IT

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Da gennaio 2019 ad aprile 2020

Crypto-jacking

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Il cryptojacking (noto anche come cryptomining) è l'uso non autorizzato delle risorse di un dispositivo per il mining di criptovalute. Il bersaglio può essere costituito da qualsiasi dispositivo connesso, come computer e telefoni cellulari, anche se i criminali informatici mirano sempre più alle infrastrutture cloud.[1] Questo tipo di attacco non ha destato l'attenzione delle autorità di contrasto e il suo abuso viene di rado denunciato[2], soprattutto a causa delle conseguenze negative relativamente limitate. Ciononostante le organizzazioni possono osservare un incremento dei costi informatici, la degradazione dei componenti dei computer, un aumento del consumo di elettricità e una riduzione della produttività dei collaboratori causata dalla maggiore lentezza delle postazioni di lavoro[3]

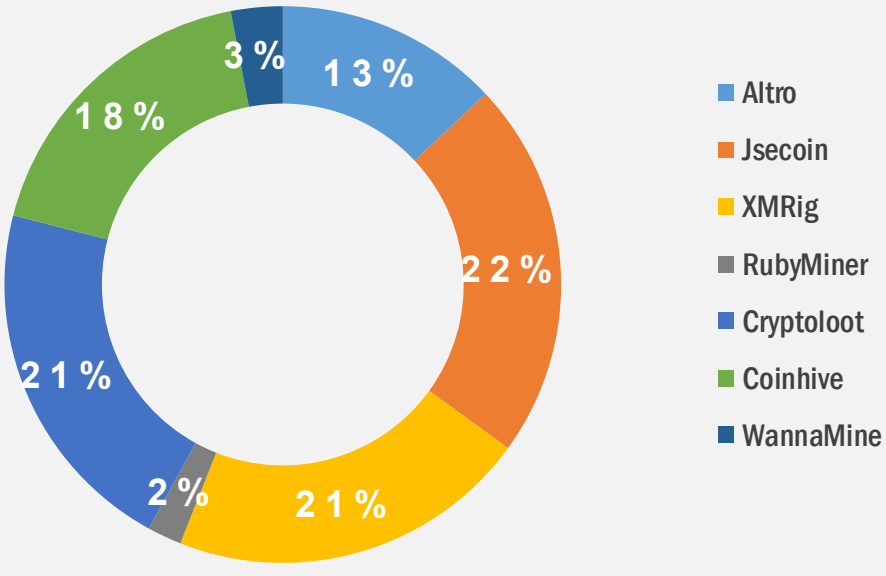


Figura 1. Principali malware di cryptomining a livello globale. Fonte: Check Point[9]

Risultati

64,1_milioni di attacchi cryptojacking alla fine del 2019

78%_di calo delle attività di cryptojacking nel secondo semestre del 2019 rispetto al primo semestre

Le attività hanno registrato una crescita del 9% nella prima metà del 2019, rispetto ai precedenti 6 mesi del 2018.[4,5]

Il 65%_delle 120 piattaforme di scambio più popolari nel terzo trimestre del 2019 aveva processi KYC (Know Your Customer) deboli o porosi

Il 32% delle piattaforme di scambio negoziava privacy coin.[6]

Il 39,3%_delle infezioni da cryptomining del 2019 ha preso di mira il Giappone.

Il 20,8% delle infezioni da cryptomining ha avuto come bersaglio l'India e il 14,2% Taiwan, la figura 1 mostra i cinque paesi con il maggior numero di tentativi di infezioni da malware di cryptomining rilevati per il 2018 e il 2019.[7]

Il 13%_degli incidenti di cryptojacking è attribuito a trojan.Win32.Miner.bbb

Nel periodo tra novembre 2018 e ottobre 2019, gli altri miner più attivi sono stati Trojan.Win32.Miner.ays (11,35%) e Trojan.JS.Miner.m (11,12%).[6]

