enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Attacchi alle applicazioni web

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Le applicazioni e le tecnologie web sono diventate una parte essenziale di Internet, adottando usi e funzionalità diversi. L'aumento della complessità delle applicazioni web e dei loro servizi diffusi pone delle sfide in termini di protezione da minacce che hanno motivazioni eterogenee, che vanno dal danno economico o reputazionale al furto di informazioni critiche o personali.[1] I servizi e le applicazioni web dipendono principalmente dai database per l'archiviazione o la fornitura delle informazioni richieste. Gli attacchi di tipo SQL Injection (SQLi) sono un esempio noto e costituiscono le minacce più comuni mirate tali servizi. Un altro esempio è rappresentato dagli attacchi di tipo cross-site scripting (XSS). In questo tipo di attacco, l'attore malintenzionato sfrutta i punti deboli contenuti in modelli o altre funzionalità di inserimento delle applicazioni web, che portano ad altre funzioni dannose, ad esempio il reindirizzamento verso un sito web malevolo.[2]

Sebbene le organizzazioni stiano diventando esperte e sviluppino un'automazione più coerente nel ciclo di vita delle loro applicazioni web, esigono la sicurezza come parte più cruciale della loro offerta e definizione delle priorità. L'introduzione di ambienti complessi determina l'adozione di nuovi servizi come le interfacce di programmazione delle applicazioni (API). Le API, che generano nuove sfide per la sicurezza delle applicazioni web, possono richiedere misure di prevenzione e di rilevamento aggiuntive. Ad esempio, circa l'80% delle organizzazioni che adottano le API ha implementato controlli sul proprio traffico in entrata.[3] In questa sezione si prende in esame il panorama delle minacce per le applicazioni web nel corso del 2019.

_Tendenze

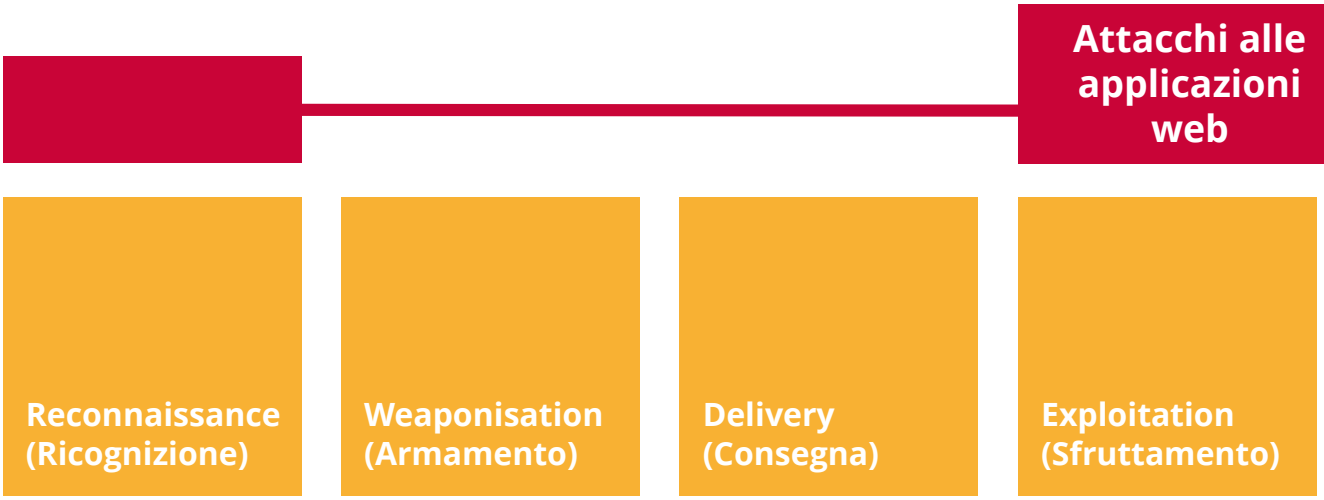
Il 20%_ **delle aziende e delle organizzazioni ha segnalato attacchi DDoS quotidiani ai propri servizi applicativi.**[5]
Il buffer overflow, ovvero il sovraccarico delle memoria tampone, è stata la tecnica più comunemente utilizzata (24%). Altre tecniche comuni impiegate sono state HTTP flood (23%), riduzione delle risorse (23%), HTTPS flood (21%) e Low & Slow (21%).

