enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Incidenti principali nell'UE e a livello mondiale

Panorama delle minacce analizzato dall'ENISA

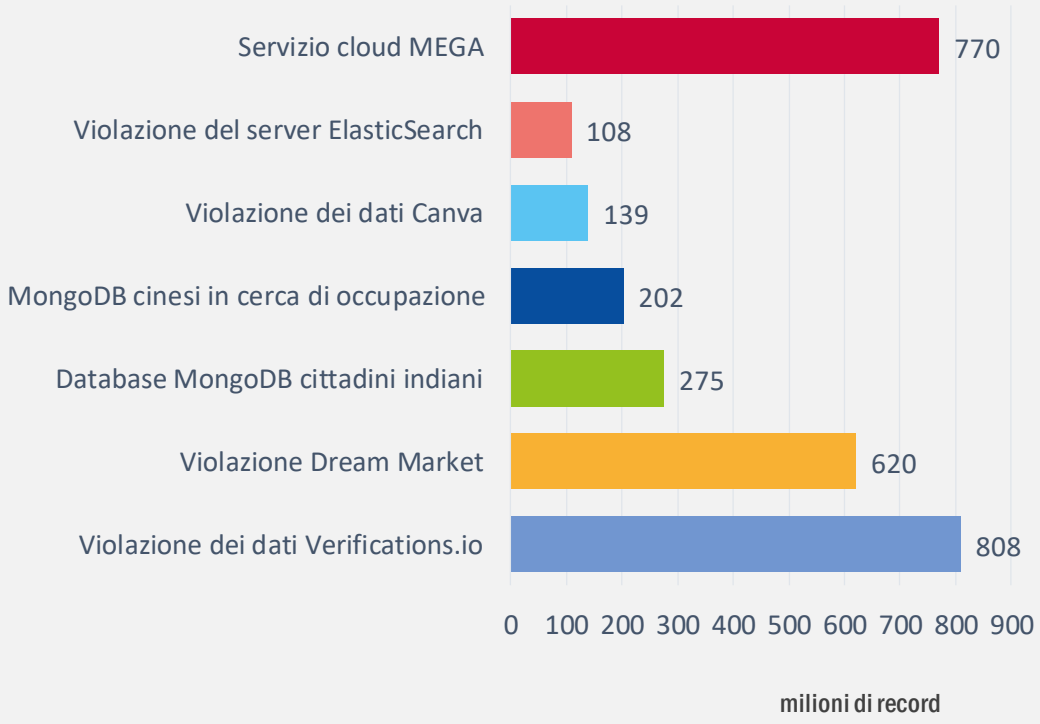
Quadro generale

La sofisticatezza delle competenze in materia di minacce è aumentata nel 2019, con molti avversari che utilizzano exploit, furto di credenziali e attacchi a più livelli. Il numero di incidenti di violazioni dei dati è ancora molto elevato e cresce la quantità di informazioni finanziarie e di credenziali utente rubate. In alcuni casi la mancata correzione in tempi ragionevoli di una vulnerabilità nota, che può potenzialmente interessare il software o le librerie in uso, può avere gravi ripercussioni.

Nell'ultimo decennio **il malware è entrato nell'elenco delle prime 15 minacce stilato dell'ENISA; eppure ancora oggi molti sistemi di sicurezza non sono in grado di rilevare questa minaccia**. Per molti anni il malware si è diffuso principalmente attraverso lo spam tramite e-mail malevole e, più di recente, con messaggi di phishing finemente elaborati. Le aziende tecnologiche così come i fornitori di servizi di posta elettronica hanno investito in filtri antispam, migliorando il rilevamento degli allegati malevoli. Tuttavia, **gli avversari si stanno evolvendo per aumentare le probabilità di raggiungere le potenziali vittime.** Molte innovazioni introdotte dagli attori malintenzionati hanno dato i loro frutti durante questo periodo.

La pandemia di COVID-19 ha messo sotto pressione le organizzazioni e gli operatori della sanità in tutto il mondo e la salute è diventata uno dei settori più critici da proteggere contro gli attacchi informatici. Il numero di incidenti di ransomware diretti verso il settore sanitario era già elevato, ma è aumentato durante la pandemia.

