli attacchi DDoS. Disporre di un piano di comunicazione chiaro e di un di canale di comunicazione con tali fornitori è fondamentale per una risposta efficace a un attacco di negazione del servizio.
- Elaborare una posizione di difesa forte e proattiva prima che si verifichi un guasto critico, coinvolgendo il team e i fornitori collegati per configurare e mettere a punto controlli basati su requisiti aziendali specifici.[22] Utilizzare i server di cache o eliminare alla fonte query/richieste inappropriate nel livello applicativo e attuare le migliori prassi correnti (BCP)[23] per i fornitori di servizi sono validi esempi di misure proattive.
- Assicurare di sottoporre a test e a nuova valutazione le tecniche, le tecnologie e i fornitori di servizi relativi alla difesa.
- Creare un registro dei rischi analizzando il proprio ambiente a fondo. Partire dagli asset critici all'interno e proseguire fino all'impronta e alla presenza su Internet.[24]

«Sebbene gli attacchi DDoS non siano una novità per chi si occupa di cibersicurezza e difesa delle reti, il loro livello di complessità è in aumento e si osserva che gli attori malintenzionati eseguono più attività di ricognizione rispetto a prima»

in ETL 2020



Riferimenti bibliografici

1. «Understanding Denial-of-Service Attacks» 20 novembre 2019. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q1 2019» 21 maggio 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. «Q4 2019 - The State of DDoS Weapons Report.» 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. «Anatomy of a SYN-ACK Attack.» 2 luglio 2019. Akamai. https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html

5. Brandon Vigliarolo. «A new type of DDoS attack can amplify attack strength by more than 15,300%.» 18 settembre 2019. TechRepublic. https://www.techrepublic.com/article/a-new-type-of-ddos-attack-can-amplify-attack-strength-by-more-than-15300/

6. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q4 2018» 7 febbraio 2019. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q3 2019» 11 novembre 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. «2019 Website Threat Research Report.» 2019. sucuri

9. «DDoS attacks up 241% in Q3 2019 compared to same period last year.» 19 novembre 2019. Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

10. «2019 Half-Year DDoS Trends Report.» 2019. Corero Security. https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

11. Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. «2019 Global DDoS Threat Landscape Report.» 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

12. Tomer Shani. «Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important.» 30 aprile 2019. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

13. «Web Services Dynamic Discovery (WS-Discovery) Version 1.1» 1° luglio 2009. OASIS. http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

14. Jonathan Respeto. «New DDoS Vector Observed in the Wild: WSD attacks hitting 35/Gbps.» 18 settembre 2019. Akamai. https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

15. «Threat Alert: TCP Amplification Attacks.» 9 novembre 2019. Radware. https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

16. «Kaspersky report finds over half of Q3 DDoS attacks occurred in September.» 11 novembre 2019. Kaspersky. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september

17. «DDoS Threat Report 2019 Q1.» 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. «International traffic – DDoS.» 22 settembre 2019. Cool Ideas. https://coolzone.cisp.co.za/announcements.php?announcement=2038-international-traffic-ddos-cool-ideas

19. Catalin Cimpanu. «Carpet-bombing' DDoS attack takes down South African ISP for an entire day.» 24 settembre 2019. ZDNet. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

20. «Guidance following recent DoS attacks in the run up to the 2019 General Election.» 13 novembre 2019. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

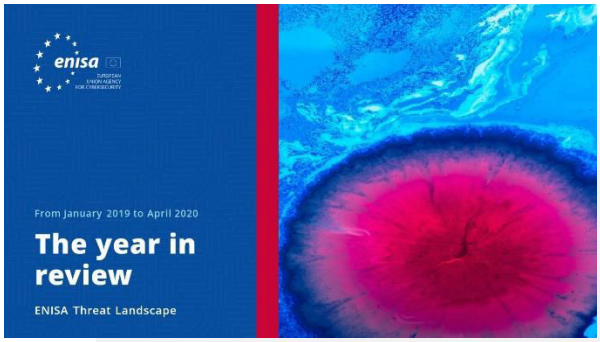
21. V. Revuelto, S. Meintanis, K. Socha. «DDoS Overview and Response Guide.» 10 marzo 2017. CERT-EU. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