Il 63%_ **degli intervistati nell'indagine di CyberEdge utilizza un firewall per applicazioni web (WAF)**
Il 27,5% ha in programma di utilizzare questa tecnologia, mentre il 9,5% non lo prevede.[15]

52%_ **di aumento del numero di attacchi ad applicazioni web nel 2019, rispetto al 2018**
Secondo un ricercatore della sicurezza, la curva degli attacchi alle applicazioni web è stata pressoché piatta rispetto al 2018, con un netto aumento negli ultimi mesi dell'anno.[4]

L'84%_ **delle vulnerabilità osservate nelle applicazioni web era costituito da errori di configurazione della sicurezza**
A questi facevano seguito il cross-site scripting (53%) e, dato interessante, la broken authentication (45%).[9]

Kill chain



Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Installazione

Command & Control (Comando e controllo)

Actions on Objectives (Azioni sugli obiettivi)

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

Descrizione

Miglioramento della collaborazione tra sicurezza delle applicazioni e sviluppo di applicazioni

Secondo l'indagine condotta da un ricercatore della sicurezza[5], uno dei fattori che contribuiscono a rendere la sicurezza inefficace potrebbe essere il processo decisionale sulla proprietà degli strumenti applicati. L'indagine ha presentato i pareri delle figure più influenti in questo settore, citando i dirigenti IT e gli imprenditori e non il direttore della sicurezza delle informazioni (CISO).

Crescente importanza delle interfacce di programmazione delle applicazioni (API)

Le API non sono una novità nell'architettura delle applicazioni web e il loro ormai ampiamente accettato utilizzo ripropone i rischi esistenti e la probabilità che siano sfruttati in seguito all'ampliamento del panorama delle minacce. Di conseguenza, l'Open Web Application Security Project (OWASP) ha pubblicato un elenco delle prime 10 misure di sicurezza per le API[6], offrendo un modo basato su priorità per garantire tale capacità nell'architettura delle applicazioni web. Un esempio di minaccia è costituito dagli attacchi alle API in PHP: secondo un altro ricercatore nel campo della sicurezza, l'87% delle scansioni del traffico API era alla ricerca di API in PHP disponibili.[7]

Errori di autorizzazione e autenticazione

Si tratta in genere della causa principale di accesso da parte di attori malintenzionati a informazioni critiche (ad esempio, la violazione di Fast Retailing[8]). Secondo un ricercatore della sicurezza, le violazioni di dati critici rappresentano la seconda minaccia più pressante per la sicurezza delle applicazioni web.[9]

Tendenza in crescita con l'SQL Injection (SQLi)

Una ricerca recente sulla sicurezza ha riscontrato che due terzi degli attacchi alle applicazioni web includono attacchi SQLi. Mentre altri vettori di attacco alle applicazioni web sono rimasti stabili o sono in aumento, gli attacchi SQLi hanno continuato a crescere in modo netto, con una particolare escalation durante il periodo delle festività del 2019.[11] I risultati di questa ricerca hanno inoltre evidenziato che, rispetto ad altri, il settore finanziario è quello più colpito da attacchi di Local File Inclusion (LFI).[12]

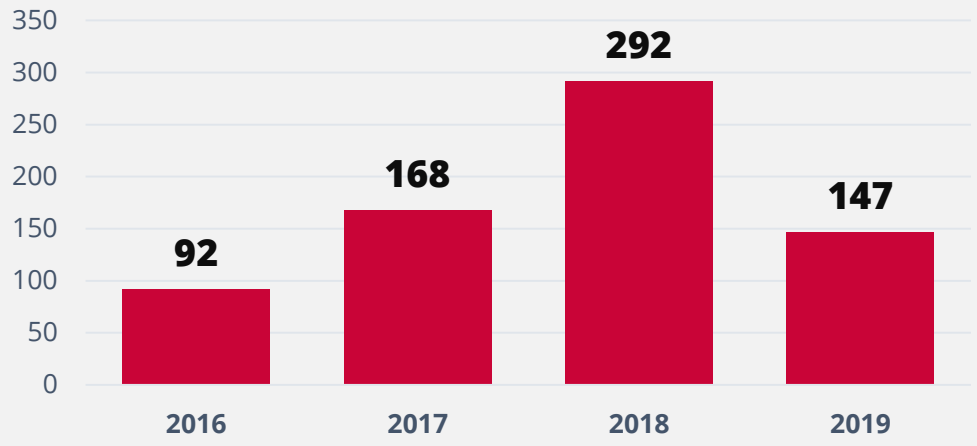


Figura 1. Riduzione del numero di file puliti per ogni sito compromesso. Fonte: Sucuri[10]