I principali incidenti di violazione dei dati



Sequenza

2019

_ Gennaio

MEGA cloud (NZ) ha subito una violazione dei dati che ha provocato l'esposizione di 770 milioni di e-mail e 21 milioni di password.[1]

_ Febbraio

Verification.io (USA) ha divulgato circa 800 milioni di record.[2]

_ Marzo

Norsk Hydro (NO) vittima di un attacco di ransomware.[3]

_ Agosto

L'agenzia delle entrate bulgara (BG) ha subito una violazione dei dati che ha comportato la divulgazione di informazioni sull'identità di tutti i cittadini adulti.[8]

_ Settembre

Mastercard (BE) ha subito una violazione dei dati che ha interessato circa 90 000 clienti in Europa.[9]

_ Ottobre

Siti web e l'emittente televisiva nazionale in Georgia (GE) hanno subito un attacco informatico coordinato.[30]

_ Novembre

UniCredit (IT) vittima di una violazione dei dati, con esposizione di 3 milioni di record.[10]

_ Dicembre

Prosegur (SP) ha subito un attacco di ransomware che ha interrotto le sue attività operative.[11]

2020

_ Gennaio

Il ministero degli esteri austriaco (AT) bersaglio di un attacco informatico.[12]

_ Aprile

Facebook (USA) ha denunciato una violazione dei dati che ha rivelato 540 milioni di record di utenti su server esposti.[4]

_ Maggio

Thyssen-Krupp e Bayer (DE) bersaglio di un malware di spionaggio.[5]

_ Luglio

City Power (ZA) vittima di un attacco di ransomware che ha interrotto l'erogazione di energia a Johannesburg.[7]

_ Giugno

Cinque ospedali in Romania (RO) colpiti dal ransomware Badrabbit.[6]

_ Febbraio

Il gruppo INA (HR) vittima di un attacco di ransomware.[13]

_ Marzo

Compromessa la rete di ENTSO-E (BE), vittima di un'intrusione.[14]

_ Aprile

Oltre 500 000 account di Zoom (USA) scoperti in vendita sul dark web.[31]

Settori più colpiti

_Sotto tiro

I settori maggiormente presi di mira in questo periodo sono stati i servizi digitali, l'amministrazione pubblica e l'industria della tecnologia. Gli attacchi ai fornitori di servizi digitali fungono spesso da proxy per raggiungere altri obiettivi più interessanti. Gli attacchi all'industria della tecnologia hanno invece permesso ad attori malintenzionati di compromettere la catena di fornitura o di cercare vulnerabilità da sfruttare.

La piattaforma di posta elettronica **verifications.io**[18] ha subito un'importante violazione dei dati[7] a causa di un database MongoDB non protetto. Sono stati rivelati i dati di oltre 800 milioni di e-mail contenenti informazioni sensibili, incluse sull'identità.

Oltre 770 milioni di indirizzi e-mail e 21 milioni di password uniche sono stati rivelati in un popolare forum di hacking ospitato dal servizio cloud **MEGA**[1]. L'incidente è diventato la più significativa raccolta di credenziali personali violate della storia, denominata «Collection #1».

Citrix, azienda che fornisce servizi cloud e di virtualizzazione, è stata vittima di un attacco informatico mirato. Per accedere ai sistemi di Citrix, gli aggressori hanno sfruttato diverse vulnerabilità critiche del software, come CVE-2019-19781, e utilizzato una tecnica denominata «password spraying».

Il fornitore di servizi di cloud hosting **iNSYNQ**[19] ha subito un attacco ransomware[7] che ha impedito ai clienti di accedere ai loro dati per più di una settimana, costringendoli a ricorrere ai backup locali.

Settori più colpiti

Servizi digitali_ Servizi come posta elettronica, piattaforme sociali e collaborative e fornitori di cloud sono stati bersaglio di attacchi nel corso del 2019. Sono stati utilizzati anche come proxy per ulteriori attacchi.