Kill chain

Cryptojacking

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

Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Cryptojacking

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

Tendenze

_Il popolare servizio di cryptomining Coinhive ha chiuso i battenti

Coinhive è nato nel settembre 2017, pubblicizzandosi come flusso di ricavi alternativo per sviluppatori web, al posto dei banner pubblicitari.[24] Utilizzava librerie JavaScript, che potevano essere installate sui siti web, e la potenza di calcolo del visitatore per il mining legittimo di criptovalute. Fino alla sua chiusura, nel marzo 2019, era stato spesso oggetto di abuso da parte di attori delle minacce, che iniettavano codice nei siti web attaccati per il mining della criptovaluta Monero e il dirottamento dei fondi nelle loro tasche. Dopo la chiusura, il volume degli attacchi di cryptojacking basati sul web è sceso del 78% nel corso del secondo semestre del 2019.[4] In seguito a questo calo, i criminali informatici hanno iniziato a puntare l'attenzione su bersagli di maggior valore, come server potenti[9] e infrastrutture cloud.[1] Il posto di Coinhive in cima alla classifica è stato poi rilevato[9] da Jsecoin (22%), XMRig (21%) e Cryptoloot (21%). La distribuzione dei principali malware di cryptomining a livello globale è illustrata nella figura 1.

_Più attacchi sulle infrastrutture cloud

Nel primo semestre del 2019 si è osservato un tendenziale aumento degli incidenti legati ad attacchi di cryptomining sul cloud.[15,25] Gli ambienti cloud impiegano in genere meccanismi che personalizzano le risorse on-demand e rappresentano quindi bersagli remunerativi per l'esecuzione di software di mining. Questo va tuttavia a discapito dei proprietari dei siti web, che si trovano a sostenere spese più alte per il superamento delle quote.[15] Nel primo semestre 2019 le vulnerabilità nel software dei cloud container sono aumentate del 46% rispetto allo stesso periodo del 2018.[26] Gli aggressori sono riusciti a sfruttare le interfacce di programmazione delle applicazioni (API) e le piattaforme per la gestione dei container al fine di installare immagini malevole (ad esempio Docker e Kubernetes) ed eseguire il mining di criptovalute.[25]

Incidenti

Aprile 2019_ **La campagna di cryptojacking denominata Beapy ha sfruttato la vulnerabilità EternalBlue e ha colpito imprese in Cina**[3]

Maggio 2019_ **PCASTLE, il malware per il mining di Monero, ha preso di mira principalmente i sistemi con sede in Cina, utilizzando tecniche fileless**[19]

Oltre 50 000 server appartenenti ad aziende del settore sanitario, delle telecomunicazioni, dei media e dell'IT sono stati trovati infetti da malware che esegue il mining della criptovaluta TurtleCoin (TRTL).[20]

Una nuova famiglia di malware denominata BlackSquid ha utilizzato otto noti exploit, tra cui EternalBlue e DoublePulsar, diffondendosi successivamente a server web in Thailandia e negli Stati Uniti, in modo da veicolare gli script di mining di Monero.[17,21]

Agosto 2019_ **Rilevato malware di cryptojacking in 11 librerie del linguaggio di programmazione Ruby, esponendo migliaia di utenti a codice per il cryptomining**[22]

Tendenze

_Spostamento verso il cryptomining basato su file

Nel 2019 si è osservato un calo del cryptojacking basato su browser a favore del cryptomining basato su file. Gli attacchi di cryptomining basato su file[27] si sono diffusi attraverso il malware e hanno approfittato di exploit preesistenti su sistemi operativi privi di patch, quali EternalBlue e altre vulnerabilità ad alto rischio. I fattori che hanno contribuito a questo cambiamento sono stati la chiusura di Coinhive, popolare servizio di mining via web[1] e la flessione dei valori delle criptovalute.[10] Un altro fattore è che il cryptomining basato sui file è sempre stato più efficiente rispetto al mining basato sul web, risultando 25 volte più redditizio.[3] Gli attori delle minacce hanno adattato il proprio malware con strumenti supplementari, per estrarre informazioni sensibili dal computer della vittima.

