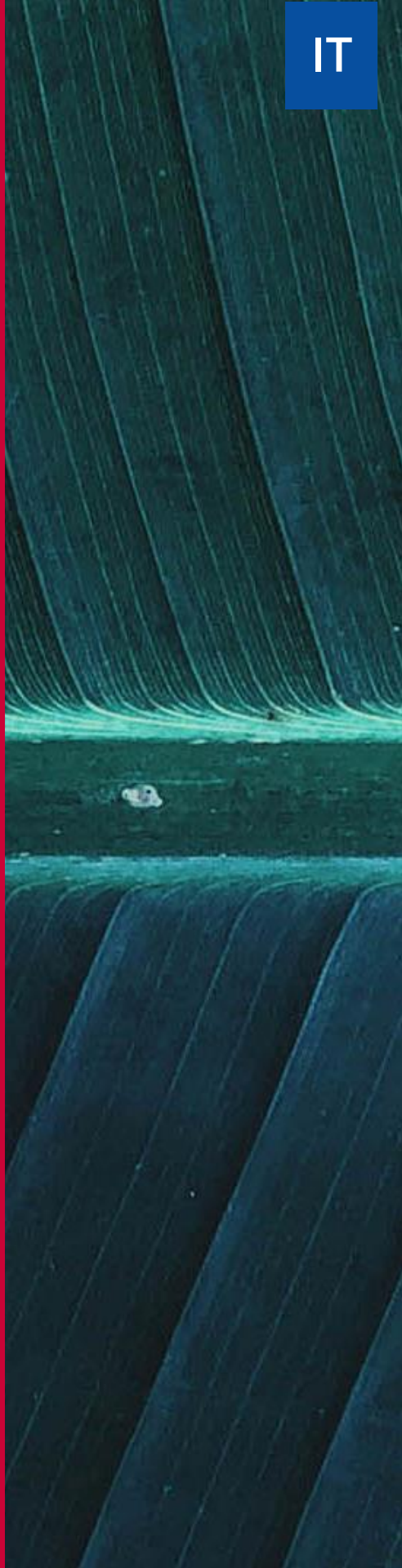
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT



Da gennaio 2019 ad aprile 2020

Spam

Panorama delle minacce analizzato dall'ENISA

Quadro generale

Il primo messaggio di spam è stato inviato nel 1978 da un responsabile del marketing a 393 persone tramite ARPANET. Si trattava di una campagna pubblicitaria per un nuovo prodotto della società per cui lavorava, la Digital Equipment Corporation. Per quei primi 393 destinatari lo spam è stato fastidioso come lo sarebbe oggi, a dispetto della novità dell'idea.[1] Ricevere spam è una seccatura, ma può anche creare per un attore malintenzionato l'opportunità di rubare informazioni personali o installare malware.[2] Lo spam consiste nell'invio di messaggi non richiesti in massa. Costituisce una minaccia per la cibersicurezza quando viene utilizzato come vettore di attacco per distribuire o attivare altre minacce.

Un altro aspetto da sottolineare è il modo in cui lo spam può talvolta essere confuso o erroneamente classificato come campagna di phishing. La differenza principale tra i due è il fatto che il phishing è un'azione mirata, che si avvale di tattiche di ingegneria sociale e ha come obiettivo il furto dei dati degli utenti. Lo spam è invece una tattica per inviare e-mail non richieste in massa a un elenco di destinatari. Le campagne di phishing possono utilizzare le tattiche di spam per distribuire messaggi, mentre lo spam può collegare l'utente a un sito web compromesso per l'installazione di malware e il furto di dati personali.

Nel corso di questi 41 anni le campagne di spam hanno approfittato di molti eventi sociali e sportivi di risonanza mondiale, come la finale della UEFA Europa League, gli US Open, tra gli altri. In ogni caso, nulla in confronto all'attività di spam osservata quest'anno con la pandemia di COVID-19.[8]

Risultati

L'85%_ **di tutte le e-mail scambiate nell'aprile 2019 era costituito da spam, il livello più alto in 15 mesi**[1]

14_ **milioni di e-mail di spam legate a ricatti sessuali sono state rilevate nel 2019**[23]

Il 58,3%_ **degli account di posta elettronica nell'industria mineraria è stato oggetto di spam**[17]

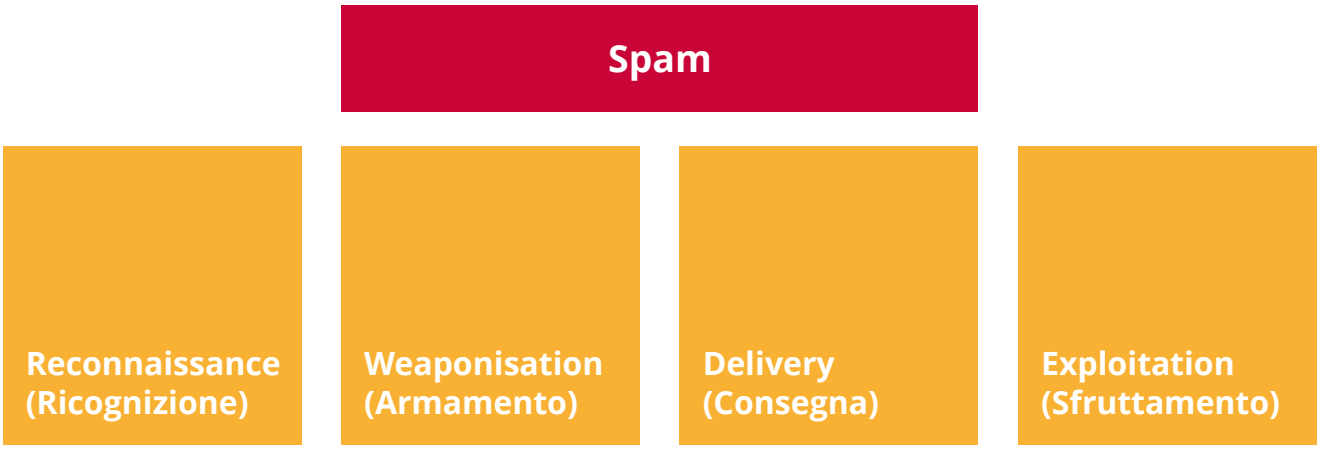
Il 10%_ **dello spam complessivamente rilevato ha preso di mira account di posta elettronica tedeschi**[2,3]

Il 13%_ **delle violazioni dei dati è stato causato da spam malevolo**[16]

L'83%_ **delle aziende non era protetto da attacchi con impersonificazione del marchio via e-mail**[20]

Il 42%_ **dei direttori della sicurezza delle informazioni (CISO) si è occupato di almeno un incidente di sicurezza causato da spam**[1]

Kill chain



Fase del flusso di lavoro dell'attacco

Ampiezza dello scopo

Installazione

Command & Control (Comando e controllo)

Actions on Objectives (Azioni sugli obiettivi)

Il modello Cyber Kill Chain® è stato sviluppato da Lockheed Martin, che lo ha adattato da un concetto militare legato alla struttura di un attacco. Per studiare un particolare vettore di attacco, si può utilizzare questo modello per mappare ogni fase del processo e fare riferimento agli strumenti, alle tecniche e alle procedure impiegate dall'aggressore.

MAGGIORI INFORMAZIONI

Descrizione

_Vecchia minaccia, nuovi bersagli

A distanza di 41 anni lo spam rimane un'importante minaccia per la sicurezza, nonostante tutte le altre molto più efficaci. Tuttavia, ancora una volta nel periodo in esame, nelle campagne di spam hanno fatto la loro comparsa nuovi gruppi target, nuovi mezzi e nuovi profitti. Nell'agosto del 2019, ad esempio, e-mail di spam hanno preso di mira più account, invitando i proprietari a condividere non solo una scansione del loro documento di identità ma anche un selfie, in modo da «vincere» uno smartphone. In un'altra campagna di spam, agli utenti è stato chiesto di inviare una foto personale. Il gruppo preso di mira dagli autori dello spam è stato poi ampliato per includere l'indirizzo e-mail utilizzato dall'utente, per attivare servizi di televisione o trasmissione in diretta a pagamento. I messaggi di spam inviati agli account indicavano false scadenze o richieste di rinnovo della licenza. Agli utenti veniva chiesto di rispondere e di inserire i dati del proprio conto bancario e le informazioni personali per il rinnovo della registrazione.[2]

_Spam al servizio di malware, ransomware e trojan di accesso remoto

Nell'agosto 2019 e-mail di spam contenenti file di immagine disco ISO malevoli sono state utilizzate per diffondere il malware LokiBot e per installare il trojan di accesso remoto (Remote Access Trojan, RAT) FlawedAmmyyy. Lo spam è servito anche per diffondere il trojan TrickBot, il trojan-spy Negasteal (noto anche come Agent Tesla), il RAT Ave Maria (noto anche come Warzone) e il famigerato, dal 2018, macro malware Pawload. Anche diverse famiglie di ransomware sono state diffuse da messaggi di spam, tra queste Dharma, Crysis e Ryuk, tutte segnalate come molto attive nell'anno in esame.[15,21]

Spam SMS

Quest'anno è stata condotta un'operazione di spam via SMS con conseguente divulgazione dei dati personali di oltre 80 milioni di utenti. Moltissimi numeri di telefono hanno ricevuto messaggi contenenti frasi come «soldi gratis» o «è vero» e link a siti fasulli. Da quel momento in poi, chiunque avesse seguito il link sarebbe stato invitato a iscriversi, fornendo informazioni sensibili. È stato dimostrato che il database utilizzato dagli autori dello spam era di proprietà della società ApexSMS, la cui legittimità è ancora sconosciuta. Sebbene ricercatori della sicurezza abbiano avuto accesso al database e cercato di recuperare il maggior numero di informazioni possibili, temendo che l'operazione si interrompesse inaspettatamente, non si sa ancora chi e per quale motivo possa avere accesso ai dati ancora disponibili e utilizzarli.[4]

L'espediente dei moduli

Gli autori dello spam hanno manipolato i moduli di feedback sui siti web di grandi aziende, utilizzati per porre domande, esprimere desideri o abbonarsi alle newsletter. Tuttavia, nell'anno in esame, anziché prendere di mira le caselle di posta collegate dell'azienda, gli autori dello spam hanno sfruttato i bassi livelli di sicurezza dei siti web, aggirato eventuali test reCAPTCHA e registrato diversi account con dati e-mail validi. Le vittime ricevevano così una risposta legittima dall'azienda, contenente il messaggio dello spammer.[2] In questo modo sono stati manipolati anche i Moduli Google per recuperare i dati degli utenti e inviare spam commerciale. Un caso più aggressivo è stato l'attacco di spam diretto agli account aziendali, con richiesta di trasferimento di denaro all'aggressore. Per convincere la vittima, gli spammer hanno affermato di poter inviare messaggi abusivi dalla posta elettronica della vittima a più di 9 milioni di indirizzi e-mail, determinando così l'inserimento dell'indirizzo dell'azienda nella blacklist.[3]

Descrizione

Chameleon spam

Diverse campagne nel 2019 hanno fatto ricorso allo stesso sistema delle botnet per distribuire messaggi di spam, anche se hanno utilizzato intestazioni e modelli casuali per la formattazione del contenuto. Per questo motivo, i ricercatori della sicurezza hanno iniziato a studiare tali campagne come un unico gruppo, denominato «Chameleon spam».[5]

I messaggi di Chameleon spam provenivano da vari paesi e contenevano falsi link a falsi annunci o offerte di lavoro, siti di prenotazione di biglietti aerei, offerte speciali sull'acquisto di prodotti o semplicemente servizi noti. I messaggi di spam utilizzavano un modello simile a quello validamente utilizzato da aziende come Google, Qatar Airways, FedEx, LinkedIn o Microsoft, in modo che il destinatario non notasse la differenza.[2]

Le solide vecchie bot

Nell'ottobre 2019 sono state ampiamente distribuite e-mail che utilizzavano modelli in inglese, tedesco, italiano e polacco aventi come oggetto comune «Payment Remittance Advice». A questi messaggi era allegato un documento contenente una macro, con invito ai destinatari di attivarla all'apertura del documento. Una volta attivata, la macro poteva avviare il processo di infezione tentando di scaricare il trojan Emotet.[13]

La botnet di spam Necurs è stata molto attiva in questo periodo, dopo una prolungata scarsa attività. Nel 2019 la botnet Gamut è risultata la terza botnet di spam più attiva. I messaggi Gamut sono per lo più legati a proposte di incontri personali, offerte di prodotti farmaceutici e opportunità di lavoro.[1]