Amministrazione pubblica_ I rendimenti economici dei riscatti pagati fanno del settore pubblico uno degli obiettivi più appetibili per gli attacchi ransomware.

Industria tecnologica_ Nel 2019 l'industria tecnologica è stata sotto tiro soprattutto con attacchi alla catena di fornitura, nel tentativo di compromettere lo sviluppo del software attraverso exploit zero-day e attacchi backdoor.

Finanza_ Il numero di incidenti riguardanti organizzazioni finanziarie, non necessariamente banche, è aumentato notevolmente durante il periodo in esame.

Assistenza sanitaria_ Il numero di attacchi contro il settore sanitario è in continua crescita.

Tendenze

A livello generale

- Nel 2019 un'intensa **attività dei trojan** è stata osservata in tutto il mondo. Emotet e Agent Tesla sono stati i tipi di malware più frequenti e pericolosi[7].
- Il **phishing**[7] si conferma una delle tecniche di maggior successo per veicolare strumenti malevoli. Mezzi di phishing efficaci comprendono truffe telefoniche, nonché fatture, pagamenti, preventivi e ordini di compravendita falsi.
- Il **ransomware**[7] continua a fruttare ricompense economiche sostanziali agli attori malintenzionati. Un recente studio ha individuato campagne di ransomware gestite da esseri umani[17], in cui gli aggressori utilizzano il furto di credenziali e il movimento laterale, metodi tradizionalmente associati ad attacchi mirati come quelli a opera di attori sostenuti da Stati nazione.
- I piani di **skimming delle carte di credito** sono diventati una minaccia significativa nel corso del 2019 e del 2020 a causa dell'aumento del numero di acquirenti online.
- La **compromissione delle e-mail aziendali (Business E-mail Compromise, BEC)** è una minaccia in crescita in conseguenza della grande quantità di credenziali e dati personali rubati nell'ultimo decennio.
- Le aziende subiscono in media 12 attacchi di **«credential stuffing»** ogni mese, in cui l'aggressore è in grado di individuare le credenziali valide.

Risultati

L'84%_ **degli attacchi informatici si affida all'ingegneria sociale**

Il 67%_ **del malware è stato veicolato attraverso connessioni HTTPS crittografate**[34]

230 000_ **nuovi ceppi di malware ogni giorno**

6_ **mesi è in media il tempo richiesto per rilevare una violazione dei dati**

Il 71%_ **delle organizzazioni ha subito attività di malware con diffusione da un dipendente all'altro**[35]

Attori

_Chi

Conoscere il responsabile o attribuire responsabilità a una persona o a un gruppo in merito a un incidente di cibersicurezza è sempre un compito molto arduo e spesso si rivela un esercizio inutile. Eppure, dal punto di vista dell'intelligence sulle minacce, è essenziale classificare i comportamenti, comprendere le dinamiche e il *modus operandi* utilizzati da alcuni avversari. Questa analisi spesso aiuta chi si occupa della difesa a cercare tracce specifiche e ad anticipare la prossima azione degli avversari.

Il **Gruppo Lazarus** ad esempio, un gruppo di minacce persistenti avanzate (APT) presumibilmente sponsorizzato da Stati, è stato, secondo quanto riferito, più attivo nel periodo in esame sia in attacchi dal movente economico sia in attacchi finalizzati allo spionaggio. Il gruppo è stato associato a diversi incidenti, tra cui la **campagna AppleJeus** mirata agli utenti della piattaforma di trading di criptovaluta e ai loro sistemi.[22] Tra i principali incidenti attribuiti a questo gruppo figurano:

- l'hacking di una centrale nucleare e di un'organizzazione di ricerca spaziale indiane nel novembre 2019;
- la compromissione di un'applicazione per il trading di criptovaluta mirata agli amministratori di una piattaforma di scambio nell'ottobre 2019;
- attacchi a sportelli automatici e banche in India, individuati nel settembre 2019;
- attacchi a utenti Android in Corea del Sud attraverso app convertite in trojan in Google Play Store, identificati nell'agosto 2019.

