enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Phishing

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Il phishing è il tentativo fraudolento di rubare i dati degli utenti, come credenziali di accesso, dati della carta di credito o anche denaro, mediante tecniche di ingegneria sociale. **Questo tipo di attacco viene in genere lanciato attraverso messaggi di posta elettronica che sembrano inviati da una fonte attendibile, con l'intento di convincere l'utente ad aprire un allegato malevolo o a seguire un URL fraudolento.** Una forma mirata di phishing denominata «spear phishing» prevede una ricerca preliminare sulle vittime in modo che la truffa appaia più autentica, rendendola così uno dei tipi di attacco alle reti aziendali più riusciti.[1]

Una risposta emotiva giustifica le azioni di molte persone quando sono vittime di phishing ed è proprio quello che gli hacker cercano. In un contesto di formazione, questo è ciò che una simulazione di phishing dovrebbe tentare di ottenere. La formazione degli utenti di posta elettronica è una delle misure spesso utilizzate per prevenire il phishing, con risultati tuttavia poco convincenti poiché gli attori delle minacce cambiano costantemente il loro *modus operandi*. Lo standard DMARC (Domain Based Message Authentication, Reporting and Conformance) assicura il blocco delle e-mail provenienti da domini fraudolenti, abbassando il tasso di successo degli attacchi di phishing, spoofing e[2] spam.

In futuro la posta elettronica continuerà a essere il meccanismo numero uno del phishing, ma non per molto. Si sta già assistendo a un aumento dell'utilizzo della messaggistica sui social media, di WhatsApp e altri nella conduzione degli attacchi. Il cambiamento di maggior rilievo riguarderà i metodi per inviare i messaggi, che diventeranno più sofisticati con l'adozione dell'intelligenza artificiale (IA) da parte degli avversari nella preparazione e nella spedizione dei messaggi. Phishing e spear phishing sono i principali vettori di attacco di altre minacce, come le minacce interne non intenzionali[2].

Risultati

26,2_ **miliardi di perdite nel 2019 con attacchi di compromissione delle e-mail aziendali (Business E-mail Compromise, BEC)[20]**

Il 42,8%_ **di tutti gli allegati malevoli era costituito da documenti Microsoft Office[25]**

667%_ **di aumento delle truffe di phishing in un 1 solo mese durante la pandemia di COVID-19[6]**

Il 30%_ **dei messaggi di phishing è stato consegnato di lunedì[29]**

Il 32,5%_ **di tutte le e-mail utilizzava la parola chiave «pagamento» nell'oggetto del messaggio[28]**

Kill chain

Phishing

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

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

Tendenze

_I tipi di servizi più presi di mira sono webmail e Software-as-a-Service

Secondo alcune proiezioni, nel primo trimestre del 2019 gli attacchi di phishing diretti ai servizi di Software-as-a-Service (SaaS) e webmail hanno superato per la prima volta quelli rivolti ai servizi di pagamento, facendone il settore maggiormente preso di mira, con il 36% di tutti gli attacchi di phishing.[2] Questo nuovo record segue la tendenza del 2018, quando i servizi SaaS e webmail avevano di poco superato il settore finanziario[3]. Nonostante il calo al 30,8% di tale dato alla fine del 2019, i servizi sopra citati sono comunque rimasti in cima alla classifica[2,3], con i **servizi Microsoft 365 come primo obiettivo degli autori di phishing.**[4]

_Gli attacchi BEC (Business E-mail Compromise) continuano a rappresentare un problema

Secondo quanto riscontrato da un recente studio, l'88% delle organizzazioni mondiali è stata vittima di attacchi di spear phishing e l'86% ha subito attacchi BEC.[16] Nel 2019 uno dei servizi più colpiti è stato Microsoft 365, con l'obiettivo principale della raccolta di credenziali.[17] Una volta acquisite tali credenziali, l'aggressore era in grado di raccogliere ulteriori dati dell'organizzazione, un processo che poteva durare settimane o mesi[18] e che avrebbe poi portato ad attacchi di spear-phishing. L'aggressore si spacciava per un dipendente, un amministratore delegato (CEO) o persino un fornitore di fiducia per dirottare fondi o reindirizzare i pagamenti verso conti di terzi.[14] Nel primo trimestre del 2019 le aziende sono state bersaglio di attacchi BEC con una frequenza del 120% superiore a quella dell'anno precedente[19], con conseguenti perdite addirittura di 26,2 miliardi di dollari USA (circa 22,2 miliardi di euro).[20]