22. «State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1.» 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

23. P. Fergusson, D. Senie. «Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.» Maggio 2000. IETF Tools. https://tools.ietf.org/html/bcp38

24. Pierluigi Paganini. «Cyber Defense Magazine Sept Edition 2019.» 4 settembre 2019. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

Correlati



Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Elenco delle prime 15 minacce

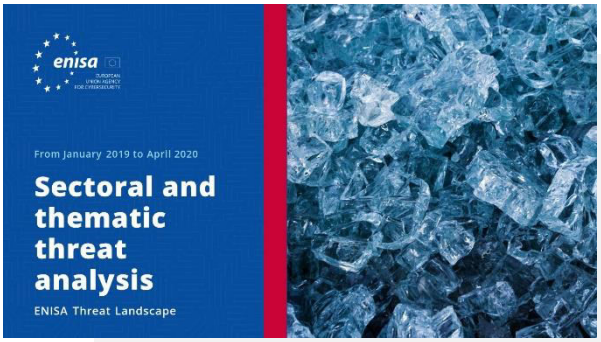
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Argomenti di ricerca

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.

LEGGI LA RELAZIONE



Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Quadro generale dell'intelligence sulle minacce informatiche

Situazione attuale dell'intelligence sulle minacce informatiche nell'UE.

LEGGI LA RELAZIONE

Informazioni

_ L'agenzia

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) e Thomas Hemker.

Redattori

Marco Barros Lourenço (ENISA) e Louis Marinos (ENISA).

Contatti

Per informazioni sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

Avvertenza legale

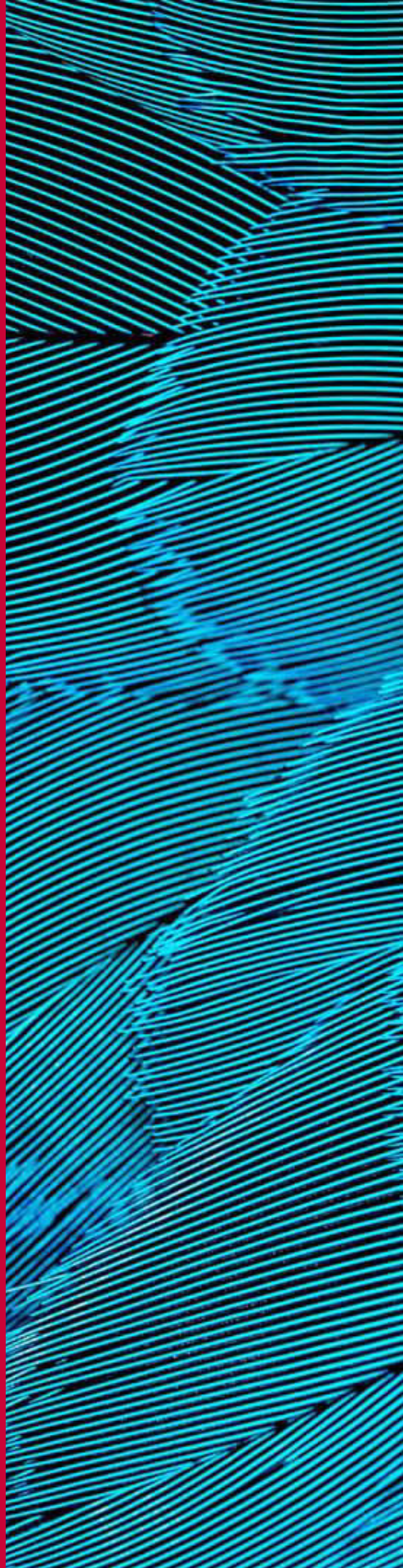
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. La presente pubblicazione non rappresenta necessariamente lo stato dell'arte e l'ENISA si riserva il diritto di aggiornarla di volta in volta.

Secondo necessità, sono state citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu