enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Furto d'identità

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Il furto d'identità o frode d'identità è l'uso illecito delle informazioni di identificazione personale (Personal Identifiable Information, PII) di una vittima da parte di un impostore, al fine di spacciarsi per tale persona e conseguire vantaggi economici e altri benefici.

Secondo un rapporto annuale sulla sicurezza, sono stati individuati almeno 900 casi internazionali di furti d'identità o di reati connessi all'identità[1]. Tra gli incidenti più significativi segnalati figurano:

- la divulgazione di quasi 106 milioni di dati personali di clienti bancari americani e canadesi, in conseguenza dell'incidente di violazione dei dati di Capital One nel marzo 2019[2];
- la divulgazione di 170 milioni di nomi utente e password utilizzati da Zynga, sviluppatore di giochi digitali, nel settembre 2019;
- il furto di 20 milioni di account dal servizio di streaming audio britannico Mixcloud[3];
- la compromissione dei dati personali di 600 000 conducenti e 57 milioni di utenti a seguito dell'incidente di violazione dei dati di Uber nel novembre 2019;[3]
- e il furto di 9 milioni di record personali di clienti EasyJet, tra cui carte d'identità e carte di credito.

La tendenza osservata nel furto d'identità si rispecchia in gran parte nelle violazioni dei dati, che, rispetto al 2018, hanno registrato un numero record di 3 800 casi divulgati pubblicamente, 4,1 miliardi di record esposti e un aumento del 54% del numero di violazioni segnalate.[4]

Risultati

Figura 1. Fonte: Da IBM Security Study – Cost of Insider Threats: Global Report[13]

La minaccia del furto d'identità

Nel 2019 alcuni attori malintenzionati responsabili dei principali incidenti degli ultimi anni sono stati consegnati alla giustizia. A giugno il dipartimento di polizia di New York, in collaborazione con l'FBI, ha arrestato i componenti di un giro di frodi che agivano all'interno e all'esterno degli Stati Uniti e che nel 2012 sono riusciti a rubare credenziali degli iPhone per un valore di 1 milione di dollari USA (circa 846 000 euro) in un'operazione di furto d'identità su larga scala. Fino all'arresto del gruppo l'importo totale del furto ha raggiunto i 19 milioni di dollari USA (circa 16 milioni di euro)[4]. Un mese dopo è stata annunciata pubblicamente la «transazione Equifax»[5]. Equifax è stata costretta ad accettare di risarcire la commissione federale per il commercio degli Stati Uniti (Federal Trade Commission), l'ufficio di tutela dei consumatori (Consumer Financial Protection Bureau), 48 stati, il District of Columbia e Portorico per la violazione dei dati del 2017, per un costo di almeno 575 milioni di dollari USA (circa 487 milioni di euro). In seguito a tale violazione dei dati, che è stata giudicata «totalmente evitabile», sono stati divulgati quasi 148 milioni di indirizzi e numeri di previdenza sociale americani. A fine anno il Brasile ha comminato a Facebook negli Stati Uniti una sanzione pecuniaria di 1,6 milioni di dollari USA (circa 1,35 milioni di euro) a nome dei cittadini brasiliani per la fuga di dati di Cambridge Analytica.[3]

Kill chain

Furto d'identità

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

Tendenze

_Attacchi di impersonificazione del marchio (brand impersonation)

In linea con la tendenza del 2018, alcuni marchi sono preferiti negli attacchi di impersonificazione, per via della loro solida reputazione. Sebbene tali aziende, come Microsoft (44%) e Amazon (17%), restino in cima alla classifica degli attacchi di impersonificazione del marchio del 2019, è degno di nota l'ingresso di nuove realtà, come l'agenzia delle entrate statunitense (Internal Revenue Service, IRS).[7] I dati sensibili inclusi nel Wage and Tax Statement (W-2), la certificazione dei redditi da lavoro dipendente, hanno sempre attratto gli impostori, che nell'anno in esame si sono spacciati per l'IRS nel 10% delle e-mail basate sulla frode d'identità. Di conseguenza, moduli W-2 validi e moduli standard per la dichiarazione dei redditi delle persone fisiche negli Stati Uniti (1040) sono disponibili sul dark web a un costo compreso tra 1 e 52 dollari USA.

