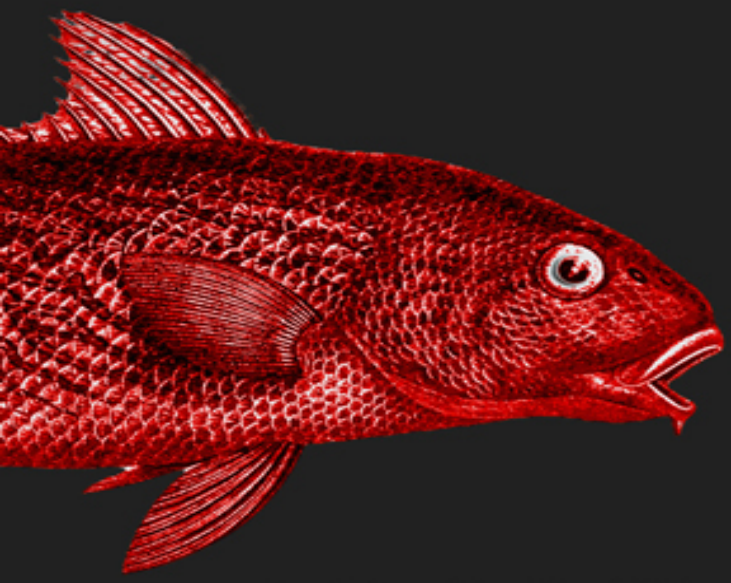


EMAIL, PHISHING & CYBERSECURITY

GUIDA COMPLETA ALLA SICUREZZA INFORMATICA SPIEGATA DA UN HACKER

MARCO FABBRI
ETHICAL HACKER MASTER

Codice ISBN: 9798308332121

Le informazioni presenti in questo libro sono fornite "così come sono", senza alcuna garanzia esplicita o implicita. L'autore ha curato con la massima attenzione la redazione dell'opera, ma non si assume alcuna responsabilità per eventuali errori, omissioni o danni (diretti, indiretti, incidentali o consequenziali) derivanti dall'uso delle informazioni, degli esempi o dei programmi in esso contenuti. La presenza di eventuali istruzioni o suggerimenti tecnici non sostituisce la competenza di professionisti o la consulenza di figure specializzate. Chi utilizza le informazioni, i programmi e gli esempi illustrati in questo libro, lo fa a proprio rischio e pericolo, assumendosi la piena responsabilità di ogni conseguenza. Qualsiasi uso non autorizzato dei siti o strumenti indicati in questo libro costituisce una grave violazione delle normative in materia di sicurezza informatica e può comportare sanzioni penali e civili. L'autore declina ogni responsabilità per eventuali abusi, usi impropri o attività illegali compiuti da terzi sulla base delle informazioni contenute in questo libro. Il lettore è responsabile di assicurarsi che ogni azione intrapresa sia conforme alle leggi applicabili e agli standard etici.

Attenzione: Il fatto di ospitare riferimenti, immagini o nomi tutelati da copyright non implica alcun endorsement o relazione commerciale con i legittimi proprietari, né vi è volontà di appropriazione dei suddetti contenuti. Se, inavvertitamente, fosse stata inserita qualche immagine o materiale protetto da diritti esclusivi, l'autore è disponibile a rimuoverlo o rettificarlo su semplice richiesta degli aventi diritto.

EMAIL, PHISHING E CYBERSECURITY

Guida completa alla sicurezza informatica spiegata da un hacker

* * *

MARCO FABBRI

Ai miei colleghi e seconda famiglia:
Alessandro, Alessio, Marco, Michele e Mosè.

Prefazione

1	Introduzione	5
2	A chi è rivolto	7
3	La differenza tra spam e phishing	9
4	Perché è importante saper difendersi	11
5	La psicologia dietro al phishing	15
6	La nascita delle email	21
7	Dietro le quinte	23
8	L’header	29
9	Body e allegati	35
10	Invia/ricevi	39
11	Tipologie di phishing	45
12	Tipologie di allegati malware	53
13	Come leggere l’header	61
14	MXToolbox e MailHeader	69

15	Riconoscere il phishing dagli indirizzi email	77
16	Riconoscere il phishing dal testo	85
17	Riconoscere il phishing dai link	91
18	URL shortener e QR code	97
19	Virustotal, MITRE ATT&CK e altri strumenti di difesa	101
20	Smishing e vishing	111
21	Phishing tramite browser	119
22	Come funziona un filtro antispam	123
23	Blacklist e whitelist	131
24	Come l'AI sta cambiando il phishing	135
25	Social engineering tra scam, profiling e OSINT	141
26	Haveibeenpwned	147
27	MFA e passkey	149
28	Chiavette USB	153
29	Le conseguenze del phishing: ransomware, sextortion e double extortion	157
30	SPF, DKIM e DMARC	163
31	Quanto è complesso organizzare un attacco	171
32	Le 10 domande più frequenti sul phishing	173
	Fonti	177
	L'autore	181

PREFAZIONE

Chiudete gli occhi e immaginate un lago di montagna, l'acqua che rispecchia il verde dei boschi e i monti tutt'attorno. Il lago è così chiaro e trasparente da riuscire a scorgere le trote nuotare. Prendete la vostra canna da pesca, montate l'esca sull'amo e lanciate, increspando la superficie cristallina. Dopo qualche secondo, un bellissimo pesce sta srotolando con decisione il vostro mulinello. Tranquillamente e con pazienza iniziate a riavvolgere, sicuri che la trota non si sgancerà; e anche se fosse, un'altra abboccherà dopo pochi secondi, magari sarà anche più grossa.

Ora prendete questa immagine e portatela nel mondo della cybersecurity e del phishing: nulla è cambiato, soltanto che voi siete il pesce, non il pescatore, e fuori dal lago ci sono, assieme al vostro cibo, milioni di esche che svolazzano, pronte a tirarvi su a riva e mangiarvi. Questo è il mondo del ransomware che, ancora oggi, ha come primo vettore di diffusione la mail. Questo è il mondo della truffa e del ricatto, dove se non sei preparato vieni mangiato, dove a volte conviene tenersi la fame. Purtroppo, per uno che si salva altri mille abboccano. E così assistiamo a fughe di dati, data leak di credenziali, furti digitali e milioni in denaro che escono ogni anno. Che ci fanno capire che nessuno è pronto. Che ci ricordano che nessuno è immune. E per quanto ci si provi a salvarsi, nonostante tutti i nostri sforzi, prima o poi sentiremo l'accenno di un amo acuminato e qualcosa accadrà.

Ecco che in quel momento, proprio in quel preciso momento, quando sentiremo la lenza tirare, riusciremo a salvarci con un colpo di coda e tornare in acque tranquille.

Ecco il perché, di un libro sul phishing.

Buona lettura.

Alessandro Vannini

1 INTRODUZIONE

Tutti riceviamo email di phishing. Dagli avvisi di presunto blocco della carta di credito o account online alle promesse di improbabili vincite di prodotti all'ultimo grido. Sono email false. Più il vostro indirizzo è presente su Internet, attraverso registrazioni a portali web o comunicazioni via email, più diventa un possibile bersaglio di liste utilizzate nell'invio massivo di campagne di spam o di phishing. Non è questione di "se" lo riceverete, ma di "quando". Saper riconoscere questi tentativi di frode ed evitare di diventarne vittime diventa quindi fondamentale per chiunque navighi sul web, indipendentemente dal livello di conoscenza della materia, dove persino una semplice ricerca su Google può esporci a tali minacce (come vedremo più avanti in un capitolo dedicato). Questo testo, frutto della mia esperienza diretta sul campo come esperto di cybersecurity ed ethical hacker master, si propone come una guida completa ed esaustiva del fenomeno dal punto di vista di chi difende, analizzando casi reali nelle loro diverse varianti che possono raggiungere le vostre caselle, smartphone o chat istantanee. Partendo dalla teoria del funzionamento delle email e dalla loro creazione, per arrivare alla pratica attiva di riconoscimento del phishing in tutti i suoi dettagli, esploreremo come gli strumenti gratuiti online a nostra disposizione possano aiutarci a riconoscerlo efficacemente, non soltanto analizzando header e body, ma anche il contenuto stesso del messaggio. Un capitolo è dedicato all'approfondimento dello studio psicologico che si cela dietro al phishing, argomento apparentemente poco citato nei testi e nelle fonti legate all'informatica applicata all'uomo, ma estremamente interessante. A lettura conclusa, la mia speranza è che vi ritroverete con un bagaglio di esperienza tale da rendervi attori preparati e consapevoli del mondo digitale e delle sue minacce. Un libro senza fronzoli che contiene solo ciò

che è realmente utile sapere, per affrontare il phishing in modo attivo e consapevole. Così, quando riceverete la prossima email malevola, la riconoscerete e segnalerete senza esitazione.

Nota importante:

Le informazioni, gli strumenti e gli esempi contenuti in questo libro sono forniti esclusivamente a scopo educativo e informativo, con l'obiettivo di aumentare la consapevolezza sulle minacce informatiche e fornire nozioni e strumenti di difesa efficaci. È tuttavia fondamentale sottolineare che qualsiasi uso improprio o non autorizzato degli strumenti e delle tecniche descritte costituisce una grave violazione delle normative vigenti, comportando possibili sanzioni penali e civili. Tutti i metodi analizzati in queste pagine devono essere utilizzati nel pieno rispetto delle leggi applicabili e solo con l'esplicita autorizzazione dei soggetti coinvolti. Questo libro non fornisce alcuna garanzia sul vostro utilizzo dei contenuti: ogni azione intrapresa rimane sotto la vostra esclusiva responsabilità. Siate etici e agite nel rispetto delle normative, sempre.

2 A CHI È RIVOLTO

Questo libro è rivolto a tutti gli utenti del mondo digitale: dai principianti che si avvicinano per la prima volta all'utilizzo della posta elettronica, fino agli esperti che desiderano approfondire l'argomento per migliorare la postura di sicurezza della propria azienda. Il testo contiene materiale utile anche per i professionisti IT di primo e secondo livello. I contenuti sono strutturati in piccoli capitoli essenziali e senza inutili riempitivi, in cui gli argomenti vengono affrontati in modo graduale e accessibile, con l'obiettivo di rendervi preparati e sicuri nell'affrontare queste minacce al termine della lettura.

Se siete quindi alle prime armi con la posta elettronica, questo libro è perfetto per voi. Vi fornirà le conoscenze basilari e gli strumenti essenziali per comprendere il funzionamento delle email e proteggere i vostri dati e account. Ogni argomento è presentato con un linguaggio chiaro e diretto, evitando tecnicismi superflui. Solo l'essenziale, niente di più.

Se siete esperti del settore, troverete indicazioni preziose e spesso date per scontate, che miglioreranno le vostre policy di sicurezza. Una lettura scorrevole e piacevole, ma ricca di contenuti di valore per chi combatte quotidianamente il phishing con il proprio team IT aziendale.

Se cercate un libro sulla sicurezza informatica applicata al lato blu dell'argomento, ovvero da chi ogni giorno deve difendersi da queste minacce, o se volete intraprendere un percorso nella cybersecurity, questa è una lettura giusta, se invece cercate un romanzo o un libro di hacking, questo testo non fa per voi, ma grazie ugualmente di aver dato a queste pagine un'occasione.

I capitoli possono essere letti sia in sequenza come sono presentati, sia in modo indipendente, dato che ogni argomento è autonomo e completo in sé stesso.

3 LA DIFFERENZA TRA SPAM E PHISHING

Prima di affrontare il tema nel dettaglio, è fondamentale comprendere la differenza tra spam e phishing, due termini spesso confusi e utilizzati erroneamente come sinonimi.

Lo spam consiste in messaggi non richiesti e indesiderati, inviati attraverso vari mezzi di comunicazione come email, chat o social network, con scopi principalmente promozionali o commerciali. L'obiettivo primario dello spam è pubblicizzare un prodotto o un servizio con una modalità non richiesta da parte del destinatario. Di per sé, questo tipo di messaggio raramente risulta dannoso.

Il phishing, invece, è una forma di comunicazione fraudolenta progettata per sembrare legittima, ma il cui vero scopo è ingannare l'utente finale, inducendolo a fornire informazioni sensibili come credenziali di accesso, dati bancari o personali.

È questa la differenza fondamentale: lo spam si trasforma in phishing quando contiene link dannosi o mira a rubare dati personali. Quando ci si è imbattuti per la prima volta nella storia nelle due tipologie di comunicazione? La prima email di spam risale al 1978, dove un messaggio pubblicitario fu inviato a circa un centinaio di computer collegati alla rete ARPANET, una rete di computer del Dipartimento della Difesa degli Stati Uniti d'America e precursore dell'Internet moderno, per promuovere un vendor di hardware locale, come mostrato in Figura 1 la cui fonte è riportata nel capitolo dedicato "Fonti" alla fine del libro [1]. Per quanto riguarda il phishing, invece, la prima segnalazione è attestata intorno al 1995, quando un gruppo di hacker si spacciò per dipendenti di AOL (America Online, una delle prime aziende di servizi internet in

America) nel tentativo di sottrarre credenziali e relativi account, riuscendo nel loro intento.

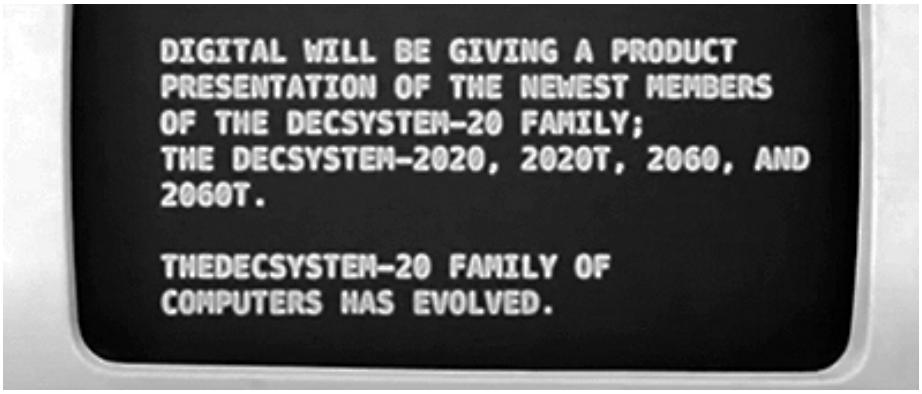


Figura 1 - Prima comunicazione di spam

Voglio subito tranquillizzare il lettore, questo libro non si soffermerà sull'evoluzione storica del phishing, ma si concentrerà invece sul panorama IT attuale. Per gli approfondimenti storici, vi invito a consultare testi e articoli autorevoli e specifici sull'argomento. È importante sottolineare infine che, ai giorni nostri, lo spam è regolamentato da normative specifiche, come il GDPR nell'Unione Europea e il CAN-SPAM Act negli Stati Uniti, ed è possibile cancellare l'iscrizione alle liste di spam, pubblicità e marketing per mezzo dei link sempre disponibili per legge, generalmente presenti al termine della mail, etichettati come "Disiscriviti" o "Unsubscribe". Verificatene sempre, prima cliccare, la destinazione finale.

4 PERCHÉ È IMPORTANTE SAPERSI DIFENDERE

Il phishing è una delle forme più comuni di frode sia nella vita reale che in quella digitale. Consiste, come già accennato, in un tentativo fraudolento di far apparire una comunicazione come legittima, quando in realtà essa nasconde al suo interno minacce di vario tipo: dalle truffe vere e proprie al malware, dalle tecniche volte alla sottrazione di informazioni sensibili come credenziali o password, ai punti di accesso al sistema vulnerabili dei dispositivi in uso. Questa comunicazione può avvenire tramite molteplici canali come email, SMS, messaggi istantanei, telefonate e persino lettere cartacee recapitate direttamente nella buca delle lettere aziendale o privata. Per riassumere il fenomeno in poche parole, il phishing è una comunicazione malevola che tenta di apparire legittima per ingannare il destinatario. Ogni variante del phishing prende un nome specifico e solo comprendendole tutte possiamo adottare e adattare strategie efficaci per combatterlo. Tutte le forme di phishing condividono un obiettivo comune: generare un guadagno per il malintenzionato. Questo può essere di natura economica, attraverso il furto di denaro o l'estorsione, o di natura digitale, sfruttando un asset di valore sempre più centrale nella società moderna: i dati e le informazioni sensibili, che possono poi essere rivendute sul dark web al migliore offerente o sfruttate per ampliare la superficie di attacco e colpire i bersagli in maniera mirata ed efficace.

Il phishing si rivela particolarmente insidioso perché, molto spesso, riesce a replicare il layout grafico e lo stile espressivo dei marchi più noti o di uso quotidiano. Gli attaccanti accedono infatti alle relative comunicazioni

ufficiali e, combinando elementi autentici di email e post sui social network, creano un messaggio che richiama una comunicazione già elaborata dall'utente in passato. In questo modo sfruttano il cosiddetto "pensiero veloce", ovvero l'elaborazione automatica e superficiale delle informazioni da parte del cervello [2] poiché, appunto, la comunicazione risulta familiare. Il "pensiero lento" e più analitico, se si è disattenti o sotto pressione da multitasking, non viene inizialmente richiamato nella mente dell'utente, concedendo il fianco digitale ai malintenzionati.

Con l'avvento dell'intelligenza artificiale, gli scenari d'inganno si sono evoluti ulteriormente, innalzando il livello di minaccia e pericolosità del phishing. Si passa infatti dalle fake news, capaci di manipolare le opinioni degli utenti, alla creazione di alter ego digitali realistici, clonando le fattezze e il timbro vocale di una persona reale o creandone una addirittura da zero. Si prospetta che il livello d'inganno che si riuscirà a raggiungere nel 2030 sia estremamente più credibile di quello attuale. Secondo una statistica pubblicata da **securelist.com** a maggio 2024 e condotta da Kaspersky, che vi invito a visionare all'indirizzo in fonte [3], nel 2023 il phishing si è focalizzato principalmente su obiettivi finanziari evidenziando un'evoluzione mirata verso i settori economicamente più redditizi: questi includono i conti bancari, gli account di shopping online, i wallet di criptovalute e altri asset legati al mondo finanziario; se quindi circa un terzo degli attacchi totali ha preso di mira specificamente il settore finanziario, quasi la metà ha sfruttato come esca i marchi più popolari del commercio elettronico e dei sistemi di pagamento digitali. Nel campo delle criptovalute, gli attacchi di phishing hanno registrato una crescita del 16% anno su anno, alimentata dalla crescente adozione e popolarità di questi strumenti su larga scala della popolazione attiva. Parallelamente, il settore mobile ha subito un incremento del 32% degli attacchi riusciti, dove per riusciti si intende l'installazione effettiva di malware sui dispositivi.

Come vedete si tratta di un pericolo reale dal quale occorre saper difendersi. Questo libro, con i capitoli che seguiranno, sarà il vostro primo passo alla difesa attiva.

5 LA PSICOLOGIA DIETRO AL PHISHING

Il phishing sfrutta le debolezze umane attraverso tecniche di social engineering, facendo leva su emozioni e schemi mentali per manipolare le decisioni delle vittime. Una vulnerabilità chiave dell'essere umano è la tendenza a fidarsi del prossimo in situazioni percepite come urgenti o pericolose. Il successo del phishing risiede proprio nella sua capacità di indurre una risposta automatica e impulsiva, aggirando il ragionamento analitico. Questo avviene giocando su emozioni primarie quali paura, curiosità, empatia, familiarità e, soprattutto, urgenza. Oltre alle emozioni sono presi di mira anche i bias cognitivi, gli schemi di pensiero e scorciatoie mentali che il cervello utilizza per prendere scelte rapide, riuscendo così a mantenere un mix di velocità di decisione e risparmio energetico dello stesso.

Nel caso del phishing, tra i bias che possono portare a conclusioni errate o irrazionali troviamo:

- l'ancoraggio, ovvero fidarsi eccessivamente della prima informazione ricevuta, senza validarla;
- l'autorità, accettando la situazione senza mettere in discussione le figure autorevoli o gli enti riconosciuti;
- la familiarità, che ci porta a seguire comportamenti abituali senza riflettere davvero;
- la perdita, temendola maggiormente rispetto al suo relativo guadagno;

- l’unicità, che ci porta a ricercare continuamente il desiderio di sentirci speciali.

Proviamo ora a richiamare alcuni esempi che sicuramente avrete ricevuto almeno una volta nella vostra casella:

- “Abbiamo rilevato un addebito sospetto di 100€ sul tuo conto corrente, clicca qui per bloccarlo.”
- “Non è stata pagata una multa, segue IBAN nella email per procedere subito ed evitare ulteriori sanzioni.”
- “Nuovo ordine nel tuo account, segui il link e guarda ora.”
- “Il tuo account è stato bloccato, clicca qui per sbloccarlo.”
- “Sei stato scelto e hai vinto l’ultimo iPhone, clicca il banner per ricevere il tuo premio!”