_Più di due terzi dei siti di phishing hanno adottato il protocollo HTTPS

Negli ultimi anni si è registrata una forte crescita[13] del numero di siti di phishing che hanno adottato il protocollo HTTPS. Nell'ultimo trimestre del 2019 il 74% dei siti di phishing utilizzava l'HTTPS[32], con un incremento significativo rispetto ad appena il 32% di soli 2 anni prima. Sebbene tecnologie come HTTPS e SSL siano concepite per proteggere le comunicazioni tra un client e un server, la presenza di un lucchetto in un'icona nella barra degli indirizzi del browser può creare l'illusione che si tratti d un sito web affidabile.

Gli attori delle minacce possono anche avvalersi di siti legittimi da loro violati per ospitare contenuti di phishing, rendendo così difficile per l'utente finale distinguere un sito non sicuro[14]. Altri fattori che contribuiscono al forte aumento dell'utilizzo di HTTPS sono la miriade di servizi di certificazione gratuiti, come Let's Encrypt,[15] e il fatto che i moderni browser contrassegnino ogni sito HTTPS come sicuro, senza ulteriori controlli.

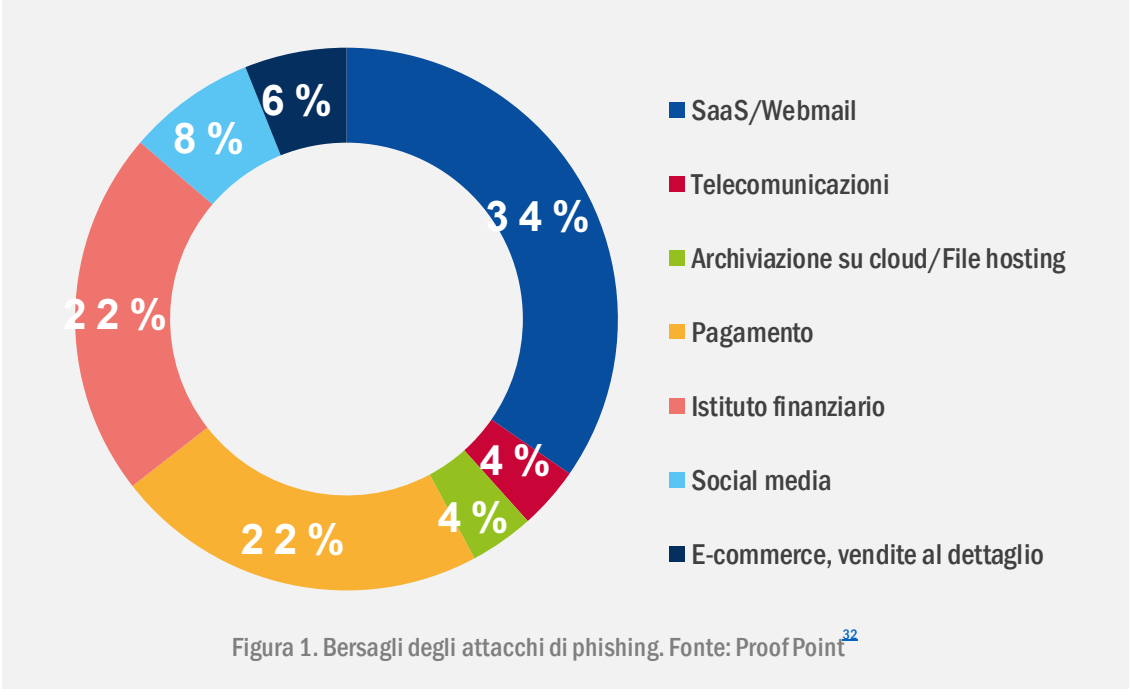


Figura 1. Bersagli degli attacchi di phishing. Fonte: Proof Point[32]