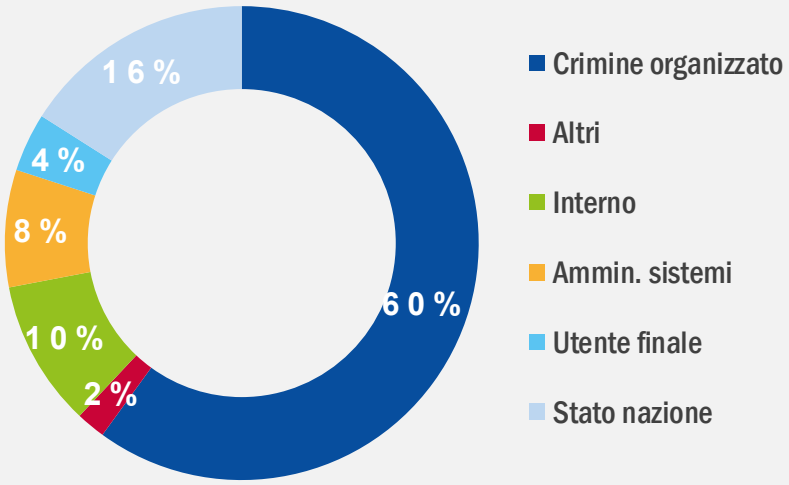
Attori più attivi

TURLA_ Secondo quanto riferito, nel 2019 il gruppo ha preso di mira i server di posta elettronica di Microsoft Exchange nei settori istruzione, pubblica amministrazione, militare, ricerca e farmaceutico in più di 40 paesi.[23]

APT27_ Il gruppo avrebbe compromesso i server SharePoint di organizzazioni governative in due diversi paesi del Medio Oriente.

VICIOUS PANDA_ Nell'aprile 2020 la pubblica amministrazione mongola è stata presumibilmente bersaglio di attacchi del gruppo.[24]

GAMAREDON_ Il gruppo avrebbe preso di mira il Ministero della difesa ucraino in una campagna di spear phishing del dicembre 2019.[25]



Motivazioni

_Perché

Sebbene sia difficile stabilire la motivazione principale dietro gli attacchi informatici, è comunque possibile classificarli in base all'esito dell'incidente.

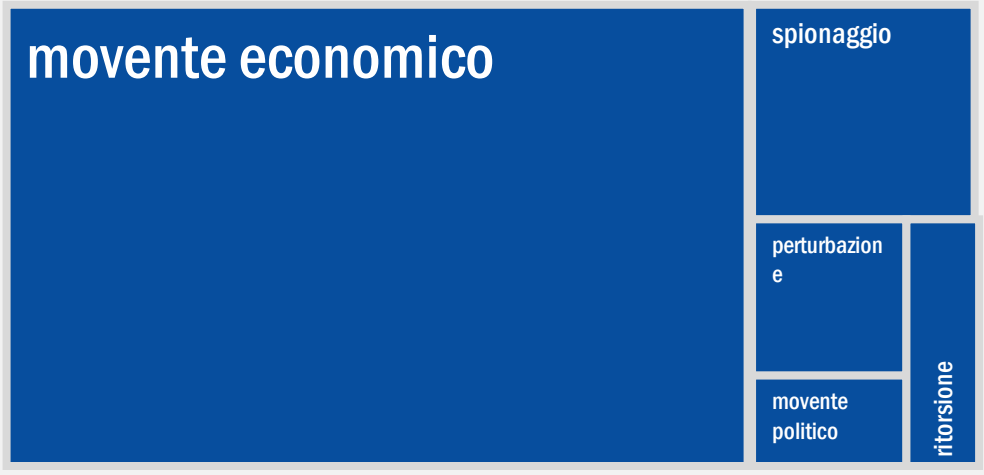
Movente economico Il numero di incidenti che hanno portato al furto di informazioni, dati e credenziali degli utenti è il più alto osservato nel periodo in esame. Nella maggior parte dei casi l'intenzione è rubare dati/informazioni e venderli sul dark web. È possibile individuare anche altri utilizzi di queste informazioni e di questi dati per consentire altri tipi di attacchi con un esito completamente diverso, come lo spionaggio o la frode finanziaria. Più di 620 milioni di dati di account sono stati sottratti da 16 siti web hackerati e messi in vendita su Dream Market, popolare marketplace del dark web.