Se almeno una di queste vi ha fatto sorridere e richiamato la vostra attenzione a una email processata in passato, sapete bene come queste siano minuziosamente create per sembrare autentiche. A rendere ancora più efficace il phishing contribuiscono anche le già citate tecniche di manipolazione. Tra queste spiccano la creazione di storie credibili e l’uso di un tono familiare tipico di un mittente conosciuto, che favoriscono l’illusione di autenticità delle narrazioni coerenti con il contesto della vittima che tenderà a fidarsi della richiesta ricevuta. Un messaggio di phishing che combina diversi elementi manipolativi, tenendo conto di questi fattori psicologici, ha una probabilità maggiore di convincere il destinatario ad agire senza sospetti ottenendo così un tasso di successo notevolmente elevato, che arriva fino all’81% [17]. I social media sono una vera miniera di informazioni personali utilizzabili per creare un contesto che ha una certa risonanza con la vittima designata. Dai luoghi visitati alle preferenze, dalla rete di contatti alle abitudini quotidiane, esistono strumenti specifici per raccogliere ed elaborare questi dati, permettendo di creare campagne di phishing sempre più personalizzate ed efficaci.

Alcuni esempi di contesti accettati senza sospetto possono essere:

- l’offerta di un vantaggio unico e irripetibile, ma della giusta dimensione da non sembrare assurdo;

- una comunicazione di avviso proveniente da una banca, un ente governativo o un’azienda conosciuta e già contattata in passato;

- il richiamo a situazioni o esperienze già vissute dalla vittima, siano esse positive o negative.

Il ventaglio di aspetti della vita sociale sfruttabili è estremamente vasto e comprende anche la reputazione personale o professionale, fino ad arrivare a minacce dirette come la sextortion. In tali circostanze, la percezione di una possibile perdita della propria posizione sociale o dell’immagine pubblica diventa un fattore psicologico estremamente potente e stressante, soprattutto nel contesto online dove il controllo della propria immagine è spesso fragile e facilmente manipolabile tra informazioni false o comportamenti tossici della community. In tutti questi casi viene richiamata direttamente nella vittima una risposta di tipo fight-or-flight [4] alla minaccia, che tradotto nella nostra lingua sarebbe “combatti o scappa”. Si tratta di un’eredità dell’istinto di sopravvivenza dei nostri avi per preparare il corpo a combattere o fuggire alle minacce fisiche reali. Nel mondo digitale un evento stressante si traduce in una minaccia esistenziale a livello psicologico ed elaborata similmente a una minaccia fisica, attivando il sistema nervoso simpatico e rilasciando nel corpo ormoni come adrenalina, noradrenalina e cortisolo. Si attiva così il pensiero veloce anziché quello lento e analitico, inducendo la vittima a cliccare prima ancora di pensare. Gli attacchi di phishing sfruttano proprio il nostro sistema di risposta allo stress per indurre errori impulsivi e digitalmente fatali.

Altri bias cognitivi frequentemente sfruttati dalle campagne malevole sono:

- la riprova sociale, se tutti nella società fanno una determinata azione allora deve essere giusto;

- la scarsità, quando il tempo a disposizione per ottenere qualcosa sta per scadere.

Infine non vanno dimenticate o sottovalutate le truffe di phishing che sfruttano le emozioni più profonde come i sentimenti romantici, la gelosia o la felicità, che eludono completamente il ragionamento critico e portano la vittima ad agire rapidamente. Quando tutto questo non funziona, i truffatori tentano di far cedere la vittima con il micro-commitment, ovvero la truffa a piccoli passi: non chiedono subito le credenziali o i dati della carta di credito, ma ci arrivano gradualmente; prima con un link apparentemente innocuo, poi con una conferma via mail e infine con la richiesta del dato sensibile. Questi micro-commitment puntano a mettervi a vostro agio, spingendovi a completare la procedura senza farvi accorgere della sua natura fraudolenta.

Ma come possiamo difenderci concretamente da questi attacchi, ora che abbiamo compreso la psicologia che li governa? Un'arma efficace è quella di imparare a riconoscere i segnali di stress digitale e prendersi un istante per rallentare, anche solo per pochi secondi. In questo modo, l'impulso veloce si attenua fino a sfumare, riattivando il pensiero analitico e consentendoci di valutare con lucidità e a mente fredda i link su cui ci invitano a cliccare o i moduli che siamo richiesti compilare. Riprendete fiato e verificate sempre le informazioni, consultate una persona fidata o un esperto del settore. Potete anche contattare direttamente l'ente citato nella comunicazione, cercando i recapiti sui siti ufficiali o sui motori di ricerca, e non utilizzando quelli forniti nel messaggio sospetto. Inoltre, e questo vi rasserenerà, l'utilizzo degli strumenti che vedremo nei prossimi capitoli può ridurre significativamente il rischio di diventarne vittima.

6 LA NASCITA DELLE EMAIL

La comunicazione digitale tra gli utenti fu ideata negli anni ‘60, ma si dovette attendere fino al 1971 per vedere la prima mail inviata tra dispositivi, ben prima dell’Internet che conosciamo oggi, da parte di Raymond Samuel Tomlinson sulla rete di computer dell’ARPANET, con un sistema di utilizzo non molto differente dai giorni nostri. E se oggi siamo abituati alle email sofisticate tra caratteri speciali, immagini, sfondi colorati e persino gif animate o video incorporati, agli albori erano composte solo da semplice testo ASCII su sfondo monocromatico. Niente immagini e niente personalizzazioni, soltanto una semplice ed essenziale comunicazione digitale. La vera evoluzione è arrivata poi nel 1992 con l’introduzione di nuovi standard e protocolli come il Multipurpose Internet Mail Extension o MIME, arricchendosi così di immagini, codice HTML e allegati, diventando non solo più gradevoli esteticamente ma anche più funzionali.

Un aneddoto interessante è poi la storia dietro la scelta del simbolo **@** introdotto da Raymond proprio nel 1971, che venne opzionato poiché era un carattere assente sia nei nomi utente che nei nomi macchina, e quindi perfetto come separatore. Il simbolo **@** venne così adottato per consentire l’invio di messaggi verso computer diversi dal localhost, creando un sistema di comunicazione simile a quello attuale basato sullo schema **username@host**, dove il nome utente precede la **@**, seguito dal nome della macchina. Solo dal 1979 questa comunicazione venne universalmente chiamata col nome di “email”, diminutivo della precedente definizione assegnata di “electronic mail message”.

it	il nome della cassetta postale
@	simbolo di separazione
cyberadmin.it	è il dominio di riferimento

Figura 2 - Formato di un indirizzo mail

Con l’avvento di Internet e l’introduzione dei DNS (Domain Name System), quindi con la possibilità di poter effettuare richieste di instradamento dei pacchetti sull’Internet verso domini i cui indirizzi IP pubblici non sono inizialmente conosciuti dal mittente, il formato delle email è evoluto nell’attuale standard **casella@dominio** come mostrato in Figura 2. Se inizialmente l’utilizzo delle mail era limitato agli addetti di settore e considerato uno strumento di nicchia, oggi è diventato il mezzo di comunicazione più diffuso, secondo solo alla messaggistica istantanea, grazie anche a servizi come Hotmail e Yahoo! Mail che alla fine degli anni ‘90 permettevano a chiunque di creare un indirizzo mail gratuito e utilizzarlo direttamente dal browser, senza dover configurare software più o meno complessi, non soltanto per fini lavorativi, ma anche per scopi personali e di svago. Oggi, ogni giorno, gli utenti inviano e ricevono una quantità impressionante di messaggi, dalle comunicazioni ufficiali alle promozioni commerciali, dalle ricevute digitali alle fatture e ai documenti legali. È proprio questa onnipresenza nel mondo della comunicazione digitale che le rende il vettore ideale per il phishing.

7 DIETRO LE QUINTE

Chi si avvicina per la prima volta al dietro le quinte delle mail potrebbe sorprendersi nello scoprire cosa le rende ciò che sono. Seguono infatti uno standard ben preciso definito da una documentazione universalmente accettata: l'RFC 5322 [5] o "Request for Comments 5322". Si tratta di uno standard internet elaborato e pubblicato dall'IETF (Internet Engineering Task Force) nell'ottobre del 2008 che stabilisce le regole sulla corretta forma delle email. Questo documento di 57 pagine, disponibile al link:

https://datatracker.ietf.org/doc/html/rfc5322

rappresenta il vero pilastro delle comunicazioni online, fornendo una standardizzazione globale che ne garantisce la compatibilità su qualsiasi applicazione e dispositivo, rendendole di fatto uno strumento universale e accessibile a tutti.

Da menzionare come la pubblicazione del 2008 vada a sostituire i precedenti standard RFC 2822 e RFC 822, rispettivamente pubblicati nell'aprile 2001 e agosto 1982, che hanno contribuito a definire lo stato dell'arte odierno delle email. Un'evoluzione necessaria: mentre all'inizio era sufficiente gestire del testo in inglese e poche informazioni aggiuntive, con l'internazionalizzazione dello strumento di posta elettronica sono emerse nuove esigenze tra cui l'implementazione di caratteri non ASCII, l'aggiunta di campi per la gestione degli header e una maggiore segmentazione tra corpo del messaggio e gli allegati, che hanno richiesto aggiornamenti di definizione sia lato client che lato server per mantenerne la compatibilità in tutto il mondo. In sostanza l'RFC 5322, la cui pagina iniziale è mostrata di seguito in Figura 3, definisce la struttura

fondamentale di una email e composta di due parti principali: l’header e il body. L’header, o intestazione, contiene le informazioni di controllo e i metadati del messaggio quali mittente, destinatario (o destinatari), oggetto e data. Il body, o corpo, rappresenta invece il contenuto vero e proprio del messaggio, che può essere in formato testo semplice o HTML e può includere diverse tipologie di allegati.

Network Working Group — P. Resnick, Ed.
Request for Comments: 5322 — Qualcomm Incorporated
Obsoletes: 2822 — October 2008
Updates: 4021
Category: Standards Track

Internet Message Format

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies the Internet Message Format (IMF), a syntax for text messages that are sent between computer users, within the framework of "electronic mail" messages. This specification is a revision of Request For Comments (RFC) 2822, which itself superseded Request For Comments (RFC) 822, "Standard for the Format of ARPA Internet Text Messages", updating it to reflect current practice and incorporating incremental changes that were specified in other RFCs.

Figura 3 - RFC 5322

E mentre la RFC 5322 regola l’intestazione e il corpo delle mail, per gestire immagini, video e allegati di qualsiasi tipo è stata introdotta un’estensione aggiuntiva: il Multipurpose Internet Mail Extension o MIME, definito nelle RFC 2045-2049. Questa estensione permette di codificare tutti i contenuti extra integrandoli nel corpo della mail ed evolvendola da semplice componente testuale a messaggio complesso vero e proprio.

Network Working Group
Request for Comments: 2045
Obsoletes: 1521, 1522, 1590
Category: Standards Track

N. Freed
Innosoft
N. Borenstein
First Virtual
November 1996

Multipurpose Internet Mail Extensions
(MIME) Part One:
Format of Internet Message Bodies

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

STD 11, RFC 822, defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for

(1) textual message bodies in character sets other than US-ASCII,

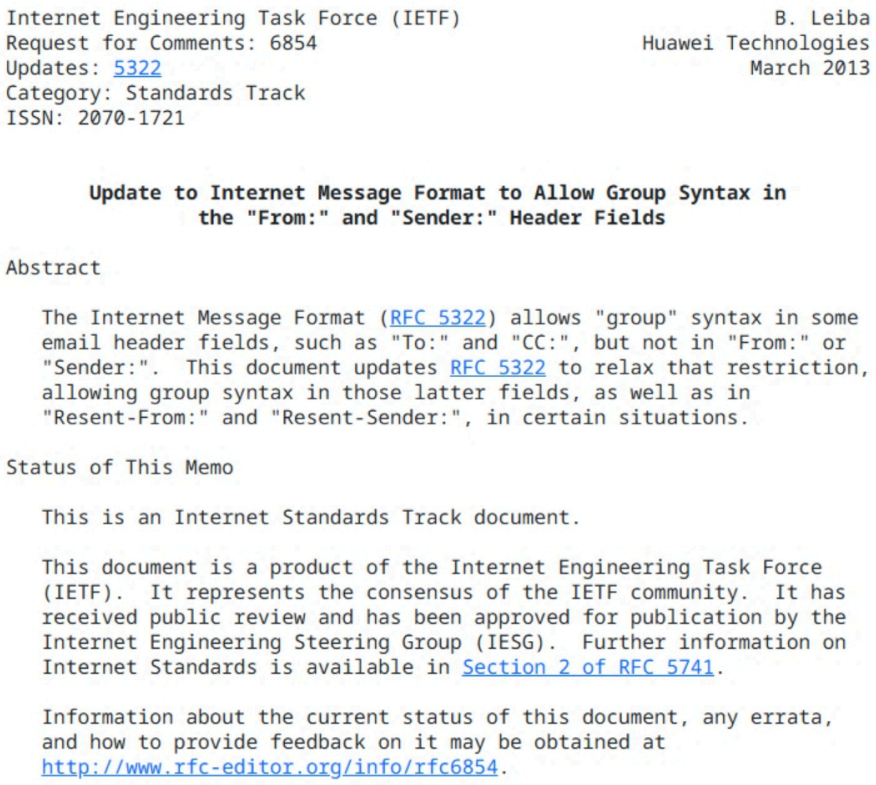
(2) an extensible set of different formats for non-textual message bodies,

(3) multi-part message bodies, and

(4) textual header information in character sets other than US-ASCII.

Figura 4 - MIME RFC 2045

Seguendo queste direttive universali, le email vengono interpretate correttamente sia dai client che dai server di posta, garantendo così una comunicazione affidabile e sicura; in caso contrario, potrebbero verificarsi problemi come la perdita parziale o totale del contenuto del messaggio. Un esempio emblematico risale a qualche anno fa: varie mail venivano ricevute, indipendentemente dai vari contesti applicativi e differenti domini di posta, come messaggi vuoti contenenti un file solo denominato “winmail.dat”. Ciò accadeva perché il client mittente, non diremo quale, non seguiva correttamente le specifiche causando la corruzione del corpo del messaggio e rendendo i messaggi inviati illeggibili per i client di posta dei destinatari.



Internet Engineering Task Force (IETF) B. Leiba
Request for Comments: 6854 Huawei Technologies
Updates: 5322 March 2013
Category: Standards Track
ISSN: 2070-1721

Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields

Abstract

The Internet Message Format (RFC 5322) allows "group" syntax in some email header fields, such as "To:" and "CC:", but not in "From:" or "Sender:". This document updates RFC 5322 to relax that restriction, allowing group syntax in those latter fields, as well as in "Resent-From:" and "Resent-Sender:", in certain situations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6854.

Figura 5 - RFC 6854

Non aderire alle specifiche può causare non solo la perdita del contenuto appena descritta, ma anche compromettere la reputazione del mittente portando i filtri antispam dei server di destinazione a identificarlo come spammer, riducendo significativamente la probabilità che le sue successive mail inviate raggiungano la casella di posta del destinatario.
In aggiunta a tutto questo, è stato pubblicato nel gennaio 2013 il documento RFC 6854 che integra e non sostituisce il 5322, supportando particolari casi in cui è necessaria una flessibilità sui caratteri accettati o sull'uso di null-sender. Ma entriamo ora più nel dettaglio e, più precisamente, parliamo dell'header delle email.

8 L’HEADER

L’header, o intestazione, di una email è composto da una serie di campi con scopi specifici ben definiti, contenenti informazioni essenziali per la corretta interpretazione e consegna del messaggio.

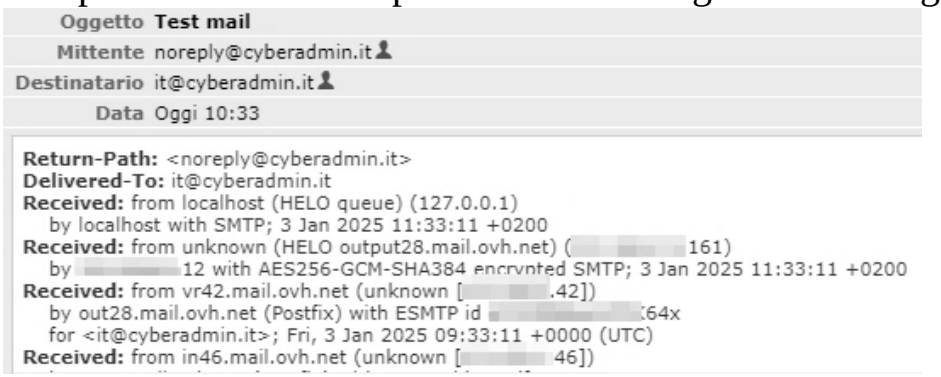


Figura 6 - Header di una mail

Tra i campi principali troviamo:

- **From** (Da), specifica l’indirizzo email del mittente e il relativo nome di visualizzazione. Attenzione: il nome di visualizzazione può essere personalizzato e differire dall’indirizzo email reale;

- **To** (A), indica l’indirizzo email del destinatario principale;

- **Subject** (Oggetto), contiene una breve descrizione del contenuto della email;
- **Date** (Data), riporta la data e l’ora di invio del messaggio;

- **CC** (Copia carbone), elenca i destinatari aggiuntivi visibili della email;

- **BCC** (CCn o Copia Carbone nascosta), elenca i destinatari aggiuntivi nascosti della email;

- **Return-path**, definisce l'indirizzo email a cui recapitare eventuali errori o notifiche. Se non specificato, viene usato il valore del campo **From**;

- **Message-ID**, fornisce un identificativo univoco associato alla email;

- **Content-Type**, descrive il tipo di contenuto del messaggio, distinguendo tra testo semplice (text/plain) e HTML (text/html);

- **Received**, traccia gli indirizzi IP dei server SMTP coinvolti nel trasporto della email, aggiungendo progressivamente in cima alla lista i dettagli dei server attraversati. L'IP del server del mittente si troverà pertanto sempre alla fine;

- **Authentication-Results**, riporta i risultati delle verifiche di autenticità tra il mittente dichiarato e quello reale.

Tutti i valori degli header sono case-insensitive, il che significa che non c'è distinzione tra lettere maiuscole e minuscole purché i caratteri appartengano al set ASCII per garantire la compatibilità universale con sistemi e dispositivi. Ad esempio, l'indirizzo email del destinatario può essere scritto sia in maiuscolo che in minuscolo senza alterare la validità e l'interpretazione della mail stessa. Analizziamo ora l'header mostrato in Figura 6. Possiamo osservare che:

- l'oggetto della mail è "Test mail"

- il mittente è **noreply@cyberadmin.it**

- il Return-path coincide con l'indirizzo del mittente indicato, **noreply@cyberadmin.it**, confermando l'autenticità

- il campo Delivered-To indica il destinatario del messaggio, e in questo caso:

it@cyberadmin.it

- il campo Received documenta la catena di server di posta elettronica coinvolti nella consegna del messaggio
- infine Data mostra l'esatto momento di ricezione della mail

I valori presenti nei campi **From** e **To**, così come quelli degli altri campi contenenti un indirizzo email, devono rispettare le specifiche di sintassi stabilite dalla RFC 5322 e sono costituiti, da tre elementi fondamentali:

- il nome della cassetta postale
- il simbolo **@**
- il dominio di appartenenza

Quando questi valori sono corretti e coerenti, ovvero quando c'è corrispondenza tra i valori dichiarati e i valori reali, si dice che i campi sono allineati.

Figura 7 - Allineamento dei campi case-insensitive

Tornando alla Figura 6, noterete che tra i campi sempre visibili in alto non è presente il Return-Path, ma occorre cercarlo all'interno del codice della mail. Questo valore, spesso trascurato dagli utenti perché non immediatamente visibile nei menu dei client di posta, è in realtà

essenziale per verificare l'autenticità della mail poiché definisce l'indirizzo cui il server di destinazione invierà gli errori di recapito, i cosiddetti "bouce message". Deve esserci sempre una corrispondenza tra questo valore e l'indirizzo email mostrato nel campo del mittente, perché a meno di casi ben motivati come vedremo nei capitoli successivi, significa che la mail indicata nel campo From potrebbe non essere quella reale del mittente, e quindi trovarci di fronte a un messaggio di phishing.

Per completezza di informazione, un altro campo presente degno di nota è il **MIME-Version** che specifica la versione del protocollo Multipurpose Internet Email Extensions, indispensabile per gestire correttamente le immagini e gli allegati all'interno della email. Ad oggi l'unica versione esistente e supportata è la **MIME-Version: 1.0**, regolamentata dalle RFC 2045-2049 del novembre 1996.

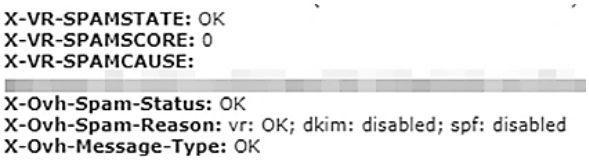


Figura 8 - Parte dell'header contenente i campi relativi lo spam

Alcuni campi come **X-SPAM-STATUS** e **X-SPAM-LEVEL**, seppur sempre più largamente accettati e adottati dai server di posta, non fanno parte né sono regolamentati da alcuna RFC, bensì sono stati introdotti dai vari servizi antispam a livello globale. Sempre per restare in tema, il livello di spam si misura con un punteggio negativo/positivo o con un quantitativo di asterischi (*****): maggiore sarà il loro numero, maggiore sarà la probabilità che il messaggio sia classificato come spam dai filtri stessi.