Tendenze

_Phishing-as-a-Service (PhaaS) in aumento

Questi tipi di servizi si basano in genere su abbonamento o sono forniti sotto forma di kit, disponibile per il download a pagamento, ed eliminano le barriere tecnologiche all'ingresso, consentendo anche a individui con minori competenze tecniche di condurre un attacco mirato. Una relazione di un ricercatore in materia di sicurezza[21] ha individuato, nel giugno 2019, 5 334 kit di phishing unici disponibili. L'aspetto ancora più preoccupante era il costo relativamente basso di queste soluzioni, intorno a 50-80 dollari USA per un abbonamento mensile. La stessa relazione affermava che l'87% dei kit comprende meccanismi di elusione, come la codifica dei caratteri HTML e la crittografia dei contenuti. È interessante sottolineare che alcuni di questi servizi erano ospitati su servizi cloud legittimi con sistemi dei nomi di dominio (Domain Name System, DNS) e certificati appropriati. Bastano le statistiche relative a uno solo di questi mercati darknet per evidenziare il successo degli attacchi, che consentono all'aggressore o al gruppo di sottrarre circa 65 000 account al mese.[22]

_Tendenze negli incidenti

- Si è notato un cambiamento nell'efficacia degli attacchi di phishing che utilizzano l'archiviazione su cloud, DocuSign e i servizi cloud di Microsoft.
- Gli attacchi a opera di impostori comprendono schemi quali la compromissione delle e-mail aziendali (BEC) e tecniche di frode d'identità basate sull'ingegneria sociale per rendere più efficaci le campagne di phishing.
- Il phishing mediante i servizi Microsoft 365 è stato lo schema principale, anche se l'attenzione rimane concentrata sulla raccolta di credenziali.
- Oltre il 99% delle e-mail che distribuiscono malware ha richiesto, per essere efficace, un intervento umano, come l'apertura di link o documenti, l'accettazione di avvisi di sicurezza e altri comportamenti.[44]

Principali tematiche di phishing nel 2019

- Raccolta di credenziali e-mail generiche
- Phishing legato a Office 365
- Phishing legato a istituti finanziari
- Phishing legato a Microsoft OWA
- Phishing legato a OneDrive
- Phishing legato ad American Express
- Phishing generico Chalbhai
- Phishing legato ad account Adobe
- Phishing legato a DocuSign
- Phishing legato a Netflix
- Phishing legato ad account Dropbox
- Phishing legato ad account LinkedIn
- Phishing legato ad account Apple
- Phishing legato ad aziende di servizi postali/di spedizione
- Phishing legato a documenti Microsoft online (Excel e Word)
- Phishing legato a impostazioni di Windows
- Phishing legato a Google Drive
- Phishing legato a PayPal

Fonte: Proof Point[32]

La COVID-19 come esca per il phishing

I criminali informatici approfittano della paura generale per la pandemia di COVID-19, che ha fatto la sua comparsa negli ultimi mesi del 2019. Secondo quanto segnalato, gli attacchi di phishing che riguardano il virus sono aumentati del 667% nell'arco di un mese (tra la fine di febbraio 2020 e la fine di marzo 2020) e questo tipo di schema, da solo, ha rappresentato addirittura il 2% di tutte le truffe di phishing.[5]

Le nuove truffe hanno riguardato e-mail di phishing progettate per sembrare provenienti dal centro per il controllo delle malattie (Center of Disease Control, CDC) statunitense[6], l'Organizzazione Mondiale della Sanità[7] o perfino da équipe sanitarie di università[8]. Queste sostenevano falsamente di mostrare casi di infezione nella zona della vittima o condividevano opinioni di esperti medici per indurre la vittima a seguire un link malevolo. Per questo motivo l'FBI e l'OMS hanno emesso avvertimenti.[8,9] Dato che molte persone in quarantena lavoravano da casa, spesso utilizzando sistemi di sicurezza obsoleti[11], i criminali informatici hanno cercato di sfruttare le opportunità e le vulnerabilità emergenti[12].