Spionaggio Si tratta di un movente alla base di un numero crescente di attacchi segnalati, soprattutto a causa delle continue tensioni geopolitiche e commerciali. Il numero di incidenti non è sostanziale, ma le dimensioni e la portata lo collocano al secondo posto nell'elenco delle prime 5 motivazioni stilato dall'ENISA. Tra gli incidenti degni di nota figura quello segnalato nell'aprile 2019, in cui un dipendente della General Electric e un uomo d'affari cinese sono stati accusati dal Dipartimento di giustizia degli Stati Uniti di spionaggio economico e furto di segreti commerciali della General Electric.[20] AgenceFrance Presse (AFP) ha riferito che Airbus è stata vittima di una sofisticata campagna di ciberspionaggio. Gli aggressori avrebbero violato i sistemi informatici di diversi fornitori di Airbus e da questi sarebbero penetrati nei sistemi informatici dell'azienda.[21]

Le prime cinque motivazioni: movente economico, spionaggio, perturbazione, movente politico e ritorsione.

Principali motivazioni

La figura seguente mostra che quello **economico** è ancora il movente principale della maggior parte degli attacchi informatici. In alcuni casi, all'interno di un singolo attacco è possibile individuare più motivazioni. Ad esempio, i moventi di spionaggio, politico, economico e di perturbazione sono spesso associati. Molti incidenti hanno origine da sistemi automatizzati e vengono veicolati in modalità «as-a-service», pagati in criptovaluta. Questi servizi comprendono attività di distribuzione di ransomware, comando e controllo (C2), attacchi distribuiti di negazione del servizio (DDoS), spam e altre attività illecite.



Vettori di attacco

_ Come

Gli attacchi informatici richiedono in media tre passaggi per raggiungere i preziosi asset della vittima. Nell'esaminare i vettori di attacco più frequentemente utilizzati, occorre definire le priorità del punto di ingresso, della linea di condotta e dell'azione sugli asset. Si tratta delle fasi più critiche, che dovrebbero costituire approcci distinti in una strategia di difesa.

Punto di ingresso Nel corso del 2019 le tecniche più di frequente utilizzate per lanciare un attacco informatico comprendono la forza bruta con credenziali rubate, l'ingegneria sociale, gli errori di configurazione e lo sfruttamento delle applicazioni web. Lo sfruttamento delle applicazioni web, ad esempio, è stato spesso impiegato come punto di ingresso per via della crescente diffusione di questo tipo di applicazioni per trasferire i dati nel cloud. Gli errori di configurazione del cloud e l'uso improprio dei sistemi hanno costituito un punto di ingresso essenziale in numerosi incidenti. Il ricorso all'ingegneria sociale per pianificare un attacco sfrutta strumenti come il phishing e la compromissione delle e-mail aziendali (BEC)[16]. Altre tecniche meno frequenti, ma ugualmente importanti, sono lo sfruttamento delle vulnerabilità (da sistemi privi di patch e zero-day) e le backdoor nel software, spesso utilizzate in attacchi più complessi e sofisticati.

Linea di condotta L'installazione di malware è la tecnica più utilizzata nella fase di definizione della «linea di condotta». Una volta installato, aiuta l'aggressore a compiere ricognizioni, a muoversi nei sistemi e nelle reti della vittima, a installare strumenti aggiuntivi come un ransomware, a sottrarre dati e a comunicare con un server C2.

_I cinque asset più desiderati dai criminali informatici

01_Proprietà industriale e segreti commerciali

La proprietà industriale e i segreti commerciali costituiscono gli asset più desiderabili per via dell'elevato valore che essi hanno per i rispettivi proprietari, il mercato e in alcuni casi il mondo criminale.