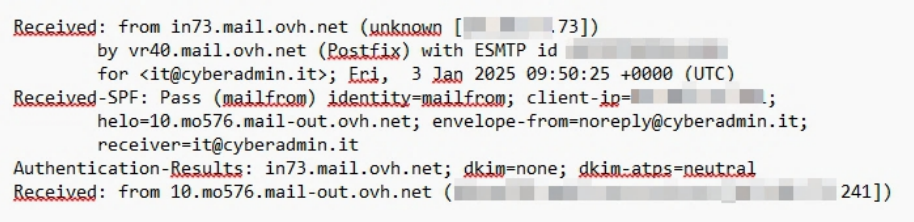


Figura 9 - Parte di header relativo a SPF

Seguono poi ulteriori controlli di sicurezza più avanzati, come SPF, DKIM e DMARC, come mostrati in Figura 9, ma li vedremo più avanti in un capitolo dedicato. Per ora è sufficiente conoscere la loro esistenza all'interno dell'header.

9 BODY E ALLEGATI

Il body, o corpo del messaggio in italiano, costituisce la parte centrale e il contenuto effettivo della email. Può essere composto da semplice testo ASCII o da un insieme più articolato di testo, immagini e allegati. Nel primo caso non è necessaria alcuna codifica e il contenuto viene trasmesso direttamente nel corpo del messaggio come testo semplice.

Figura 10 - Mail in HTML con relativo codice nel body

Nel secondo caso invece, ovvero in presenza di caratteri speciali, codice HTML, immagini o allegati di qualsiasi formato e dimensione entra in gioco il protocollo MIME, estensione opzionale della già citata RFC 5322, che definisce la formattazione e la suddivisione degli stessi. Questa sezione del messaggio è separata, rispetto agli header, da una riga vuota: per gli appassionati di tecnicismi la riga in questione è rappresentata a livello di codice dalla sequenza CRLF (Carriage Return Line Feed), per tutti gli altri lettori è un semplice a capo. A differenza degli header, il body non contiene informazioni essenziali per garantire la corretta consegna della email e non ha restrizioni sul tipo di contenuto. Si tratta di un semplice contenitore sviluppato in codice HTML o in testo semplice che

racchiude tutto il contenuto della mail. Guardando la parte grezza del body, ovvero il codice che lo costituisce e la sezione a destra di Figura 10, è un insieme di sezioni e campi meglio mostrato in Figura 11, dove **Content-Type** e **Content-Disposition** definiscono rispettivamente il tipo di file e la sua modalità di presentazione all'interno del corpo della mail. Proviamo a rendere questo concetto più semplice prendendo come esempio un'immagine inserita all'interno del testo, come il gatto di Figura 10. Il codice HTML del body può gestirle in due modi differenti: incorporandole direttamente nel codice tramite il tag **<img>** oppure elencandole separatamente insieme agli altri file allegati. La prima soluzione rende il corpo del messaggio più uniforme e coeso grazie all'integrazione diretta nel codice HTML, mentre il secondo metodo porta l'email ad essere più pesante e meno leggibile, poiché le immagini risultano parti distinti.

Nell'esempio della Figura 11 possiamo osservare due diversi campi:

- Content Type: text/plain, che contiene il testo "Here's a pic of a cat";
- Content Type: image/jpeg, che identifica l'immagine allegata.

Proprio quest'ultimo campo presenta un altro indicatore, ovvero **Content-Disposition: inline** e colloca l'immagine inserita in linea con il testo. Al contrario, un allegato avrebbe avuto come indicazione:

Content-Disposition: attachment;
filname="Allegato.pdf"

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="=_3bc96edfbefffb9af9ba1378b5e2bd2a"

--=_3bc96edfbefffb9af9ba1378b5e2bd2a
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=US-ASCII; format=flowed

Here's a pic of a cat

--=_3bc96edfbefffb9af9ba1378b5e2bd2a
Content-Type: multipart/related; boundary="=_64a458b205095e9d5cc73010b61a7c50"

--=_64a458b205095e9d5cc73010b61a7c50
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset=UTF-8

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  </head>
  <body style="font-size: 10pt;">
    <div class="pre" style="margin: 0; padding: 0; font-family: monospace">
      Here's a pic of a cat
    </div>
    <img src="localhost" alt="" width="600" height="314" />
  </body>
</html>

--=_64a458b205095e9d5cc73010b61a7c50
Content-Transfer-Encoding: base64
Content-Type: image/jpeg; name="Cat.jpg"
Content-Disposition: inline; filename="Cat.jpg"; size=170722

/9j/2wBDAAMCAgMCAgMDAwMEAwMEBQgFBQQEBQoHBwYIDAoMDAsKCwsNDhIQDQ4RDgsLEBYQERMU
FRUVDA8XGBYUGBIUFRT/2wBDAQMEBAUEBQkFBQkUDQsNFBQUFBQUFBQUFBQUFBQUFBQUFBQU
```

Figura 11 - Esempio di struttura multipart

È infatti importante sapere che gli allegati sono trattati separatamente dal messaggio e posizionati alla sua fine, in una sezione distinta della mail spesso definita “multipart/mixed”, aggiunta dopo il corpo principale della mail. Questi vengono codificati in base64, un processo che converte i file, qualsiasi esso sia il formato, in puro testo per renderli compatibili con il formato delle email. Semplificando, la stringa **Ciao** codificata in base64 diventa **Q2lhbw==**. Tale codifica aumenta la dimensione dei file di circa il 30% rispetto al peso originale, un aspetto molto spesso trascurato dagli utenti quando inviano allegati di grandi dimensioni, portando di conseguenza a errori di spedizione per il superamento dei limiti consentiti.

```
--=_aecf76c9aff9549e116cdad3a6cb127c
Content-Transfer-Encoding: base64
Content-Type: image/jpeg;
 name=winmail.dat
Content-Disposition: attachment;
 filename=winmail.dat;
 size=213642