Questo materiale, associato ai numeri di previdenza sociale e alle date di nascita, anch'essi disponibili, consente ad hacker anche inesperti che vogliano investire 1 000 dollari USA (circa 846 EUR) di accedere legalmente a un conto bancario con sede negli Stati Uniti, presentare una falsa dichiarazione dei redditi e richiedere un rimborso, raddoppiando o triplicando l'investimento iniziale. Secondo la divisione indagini penali dell'IRS, più di 10 000 dichiarazioni dei redditi di persone fisiche con richieste di rimborso per oltre 83 milioni di dollari USA (circa 70 milioni di EUR) erano potenzialmente fraudolente.[9]

Il ciclo di passaggi per la truffa fiscale «Dirty Dozen»

Figura 2 - Fonte: BDO[19]

Tendenze

_SIM swapping

Si tratta di una tecnica in uso dal 2016, a danno dei possessori di criptovaluta. Tuttavia, nel 2019 la stessa tecnica è stata utilizzata contro individui o account di alto profilo con l'intenzione di impadronirsi dell'identità della vittima. Si sono registrate diverse vittime di SIM swapping, tra cui Jack Dorsey (amministratore delegato di Twitter), Jessica Alba (attrice), Shane Dawson (attore), Amanda Cerny (attrice, vittima di due attacchi), Matthew Smith (attore, vittima di quattro attacchi) e King Bach (artista).[10] Il SIM swapping è stato inoltre utilizzato in modo massiccio in due casi: nella più grande banca del Mozambico, dove sono stati sottratti fino a 50 000 dollari USA (circa 42 300 EUR) da conti aziendali di alto profilo, e in Brasile, dove i conti di 5 000 vittime, soprattutto politici, ministri e governatori, sono stati oggetto di hacking da parte di una banda organizzata.[11]

_Carte regalo utilizzate come cavallo di troia per la compromissione delle e-mail aziendali (Business E-mail Compromise, BEC)

Gli attacchi BEC hanno causato la perdita di miliardi di euro nel 2019. In tali incidenti l'aggressore si spaccia per una persona di fiducia, di solito interna all'azienda, e la vittima viene convinta con l'inganno a effettuare un'operazione finanziaria o a divulgare dati sensibili, personali o aziendali. In più della metà degli attacchi BEC, la vittima veniva indotta ad acquistare una carta regalo. Nel corso del processo di acquisto venivano intercettati dati sensibili, come le credenziali di accesso al conto bancario. La vittima veniva inoltre costretta a inviare la carta regalo all'aggressore, che realizzava così un guadagno anonimo, irreversibile e diretto. L'importo medio sottratto tramite carte regalo ha raggiunto 1 500 dollari USA (circa 1 269 EUR).[12]

Risultati

Il 20%_ degli attacchi con frode d'identità ha utilizzato account compromessi[7]

Il 30%_ degli attacchi diretti verso gli account di dirigenti apicali è stato eseguito con l'inganno del nome visualizzato (display name)[7]

Il 65%_ degli attacchi BEC ha indotto le vittime ad acquistare carte regalo[12]

3,32_ milioni di euro è il costo medio di una violazione dei dati

Il 95%_ degli intervistati di un'indagine Eurobarometro considera il furto d'identità un reato grave

Tendenze

_Doppelgänger digitali

La tecnica antifrode delle «maschere digitali» è stata divulgata quando più di 60 000 identità digitali rubate sono apparse come prodotto di scambio su Genesis, marketplace illegale sul dark web, nell'aprile 2019. Questi doppelgänger erano disponibili per l'acquisto a 5-200 dollari USA ciascuno. Chi possiede un doppelgänger può più facilmente fingersi un utente reale in un negozio online o in un servizio di pagamento, soprattutto se a ciò si associano login e password rubati. Oltre all'acquisto di doppelgänger digitali, sono comparsi nuovi strumenti per assistere il potenziale impostore, come il browser Tenebris, in cui è integrato un generatore che permette di sviluppare impronte digitali e maschere digitali uniche.[11]

Negli ultimi anni autori di skimming, rovistatori di cassonetti, hacker, finti amministratori e phisher sono stati individuati come i principali gruppi responsabili degli attacchi di furto d'identità. Nel 2019 l'elenco si è ampliato, con l'aggiunta di autori di vishing e smishing. Il vishing è una forma di phishing telefonico. A differenza della sostituzione di persona tramite telefono, nel vishing si finge di rappresentare un'organizzazione nota, offrendo alla vittima assistenza con un servizio, ad esempio la gestione di software, finanze o una richiesta di rimborso di imposte. Lo smishing consiste nell'invio di falsi messaggi SMS e, in caso di risposta del destinatario, nel dirottamento o reindirizzamento diretto del dispositivo della vittima verso un sito web di phishing.