02_Informazioni classificate statali/militari

Tale risorsa comprende qualsiasi informazione che uno Stato ritenga sensibile. Nel 2019 le tensioni commerciali e diplomatiche tra i paesi hanno reso questo tipo di informazioni ancora più appetibili.

03_Infrastruttura server

L'infrastruttura server è il primo asset sensibile non costituito da dati. In molti attacchi, acquisire il controllo dell'infrastruttura server della vittima rappresenta l'obiettivo primario.

04_Dati di autenticazione

I dati di autenticazione sono asset preziosi per generare utili, ma anche come obiettivo per sostenere un attacco.

05_Dati finanziari

I dati finanziari, come informazioni relative a carte di credito, operazioni bancarie e pagamenti,
rappresentano sempre un valore per i criminali informatici.

Intelligence strategica

_Che cosa è cambiato nel panorama con la pandemia di COVID-19?

Nel 2019 l'ENISA ha continuato a mappare il panorama delle minacce, aiutando decisori e responsabili delle politiche a definire strategie per difendere i cittadini, le organizzazioni e il ciberspazio. Questo lavoro rientra nella strategia dell'ENISA volta a fornire informazioni strategiche ai portatori di interessi. Il tema centrale nel 2019 è stata la prossima generazione di telecomunicazioni mobili, o 5G, a seguito di una richiesta della Commissione europea e degli Stati membri. **L'agenzia continuerà a elaborare questi panorami tematici delle minacce e nel 2020** l'attenzione sarà puntata sull'intelligenza artificiale.

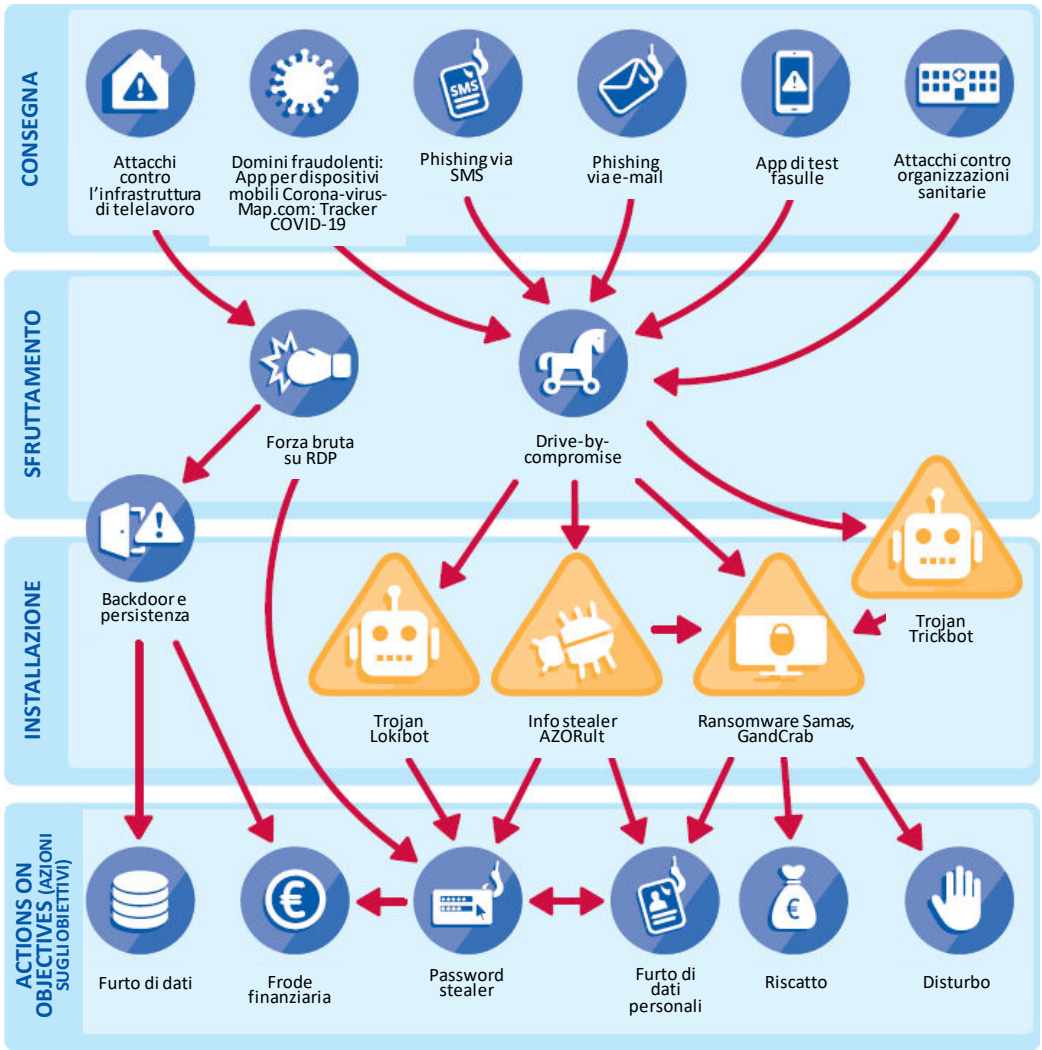
La pandemia di COVID-19 è stata un periodo prolifico per gli attori malintenzionati che hanno condotto attacchi contro aree sensibili, come i fornitori di servizi sanitari e le persone che lavorano da casa. L'ENISA sta mappando il panorama delle minacce delineatosi durante la pandemia e fornisce consulenza sulle misure di mitigazione, nel tentativo di ridurre l'esposizione alle minacce.