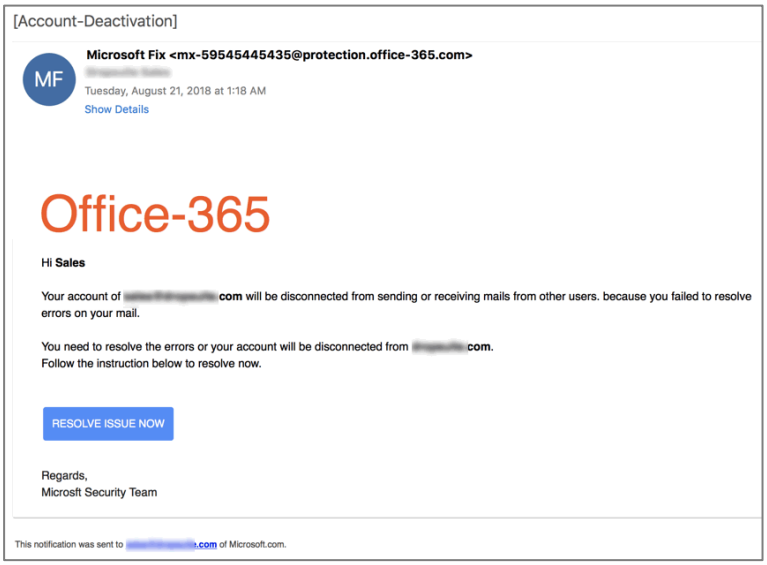


Figura 2. E-mail di phishing Office 365, fonte: Dropsuite[45]

La risposta dell'ENISA alla pandemia di COVID-19

Lo scoppio della pandemia di COVID-19 ha determinato un enorme cambiamento nel nostro modo di vivere. In questo mondo sempre più connesso, possiamo per fortuna continuare la nostra vita professionale e privata in modo virtuale. In questo periodo senza precedenti, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha condiviso le sue raccomandazioni di cibersicurezza[46] su svariati argomenti, tra cui il lavoro a distanza, gli acquisti online e la sanità elettronica, oltre a fornire aggiornamenti sui consigli di sicurezza essenziali su misura per i settori interessati. L'ENISA esamina il panorama delle minacce durante la pandemia e fornisce consulenza sulle modalità di mitigazione dei rischi derivanti dalle minacce più critiche. Particolare attenzione è dedicata al phishing, a causa dell'escalation del numero di attacchi.

Figura 3. Video YouTube dell'ENISA sulla COVID-19. Fonte: ENISA

Incidenti

_Settori colpiti

Il settore sanitario è stato pesantemente colpito da attacchi di phishing (o spear phishing) nel 2019. Un ricercatore in materia di sicurezza[42] ha ritenuto il phishing il principale vettore di attacco dell'anno, attraverso il ricorso a tattiche di ingegneria sociale per veicolare e-mail infettate da malware[7] o contenenti link a siti web infetti. Anche altri settori sono stati bersaglio degli attacchi di phishing, come i governi e altri organismi della pubblica amministrazione. A novembre e dicembre 2019, ad esempio, diversi diplomatici e funzionari del governo ucraino hanno ricevuto e-mail di spear phishing che li indirizzavano a siti web compromessi.[43]

_Vettori di attacco

Lo spear phishing resta una delle tecniche di accesso iniziale prevalentemente utilizzate dagli attori malintenzionati. Questi utilizzano svariate tattiche di ingegneria sociale per indurre i destinatari ad aprire gli allegati o a navigare verso un sito web infetto. I messaggi di spear phishing contengono in genere documenti Microsoft Office malevoli con attivazione macro o un link a tali documenti. Quando l'utente seleziona «Abilita contenuto», la macro incorporata inizia in genere l'esecuzione di una catena di script offuscati, che porta infine al download di malware di fase uno o dropper. JavaScript e PowerShell sembrano confermarsi i linguaggi di scripting più diffusi a questo scopo.