Vettori di attacco

_Vettori di attacco alle applicazioni web

La percezione generale è che gli attacchi alle applicazioni web siano piuttosto eterogenei. I dati delle ricerche sulla sicurezza suggeriscono tuttavia che la maggior parte degli attacchi alle applicazioni web sia circoscritta a SQLi o LFi.[11,13,14] Un altro rapporto indica che SQLi, directory traversal, XSS, broken authentication e gestione delle sessioni sono in cima alla lista dei vettori impiegati in questo tipo di attacchi.[4]

Anche SONICWALL ha riferito una tendenza analoga per i principali attacchi alle applicazioni web nel 2019. Nella lista, SQLi, directory traversal, XSS, broken authentication e gestione delle sessioni occupavano le prime posizioni.[4]

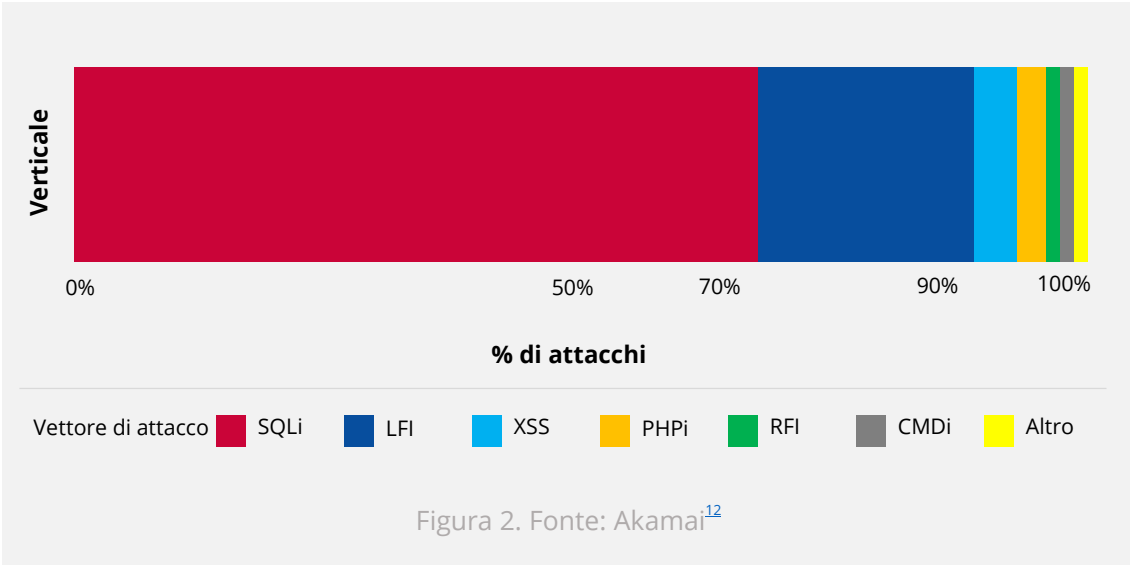


Figura 2. Fonte: Akamai[12]