L'ENISA condivide le sue raccomandazioni di cibersicurezza in relazione alla pandemia di COVID-19 su svariati argomenti, tra cui il lavoro a distanza, gli acquisti online e la sanità elettronica, fornendo ai settori interessati preziosi consigli aggiornati sulla sicurezza.[32]

L'**ospedale universitario di Brno,** nella Repubblica ceca, ha subito un attacco informatico[33] nel pieno della pandemia di COVID-19, che lo ha costretto a dirottare i pazienti e a rimandare gli interventi chirurgici. L'incidente è considerato critico, poiché l'ospedale è uno dei più grandi laboratori per i test relativi alla COVID-19 della Repubblica ceca.

_Il panorama delle minacce legato alla COVID-19

L'ENISA ha predisposto molte risorse per una campagna di sensibilizzazione e ha condiviso altre risorse interne ed esterne dedicate agli esperti di cibersicurezza, trattando le questioni di sicurezza associate alle sfide affrontate durante la pandemia di COVID-19. Una di queste risorse era un'analisi delle minacce più critiche durante questo periodo.



Riferimenti bibliografici

1. «MEGA Data Breach Exposed 773 Million Email Addresses and Passwords.» 19 gennaio 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

2. «Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records.» 8 aprile 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

3. «LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company.» 20 marzo 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

4. «Researchers find 540 million Facebook user records on exposed servers.» 3 aprile 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

5. «Winnti: Attacking the Heart of the German Industry» 24 luglio 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

6. «Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked» 20 giugno 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

7. «Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions» 25 luglio 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

8. «Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged.» 30 agosto 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

9. «Breach Of Mastercard Loyalty Program Affected 90K Germans' Data» 23 agosto 2019. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

10. «UniCredit confirms data breach» 28 ottobre 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

11. «Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware» 28 novembre 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

12. «Serious cyber-attack' on Austria's foreign ministry» 5 gennaio 2020. BBC. https://www.bbc.com/news/world-europe-50997773

13. «Croatia's largest petrol station chain impacted by cyber-attack» 20 febbraio 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

14. «European power grid organization says its IT network was hacked» 9 marzo 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

15. «FullzHouse hackers pivot from phishing to Magecart card skimming attacks» 26 novembre 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

16. «FBI warns of cloud based BEC attacks.» 8 aprile 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

17. «Microsoft Alerts Healthcare to Human-Operated Ransomware» 1° aprile 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

18. «Verification.io suffers major data breach.» 15 marzo 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

19. «Inside the Insynq attack: 'We had to assume they were listening'» 8 agosto 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