La figura seguente mostra i principali tipi di dati persi nel 2019, dove i dati delle e-mail rappresentano il maggior numero di record persi o rubati. Queste cifre mostrano la gravità della situazione, se si considera che le e-mail possono contenere dati personali, aziendali e governativi sensibili.

Principali tipi di dati persi nel 2019

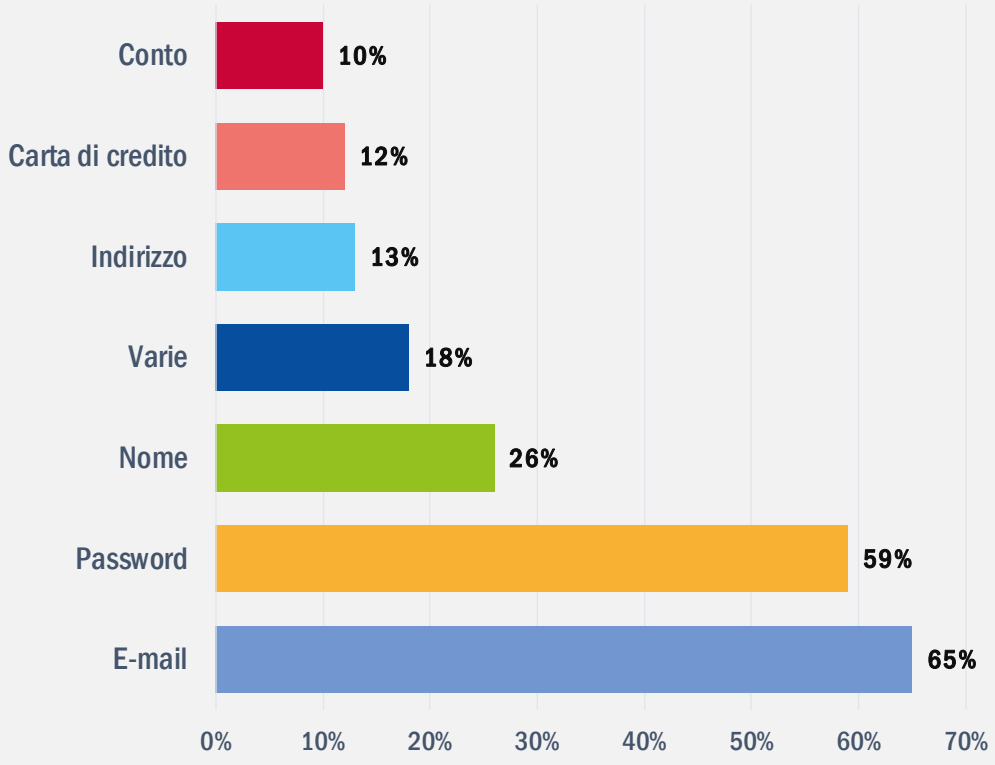


Figura 3 - Fonte: RiskBased SECURITY[8]

Vettori di attacco

Come

- **IL CLOUD COME INTERFACCIA DI ATTACCO PER I DATI DEI CLIENTI**. Nell'anno in esame Amazon CloudFront, una rete di distribuzione di contenuti (Content Delivery Network, CDN), è stata compromessa.[14] I siti web ospitati o collegati alle librerie sull'infrastruttura di Amazon sono stati esposti, svelando i contenuti caricati esternamente, inclusi i dati delle carte di credito.
- **URL DI PHISHING**. Le comuni tecniche di URL di malware[16] di cybersquatting, domain shadowing e strumenti di abbreviazione degli URL sono state nuovamente impiegate nel 2019. Nell'ultimo trimestre del 2019 si è notato che il 26% dei domini malevoli utilizzava un certificato di sicurezza e uno di questi certificati su tre era SSL. Questo trucco ha interferito con il giudizio del visitatore, che faceva affidamento all'icona del lucchetto nel browser come segno di sicurezza.[15]
- **TRUFFA LEGATA AL MODULO W2** Un altro attacco che prende di mira i documenti di aziende e organizzazioni per accedere a dati sensibili è la truffa legata al modulo W2. La truffa inizia con il fingersi un dirigente del reparto finanza o risorse umane per ottenere documenti dei dipendenti. Questi documenti vengono poi utilizzati per il furto d'identità. La truffa prende il nome dal modulo fiscale W2 utilizzato negli Stati Uniti per la dichiarazione degli stipendi dei dipendenti. Sebbene di vecchia data (è stata segnalata dall'IRS per la prima volta nel 2016), questa truffa di ingegneria sociale ha registrato un aumento del 10% annuo negli ultimi anni.[9,17]
- **NIMCY**. Nel 2019 uno strumento di spear phishing, Nimcy, è stato introdotto dal gruppo responsabile della famiglia di malware Zebrocy. È stato sviluppato con il linguaggio di programmazione Nim (ex Nimrod), creato dallo stesso gruppo di hacker. Questo nuovo downloader e backdoor è stato utilizzato per il furto di credenziali di accesso, digitazioni, comunicazioni e file a danno di diplomatici, funzionari della difesa e personale ministeriale nel settore degli affari esteri. Gli aggressori sembravano concentrarsi sui governi dell'Asia centrale, in particolare Pakistan e India.[14]