Esempi

_Un attacco di phishing a studenti della Lancaster University ha causato la perdita di dati personali[37]

_Con un attacco di phishing, gli hacker si sono impadroniti delle credenziali di accesso di 2500 utenti di Discord[38]

_Fornitore di servizi di fitness online vittima di un attacco di phishing[39]

_Pazienti interessati da un attacco di phishing ai danni di UConn Health[41]

_Una filiale di una casa automobilistica ha perso 37 milioni di dollari USA (circa 31 milioni di euro) per una truffa BEC[33]

Mitigazione

_Azioni proposte

- Istruire il personale a identificare le e-mail false e malevole e a rimanere vigile. Lanciare campagne di phishing simulate per mettere alla prova l'infrastruttura dell'organizzazione e la reattività del personale.
- Considerare l'uso di un gateway e-mail di sicurezza con manutenzione regolare (eventualmente automatizzata) dei filtri (anti-spam, anti-malware, filtraggio basato su policy).
- Considerare l'applicazione di soluzioni di sicurezza che utilizzano tecniche di apprendimento automatico per individuare i siti di phishing in tempo reale.
- Disabilitare nei client di posta l'esecuzione automatica di codice, macro, rendering della grafica e precaricamento dei link inviati ed eseguire aggiornamenti frequenti.
- Implementare uno degli standard per la riduzione delle e-mail di spam: SPF (Sender Policy Framework)[34], DMARC (Domain-based Message Authentication, Reporting & Conformance)[35] e DKIM (Domain Keys Identified Mail).[36]
- Idealmente utilizzare comunicazioni di posta elettronica sicure, mediante firme digitali o crittografia, per le operazioni finanziarie critiche o per lo scambio di informazioni sensibili.
- Implementare il rilevamento di frodi e anomalie a livello di rete, per le e-mail sia in entrata sia in uscita.
- Evitare di fare clic su link casuali, in particolare i link brevi presenti nei social media.
- Non aprire link né scaricare allegati se non si è assolutamente sicuri dell'origine di una e-mail.

- Evitare di condividere troppi dati personali sui social media, ad esempio la durata dell'assenza dall'ufficio o da casa, le informazioni sui voli, ecc., che vengono attivamente sfruttati dagli attori delle minacce per raccogliere informazioni sui loro obiettivi.
- Controllare il nome del dominio dei siti web visitati per verificare la presenza di errori di battitura, in particolare per i siti web sensibili come quelli bancari. Gli attori delle minacce registrano in genere domini falsi, all'apparenza simili a quelli legittimi, e li usano per «pescare» i loro obiettivi. Non è sufficiente verificare che la connessione sia HTTPS.
- Abilitare l'autenticazione a due fattori, ove pertinente, per impedire l'acquisizione di controllo dell'account.
- Utilizzare una password forte e unica per ogni servizio online. Il riutilizzo della stessa password per vari servizi costituisce un serio problema di sicurezza e dovrebbe essere sempre evitato. L'utilizzo di credenziali forti e uniche per ogni servizio online limita il rischio di una potenziale acquisizione di controllo di un account al solo servizio in questione. L'utilizzo di un software di gestione delle password renderà il compito più semplice.
- Quando si esegue un bonifico su un conto, ricontrollare le informazioni del beneficiario della banca attraverso un altro mezzo. Non fidarsi di e-mail non crittografate e non firmate, soprattutto per i casi d'uso sensibili come questo.
- Verificare come funzionano i moduli di contatto, registrazione, abbonamento e feedback sul proprio sito web e aggiungere regole di verifica, se necessario, in modo che non possano essere presi di mira dagli aggressori.

Riferimenti bibliografici

1. «What Is Phishing?». Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. «Phishing Activity Trends Report Q1». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. «2018 Phishing Trends & Intelligence Report» 2018. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. «Microsoft remains phishers' #1 target for the fifth straight quarter» 22 agosto 2019. Vade Secure.
https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. «Threat Spotlight: Coronavirus-Related Phishing». 26 marzo 2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6. «Coronavirus phishing emails: How to protect against COVID-19 scams» 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. «Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer». 2020. IBM.
https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. «Abnormal Attack Stories #6: Coronavirus Credential Theft» 13 marzo 2020.
https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. «FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic». 20 marzo 2020. FBI.
https://www.ic3.gov/media/2020/200320.aspx

10. «Beware of criminals pretending to be WHO». 2020. OMS. https://www.who.int/about/communications/cyber-security