/9j/4QAYRXhpZgAASUkqAAgAAAAAAAAAAAAP/sABFEdWNreQABAAQAAABkAAD/4QMraHR0cDov
L25zLmFkb2JlLmNvbS94YXAvMS4wLwA8P3hwYWNrZXQgYmVnaW49Iu+7vyIgaWQ9Ilc1TTBNcENl
aGlIenJlU3pOVGN6a2M5ZCI/PiA8eDp4bXBtZXRhIHhtbG5zOng9ImFkb2JlOm5zOm1ldGEvIiB4
OnhtcHRrPSJBZG9iZSBYTVAgQ29yZSA1LjAtYzA2MSA2NC4xNDA5NDksIDIwMTAvMTIvMDctMTA6
NTc6MDEgICAgICAgICI+IDxyZGY6UkRGIHhtbG5zOnJkZj0iaHR0cDovL3d3dy53My5vcmcvMTk5
OS8wMi8yMi1yZGYtc3ludGF4LW5zIyI+IDxyZGY6RGVzY3JpcHRpb24gcmRmOmFib3V0PSIiIHht
bG5zOnhtcD0iaHR0cDovL25zLmFkb2JlLmNvbS94YXAvMS4wLyIgeG1sbnM6eG1wTU09Imh0dHA6
```

Figura 12 - Esempio con allegato

Per completezza, e per placare eventuali allarmismi, quando il corpo della mail contiene codice JavaScript che dovrebbe essere eseguito all'apertura della mail stessa, esso sia malevolo o legittimo, viene bloccato dalla quasi totalità dei client di posta elettronica aggiornati e di corrente generazione proprio per questioni di sicurezza. Per questo motivo, l'anteprima di una mail generalmente non rappresenta un rischio, anche in caso di phishing. Esistono al massimo tecniche avanzate per tracciarne l'apertura, i cosiddetti web beacon o pixel di tracciamento, immagini minuscole di 1x1 pixel caricate da un server remoto al momento dell'apertura della mail, trasmettendo così informazioni quali indirizzo IP e orario di caricamento. Ma non è questa la sede per approfondire l'argomento poiché questi strumenti non rappresentano un pericolo diretto per l'utente, se non per una questione di tracciabilità del comportamento.

10 INVIA/RICEVI

Vi siete mai chiesti quale sia il viaggio di una mail dall'istante in cui premiamo il pulsante "Invia" fino alla sua ricezione in "Posta in arrivo" nella casella postale del destinatario? A prescindere dalla vostra risposta, scopriamolo insieme.

1. Il client di posta del mittente, anche definito come Mail User Agent o MUA, che può essere un'applicazione installata sul dispositivo o un servizio di webmail, elabora il messaggio dividendo header e body secondo le specifiche viste nei capitoli precedenti e si connette a un Mail Submission Agent o MSA, generalmente in ascolto sulla porta 25 o 587.

2. L'MSA si connette al Mail Transfer Agent o MTA, il quale, prima di accettare l'email, verifica che la dimensione totale del messaggio non superi i limiti consentiti e, qualora disponesse anche di sistemi antispam o antivirus come funzionalità aggiuntive, effettua un primo controllo. Se tutte le verifiche hanno esito positivo, allora prende in carico la mail attraverso un Mail Delivery Agent o MDA.

3. L'MTA utilizza il Domain Name System o, più semplicemente DNS, per individuare l'indirizzo IP del server di posta del destinatario, basandosi sul dominio presente all'interno del campo **To** nell'header della mail e richiedendo il record MX associato al dominio, dove MX sta per Mail eXchange record. Trovato il server, avvia una

connessione sulla porta standard del Simple Mail Transfer Protocol, o SMTP, che generalmente è in ascolto sulla porta 25.

4. Una volta stabilita la connessione i due server eseguono un handshake: l'MTA mittente invia un comando EHLO per identificarsi e negoziare eventuali estensioni come STARTTLS, poi seguono i comandi MAIL FROM e RCPT TO per specificare mittente e destinatario. Se la casella del destinatario esiste, il server destinatario allora risponde OK e prende in carico la email. In caso contrario, risponde con NO SUCH USER e invia una email di errore al mittente.

5. A questo punto l'MTA del destinatario effettua ulteriori controlli sulla mail per appurare che rispetti i limiti di dimensione del server e che non contenga malware o sia spam, oltre a verificare i record SPF, DKIM e DMARC. Se non emergono problemi, il messaggio viene consegnato tramite il Mail Delivery Agent del server di posta del destinatario. In caso contrario, la mail viene scartata o contrassegnata come spam.

A prima vista può sembrare complesso, ma in termini semplificati il processo è questo: il client di posta prepara il messaggio e lo inoltra al server di posta del mittente, il quale a sua volta contatta il server di posta del destinatario. Se non emergono problemi di casella inesistente, limiti di dimensione o filtri antispam, o anche semplicemente un rifiuto del server dovuto alla casella piena, la mail viene consegnata al destinatario.

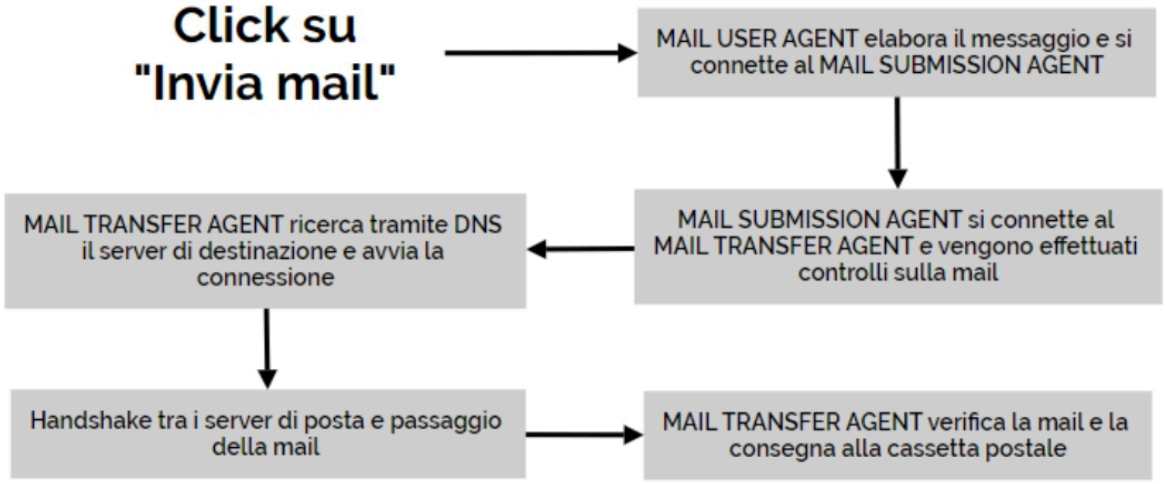


Figura 13 - Schema di invio mail

L'intero processo avviene generalmente in pochi secondi grazie ai protocolli standard adottati da tutti i server che assicurano coerenza e integrità durante la trasmissione, dove l'email viene suddivisa in pacchetti più piccoli e instradati anche attraverso percorsi differenti tra i vari nodi della rete Internet, fino a raggiungere il server di destinazione. Solo in sporadici casi possono verificarsi congestioni di rete che ritardano la consegna della email, con tempistiche che variano da poche ore fino a un massimo di cinque giorni nei casi eccezionali. Oltre quel tempo massimo, l'MTA incaricato della consegna restituisce errore al mittente.

Il protocollo SMTP poi non si limita al solo invio dei messaggi, ma utilizza anche una serie di codici di stato per segnalare l'andamento dell'operazione:

- la serie 200 (2xx) indica il successo dell'operazione, confermando che il server ha accettato la richiesta senza errori. Ad esempio, il codice 250 "Requested mail action okay, completed" conferma che la mail è stata correttamente accettata.

- la serie 300 (3xx) rappresenta la continuazione delle operazioni. Un esempio è il codice 354 "Start mail input", che segnala che il server ha ricevuto l'header ed è in attesa del body del messaggio.

- la serie 400 (4xx) riguarda errori temporanei o condizioni di attesa, principalmente dovuti a problemi del server ricevente. I codici 421 e 450 indicano rispettivamente che il server ricevente o la casella di posta non sono momentaneamente disponibili.

- la serie 500 (5xx) infine evidenzia errori gravi e permanenti che bloccano definitivamente lo scambio mail, solitamente causati dal mittente. I codici 550 o 553, ad esempio, segnalano l'impossibilità di contattare la casella del destinatario per blocchi o blacklist, portando al rifiuto definitivo della mail.

In quest'ultimo caso, quando un'email non può essere consegnata, il server di posta genera un bounce message, inviando al server del mittente un messaggio di mancata consegna dove è riportata la causa specifica dell'errore.
Dopo aver visto come l'email viaggia dal mittente al server del destinatario, è utile capire come il destinatario legga effettivamente la posta. Per farlo vengono in aiuto due protocolli: il Post Office Protocol 3 (o POP3) e l'Internet Message Access Protocol (o IMAP). Con POP3 il client scarica in locale tutti i messaggi presenti sul server con un approccio semplice e diretto, ma non offre possibilità di sincronizzazione tra dispositivi quando la casella viene consultata da più postazioni. IMAP, d'altro canto, lascia i messaggi sul server e sincronizza tutte le cartelle in tempo reale, così ogni email mantiene lo stesso stato su ogni punto di consultazione. Se sembrerebbe che quest'ultimo sia nettamente preferibile rispetto a POP3, è necessario considerare altri fattori prima di decidere quale sia il più adatto alla situazione. Mi spiego meglio: con POP3 i messaggi scaricati sono disponibili offline anche senza connessione Internet, cosa che invece non avviene con IMAP che generalmente, se non configurato, si limita a scaricare esclusivamente le intestazioni delle email, rendendo impossibile leggere i messaggi fino al ripristino della connettività. Inoltre, scaricare le mail in locale alleggerisce il carico sui server, evitando che la casella postale si riempia e non accetti più nuovi messaggi. Questo però richiede all'utente di mantenere un backup valido dei propri dati per prevenire perdite dovute a danni hardware o

cancellazioni accidentali, e se l’utente è solito consultare quotidianamente la posta su più dispositivi POP3 diventa molto limitante a meno di accettare la mancata sincronizzazione.

Potrebbero dirvi che IMAP elimina completamente la necessità di gestire manualmente i backup, dato che i messaggi restano sul server, ma sarebbe un errore molto grave oltre una vera e propria menzogna. Avere una copia dei propri messaggi sul server di posta elettronica non significa avere un backup: se infatti una mail viene cancellata e sincronizzata o se il server ha un guasto, i messaggi sono irrimediabilmente persi. Il backup dei propri dati seguendo la regola del 3-2-1 (almeno tre copie del dato su due supporti differenti e uno offline e off-site) rimane fondamentale a prescindere dal protocollo scelto. In questo libro gli argomenti principali sono email e phishing, ma la regola appena descritta è imperativo applicarla a ogni contesto digitale.

Quanto descritto finora sui protocolli resta rilevante anche se l’utente consulta la posta via webmail con servizi come Gmail o Outlook Web Access, che consentono l’accesso alla propria casella postale da qualsiasi browser senza necessità di configurazioni particolari, perché l’utilizzo è concettualmente simile al protocollo IMAP.

11 TIPOLOGIE DI PHISHING

Dopo aver esaminato la struttura e il funzionamento delle email attraverso i server di posta elettronica e i client che le visualizzano, analizziamo le diverse tipologie di phishing e la loro classificazione secondo gli esperti di cybersecurity. Inizia finalmente il nostro deep dive sull'argomento.

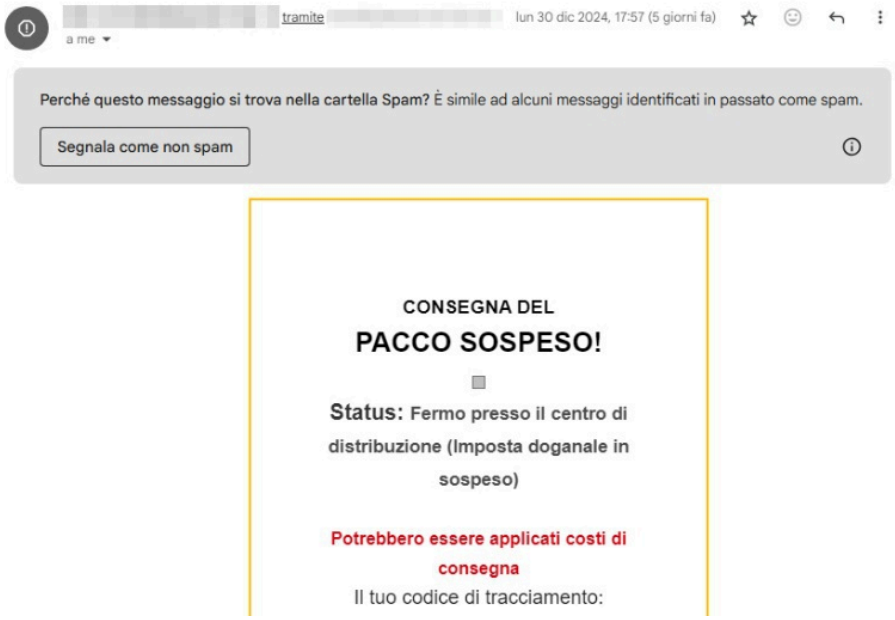


Figura 14 - Esempio di mail di phishing

Conoscere queste varianti è fondamentale per proteggersi, poiché ogni forma di phishing, sia appartenente al mondo digitale che quello reale, utilizza tecniche e strategie specifiche per raggiungere il proprio obiettivo. Il phishing classico è la forma più comune e diffusa di phishing: l'attaccante invia una email fraudolenta mascherata da comunicazione ufficiale di enti o aziende legittime, con l'obiettivo di ingannare la vittima

per ottenere credenziali di accesso e altri dati sensibili o indurre il download di malware sul dispositivo. L'esempio in Figura 14 mostra una tipica mail di phishing contenente un link malevolo sul pulsante che "dovrebbe" risolvere la situazione, badate bene al condizionale.

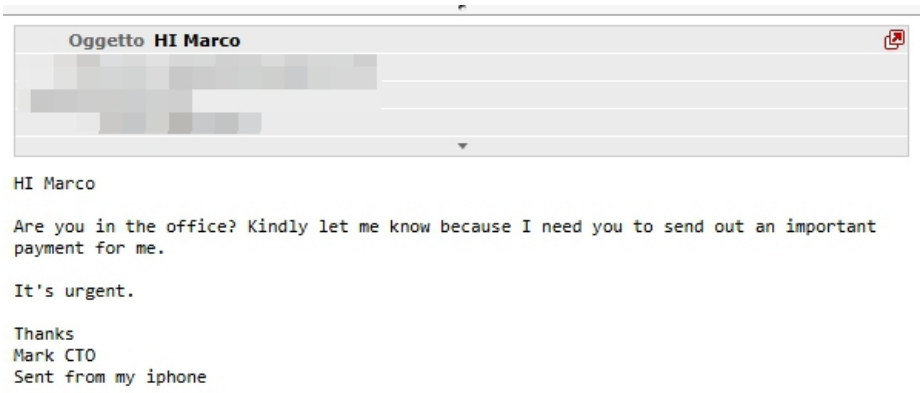


Figura 15 - Esempio di spear phishing e whaling

Nello spear phishing gli attaccanti conducono ricerche preliminari, chiamate OSINT (Open Source INTelligence) per raccogliere informazioni specifiche sulla vittima. Questo permette di creare messaggi personalizzati e credibili. Gli attaccanti puntano target precisi come individui, gruppi o aziende, per massimizzare le probabilità di successo.

Il whaling è una variante dello spear phishing, tanto che la Figura 15 può rappresentare entrambe le tipologie. Si tratta ancora una volta di un attacco mirato che richiede ricerche preliminari approfondite ed è personalizzato per colpire figure di alto profilo: CEO, CFO e altri dirigenti aziendali. Come mostrato in Figura 15, viene generalmente inviato a persone con accesso alle operazioni bancarie richiedendo pagamenti urgenti da parte di finti dirigenti aziendali.