- **MINACCE LEGATE A DISPOSITIVI MOBILI.** Nel 2019 si è osservato un aumento di app mobili malevole, proseguito nel 2020. Anche le piattaforme più diffuse e fidate, come Google Play, ospitavano applicazioni finalizzate al furto di credenziali (ad esempio Acesse SantaMobile, Modulo ID). Il numero di download è stato tuttavia estremamente basso, a dimostrazione del fatto che le potenziali vittime non sono state ingannate.[20]
- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** L'ottavo trojan per dispositivi mobili in termini di diffusione e il più diffuso trojan per mobile banking, responsabile rispettivamente dell'1,75% e del 16,85% degli attacchi unici, prende di mira soprattutto le credenziali bancarie delle vittime e i codici di autorizzazione a due fattori. La maggior parte delle vittime di questo trojan si trova in Russia, che risulta così il primo paese in termini di quota di utenti attaccati da trojan per mobile banking.[21]
- **FORMJACKING.** Il formjacking era molto comune nel 2018, ma il numero di attacchi è sembrato diminuire notevolmente nel primo trimestre del 2019. A partire dal mese di maggio però, con l'attacco a un operatore sanitario americano e il furto delle credenziali di accesso, il numero di attacchi ha continuato a crescere per tutto il resto dell'anno. In quel mese si è registrato il numero record di 1,1 milioni di attacchi rilevati. I cinque paesi con il maggior numero di attacchi di formjacking rilevati nel 2019 sono Stati Uniti (51,8%), Australia (8,1%), India (5,7%), Regno Unito (4,1%) e Brasile (3,5%). Il gruppo di hacker MageCart è fortemente associato alla maggior parte degli strumenti di formjacking sviluppati e agli attacchi diretti contro British Airways, Newegg, Feedify e Ticketmaster.[22]

Mitigazione

Azioni proposte

- Evitare di utilizzare il gestore di password fornito dal browser. Se necessario, utilizzare un gestore di password offline protetto.[23]
- Verificare l'autenticità di qualsiasi mittente di una richiesta di trasferimento di denaro per telefono o di persona.[19]
- Non condividere dati sensibili come le cartelle cliniche dei pazienti in appunti scritti a mano per evitarne la perdita o l'errata collocazione. I file digitali sono più adatti per i dati con una vita breve e poi dovrebbero essere completamente distrutti.
- Utilizzare programmi di ricerca proattiva delle minacce («threat hunting») all'interno della propria azienda per rafforzare i piani di sicurezza. Tale attività è condotta da membri esperti del team del Security Operation Center (SOC) per identificare in modo proattivo le vulnerabilità ed evitare che le minacce possano sfruttarle.
- Utilizzare politiche come le regole basate sulla velocità per mitigare le frodi d'identità, in particolare per le operazioni con carte di pagamento. I dati delle operazioni valide generati automaticamente possono fornire informazioni sufficienti per una definizione ottimale della politica.
- Utilizzare il metodo di autenticazione single-sign-on (SSO), se disponibile, che consente all'utente di accedere a diverse applicazioni con la stessa serie di credenziali digitali. Il suo utilizzo è fortemente consigliato per ridurre al minimo il numero di account utente e di credenziali memorizzate.
- Installare la protezione degli endpoint mediante programmi antivirus, ma bloccare anche opportunamente l'esecuzione dei file (ad esempio bloccare l'esecuzione nella cartella dei file temporanei).
- L'autenticazione a più fattori è una misura di sicurezza per evitare l'hacking o la perdita di password e per garantire che il processo di autenticazione con chiavi multiple vada a buon fine. L'introduzione dell'autenticazione adattiva a più fattori ottimizza il processo di autenticazione sulla base del comportamento dell'utente e del contesto associato.