_Gli attacchi di cryptojacking a livello mondiale sono in calo

Nel 2019 si è osservata una tendenziale diminuzione[5] degli attacchi di cryptojacking, soprattutto in seguito alla chiusura di Coinhive[6], agli sforzi coordinati delle autorità di contrasto e al deprezzamento della criptovaluta Monero. È noto tuttavia che gli attacchi di cryptojacking seguono i valori delle criptovalute, pertanto potrebbe emergere un servizio simile a Coinhive e generare una nuova impennata. Le prime statistiche per il 2020 mostrano un aumento del 30% su base annua nel mese di marzo.

_Monero è rimasta la criptovaluta preferita

Analogamente a trend precedenti, Monero (XMR) è stata la criptovaluta preferita per le attività di cryptojacking nel 2019. Il motivo è duplice: in primo luogo, Monero si focalizza sulla privacy e sull'anonimato, rendendo perciò impossibile tracciare le operazioni. In secondo luogo, l'algoritmo Proof-of-Work è concepito per rendere il mining realizzabile con una CPU standard, rispetto ad hardware specializzato. Nel terzo trimestre del 2019 il 32% delle piattaforme di scambio negoziava privacy coin come Monero. Tuttavia, in previsione delle nuove normative antiriciclaggio, molte piattaforme di scambio hanno scelto di escludere dal listing i privacy coin.

_Paesi più colpiti

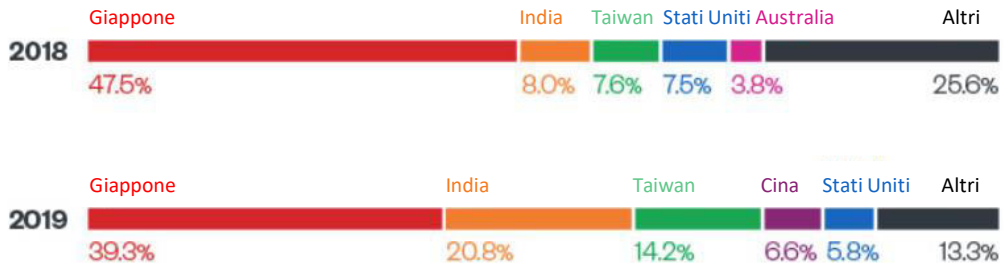


Figura 2. Paesi più colpiti dal cryptojacking. Fonte: Trend Micro[7]

Vettori di attacco

_Tecniche

I criminali informatici hanno utilizzato le tecniche sotto elencate per eseguire o veicolare i cryptominer:

- incorporando capacità di cryptojacking nel malware esistente;[10]
- compromettendo i siti web;[11]
- mediante attacchi drive-by persistenti;[12]
- utilizzando i social network;[13]
- utilizzando applicazioni per dispositivi mobili e app store;[14]
- utilizzando exploit kit;[15]
- utilizzando reti pubblicitarie e malvertising;[16]
- utilizzando supporti removibili;[17]
- e utilizzando cryptominer in grado di propagarsi autonomamente (wormable).[18]

Figura 3. Quando può guadagnare una botnet di mining di criptovalute in 30 giorni? Fonte: Broadcom[3]

_Azioni proposte

- Monitorare il consumo di batteria sui dispositivi degli utenti e, in caso di picchi sospetti nell'utilizzo della CPU, eseguire una scansione alla ricerca di miner basati su file.
- Implementare il filtraggio dei contenuti per escludere allegati indesiderati, e-mail con contenuti malevoli e spam.
- Implementare il filtraggio del protocollo di mining Stratum e inserire in blacklist gli indirizzi IP e i domini dei pool di mining più diffusi.
- Installare la protezione degli endpoint tramite programmi antivirus o plug-in del browser che bloccano i cryptominer.
- Eseguire regolari audit della sicurezza per rilevare le anomalie della rete.
- Attuare una solida gestione delle vulnerabilità e delle patch.
- Utilizzare le whitelist per impedire l'esecuzione di file eseguibili sconosciuti negli endpoint.
- Investire nella sensibilizzazione degli utenti riguardo al cryptojacking, con particolare riferimento ai comportamenti di navigazione sicura.
- Implementare patch e fix contro gli exploit noti, come Eternal Blue, su bersagli meno scontati, come sistemi di gestione delle code, terminali POS e persino distributori automatici.
- Monitorare e inserire in blacklist gli eseguibili di cryptomining comuni.