A differenza dello spear phishing, del whaling e, come vedremo poi, del watering hole che sono attacchi ben calibrati, il phishing generico si basa sulla quantità: un maggior numero di email inviate aumenta di conseguenza la probabilità di colpire almeno una vittima. In questo approccio su larga scala il valore di successo è chiamato "conversion rate". Soltanto nei primi tre casi, ovvero quando il phishing è mirato, la logica d'attacco cambia radicalmente e diventano fondamentali l'OSINT e il social engineering, per comprendere e conoscere a fondo il contesto

della vittima, includendo dettagli come la tipologia di azienda, le tecnologie utilizzate e la supply chain con cui è solita interagire.

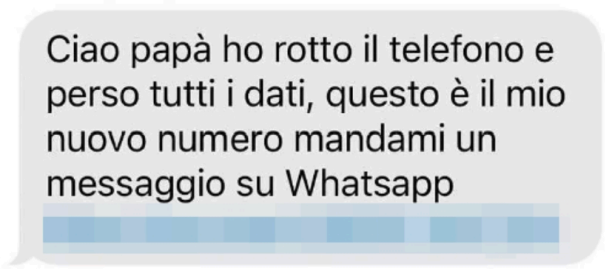


Figura 16 - Esempio di smishing

Lo smishing è il phishing effettuato tramite SMS o app di messaggistica istantanea come WhatsApp o Telegram. Mira a indurre le vittime a cliccare su link dannosi o a condividere documenti e informazioni sensibili tramite chat. Gli attacchi possono spaziare da truffe personali a false offerte di lavoro.

Il vishing sfrutta l'interazione diretta attraverso chiamate telefoniche per raggirare e ingannare le vittime. Gli attaccanti si fingono solitamente operatori di enti, banche, servizi tecnici o anche forze dell'ordine. Questo tipo di attacco risulta particolarmente efficace poiché fa leva sulla componente umana e sulla pressione psicologica esercitata durante la conversazione. Un esempio emblematico è la falsa telefonata dalla banca dove l'operatore, e truffatore, richiede di reimpostare il PIN di sicurezza per proteggere il malcapitato da movimenti di denaro sospetti.

L'angler phishing si concentra sui social media, dove gli attaccanti creano numerosi profili falsi, anche attraverso strumenti sofisticati di intelligenza artificiale, per interagire con le vittime via chat e indurle a cliccare su link malevoli o eseguire malware. Spesso sfruttano il malinteso che crea la spunta blu di "profilo verificato", considerata una garanzia di contatto sicuro.

Il SEO poisoning è invece una forma passiva di phishing che consiste nell'ottimizzare siti internet cloni e web app fasulle creati appositamente per apparire tra i primi risultati dei motori di ricerca, anche attraverso il pagamento di servizi esterni di indicizzazione. Un esempio simile di questa tecnica è mostrato in Figura 17, anche se in quel caso il risultato

deriva da un malware precedentemente installato sul dispositivo della vittima.

In stretta relazione con il SEO poisoning troviamo il website spoofing, una tecnica che prevede la creazione di una copia identica di un sito web legittimo per indurre le vittime a visitare il falso sito e, ignare del pericolo, inserire le proprie credenziali. È quindi fondamentale esaminare con attenzione ogni modulo di inserimento credenziali prima di confermare, prestando particolare attenzione a possibili segnali d'allarme o ricercando incongruenze nella forma presentata.

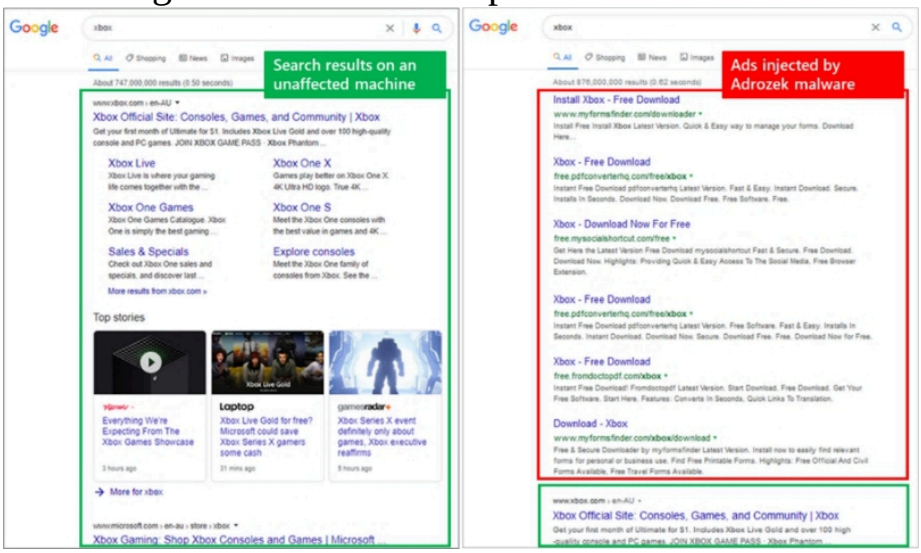


Figura 17 - Esempio di SEO poisoning, fonte: Microsoft.com [6]

Nel domain spoofing vengono utilizzati nomi di dominio che imitano quelli legittimi, sfruttando piccole variazioni nei caratteri ingannando così gli utenti meno attenti: per esempio sostituendo una **l** (elle) con un **1** (uno). Questa specifica casistica viene chiamata "typosquatting". Da notare come il domain spoofing possa mutare in DNS spoofing qualora intervenisse un malware a manipolare la risoluzione DNS del dispositivo e reindirizzare gli utenti verso siti web simili ma fraudolenti.

Il calendar phishing è tale quando è presente un link malevolo all'interno di un invito a salvare un evento nel calendario del proprio client di posta. Sebbene il file dell'invito con estensione **.ics** di per sé non contenga alcun malware, è il link presente nella mail a rendere l'utente vittima di phishing. Un chiaro esempio è mostrato in Figura 18 dove un falso invito a un evento chiede di cliccare sul link per visualizzarne i dettagli,

reindirizzando invece a un sito malevolo che scarica malware. Questa tecnica risulta particolarmente efficace poiché gli utenti tendono ad avere un falso senso di sicurezza quando gestiscono inviti ed eventi del calendario.

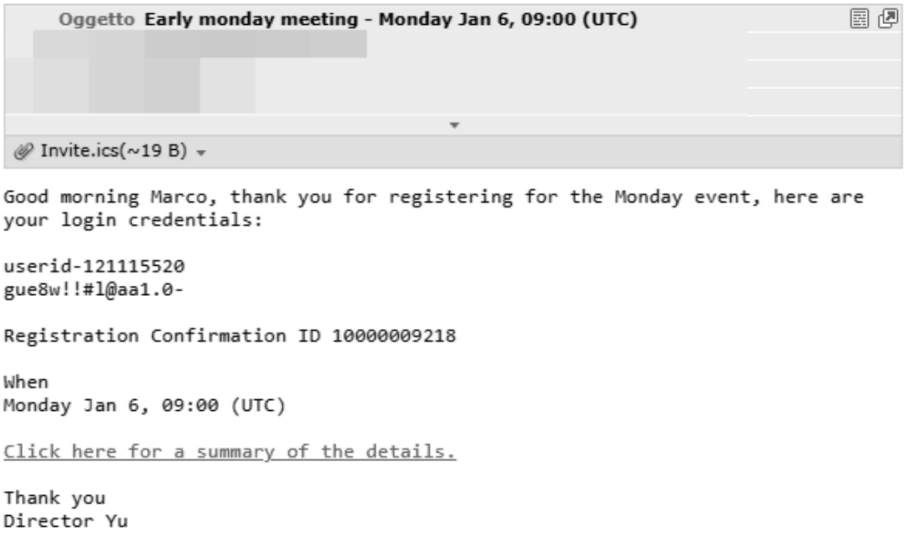


Figura 18 - Esempio di calendar phishing

L’evil twin è una forma di phishing che consiste nel clonare reti WiFi posizionandole in prossimità di quelle legittime per intercettare il traffico degli utenti che vi si connettono. Attraverso questa tecnica gli attaccanti si inseriscono nella comunicazione tra le parti, leggendo o alterando i dati trasmessi. Il caso più frequente è la clonazione delle reti WiFi aperte di hotel, bar e fast food conosciuti, dove gli utenti si sentono erroneamente al sicuro nel connettersi a una rete pubblica aperta e senza password.

Il watering hole è una tecnica di phishing avanzata che richiede sia competenze di OSINT che di hacking per essere messa in atto: prevede infatti la compromissione dei siti web visitati regolarmente dalla vittima o dall’organizzazione target. Senza interagire direttamente con l’obiettivo, gli attaccanti riescono a sottrarre credenziali e dati sensibili in due modi: attraverso form di accesso alterati o inducendo l’installazione di malware. Un esempio tipico è la compromissione della supply chain, dove attraverso notifiche del browser si spinge l’utente a installare un plugin apparentemente necessario per visualizzare il sito. Generalmente dietro questo tipo di attacchi si nasconde un gruppo di hacker altamente specializzati e/o state-sponsored.

Infine troviamo il callback phishing, una variante in cui l’attaccante spinge la vittima a ricontattarlo attraverso richieste urgenti o chiamate perse come esca, per poi utilizzare tecniche di social engineering una volta stabilito il contatto. L’esempio chiave è mostrato in Figura 19, dove si cerca il contatto via telefonica, includendo il numero all’interno della mail, o via messaggistica istantanea tramite link integrato.

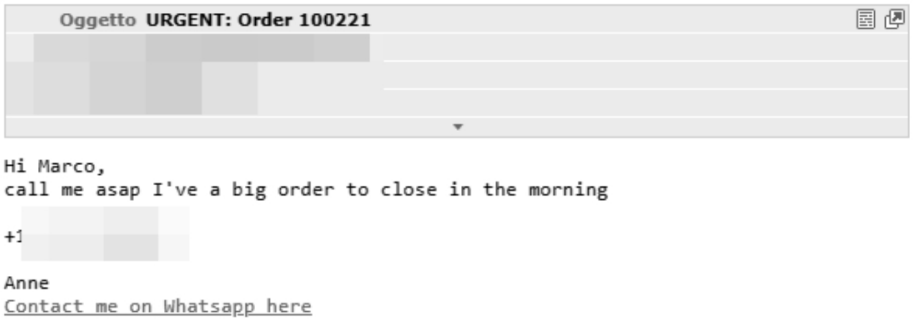


Figura 19 - Esempio di callback phishing

Queste categorie rappresentano un insieme consolidato di tecniche di phishing ampiamente diffuse a livello globale. È però necessario evidenziare come gli attaccanti tendano spesso a ibridare e combinare diverse tecniche tra loro, modificandole per adattarsi alle difese. La rapida evoluzione del phishing sottolinea l’importanza di una formazione continua e di un approccio consapevole alla cybersecurity, sia per gli operatori del settore che per gli utenti finali, aziendali o privati, e l’esistenza di questo libro ne è la prova.

12 TIPOLOGIE DI ALLEGATI MALWARE

Dopo l’analisi delle diverse tipologie di phishing, esaminiamo ora i tipi di allegati più comuni presenti in questi attacchi. Sono inviati spesso come file compressi protetti da password, una tecnica che aggira le scansioni degli antivirus endpoint e delle soluzioni anti-malware lato server, in quanto il file criptato presente nell’archivio o non può essere letto o viene ignorato dalle policy predefinite dei sistemi di protezione. Per l’utente finale, che è parte attiva nell’esecuzione del malware stesso, non costituisce un problema perché la password necessaria ad aprirli è sempre inclusa nel corpo della mail. Una volta aperto il file con il classico doppio click e inserita la password di decrittazione, si avvia una serie di operazioni che portano all’esecuzione di codice malevolo, comunemente definito malware. Se credete che in questa storia ci sia un “ma”, avete ragione. Ci arriviamo.

Iniziamo con la definizione di malware: programma, file o insieme di codice dannoso per i sistemi informatici e l’hardware stesso dei dispositivi. Non è circoscritto ai soli computer con sistemi operativi Windows, Linux o macOS, bensì anche tutti i dispositivi mobili che portiamo quotidianamente in tasca, sempre più al centro degli attacchi vista la loro diffusione in termini di vendite per persona. Ma come è possibile che un singolo link o un semplice eseguibile possa adattarsi a un panorama così vasto e complesso di dispositivi? E soprattutto, a quel punto la suite di protezione dovrebbe riconoscere la presenza di codice dannoso. Ebbene, nella maggior parte dei casi il file presente come allegato delle mail di phishing non contiene direttamente il codice

malevolo (riuscendo così anche a eludere i primi controlli da parte degli endpoint di protezione), ma un semplice “dropper”; ovvero codice legittimo che si connette a server pubblici per scaricare e installare, in step successivi, la parte di codice del malware vero e proprio. In questo modo, gli attaccanti verificano in prima battuta il tipo di dispositivo e sistema operativo, e poi scaricano la versione malware più adatta e compatibile.

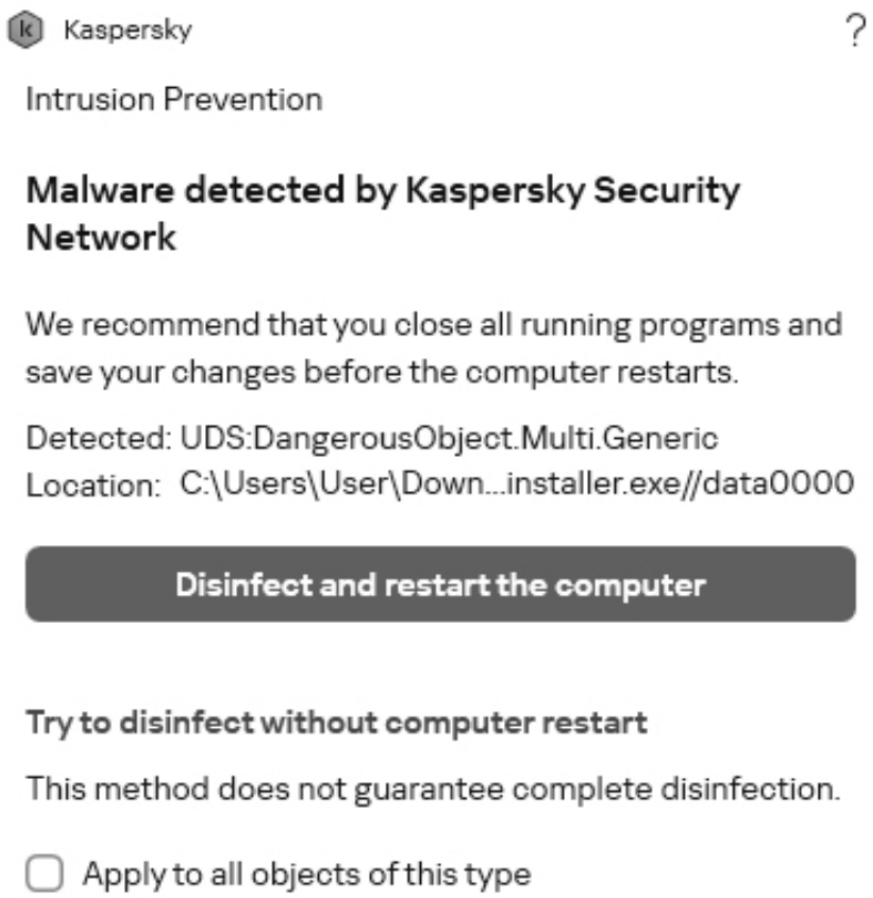


Figura 20 - Individuazione di malware da parte dell’antivirus Kaspersky

Per comprendere meglio il fenomeno, basiamoci sulle statistiche fornite da aziende leader di cybersecurity come CrowdStrike e Proofpoint [7][8] ed esaminiamo le principali tipologie di malware:

- Adware, mostra pubblicità indesiderate o convince l’utente che il dispositivo sia infetto per spingerlo ad acquistare software di terze parti. Questa definizione include anche tutti i siti web che utilizzano in modo improprio le notifiche del browser per inviare messaggi fraudolenti.

- Botnet, trasforma il dispositivo in un nodo (o bot in inglese) di una rete più grande controllata da un attaccante master, utilizzata principalmente per attacchi di tipo Distributed Denial of Service o DDOS, riuscendo così a inondare un target terzo di richieste e pacchetti dai vari nodi della rete in modo da sovraccaricare i sistemi e impedirne il corretto funzionamento.

- Fileless, applicativo o codice in esecuzione che non lascia tracce sul disco in quanto opera interamente nella memoria RAM. È una delle principali tipologie di allegati malware presenti nelle mail di phishing, poiché riesce ad eludere le più elementari scansioni antivirus che non analizzano il comportamento degli eseguibili.

- Keylogger, registra le sequenze dei tasti digitati sulla tastiera fisica e i relativi movimenti del mouse. Nelle versioni più sofisticate è in grado anche di ottenere le digitazioni sulla tastiera virtuale a schermo, oltre che le stesse videate, permettendo così di acquisire un maggior numero di informazioni sensibili.

- Ransomware, funzione matematica che crittografa i file del dispositivo, il più delle volte tralasciando quelli necessari all'avvio del sistema operativo, rendendoli inaccessibili e chiedendo un riscatto, in termini economici di notevole impatto, per ripristinarne l'accesso. È al centro dell'attenzione della maggior parte degli attacchi alle aziende ed enti governativi dell'ultimo decennio. Tale riscatto avviene perlopiù per mezzo di criptovalute come i Bitcoin e gli attaccanti, o threat actor come vengono definiti nel settore della cybersecurity, offrono un supporto diretto e un contatto di comunicazione per favorirne il pagamento.

- Rootkit, malware avanzato e generalmente invisibile alle soluzioni di sicurezza più diffuse, progettato per restare residente nel dispositivo e mantenere la sua presenza anche dopo una formattazione del disco a basso livello. Il suo

codice infatti si posiziona all’interno dei firmware e viene caricato prima del sistema operativo stesso. Per liberarsene a volte è necessario smaltire l’hardware infetto.