_Numero di C2 di botnet associati a famiglie di malware

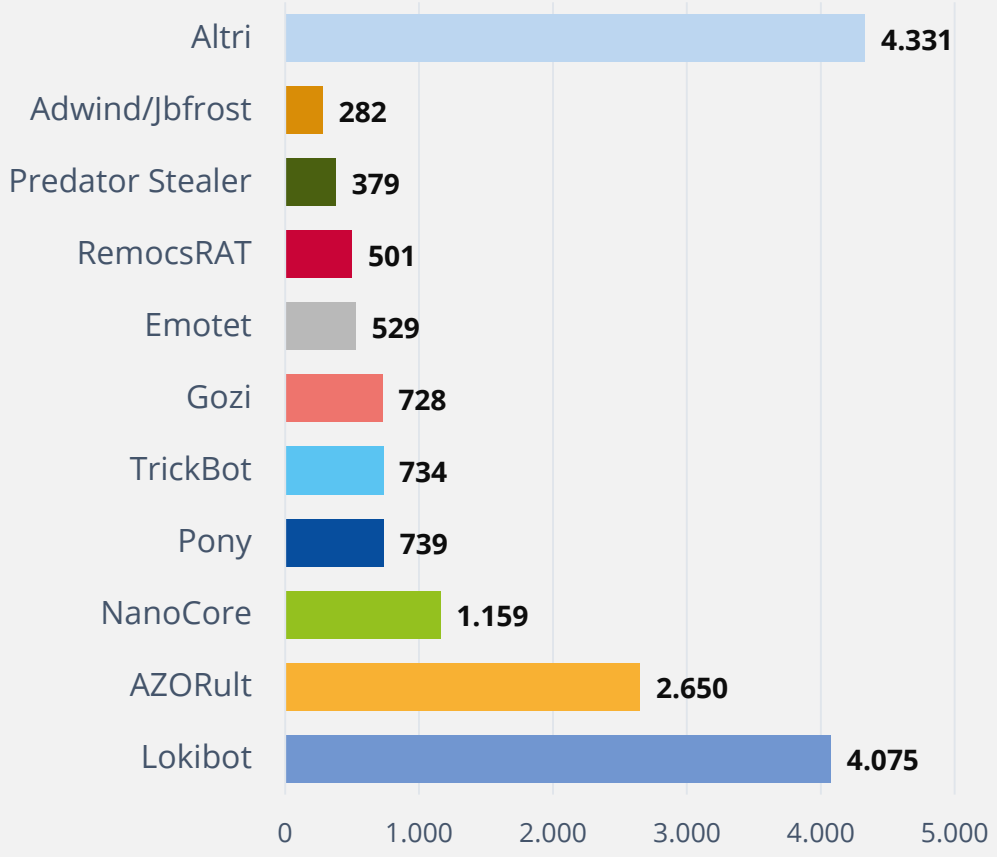


Figura 1 - Fonte: Spamhaus [14]

Descrizione

La COVID-19 ha aperto nuove porte

Poco dopo lo scoppio dell'epidemia di COVID-19 sono comparsi siti web di phishing e file malevoli veicolati via e-mail, che utilizzavano i termini coronavirus o COVID-19. Secondo quanto riferito, una campagna di spam legata alla COVID-19 avrebbe diffuso il file Eeskiri-COVID.chm19, un file keylogger camuffato. Il nome del file può far pensare che la campagna abbia avuto origine in Estonia (eeskiri significa «regola» in estone).[11] A metà febbraio 2020 si registravano solo poche centinaia di attacchi COVID-19 al giorno, ma a marzo 2020 il numero è salito più di 2 500 attacchi al giorno, lasciando prevedere un anno difficile in termini di spam.[12]

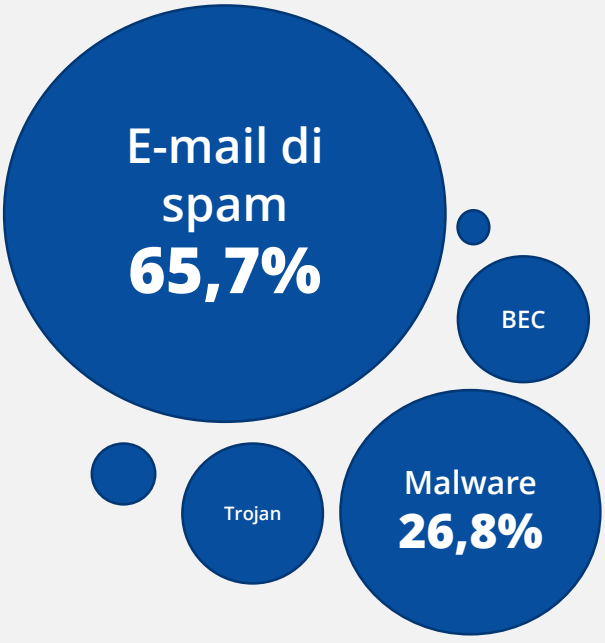


Figura 2. Minacce che sfruttano la COVID-19. Fonte: Trend Micro[11]