Attacchi alle applicazioni web

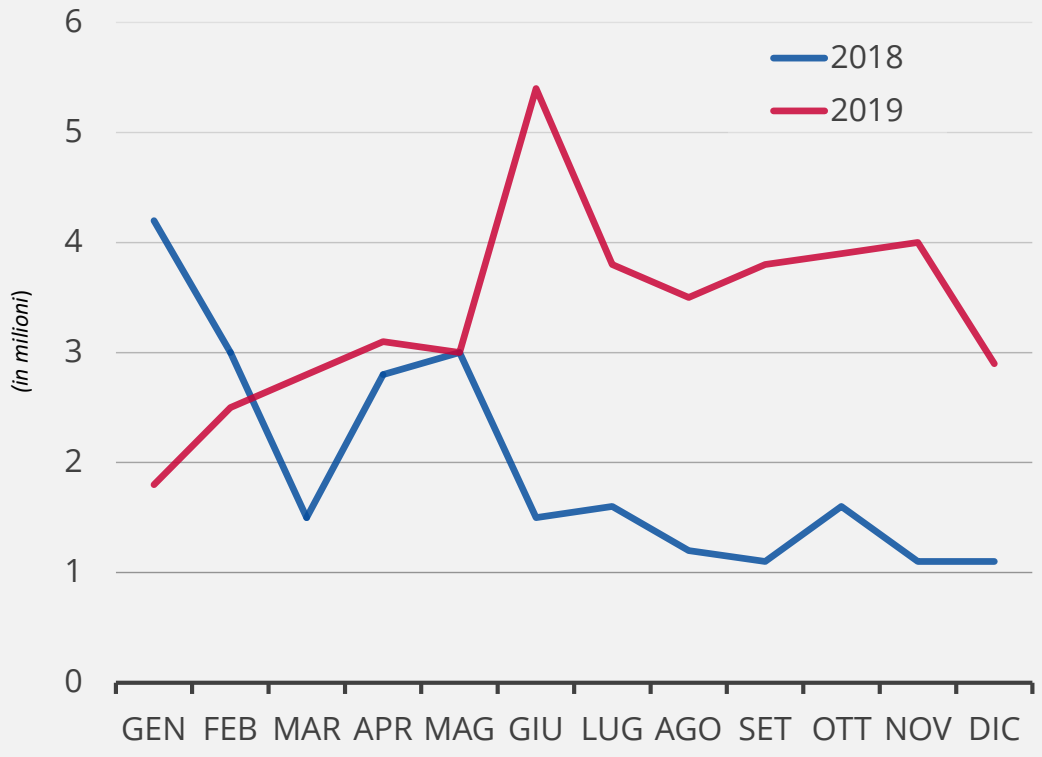


Figura 3 - Fonte: Sonicwall[4]

Mitigazione

Azioni proposte

- Utilizzare la validazione degli input e tecniche di isolamento per gli attacchi di tipo injection (ad esempio statement parametrizzati, escape degli input dell'utente, validazione degli input, ecc.)[16].
- Implementare firewall per applicazioni web per misure preventive e difensive[17](noto anche come patching virtuale).[18]
- Riguardo alle API per applicazioni web[19]:
  - implementare e mantenere un inventario delle API e convalidarle rispetto a scansioni perimetrali e individuazione interna attraverso team operativi e di sviluppo;
  - crittografare la comunicazione e la connessione delle API;
  - fornire i meccanismi di autenticazione e i livelli di autorizzazione giusti.
- Incorporare i processi di sicurezza delle applicazioni nel ciclo di vita dello sviluppo e della manutenzione delle applicazioni.[20]
- Limitare l'accesso al traffico in entrata solo ai servizi richiesti.[20]
- Implementare funzionalità di gestione del traffico e della larghezza di banda.
- Prevedere l'hardening dei server per le applicazioni web e mantenere efficaci processi di gestione e test delle patch.[21]
- Eseguire valutazioni delle vulnerabilità e dei rischi prima e durante lo sviluppo dell'applicazione web.
- Effettuare regolari test di penetrazione durante l'implementazione e dopo il rilascio.