20. «Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets». 23 aprile 2019. USA DoJ. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

21. «Airbus supply chain hacked in a cyberespionage campaign» 27 settembre 2019. CERT-EU. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

22. «Lazarus group's 'AppleJeus' sequel targets cryptocurrency traders» 10 gennaio 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

23. «Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server» 7 luglio 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

24. «Vicious Panda: The COVID Campaign» 12 marzo 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

25. «Gamaredon APT Improves Toolset to Target Ukraine Government, Military» 5 febbraio 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

26. «Virus attacks Spain's defense intranet, foreign state suspected: paper» 26 marzo 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

27. «115 Million Pakistani Mobile Users Data Go on Sale on Dark Web» 10 aprile 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

28. «Your business hit by a data breach? Expect a bill of $3.92 million» 23 luglio 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

29. «Cyber Security Statistics for 2019» 21 marzo 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

30. «Georgia 'I'll Be Back' Cyber Attack Terminates TV, Takes Down 15,000 Websites.» 29 ottobre 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

31. «Half a million Zoom accounts for sale on the dark web.» 16 aprile 2020. We Live Security by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

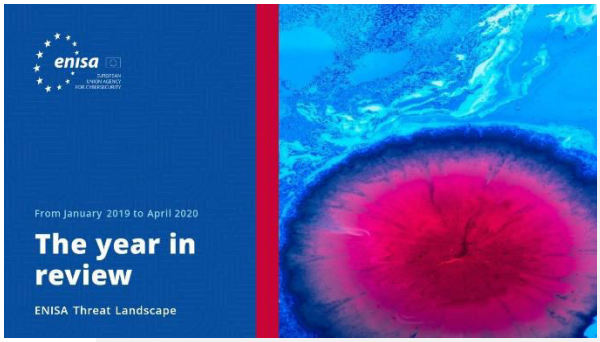
32. «ENISA COVID-19 Resources». ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

33. «Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak» 17 marzo 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

34. «Most malware in Q1 2020 was delivered via encrypted HTTPS connections». 25 giugno 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

35. «Malware statistics and facts for 2020» 29 luglio 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

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

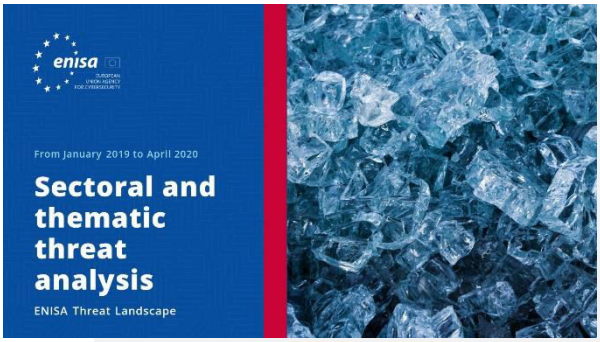
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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

Altre pubblicazioni

Roadmap on the Cooperation Between CSIRTS and LE (Tabella di marcia sulla cooperazione tra CSIRTS e autorità di contrasto)

Una tabella di marcia sulla cooperazione tra i CSIRT, in particolare con le autorità di contrasto nazionali e governative e il potere giudiziario.

LEGGI LA RELAZIONE

EU MS Incident Response Development Status Report (Relazione sullo stato dello sviluppo della risposta agli incidenti negli Stati membri dell'UE)

Uno studio finalizzato ad analizzare l'attuale assetto operativo di risposta agli incidenti all'interno dei settori previsti nella direttiva NIS e a individuare i cambiamenti recenti.

LEGGI LA RELAZIONE

ENSIA CSIRT maturity assessment model (Modello ENISA di valutazione della maturità dei CSIRT)

Versione aggiornata di «Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity» (Sfide per i CSIRT nazionali in Europa nel 2016: studio sulla maturità dei CSIRT), pubblicato dall'ENISA nel 2017

LEGGI LA RELAZIONE

«La complessità delle competenze in materia di minacce è aumentata nel 2019, con molti avversari che utilizzano exploit, furto di credenziali e attacchi a più livelli».

in ETL 2020

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