11. «Global police agencies issue alerts on Covid-related cyber-crime». 6 aprile 2020. SC Magazine.
https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. «Catching the virus cybercrime, disinformation and the COVID-19 pandemic». 3 aprile 2020. EUROPOL.
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. «New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks». 25 giugno 2019. FireEye.
https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. «HTTPS Protocol Now Used in 58% of Phishing Websites». 24 giugno 2019. Trend Micro.
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. Let's Encrypt. https://letsencrypt.org/

16. «2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike». 23 gennaio 2020. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. «Human factor report». 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. «Phishing Activity Trends Report Q3». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. «Business Email Compromise Results in $26B in Losses Over the Last Three Years». 12 settembre 2019. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. «Business Email Compromise The $26 Billion Scam» 10 settembre 2019. FBI. https://www.ic3.gov/media/2019/190910.aspx

21. «Evasive Phishing Driven by Phishing-as-a-Service». 1° luglio 2019. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. «Phishing made easy: Time to rethink your prevention strategy?». 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. «Q3 2019: Email Fraud and Identity Deception Trends». 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. «FBI: BEC Losses Soared to $1.8 Billion in 2019». 12 febbraio 2020. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. «Email: Click with Caution». Giugno 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. «Experts report a rampant growth in the number of malicious, lookalike domains». 18 novembre 2019. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. «Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more». 7 novembre 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. «Human Factor Report.» 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. «2019 Phishing and fraud report» 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. «Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019» 8 maggio 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. «Spam and phishing in Q3 2019». 26 novembre 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. «Phishing Activity Trends Report». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. «Toyota Subsidiary Loses $37 Million Due to BEC Scam» 20 settembre 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. «Domain-based Message Authentication, Reporting & Conformance». DMARC. https://dmarc.org/

Riferimenti

36. «DomainKeys Identified Mail (DKIM)». DKIM. http://www.dkim.org/

37. «Cyber incident». 22 luglio 2019. Lancaster University. https://www.lancaster.ac.uk/news/phishing-attack

38. «Hackers publish login credentials of 2500 Discord users» 22 luglio 2019. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. «Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People» 24 aprile 2019. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. «Phishing Attack Exposes 600k Health Records» 19 giugno 2019. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. «326,000 Patients Impacted in UConn Health Phishing Attack». 25 febbraio 2019. Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