- Remote Access Trojan o RAT, è una suite complessa e avanzata di codici malevoli che permette all’attaccante di assumere il controllo totale del dispositivo compromesso. Grande diffusione dei RAT sono ai danni dei dispositivi mobili Android, con l’obiettivo di sottrarre denaro al momento dell’esecuzione di mobile banking app. Infatti, se uno smartphone è infetto, all’apertura di un’applicazione bancaria questo si posizionerà di un layer superiore e invisibile rispetto all’applicazione e avvierà, ingannando l’utente, dei pagamenti di denaro verso conti esterni.

- Spyware, codice non dannoso ampiamente diffuso che monitora e raccoglie informazioni sulle attività svolte sul dispositivo dall’utente senza autorizzazione o consenso. Per sfatare un mito, i cookies che accettate durante la navigazione internet tramite browser non fanno parte di questa categoria.

- Trojan, codice malevolo che si camuffa da software legittimo per ingannare l’utente e convincerlo ad eseguirlo, molto spesso richiedendo all’utente di disabilitare la protezione dell’antivirus. La stragrande maggioranza di trojan presenti nel panorama IT odierno sono rappresentati dai crack di software a pagamento.

- Wiper, non molto diffusi a causa dell’impossibilità di trarne profitto, cancella in modo irreversibile tutti i dati memorizzati sul dispositivo che lo esegue. Sono utilizzati perlopiù nella guerra informatica tra stati o da parte di hacktivisti.

- Worms, codice malevolo che si propaga autonomamente attraverso i dispositivi connessi alla rete, replicandosi

rapidamente come un virus umano del mondo reale. In alcuni casi può essere anche privo di scopi dannosi.

Per riportare un esempio utile a comprendere quali siano le estensioni dei file dannosi presenti all'interno delle campagne di phishing, secondo il rapporto del Computer Emergency Response Team (CERT) dell'AGID italiana relativo all'ultima settimana di Dicembre 2024 e la prima di Gennaio 2025 [12], i due principali formati sono: file **.html**, che sono i file che definiscono le pagine web, e file compressi in formato zip e rar.

Oltre alle tipologie elencate di malware esistono altri scenari che, pur non utilizzando direttamente software dannoso sul dispositivo della vittima, presentano comportamenti simili o sono derivanti da azioni malevole precedentemente attuate, e costituiscono minacce altrettanto serie per l'utente finale. Al fine di offrire con questa lettura un quadro completo, le affrontiamo:

- Account takeover, accade quando un attaccante, a prescindere dalla strategia attuata per raggiungere il fine, ottiene il pieno controllo di un account online dell'utente vittima.

- Credential stuffing, ovvero l'utilizzo non autorizzato, anche non a fini malevoli, di credenziali rubate da database compromessi successivamente pubblicati online (e definiti databreach). Attenzione che attuare questo tipo di comportamento, poiché non richiede elevate competenze tecnologiche per essere messo in atto, viene erroneamente considerato come azione senza gravi ripercussioni. Niente di più sbagliato. Ogni nazione e stato ha infatti una sua regolamentazione che ne definisce le pene relative, anche molto severe.

- Clickjacking, tecnica di inganno che induce l'utente a cliccare inconsapevolmente su elementi nascosti all'interno di un sito web compromesso. Per fare un esempio reale, se su un form di accesso si sovrappone un pulsante invisibile,

indirizzando così l’utente a compiere un’azione diversa da quella intesa, si parla di clickjacking.

- Man-in-the-middle, tecnica di alto livello in cui l’attaccante intercetta e manipola i dati scambiati tra client e server posizionandosi come intermediario nella comunicazione. Così facendo è in grado di leggere tutto il traffico in uscita dal client e non solo quello in chiaro HTTP, ma rompendo la catena dei certificati SSL e forzando tramite malware installato in precedenza, un’autorità di certificazione attendibile locale sul dispositivo, anche quello HTTPS sicuro. Niente panico, questo è un caso limite avanzato che richiede l’accesso al dispositivo client vittima, e generalmente in caso di discrepanza di certificati i browser di corrente generazione avvisano sempre l’utente con un messaggio di avviso a tutto schermo, mostrato in Figura 22.

Come abbiamo visto, le minacce sono molteplici ed è fondamentale adottare una corretta postura di sicurezza informatica. Non pensate che questo riguardi solo i professionisti o gli addetti del settore: tutti possono navigare in sicurezza, seguendo alcune regole basilari, che vanno dal mantenere il sistema operativo aggiornato con le rispettive patch di sicurezza, all’utilizzare una suite di protezione efficiente e aggiornata, all’evitare di eseguire applicazioni o aprire allegati da fonti non sicure o certificate. In definitiva, è sempre l’utente l’anello debole della catena e il principale vettore su cui gli attaccanti fanno leva.

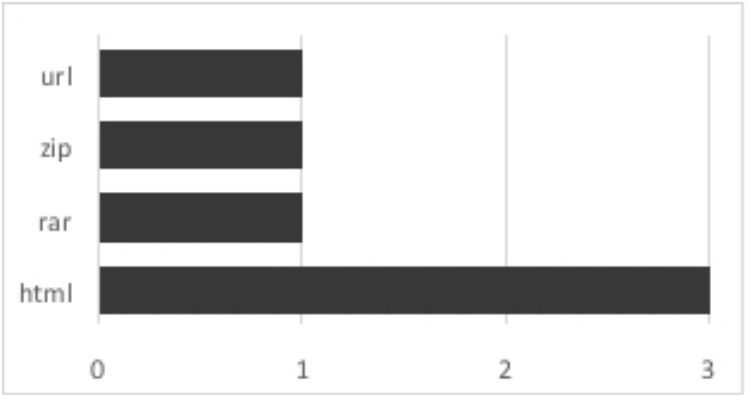


Figura 21 - Tipologie di file nella campagna di phishing, Fonte [12]

Infatti quando i sistemi operativi sono protetti e le policy di sicurezza correttamente applicate, l'unico elemento che può aprire la porta ai threat actor rimane proprio l'utente finale con un click di troppo, come viene confermato anche dalle statistiche ufficiali condivise pubblicamente da Proofpoint [9].

Figura 22 - Esempio di avviso di errore certificato

13 COME LEGGERE L’HEADER

Anche se non è necessario analizzare l’header di ogni singola email, resta fondamentale saper esaminare quelle che destano sospetti di phishing. In questo capitolo, più pratico e meno teorico dei precedenti, vedremo come leggere gli header delle email in base al client di posta utilizzato, seguendo una guida passo passo per le diverse situazioni. Potete concentrarvi sulla sezione più pertinente al vostro caso specifico o saltare direttamente al capitolo successivo se avete già dimestichezza con queste procedure.

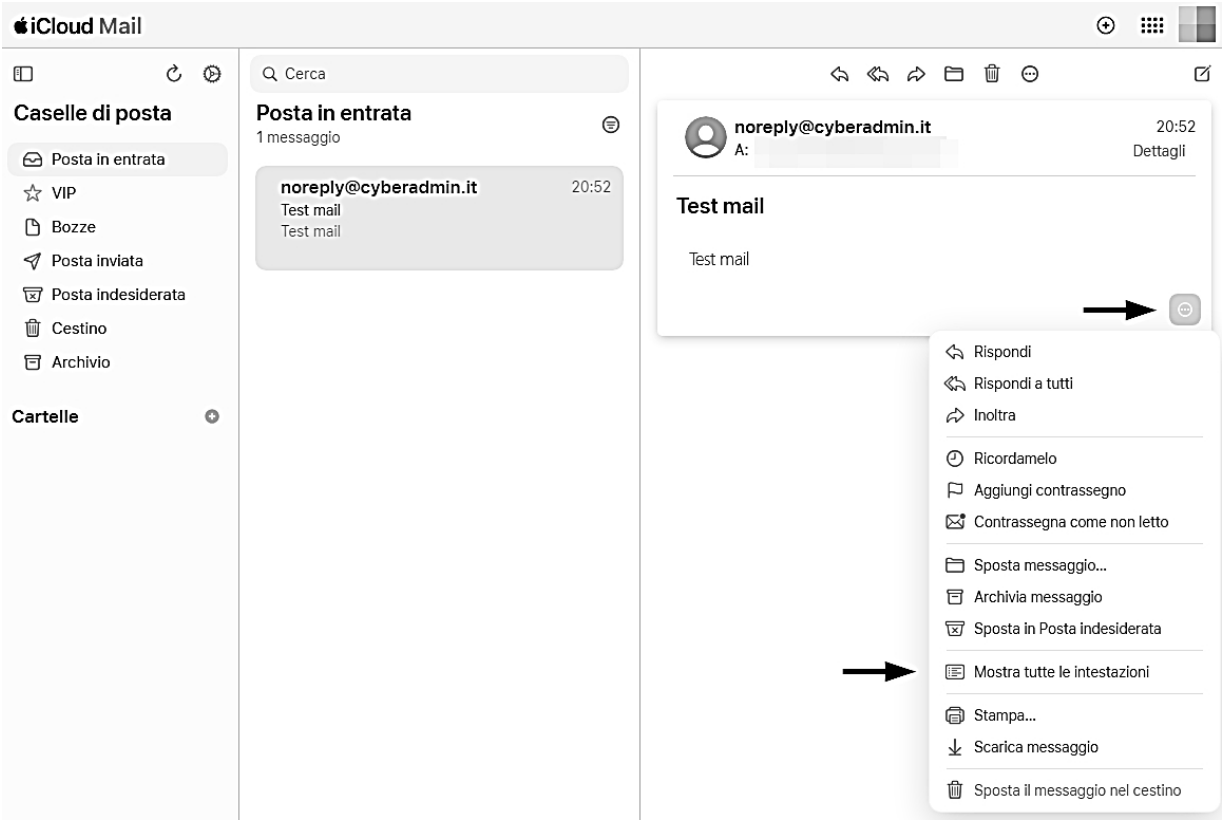


Figura 23 - Apple mail, mostra tutte le intestazioni

Partiamo dal provider di posta elettronica più diffuso nel 2024, che detiene quasi il 54% della quota di mercato secondo le fonti citate [10]. Per visualizzare l'header, selezioniamo una mail, clicchiamo sul pulsante con i tre puntini orizzontali, noto come "meatballs menu", e scegliamo "Mostra tutte le intestazioni", come illustrato in Figura 23. Il risultato è visibile in Figura 24, dove il contenuto originale della mail viene sostituito dall'header, parzialmente oscurato per motivi di privacy.

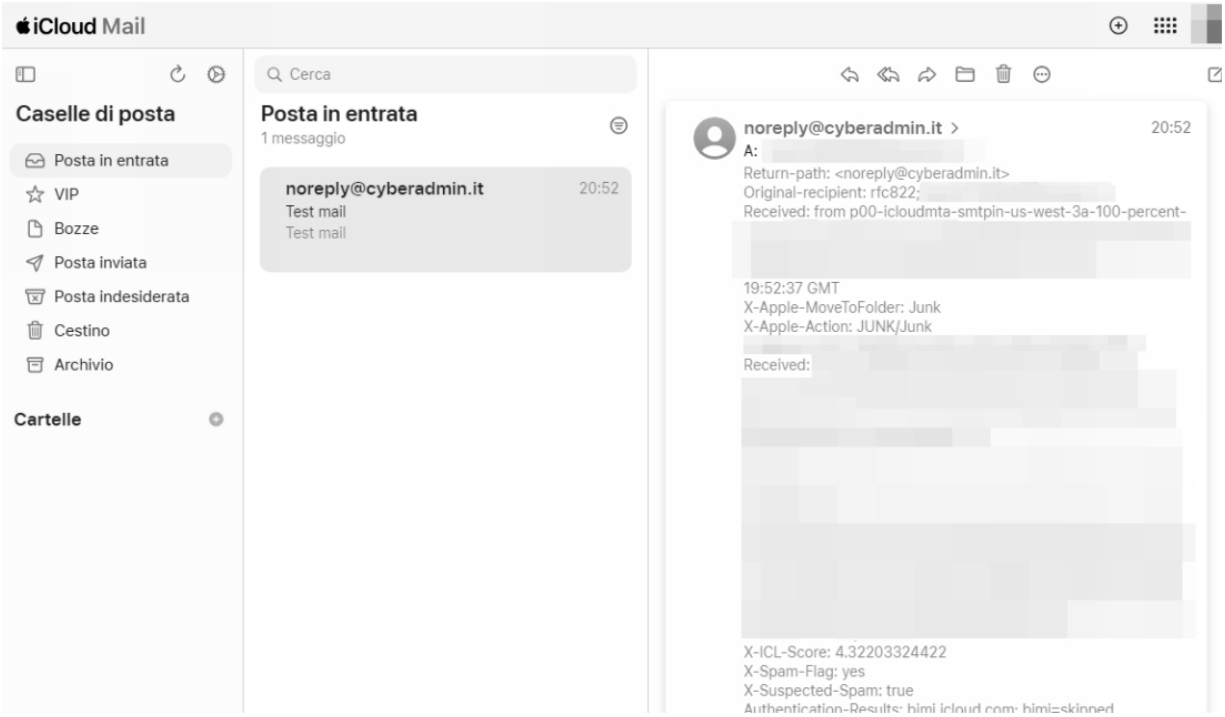


Figura 24 - Apple mail header

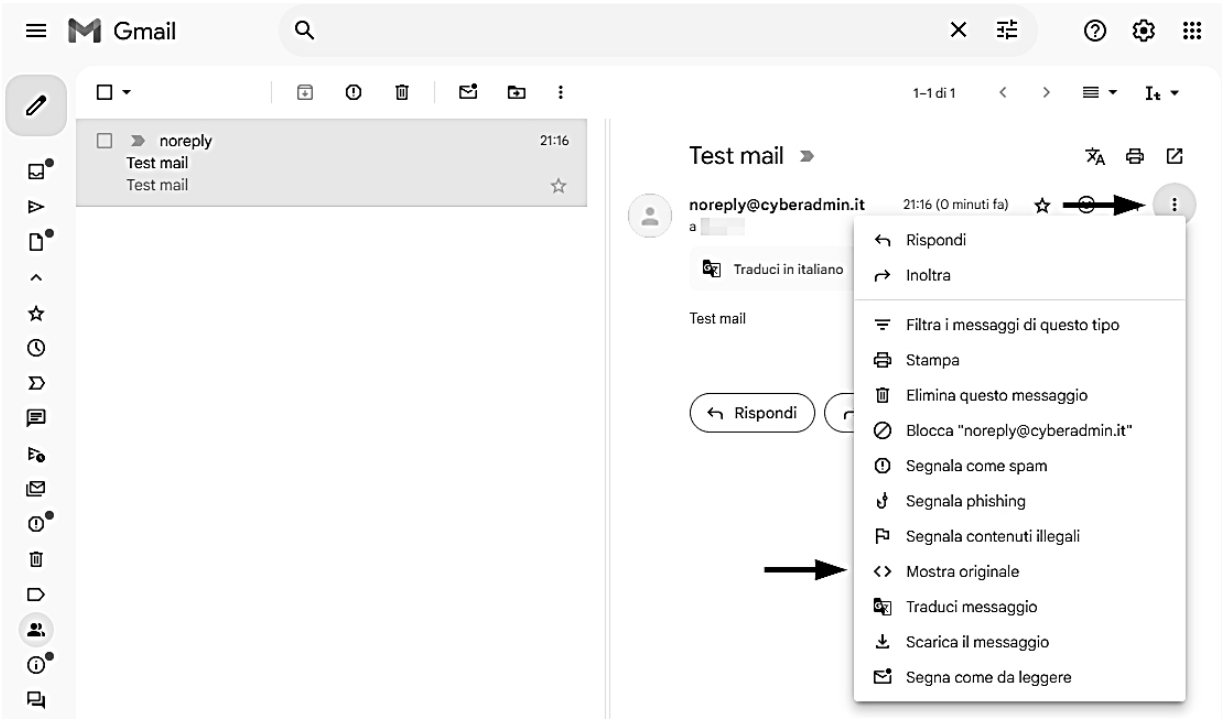


Figura 25 - Gmail, mostra originale

Segue Gmail, con il 30% di share del mercato. Anche in questo caso, dopo aver selezionato una mail, clicchiamo sui tre puntini verticali in alto a

destra, il cosiddetto “kebab menu”, e scegliamo l’opzione “Mostra originale”, come in Figura 25. Si aprirà una nuova finestra che mostra l’header completo della mail, visibile in Figura 26.

Figura 26 - Gmail header

Per Microsoft Outlook versione web, che detiene il 4% della quota di mercato, la procedura è simile.

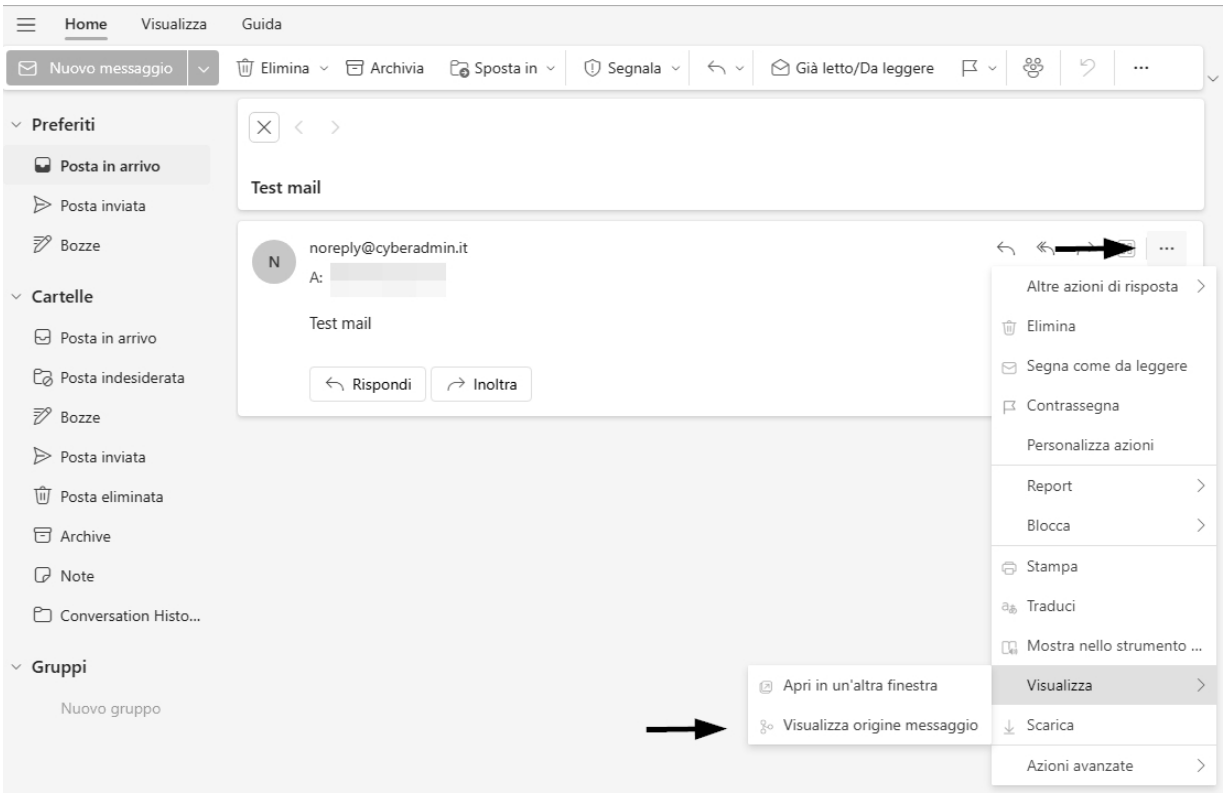


Figura 27 - Outlook web, Visualizza origine messaggio

Dopo aver selezionato la mail, clicchiamo sul kebab menu specifico del messaggio, selezioniamo “Visualizza” e infine “Visualizza origine messaggio”, come mostrato in Figura 27. L’header apparirà in sovraimpressione nella stessa schermata, vedi Figura 28.

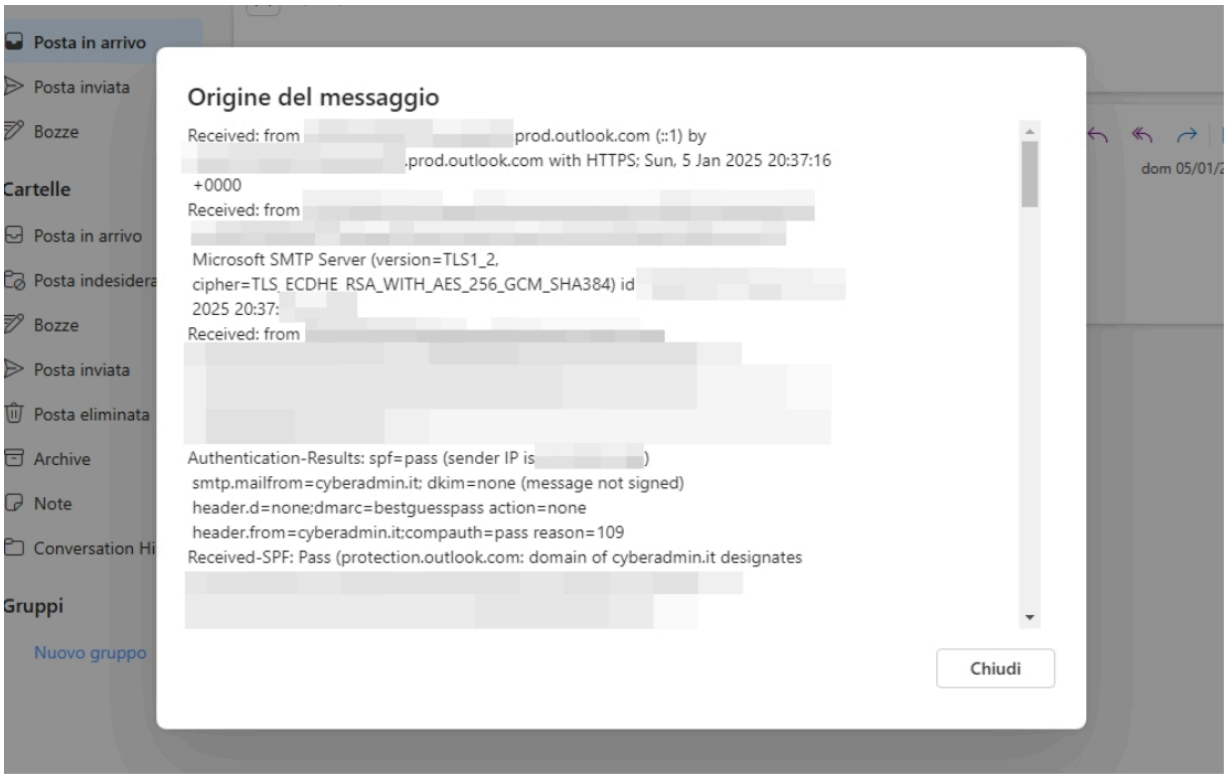


Figura 28 - Outlook header

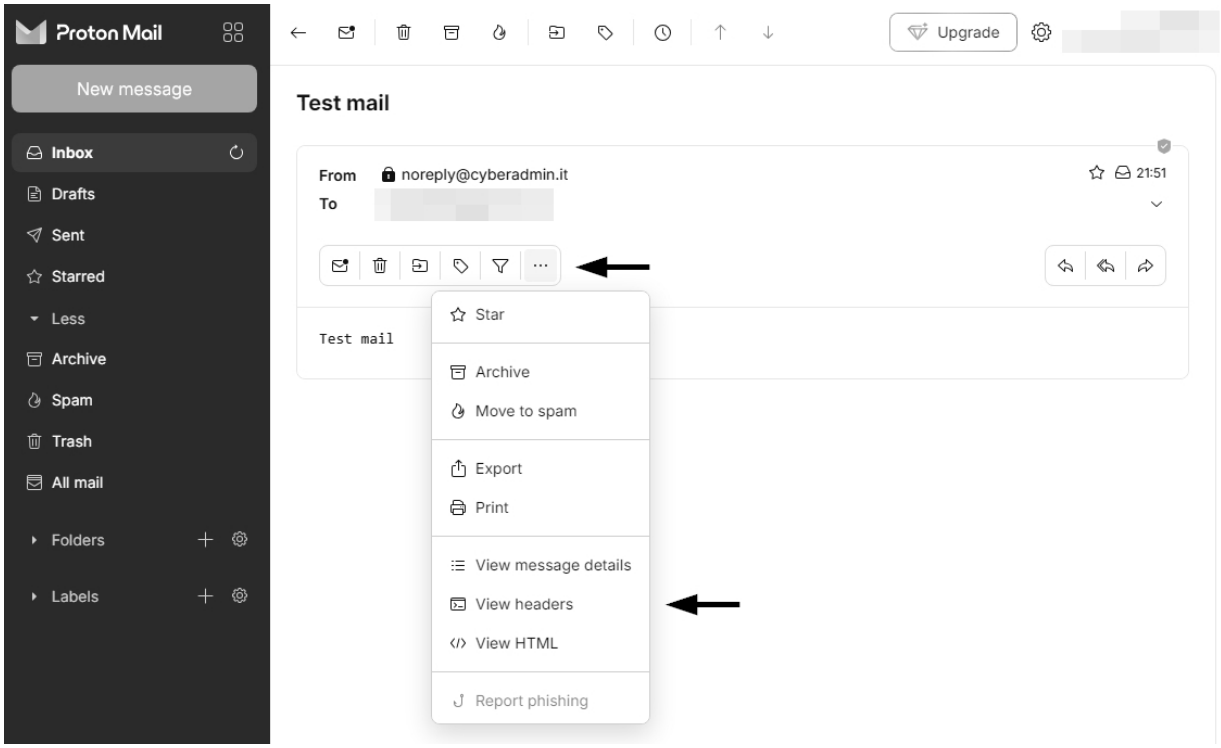


Figura 29 - Proton mail, view headers

Anche per ProtonEmail la procedura è simile: dopo aver selezionato l’email, clicchiamo sul meatballs menu e selezioniamo la voce “View headers” per visualizzare le informazioni desiderate, come in Figura 29.

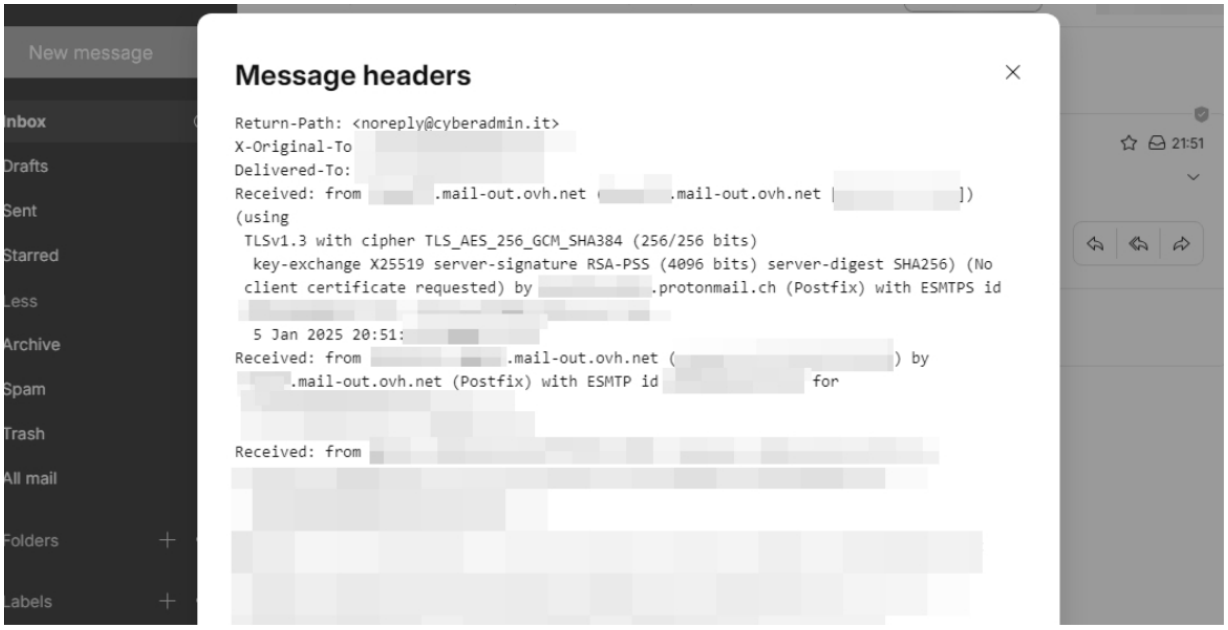


Figura 30 - Proton header

Apparirà una finestra in sovraimpressione simile a quella di Outlook web, mostrato in Figura 30.

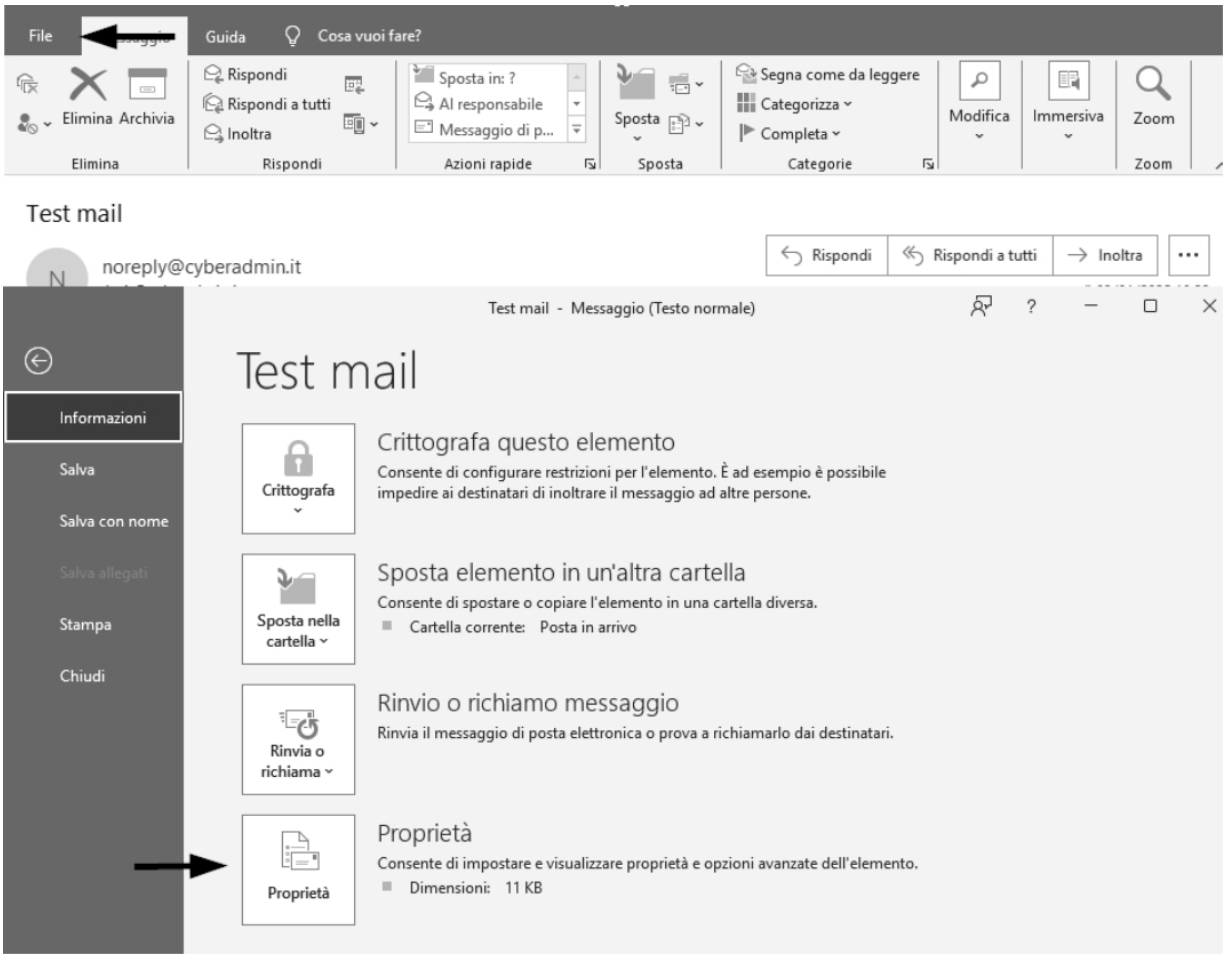


Figura 31 - Outlook, File, Proprietà

Per la versione desktop di Outlook la procedura è altrettanto semplice ma leggermente diversa. Facciamo doppio click sull'email per aprirla in una nuova finestra. Qui, clicchiamo su "File" sul menu in alto e poi su

“Proprietà”, come in Figura 31. L’header apparirà in una piccola finestra di popup, vedi Figura 32.

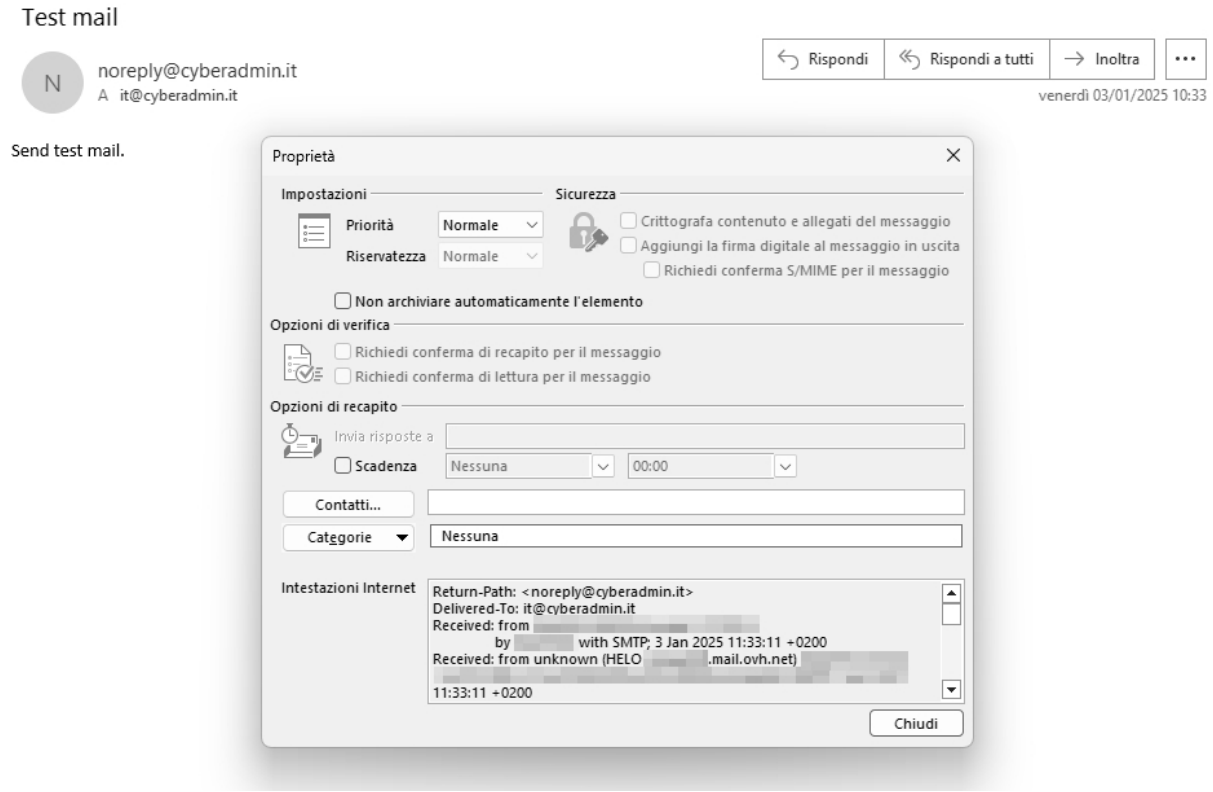


Figura 32 - Outlook desktop header

Anche in Mozilla Thunderbird il procedimento è simile. Dopo aver selezionato la mail, clicchiamo sul menu “Altro” a destra e poi su “Visualizza sorgente”, vedi Figura 33.

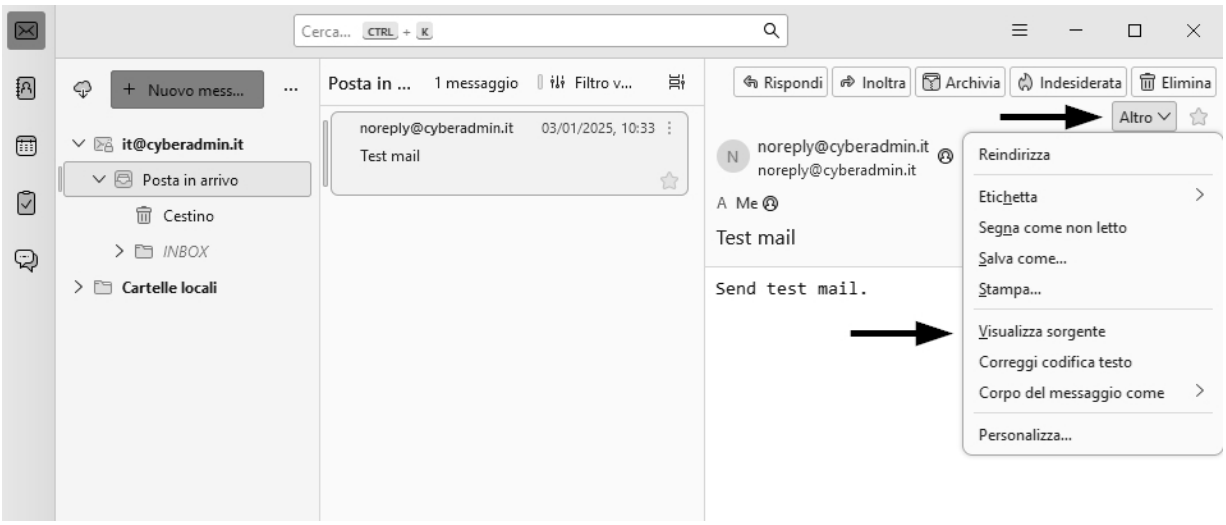


Figura 33 - Thunderbird header

Resta infine Apple Mail. La procedura è sempre la stessa: dopo aver selezionato l'email da analizzare, clicchiamo sul meatballs menu presente in alto, e poi su "Mostra tutte le intestazioni".

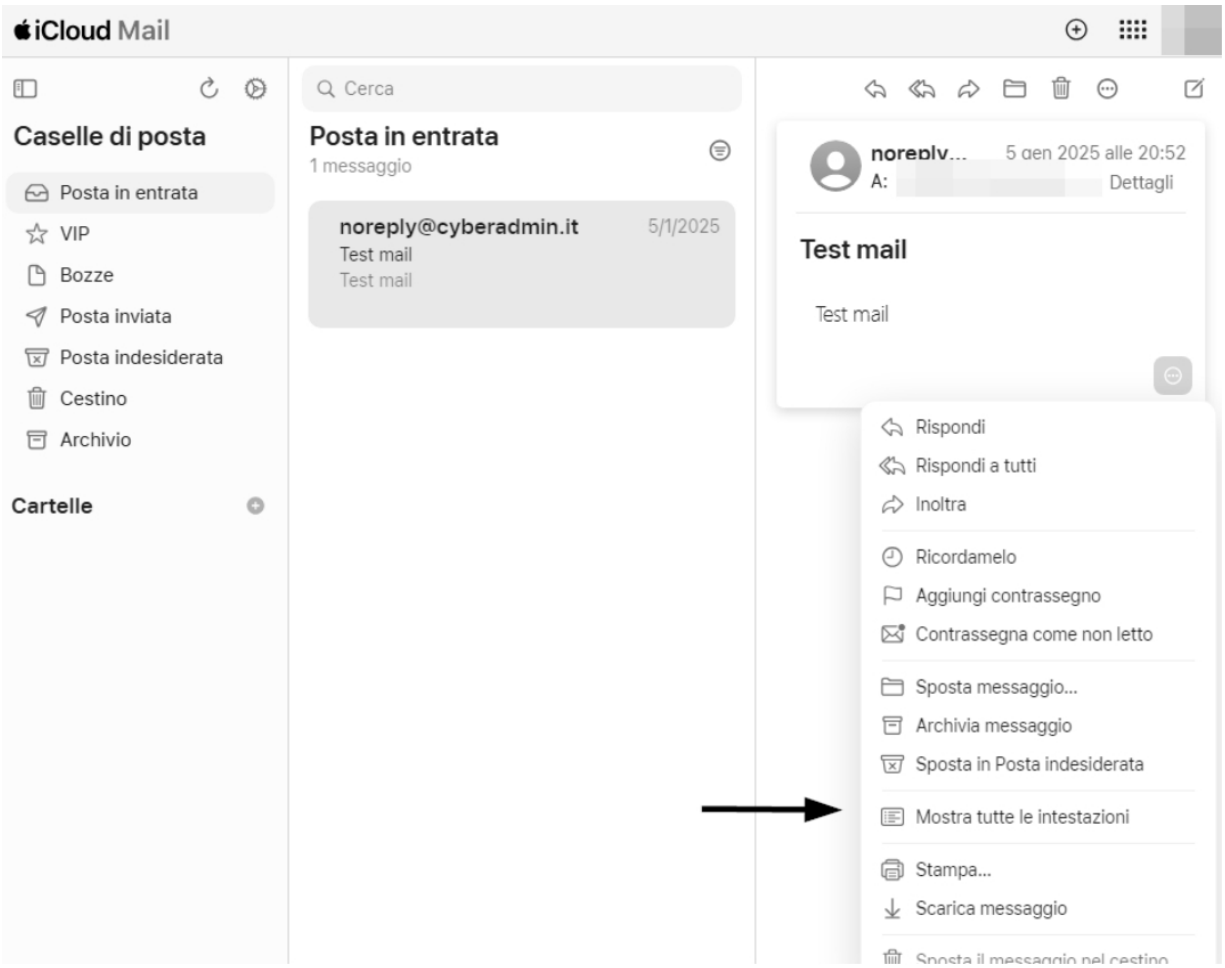


Figura 34 - Apple Mail header

L’header apparirà direttamente sopra il contenuto dell’email, senza aprire finestre separate, come nei precedenti esempi.

14 MXTOOLBOX E MAILHEADER

Una volta ottenuto l’header della mail sospetta da analizzare, esistono una serie di strumenti online gratuiti che ne esaminano la struttura, trasformando il codice complesso in una tabella semplificata e intuitiva, corredata di informazioni grafiche e rendendo l’analisi accessibile anche a chi non è un esperto di cybersecurity. I due strumenti più semplici e utilizzati, per mia esperienza diretta, sono:

- **mxtoolbox.com/EmailHeaders.aspx**
- **mailheader.org/**

Partiamo proprio da MXtoolbox, vedi Figura 35.

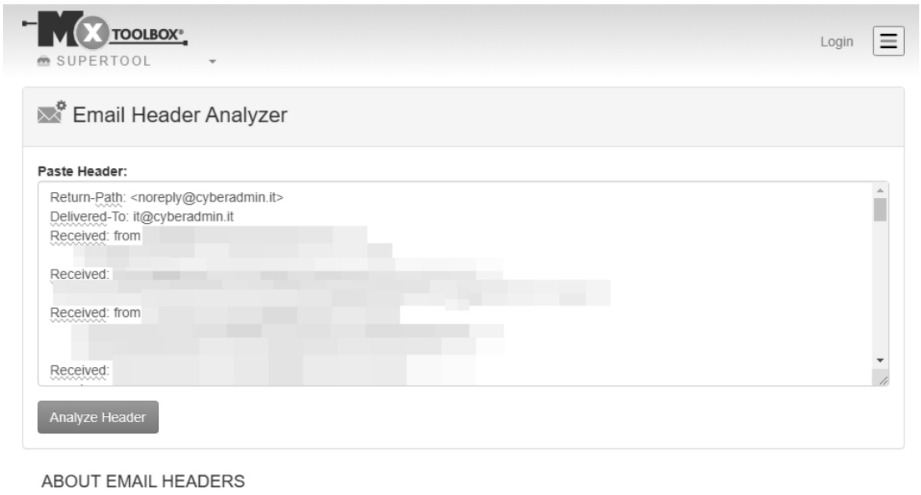


Figura 35 - MXtoolbox

Si presenta come una web app intuitiva con un unico campo compilabile, dove è possibile incollare l’header estratto secondo le modalità mostrate nel capitolo precedente. Dopo aver cliccato su “Analyze Header”,

otteniamo una rappresentazione decisamente più utile e facile da interpretare rispetto al codice grezzo dell'header estrapolato. Nella prima parte della pagina, mostrata in Figura 36, il paragrafo "Relay Information" mostra la linea temporale dei passaggi della mail attraverso i server di posta: dal primo hop o punto di partenza, fino al server di destinazione.

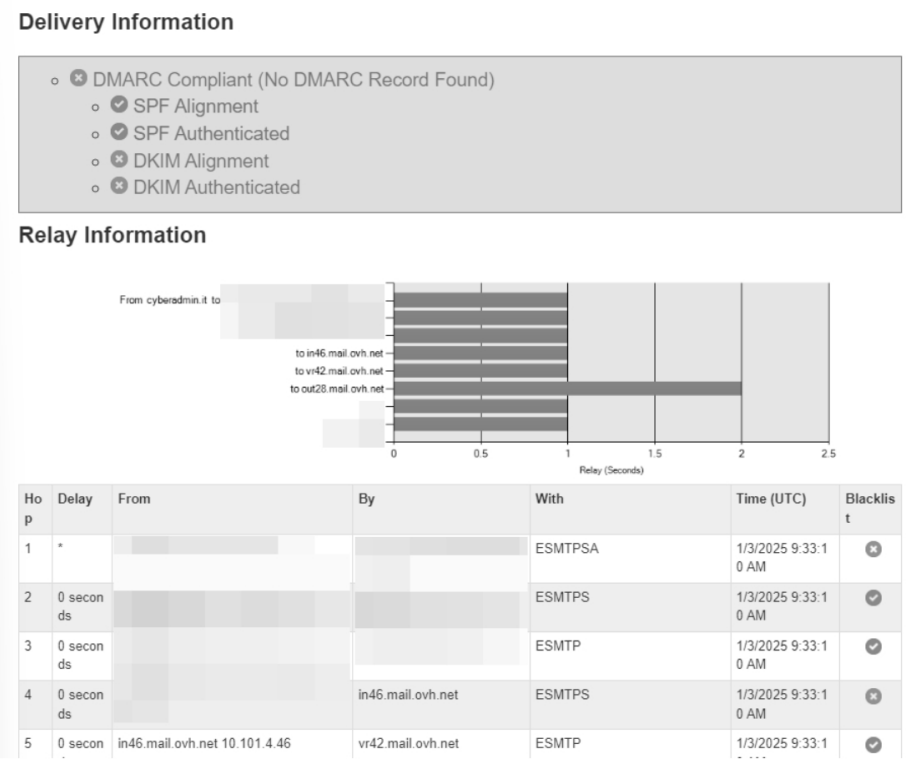


Figura 36 - Risultato della scansione dell'header con MXtoolbox

Per ogni hop vengono indicate diverse informazioni: la latenza o tempo di transizione impiegato, il Full Qualified Domain Name o FQDN del server che ha gestito la mail, la modalità di trasmissione utilizzata dai server (ESMTPSA, ESMTPS o SMTP), l'orario in formato UTC e l'eventuale presenza di uno o più IP pubblici all'interno di blacklist. È importante notare che se la mail transita attraverso server di posta condivisi tra più servizi o domini, questi potrebbero risultare già presenti in alcune liste di blacklist, a prescindere dal comportamento dell'utente. Approfondiremo poi la questione in un capitolo dedicato.

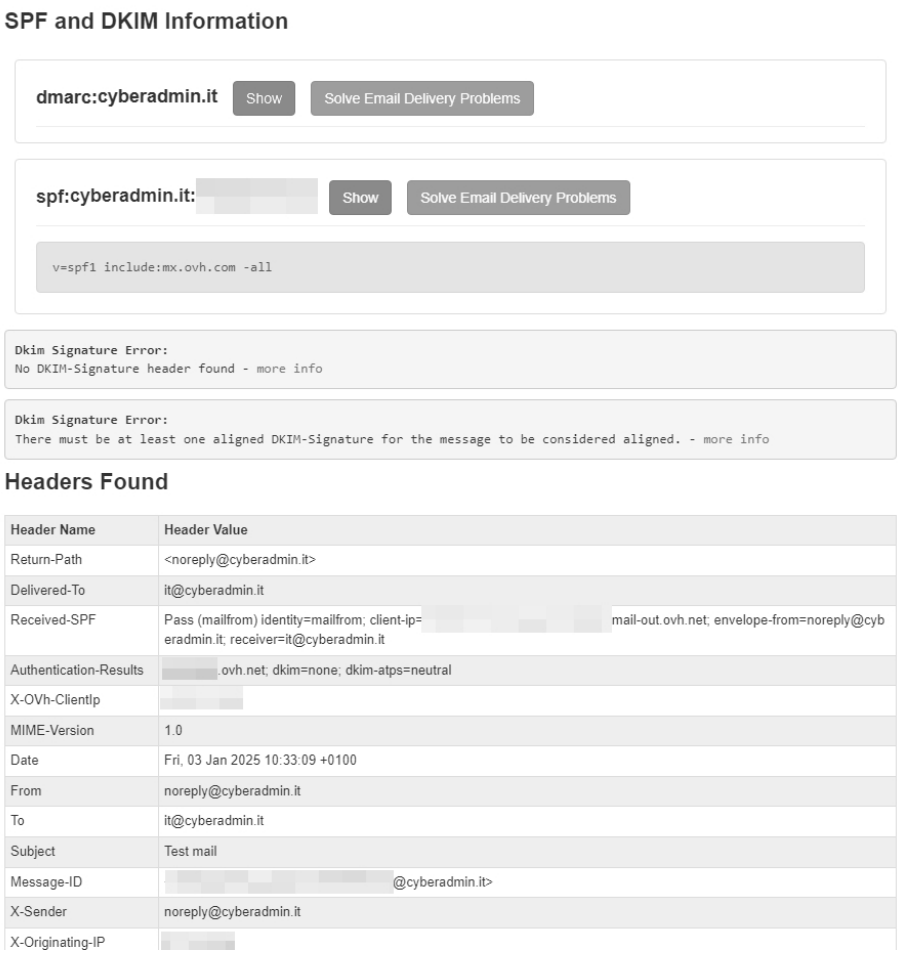


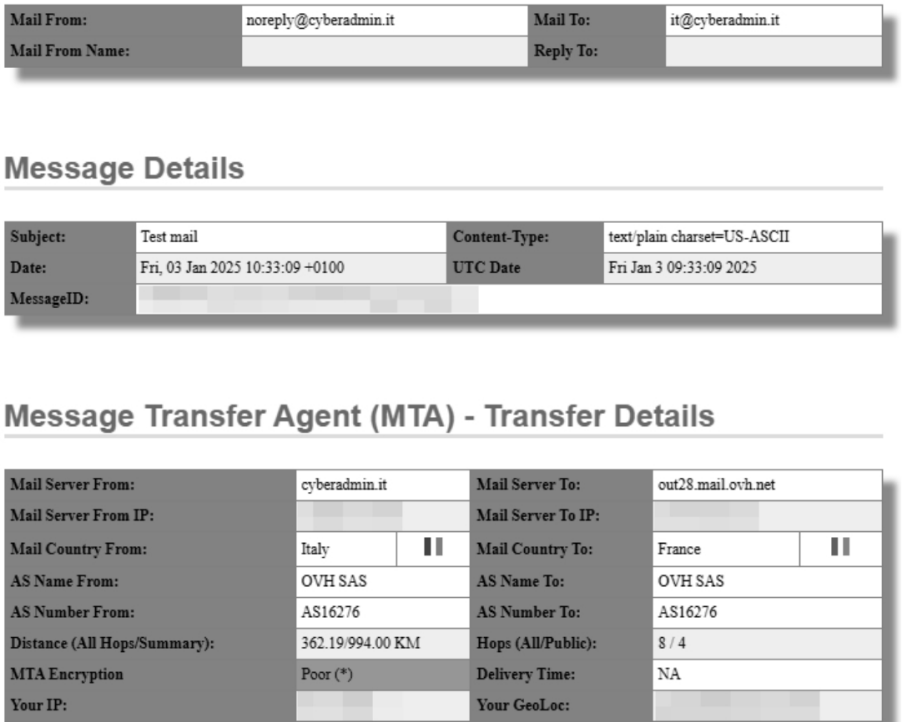
Figura 37 - Risultato avanzato della scansione dell'header con MXtoolbox