_Applicazioni web secondo la massima gravità delle vulnerabilità rilevate

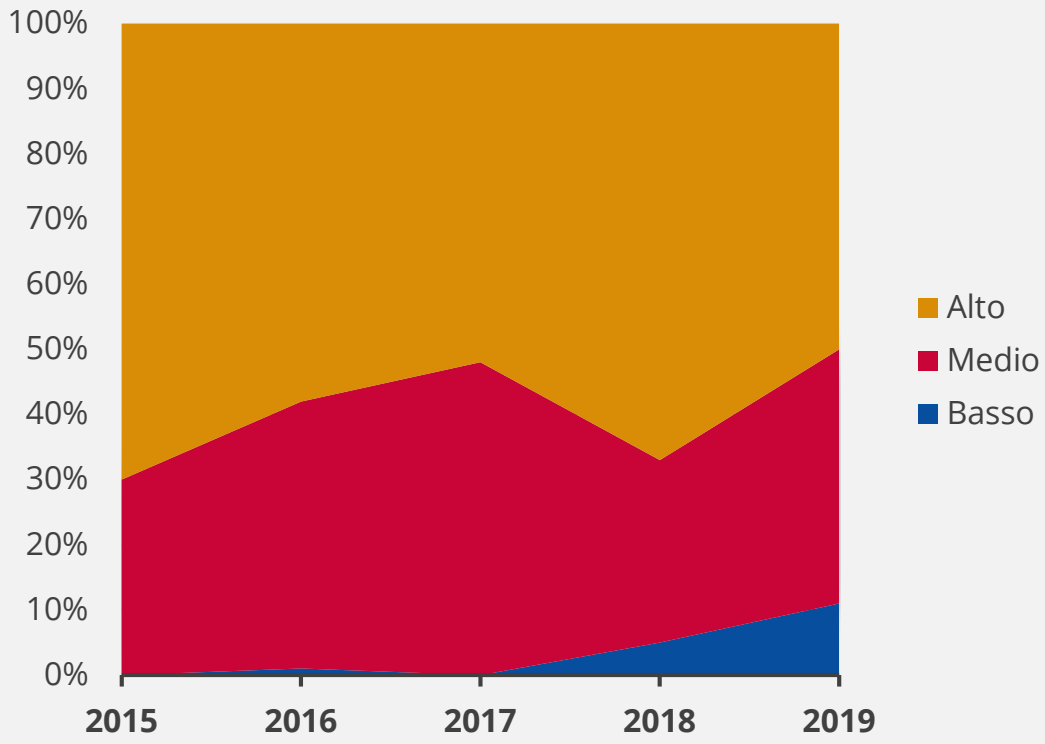


Figura 4 - Fonte: Positive Technologies[9]

Riferimenti bibliografici

1. «The Future Is the Web! How to Keep It Secure?» Ottobre 2019. Acunetix. https://www.acunetix.com/whitepaper-the-future-is-the-web/

2..«What Is a Web Application Attack and how to Defend Against It». 2019. Acunetix. https://www.acunetix.com/websitesecurity/web-application-attack/

3. «2020 State of Application Services Report» F5 Networks, 2020.. https://www.f5.com/state-of-application-services-report

4. «Sonicwall Cyber Threat Report». 2020. Sonicwall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. «The State of Web Application Security, Protecting Application in the Microservice Era.» 2019. Radware. https://www.radware.com/resources/was-report-2019/

6. «API Security Top 10 2019.» OWASP. https://owasp.org/www-project-api-security/

7. Raymond Pompon, Sander Vinberg. «Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem.» 13 agosto 2019. F5 Labs https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

8. «Unauthorized Logins on Fast Retailing Online Store Websites due to List Type Account Hacking and Request to Change Password.» 13 maggio 2019. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. «Web Applications vulnerabilities and threats: statistics for 2019.» 13 febbraio 2020. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

10. Esrtevao Avillez. «2019 Website Threat Research Report.» 2019. Sucuri. https://sucuri.net/wp-content/uploads/2020/01/20-sucuri-2019-hacked-report-1.pdf

11. «State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3).» 2017-2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-executive-summary-2019.pdf

12. «State of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6, Issue 1).» 2020. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

13. «Q4 2016 State of The Internet Security Report» 2016. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

14. «Q4 2017 State of the Internet Security Report» 2017. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

15. «2019 Cyberthreat Defense Report.» 2019. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

16. «AppSec Advisor: Injection Attacks.» Ottobre 2019. CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

17. «Cybersecurity threatscape: Q3 2019.» 2 dicembre 2019. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5

18. «Virtual Patching Best Practices.» OWASP. https://owasp.org/www-community/Virtual_Patching_Best_Practices

19. Raymond Pompon, Sander Vinberg. «Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem.» 13 agosto 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

20. «2020 Cyber Threats, Business Email Compromise.» 22 ottobre 2019. https://www.uscloud.com/blog/top-cyber-threats-in-2020/

21. Sara Boddy, Remi Cohen. «Regional Threat Perspectives, Fall 2019: Asia.» 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--fall-2019--asia

«L’aumento della complessità delle applicazioni web e dei loro servizi diffusi pone delle sfide in termini di protezione da minacce che hanno motivazioni eterogenee, che vanno dal danno economico o reputazionale al furto di informazioni critiche o personali».

in ETL 2020

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

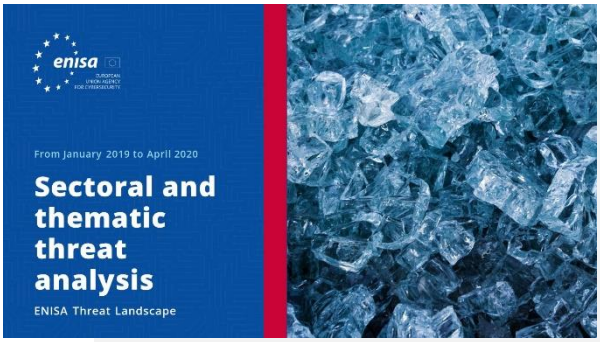
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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