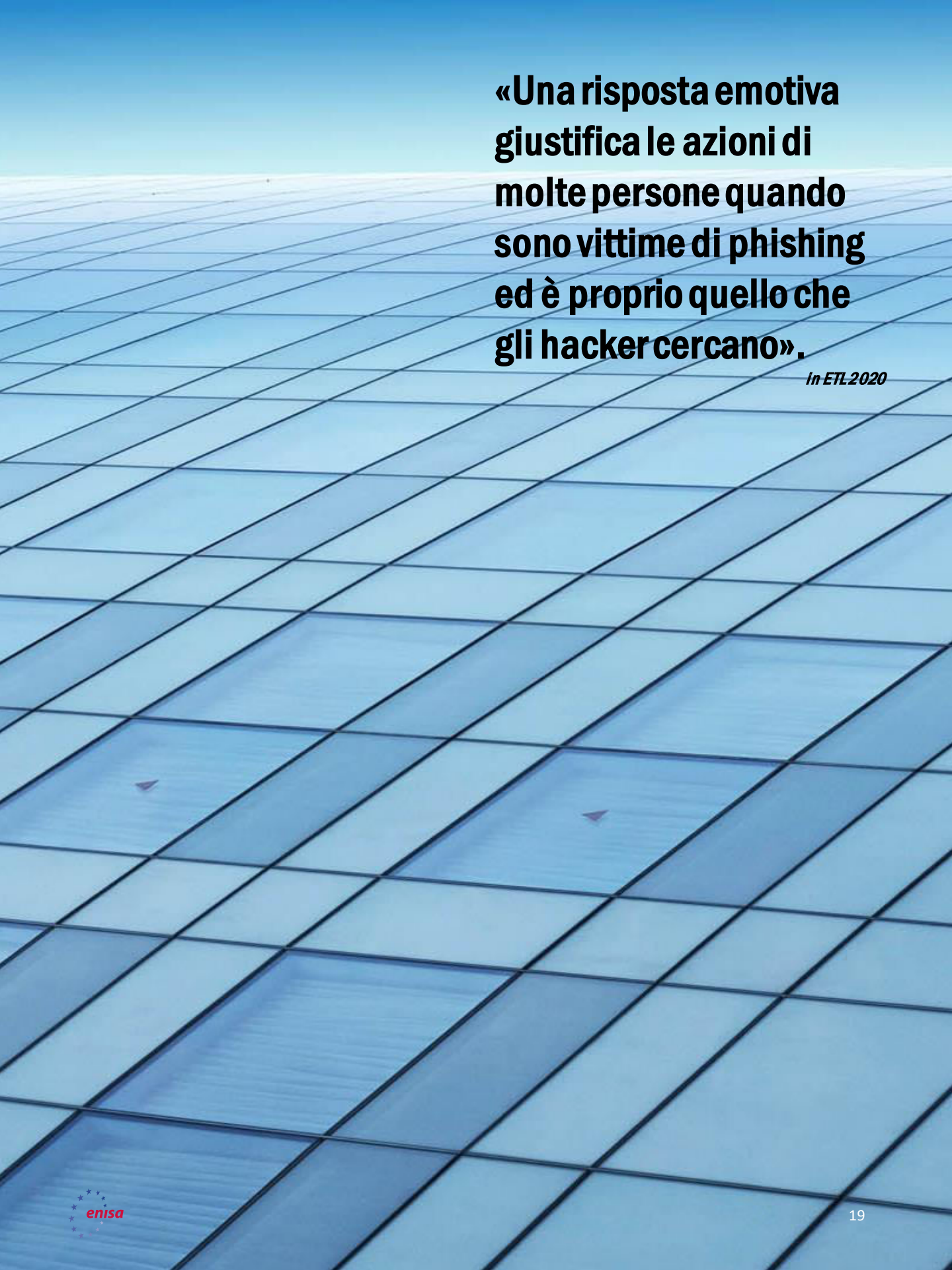
42. «Cybercrime Tactics and Techniques: the 2019 state of healthcare». 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. «Significant Cyber Incidents». 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. «More Than 99% of Cyberattacks Need Victims' Help». 9 settembre 2019. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

45. «office-365-phishing-attacks-deconstructed» https://dropsuite.com/office-365-phishing-attacks-deconstructed/

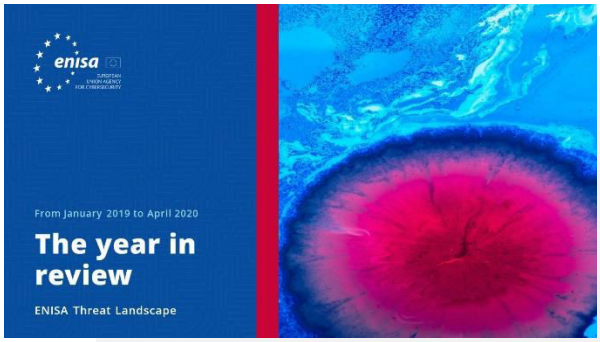
46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19



«Una risposta emotiva giustifica le azioni di molte persone quando sono vittime di phishing ed è proprio quello che gli hacker cercano».

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

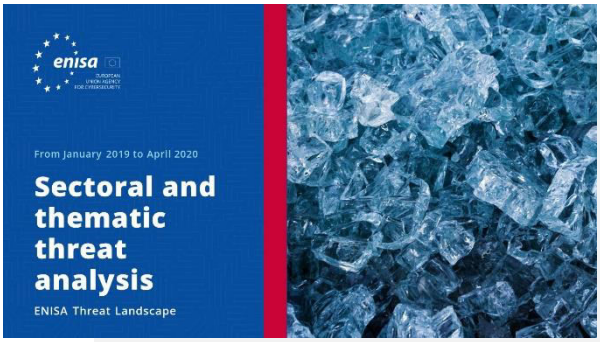
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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