- Controllare gli URL inviati per posta elettronica o visitati casualmente in base al loro indirizzo IP, all'ASN associato all'IP, al proprietario del dominio e al rapporto tra questo dominio e altri, prima di compiere ulteriori azioni.
- Le organizzazioni che utilizzano servizi cloud devono avere solide attività di sicurezza del cloud e servirsi preferibilmente di un'architettura di archiviazione in locale, archiviazione cloud privata e archiviazione cloud pubblica contemporaneamente, per proteggere i dati personali dei loro clienti.
- Applicare l'uso di metodi di crittografia forti e aggiornati, come TLS 1.3 (che utilizza chiavi effimere) per i dati sensibili, per evitare gli attacchi.
- Proteggere adeguatamente tutti i documenti di identità e relative copie (fisiche o digitali) dall'accesso non autorizzato.
- Non divulgare le informazioni di identità a destinatari indesiderati e non rispondere a richieste effettuate per telefono o posta elettronica o di persona.
- Richiedere l'uso di dispositivi protetti da password, garantendo una buona qualità delle credenziali e metodi sicuri per la loro memorizzazione.
- Garantire una buona qualità delle credenziali e metodi sicuri per la loro memorizzazione in tutti i supporti utilizzati.
- Prestare particolare attenzione quando si utilizzano le reti Wi-Fi pubbliche, che possono essere oggetto di hacking o contraffazione da parte di truffatori. In caso di utilizzo, evitare di accedere ad applicazioni e dati sensibili. Utilizzare un servizio VPN fidato per connettersi alle reti Wi-Fi pubbliche.
- Controllare regolarmente le operazione documentate da estratti conto bancari o ricevute per eventuali irregolarità.
- Installare il filtraggio dei contenuti per eliminare allegati non richiesti, messaggi e-mail con contenuti malevoli, spam e traffico di rete indesiderato.
- Richiedere l'uso di soluzioni di prevenzione della perdita di dati (Data Loss Prevention, DLP).

Riferimenti bibliografici

1. «2019 identity theft report released» 31 luglio 2019. ITIJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. «Capital One data breach: What you can do now following bank hack» 12 agosto 2019. C | Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. «Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks». 8 gennaio 2020. Cyber crime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4. «$19 million worth of iPhones stolen in massive identity theft scam» 15 giugno 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. «Equifax to pay at least $575 million as part of FTC settlement» 22 luglio 2019. C | Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6. «2019 data breaches: 4 billion records breached so far» Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. «Q1 2019: Email Fraud and Identity Deception Trends» Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. «Data Breach QuickView Report, 2019 Q3 trends.» Novembre 2019. RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. «IRS issues 2019 annual report; highlights program areas across the agency» 6 gennaio 2020. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. «Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too» 5 settembre 2019. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. «IT threat evolution Q2 2019» 19 agosto 2019. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. «Phishing Activity Trends Report» 12 settembre 2019. Anti-phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. «The Cost of Insider Threats» IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. «APT trends report Q2 2019» 1º agosto 2019. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. «Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more» Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. «Q2 2019 Cryptocurrency Anti-Money Laundering Report» Cipher Trace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

18. «Latest Quarterly Threat Report - Q1 2019» Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

19. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" Ottobre 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

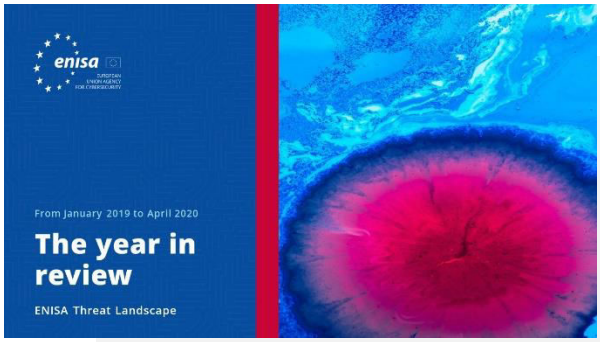
20. «IT threat evolution Q1 2019. Statistics» 23 maggio 2019. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. «IT threat evolution Q3 2019. Statistics» 29 novembre 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. «FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month» Agosto 2019. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. «Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web» VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

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

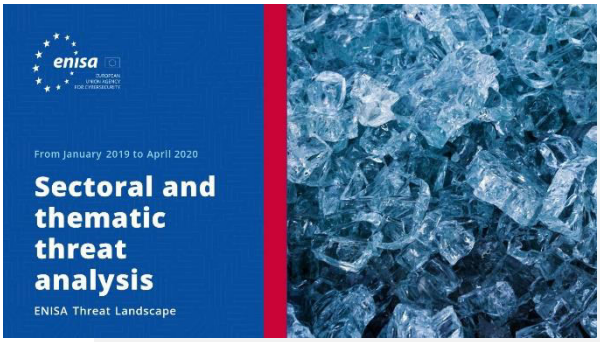
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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