Nella seconda parte della pagina, vedi Figura 37, sono mostrati i risultati delle principali verifiche di sicurezza effettuate da MXtoolbox: la presenza di un record SPF valido, l'esistenza di una firma DKIM e la corretta configurazione del DMARC, tre elementi fondamentali per la sicurezza delle email, approfonditi nel Capitolo 35. È inoltre visibile il valore SPAMSCORE della mail che ne determina la classificazione come spam o meno, meglio illustrato in Figura 40. La piattaforma offre inoltre strumenti aggiuntivi utili per analizzare problemi di consegna delle email e tra i più rilevanti, anche in termini di probabilità di utilizzo nel risolvere le problematiche descritte, troviamo: MX Lookup per l'analisi dei record MX del dominio, Blacklist Check per verificare se il dominio o gli IP del servizio di posta sono presenti in liste di blocco, e SPF Record Lookup per controllare la configurazione SPF del dominio preso in esame.

Figura 38 - MailHeader

Passiamo ora a MailHeader, uno strumento che offre un’analisi più dettagliata e completa rispetto al precedente. Il funzionamento è simile a MXtoolbox: la pagina iniziale presenta un campo dove incollare l’header estratto, come mostrato in Figura 38. Una volta cliccato su “Submit”, la web app analizza il contenuto e presenta i risultati delle informazioni rimaneggiate. Si inizia con i dati basilari di mittente e destinatario, seguite dai vari dettagli della mail come oggetto, data di ricezione, tipo di contenuto (nell’esempio text/plain) e identificativo del messaggio. Vengono poi presentati le informazioni dei server di posta, includendo gli indirizzi IP pubblici, la loro localizzazione geografica e la distanza approssimativa in chilometri tra i vari hop di transito, compreso l’IP pubblico del mittente, in un insieme di tabelle di facile lettura oltre che in formato visuale tramite mappa di Google Maps, che visualizza la posizione dei server e le loro distanze in linea d’aria. Viene anche stimata approssimativamente la distanza tra l’IP di origine e quello di destinazione per ogni hop attraversato dalla mail, come illustrato in Figura 39. Particolarmente utile è la sezione del punteggio spam, dove una tabella mostra l’analisi dettagliata con punteggi positivi o negativi per ogni regola valutata: un punteggio totale positivo indica una possibile mail sospetta, mentre uno negativo suggerisce una mail legittima. In definitiva, MailHeader offre un’analisi notevolmente più completa e dettagliata, anche se a primo impatto può essere un poco soverchiante.

Analizzando l’esempio riportato nelle Figure 38 e 39, possiamo osservare che il dominio è ospitato su OVH e il server di destinazione si trova in Francia. Il primo elemento analizzato da questi strumenti è l’allineamento tra l’indirizzo email del destinatario e quello indicato nel campo Return-Path, poiché una discrepanza rappresenta il primo segnale di un possibile tentativo di phishing. La mail ha attraversato otto hop prima di essere consegnata alla cassetta postale, con tempi di transito quasi sempre istantanei. Il punteggio di spam è negativo (-3,698), indicando che la mail non presenta segnali sospetti. È inoltre importante verificare il campo della data per individuare eventuali anomalie temporali o segni di manomissione della mail.



Mail From:	noreply@cyberadmin.it	**Mail To:**	it@cyberadmin.it
Mail From Name:		**Reply To:**	

Message Details

Subject:	Test mail	**Content-Type:**	text/plain charset=US-ASCII
Date:	Fri, 03 Jan 2025 10:33:09 +0100	**UTC Date**	Fri Jan 3 09:33:09 2025
MessageID:			

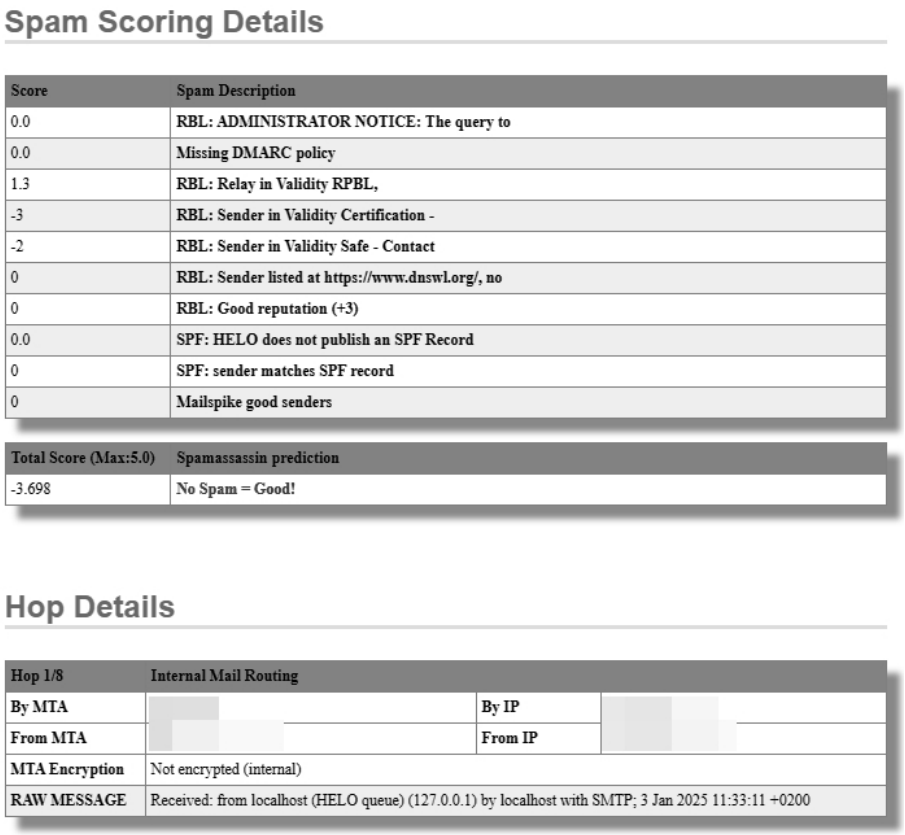
Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	cyberadmin.it	**Mail Server To:**	out28.mail.ovh.net
Mail Server From IP:		**Mail Server To IP:**	
Mail Country From:	Italy	**Mail Country To:**	France
AS Name From:	OVH SAS	**AS Name To:**	OVH SAS
AS Number From:	AS16276	**AS Number To:**	AS16276
Distance (All Hops/Summary):	362.19/994.00 KM	**Hops (All/Public):**	8 / 4
MTA Encryption	Poor (*)	**Delivery Time:**	NA
Your IP:		**Your GeoLoc:**	

Figura 39 - Risultato della scansione con MailHeader

Come avete appreso da questo capitolo, questi strumenti permettono di ricostruire in modo preciso e dettagliato la storia di un’email dalla sua origine alla sua destinazione. Ovviamente questi dettagli sono visibili solo lato destinatario, poiché l’header si popola durante il transito della mail stessa. Dal lato del mittente, se il server di posta è gestito internamente dall’azienda, è possibile consultare i log di invio per verificare se la mail è stata accettata o rifiutata in partenza, un’operazione che resta riservata agli amministratori di sistema.

Prima di concludere, è necessario sottolineare che quando si incollano gli header delle email in queste web app, sicure o meno che siano, si stanno condividendo informazioni potenzialmente sensibili con siti di terze parti. Gli header contengono infatti, oltre alle informazioni già esaminate, anche indirizzi IP locali delle infrastrutture di rete ed email di persone terze. Se doveste richiedere assistenza pubblica riguardo una determinata email, vi consiglio di anonimizzare e oscurare parti private e informazioni sensibili, come negli esempi mostrati finora. Per sapere poi come i vari siti gestiscono i vostri dati e le loro politiche di conservazione, potete consultare le Privacy Policy indicate per ciascuno a fondo pagina.



Spam Scoring Details

Score	Spam Description
0.0	RBL: ADMINISTRATOR NOTICE: The query to
0.0	Missing DMARC policy
1.3	RBL: Relay in Validity RPBL,
-3	RBL: Sender in Validity Certification -
-2	RBL: Sender in Validity Safe - Contact
0	RBL: Sender listed at https://www.dnswl.org/, no
0	RBL: Good reputation (+3)
0.0	SPF: HELO does not publish an SPF Record
0	SPF: sender matches SPF record
0	Mailspike good senders

Total Score (Max:5.0)	Spamassassin prediction
-3.698	No Spam = Good!

Hop Details

Hop 1/8	Internal Mail Routing		
By MTA		By IP	
From MTA		From IP	
MTA Encryption	Not encrypted (internal)		
RAW MESSAGE	Received: from localhost (HELO queue) (127.0.0.1) by localhost with SMTP; 3 Jan 2025 11:33:11 +0200		

Figura 40 - Risultato avanzato della scansione dell'header con MailHeader

Inoltre, nel caso di MXtoolbox ricordatevi di cliccare su "Dimentica record", sempre in fondo alla pagina dei risultati, per eliminare dal server i dati appena analizzati. Adesso che abbiamo tutte queste informazioni, come possiamo utilizzarle per comprendere se la mail che ci troviamo di fronte è, all'effettivo, una mail di phishing? Scopriamolo nei capitoli successivi.

15 RICONOSCERE IL PHISHING DAGLI INDIRIZZI MAIL

Il primo elemento da verificare è innanzitutto il nome visualizzato come mittente della mail e la sua corrispondenza con l'indirizzo email reale. Quando questi due elementi non sono allineati, ovvero quando il nome visualizzato mostra un dominio diverso da quello dell'indirizzo email reale o si presenta come totalmente alieno rispetto alla reale appartenenza, la probabilità di phishing aumenta notevolmente, senza però mai raggiungere il 100% di certezza. Esistono infatti casi legittimi di disallineamento, come nelle comunicazioni di marketing o di supporto dove, per evitare un sovraccarico dei server di posta primari, vengono utilizzati servizi esterni o indirizzi specifici all'uso. Un esempio chiarificatore è una mail di feedback che potrebbe presentarsi come "Assistenza Feedback" ma avere come indirizzo email noreply@dominio.it. Un utilizzo ampiamente diffuso e accettato, a condizione che i sistemisti del dominio di partenza abbiano configurato correttamente i loro server, in caso contrario la mail finirà in spam. Al di fuori di questi casi legittimi, un disallineamento indica quasi sempre un tentativo di phishing e può variare significativamente in base al grado di disallineamento.

Quando la mail presenta un nome casella e un dominio completamente diversi da quelli dichiarati, si parla di spoofing (dall'inglese "inganno"). Lo spoofing è una delle tecniche più diffuse nel phishing perché in assenza di efficaci filtri, sfrutta di base la ridotta attenzione degli utenti, un

fenomeno in costante crescita in tutte le fasce d'età. Chi si limita a leggere soltanto il nome visualizzato, senza verificare l'indirizzo email completo, diventa facilmente vittima dell'inganno. Ricordiamo infatti che il campo **Display From** nell'header è facilmente modificabile, mentre il campo **From**, che contiene l'indirizzo email effettivo, è più difficile da alterare.

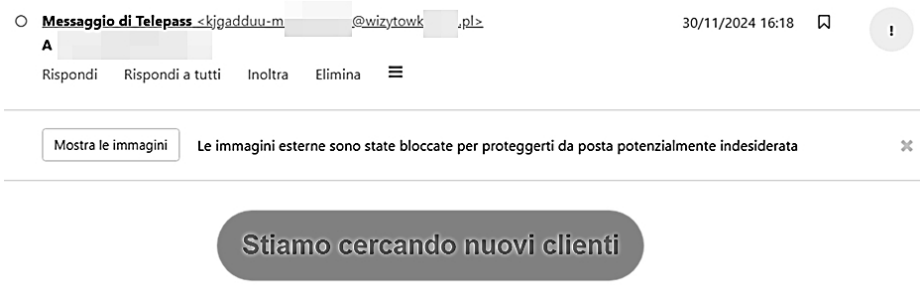


Figura 41 - Tentativo di phishing spacciandosi per Telepass

Se prendiamo in esame l'esempio mostrato in Figura 41, notiamo immediatamente che si tratta di una mail di phishing, dove il nome visualizzato è completamente diverso dall'indirizzo email reale. Quest'ultimo tra l'altro, non presenta nemmeno l'estensione di dominio italiana che ci si aspetta da un servizio nazionale. Per verificare l'indirizzo reale del mittente, è sufficiente passare il mouse sopra il nome del mittente oppure consultare la scheda "mostra dettagli", opzioni disponibili sia in Gmail che in Outlook.

È fondamentale anche verificare che il dominio di provenienza non sia camuffato attraverso il typosquatting, come abbiamo anticipato nel Capitolo 11, tecnica che cerca di ingannare la vittima modificando poche lettere del dominio con caratteri simili dell'alfabeto o dal set di caratteri ASCII. Per fare un esempio, guardate attentamente i domini che seguono:

https://www.google.com
https://www.goog1e.com
https://www.googlee.com
https://www.googlo.com
https://www.googlle.com
https://www.gogle.com

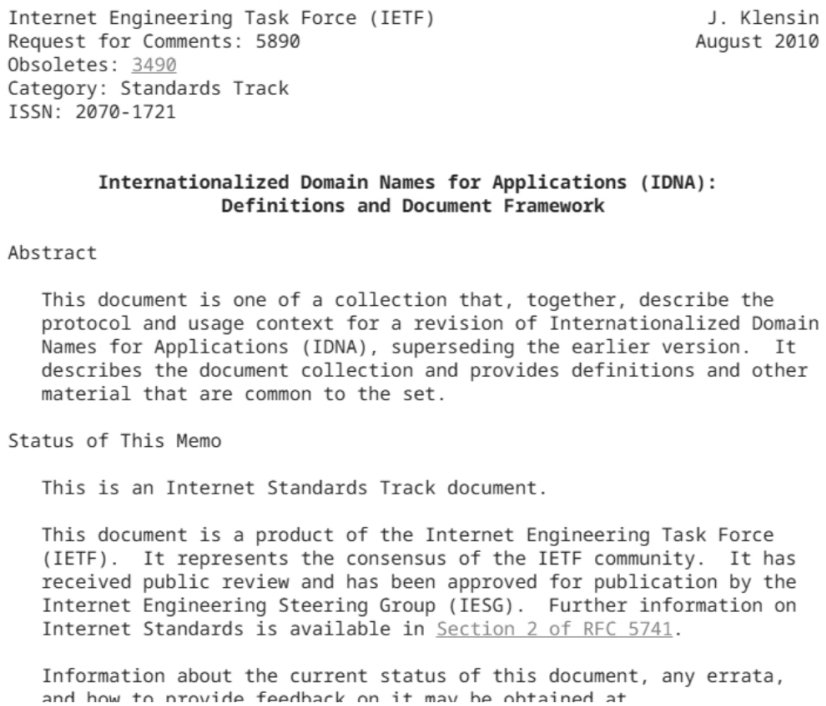
Solo il primo indirizzo è corretto, tutti gli altri sono probabili tentativi di typosquatting in cui una o più lettere sono state alterate, e che potrebbero

sfuggire a un occhio distratto di un utente abituato a cliccare rapidamente “Avanti” e “Ok” senza prestare davvero attenzione. Ecco un altro esempio:

https://www.microsoft.com
https://www.rnicrosoft.com

Questi due indirizzi potrebbero sembrare identici, ma non lo sono. Il primo è l’indirizzo corretto, mentre nel secondo la “m” di Microsoft è stata sostituita con “rn”, una “erre” seguita da una “enne”. È un esempio perfetto di typosquatting ingannevole.

Sebbene la RFC 3490 [11] stabilisse originariamente che i nomi di dominio potessero contenere soltanto caratteri ASCII standard, e chi è un frequentatore di Internet dagli albori sia magari rimasto legato a quella regola, la successiva RFC 5890 dell’agosto 2010 ha esteso ogni limitazione permettendo l’uso di lettere accentate e simboli di altre lingue direttamente nei nomi di dominio. Il tutto avviene attraverso un sistema chiamato punycode, che associa ai caratteri non ASCII non supportati da DNS una specifica combinazione di caratteri del set ASCII che, come noterete se vi capiterà di imbattervici, iniziano solitamente con il prefisso **xn--**.



Internet Engineering Task Force (IETF) J. Klensin
Request for Comments: 5890 August 2010
Obsoletes: 3490
Category: Standards Track
ISSN: 2070-1721

Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework

Abstract

This document is one of a collection that, together, describe the protocol and usage context for a revision of Internationalized Domain Names for Applications (IDNA), superseding the earlier version. It describes the document collection and provides definitions and other material that are common to the set.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at