_ Esempi

01_ L'operazione di spam di ApexSMS

ApexSMS, una società di marketing SMS, ha subito una violazione dei dati con divulgazione dei dati di contatto di oltre 80 milioni di persone.

02_ La campagna di Chameleon spam

Una persistente campagna di spam di elevato volume è scaturita da un sistema di botnet che inviava messaggi con intestazioni randomizzate e cambiando spesso il modello.

03_ Campagna di distribuzione di spam a supporto di Emotet

Campagna di spam a supporto della distribuzione del malware Emotet.

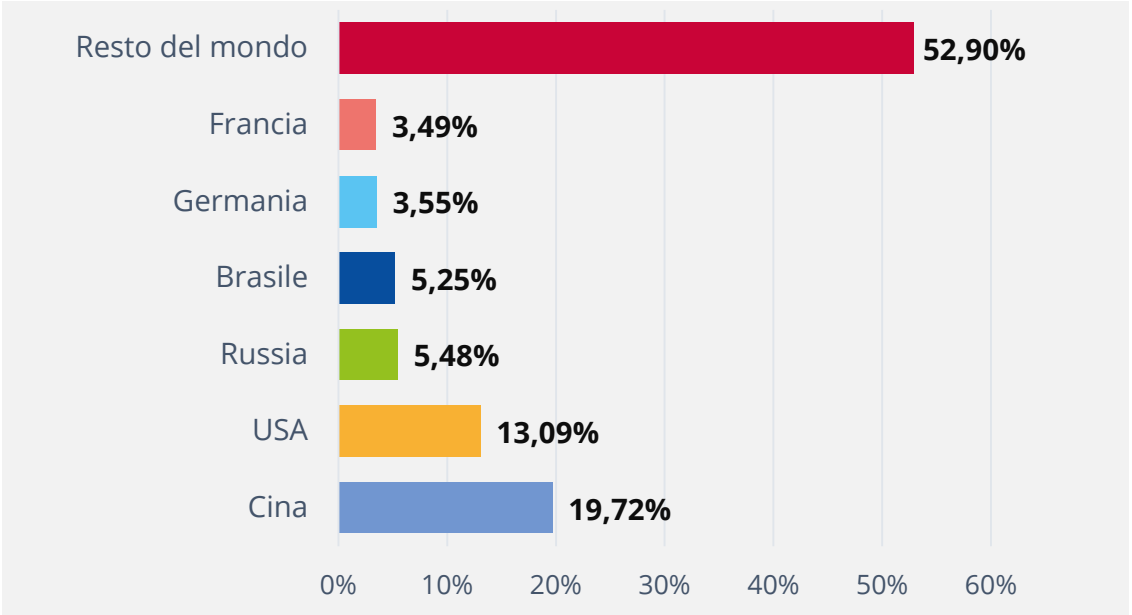
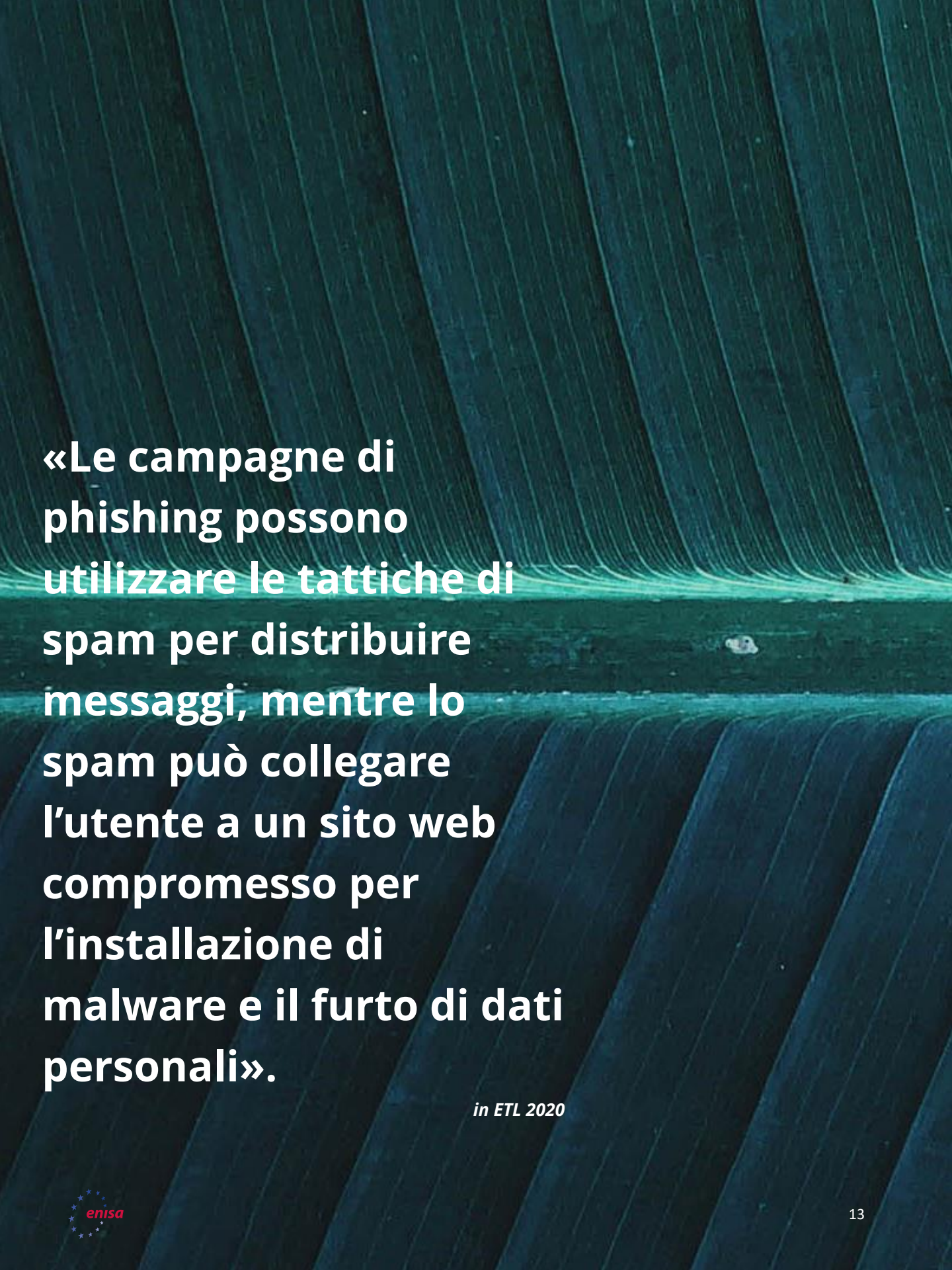