Riferimenti bibliografici

1. Sergiu Gatlan. «Cryptominers Still Top Threat In March Despite Coinhive Demise.» 9 aprile 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. «Internet Organised Crime Threat Assessment (IOCTA).» 2019. EUROPOL. https://www.europol.europa.eu/iocta-report

3. «Beapy: Cryptojacking Worm Hits Enterprises in China.» 24 aprile 2019. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

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

5. Yessi Bello Perez. «Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019.» 24 luglio 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. «A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule.» 27 novembre 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. «Defending Systems Against Cryptocurrency Miner Malware.» 28 ottobre 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. «Kaspersky Security Bulletin '19 Statistics.» 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. «CYBER SECURITY REPORT.» 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. «EternalBlue Exploit Serves Beapy Cryptojacking Campaign.» 25 aprile 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. «New mining worm PsMiner uses multiple high-risk vulnerabilities to spread.» 12 marzo 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. «New drive-by cryptocurrency mining scheme persists after you exit your browser window.» 9 novembre 2017. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. «Social Media Platforms and the Cybercrime Economy.» 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. «Abusing cryptocurrencies on Android smartphones.» 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. «2019 Midyear Security Roundup Evasive Treats Pervasive Effects.» 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. «YouTube shuts down hidden cryptojacking adverts.» 29 gennaio 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. «New cryptocurrency mining malware is spreading across Thailand and the US.» 4 giugno 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. «BlueKeep is back. For now, attackers are just using it for cryptomining.» 4 novembre 2019. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. «Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques.» 5 giugno 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. «Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware.» 29 maggio 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. «BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner.» 27 agosto 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. «Malicious cryptojacking code found in 11 Ruby libraries.» 2 agosto 2019, Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. «Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play.» 6 agosto 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. «Coinhive cryptojacking service to shut down in March 2019». 27 febbraio 2019. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

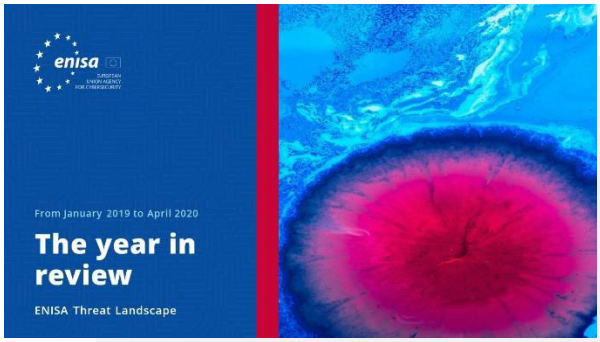
25. Tom Hegel. «Making it Rain - Cryptocurrency Mining Attacks in the Cloud». 14 marzo 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. «How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model». Agosto 2019. Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. «Cryptojacking Attacks: Who's Mining on Your Coin?». 5 aprile 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. «Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz». 12 aprile 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

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

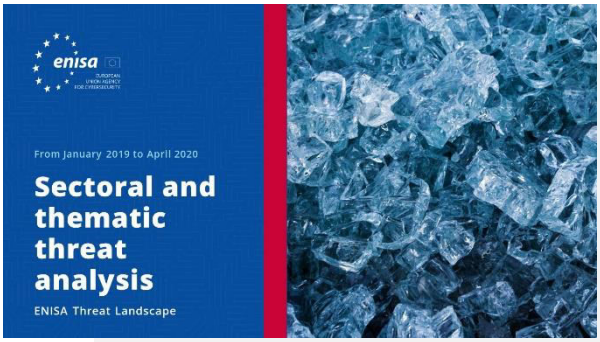
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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