Figura 3. Fonti più comuni di spam Fonti diverse[17]

Mitigazione

Azioni proposte

- Attuare il filtraggio dei contenuti per individuare allegati non richiesti, messaggi e-mail con contenuti malevoli, spam e traffico di rete indesiderato.
- Aggiornare regolarmente l'hardware, il firmware, il sistema operativo e tutti i driver o software.
- Utilizzare l'autenticazione a più fattori per accedere agli account di posta elettronica.
- Evitare trasferimenti di denaro su conti bancari non verificati.
- Evitare di accedere a nuovi link ricevuti in messaggi e-mail o SMS.
- Elaborare procedure operative e politiche standard per la gestione dei dati sensibili.
- Utilizzare gateway e-mail sicuro, se possibile con manutenzione regolare e automatizzata dei filtri (anti-spam, anti-malware, filtraggio basato su policy).
- Disabilitare l'esecuzione automatica del codice, l'attivazione delle macro e il precaricamento di grafica e link inviati per posta.
- Adottare tecniche di sicurezza come SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting & Conformance) e DKIM (Domain Keys Identified Mail).
- Aggiornare regolarmente le whitelist, i filtri basati sulla reputazione e la RBS (Real-time Blackhole List).
- Utilizzare l'IA e l'apprendimento automatico per i controlli di rilevamento delle anomalie.



«Le campagne di phishing possono utilizzare le tattiche di spam per distribuire messaggi, mentre lo spam può collegare l'utente a un sito web compromesso per l'installazione di malware e il furto di dati personali».

in ETL 2020

Riferimenti bibliografici

1. «Email: Click with Caution - How to protect against phishing, fraud, and other scams» giugno 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

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

3. «Spam and phishing in Q2 2019» 28 agosto 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. «SMS Spammers Doxxed» 9 maggio 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. «Tracking the Chameleon Spam Campaign» 25 settembre 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. «5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned» 7 giugno 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. «The world worst spammers». 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. «Naming the coronavirus disease (COVID-19) and the virus that causes it». 2020. OMS. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. «WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus» 6 febbraio 2020. OMS. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. «COVID-19 situation update worldwide, as of 11 June 2020» 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. «Developing Story: COVID-19 Used in Malicious Campaigns» 24 aprile 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. «2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape» 6 aprile 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. «Emotet is back: botnet springs back to life with new spam campaign» 16 settembre 2019. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. «Spamhaus Botnet Threat Report 2019» 28 gennaio 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. «Evasive Threats, Pervasive Effects» 27 agosto 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

16. «Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study» 28 febbraio 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. «Internet Security Threat Report» Volume 24, febbraio 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. «Spam and phishing in Q1 2019» 5 maggio 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. «Total Global Email & Spam Volume for May 2020» maggio 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

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

21. «The World's Most Abused TLDs» Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. «Trend Micro Cloud App Security Report 2019» 10 marzo 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. «The Sprawling Reach of Complex Threats». 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. «SONIC WALL Security Center Metrics». SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

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

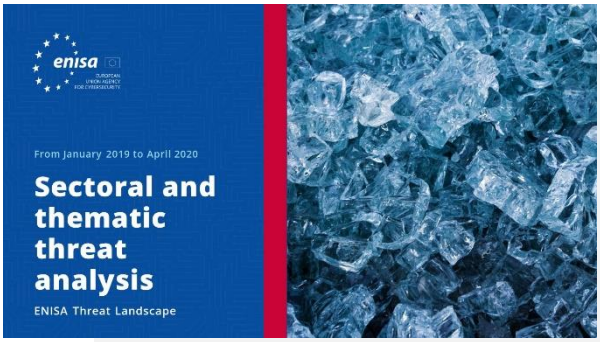
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

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



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.

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

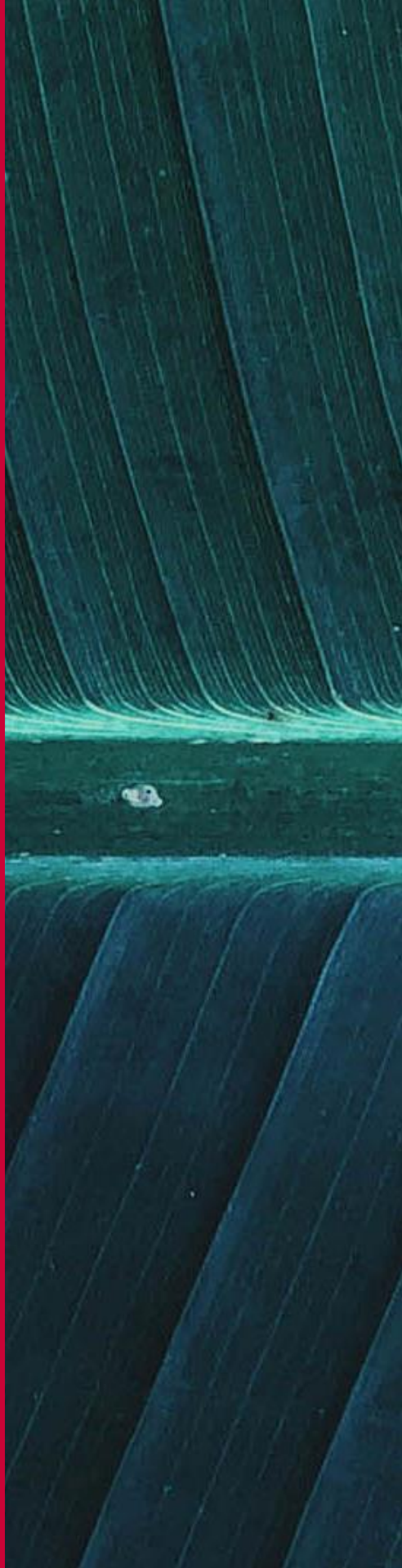
Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. 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