Figura 42 - RFC 5890

Per fare un esempio, il dominio **cyberadmìn.it** diventa **xn--cyberadmn-d5a.it**. Tale conversione può verificarsi solo all'interno del nome di dominio o nei relativi sottodomini, mai nel dominio di primo livello (TLD), ovvero la parte dopo l'ultimo punto dell'indirizzo. Quindi **.it** rimarrà sempre **.it**. Questi domini sono chiamati "Internationalized Domain Name" o domini IDN. Senza entrare troppo nel dettaglio, vi basti sapere che come typosquatting oggi si rischiano anche attacchi omografici con caratteri speciali al posto di quelli dell'alfabeto più tradizionale. Per questo motivo diventa ancora una volta fondamentale verificare attentamente il dominio di provenienza. Va però notato che se anche tecnicamente non viene proibito il mischiare set di caratteri differenti all'interno dello stesso nome, come mescolare la "a" cirillica e la "a" latina, sono ampiamente diffuse policy restrittive per i TLD che ne impediscono la combinazione; cosa però non sempre garantita nel caso dei **.com**.

Esistono anche casi in cui i malintenzionati creano e registrano domini temporanei solo per la durata dell'attacco, configurati in modo che tutte le verifiche tra cui SPF, DKIM e DMARC risultino correttamente superate. Per apparire legittimi aggiungono parole, prefissi o suffissi nel nome del dominio, per simulare organizzazioni note o brand importanti, plasmando così nuovi nomi di dominio simili ma non ufficiali. Non è quindi sufficiente vedere la conferma di SPF superato per considerare una mail sicura, poiché chiunque può impostare record DNS corretti sul proprio dominio fraudolento.

Ritorniamo agli indirizzi mail di cui, grazie a quanto appreso nel capitolo precedente, possiamo esaminare il percorso concentrandoci sul server di partenza indicato in **Received** e sul valore di **Return-Path**. Come abbiamo già visto, ogni passaggio della mail attraverso un server aggiunge una nuova riga **Received** in cima all'header. La riga più in basso di conseguenza indica il primo server che ha gestito la mail, e dunque quello di partenza. Questo deve sempre corrispondere al dominio dichiarato dalla mail, eccetto nei casi già citati di servizi o marketing. E sebbene sia utile analizzare l'intera sequenza di hop, già il primo valore fornisce un chiaro indicatore dell'autenticità della mail. Arrivando poi al valore di **Return-Path**, che è l'indirizzo a cui i server inviano le notifiche di errori di recapito, deve invece essere sempre correlato al dominio indicato dalla

mail. Una discrepanza totale tra questo valore e il dominio dichiarato può indicare soltanto un tentativo di phishing o spoofing.

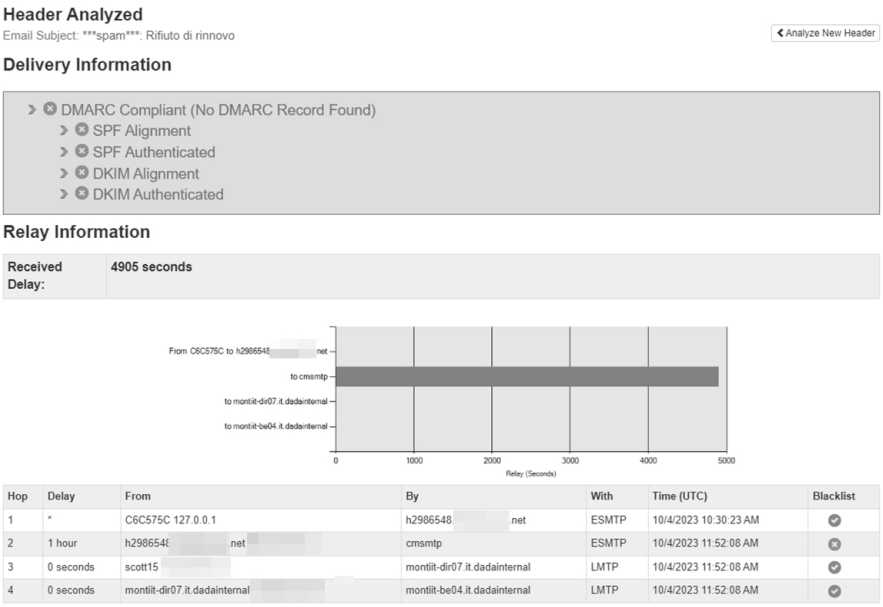


Figura 43 - Esempio di tentativo di phishing

Ho personalmente analizzato casi di spear phishing avanzato dove la mail era stata creata in modo impeccabile: la configurazione del server rispettava le più severe politiche antiphishing e antispam, il nome visualizzato corrispondeva perfettamente all'indirizzo mail dichiarato, e persino il percorso degli hop sembrava confermare l'autenticità della mail stessa. Tuttavia, l'indirizzo mail presente in **Return-path** era palesemente malevolo. È proprio attraverso le sottili discrepanze che si individuano i tentativi di spoofing. Questa semplice esperienza sul campo che vi ho riportato dimostra ancora una volta quanto sia necessario verificare tutti gli indirizzi e tutti i campi header presenti nella mail quando si notano segnali sospetti, per avere la certezza della sua legittimità prima di fare una qualsiasi operazione. Nei prossimi capitoli vedremo come una corretta configurazione di SPF, DKIM e DMARC possa ridurre il problema. Ridurre, non risolvere.

Riassumendo, per identificare un tentativo di phishing è necessario:

- verificare sempre l'indirizzo email effettivo del mittente, non limitandosi al nome visualizzato;

- controllare attentamente l’ortografia del dominio e la sua estensione di primo livello;
- digitare manualmente l’indirizzo verificato nel browser anziché cliccare su link sospetti, ma questo aspetto sarà approfondito nel capitolo 17;
- verificare, attraverso gli strumenti descritti nel capitolo precedente, l’allineamento tra il **Return-path** e il mittente dichiarato della mail.

16 RICONOSCERE IL PHISHING DAL TESTO

A differenza dei precedenti, questo capitolo sarà meno tecnico e più incentrato sull'analisi delle strategie comunicative utilizzate nelle mail di phishing, richiamando oltre al pensiero analitico anche le statistiche pubblicate da enti certificati e autorevoli. Perché nulla, in questi attacchi, è lasciato al caso. L'oggetto della mail così come il contenuto stesso rivestono un ruolo cruciale nell'identificazione di un tentativo di phishing, come abbiamo visto nel capitolo sulla psicologia degli attacchi. Secondo il rapporto del Computer Emergency Response Team (CERT) dell'AGID italiana per l'ultima settimana di dicembre 2024 e la prima di gennaio 2025 [12], i quattro temi principali utilizzati nelle campagne di phishing sono stati:

- consegne;
- banking;
- prenotazioni;
- pagamenti.

In questa fase non è importante identificare i brand specifici presi di mira dagli attacchi, anche se va notato che diventano essi stessi vittime quando i loro nomi sono sfruttati per rendere credibile il phishing, quanto osservare come il contesto storico si allinei perfettamente con la struttura e il contenuto stesso.

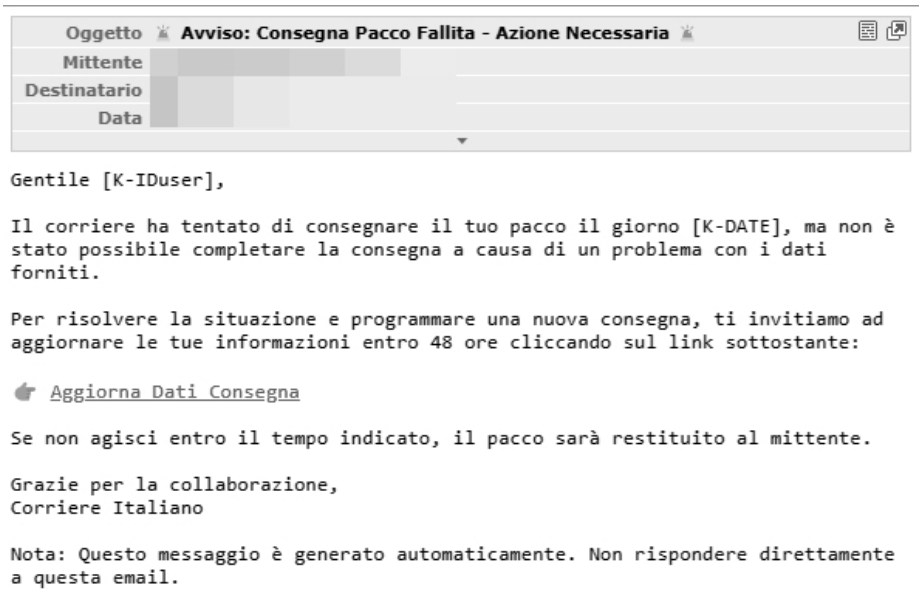


Figura 44 - Phishing in periodo festività

Non sorprende infatti che le esche riguardassero problemi di pagamento o di consegna, considerando i regali natalizi acquistati online e le prenotazioni alberghiere per le vacanze. Come riportato nella fonte citata, il periodo in esame ha visto anche un aumento delle campagne di smishing mirate a sottrarre dati personali e di pagamento, dove gli utenti venivano avvisati dell'impossibilità di consegnare un pacco e reindirizzati a un sito di phishing malevolo tramite un link presente negli SMS, che richiedeva di aggiornare le informazioni di consegna e di pagamento, mostrato in Figura 45. Analizzeremo poi nel capitolo 18 la forma del link presente in questo messaggio.

Terminato il periodo festivo, è probabile che le campagne di phishing si spostino dal contesto "delivery" a quello lavorativo, puntando sugli utenti che utilizzano le email professionali con richieste urgenti di aprire allegati o cliccare su link esterni legati a servizi come Microsoft, OneDrive e DocuSign.

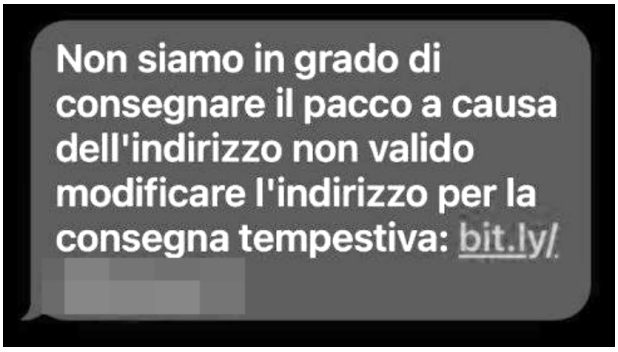


Figura 45 - Esempio di smishing reale

La pandemia di COVID-19 rappresenta un altro periodo storico spiacevole, significativo e di impatto per gli attacchi di phishing. Quando le aziende hanno dovuto attivare rapidamente il lavoro da remoto tra connessioni VPN e porte girate per il Remote Desktop, i criminali informatici hanno sfruttato la confusione e l'urgenza del momento, in particolare nella gestione delle VPN aziendali (perché le porte RDP non andrebbero mai girate sull'esterno). Gli hacker hanno infatti approfittato della situazione inviando email di phishing che richiedevano di verificare o aggiornare le credenziali VPN o di posta elettronica come in Figura 46, spingendo così le vittime a rivelare dati sensibili e scaricare malware.

Come avrete oramai memorizzato, la maggior parte il phishing si basa su parole e frasi progettate per creare un senso di urgenza nel destinatario. Questo induce uno stato di stress che attiva il meccanismo "combatti o scappa", teoria sviluppata da Walter Bradford Cannon nei primi anni del Novecento e già accennato nel capitolo intitolato "La psicologia dietro il phishing", che descrive l'istinto di sopravvivenza ereditato dai nostri antenati quando si trovavano di fronte a un pericolo imminente: le uniche opzioni erano combattere o fuggire. Per le nostre generazioni è mutato in un pericolo digitalizzato, e vero pilastro su cui il phishing fa affidamento. Comprendere come manipola la nostra psicologia ci permette di riconoscerlo e difenderci efficacemente da questi attacchi.

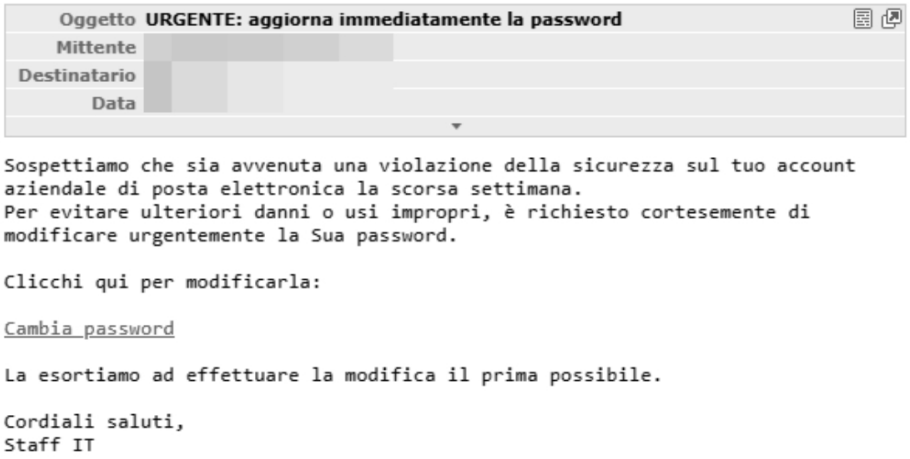


Figura 46 - Phishing in periodo lavorativo

Esistono poi anche situazioni opposte, dove non è necessario ricercare strategie avanzate: basta leggere attentamente il contenuto per individuare gravi errori grammaticali o incongruenze logiche. Questo accade perché spesso l'email di phishing, anziché essere creata da zero, è un collage di diverse mail legittime. Solo che per riconoscere questi errori è necessaria una buona padronanza della lingua in cui sono scritte e se, come succede, molti attacchi provengono dall'estero. dove l'italiano non è conosciuto o parlato correttamente, si crea per nostra fortuna una stortura riconoscibile.

Da menzionare anche le email di phishing composte principalmente da immagini. In questi casi, anche quando sembra essere presente del testo, si tratta in realtà di un'immagine prelevata da un'altra email. Questa tecnica permette di eludere i controlli sul contenuto, poiché per analizzare il testo presente nell'immagine sarebbe necessario un software OCR di cui i filtri antispam e antiphishing sono privi. Sebbene questo scenario sia sempre meno frequente, è importante citarlo per completezza.

17 RICONOSCERE IL PHISHING DAI LINK

L’ultima e più importante modalità per riconoscere il phishing è la presenza di link malevoli nelle email, dove nel capitolo successivo analizzeremo gli strumenti online gratuiti per approfondire anche questo aspetto. In questo contesto, la regola principe per salvaguardare la propria sicurezza è semplice: “prima di cliccare, pensa e osserva”. Osserva gli indirizzi mail, osserva il contenuto e osserva anche i collegamenti nel dettaglio. Sebbene i link siano spesso personalizzati per apparire il più verosimili possibile, dalla mia diretta esperienza posso dire che, molto più frequentemente di quanto si pensi, presentano caratteristiche evidenti che ne rivelano sin da subito l’illegittimità, anche a una rapida occhiata. Adesso analizzeremo un link di esempio scomponendolo nelle sue parti. Nota bene: qualora il link dovesse risultare attivo si tratta di una coincidenza non intenzionale. I nomi utilizzati sono puramente di fantasia e una ricerca su Google non ha prodotto risultati che possano far pensare che l’esempio corrisponda a una realtà veramente esistente.

Ipotizziamo ci arrivi una mail che, analizzando header e contenuto, non abbiamo ancora determinato con certezza se sia una mail di phishing oppure legittima. In una realtà dove esiste un presunto istituto bancario dal nome “Intesa San Marco”, il messaggio ci richiede di eseguire alcune operazioni sul nostro conto corrente aziendale a causa di un problema nel sistema di pagamento, da risolvere tramite il servizio di assistenza. Una situazione poco plausibile, ma abbastanza realistica. L’URL del link presente all’interno della mail è:

https://fatture.comunicazionibanca.intesasanmarco.it.cyberadmin.it

estrapolato da Figura 47.

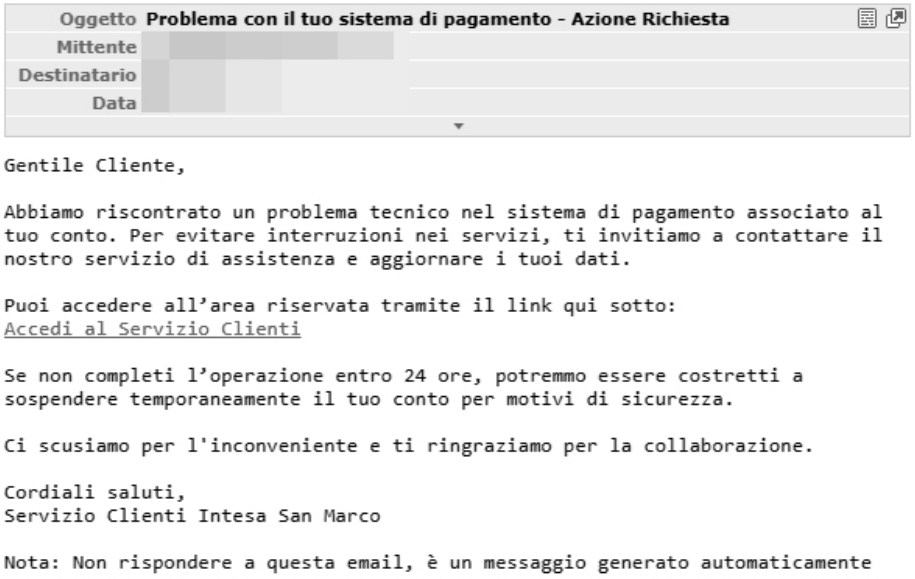


Figura 47 - Esempio di phishing bancario

Una funzionalità standard di qualsiasi applicativo o browser mail è quella di mostrare l'indirizzo completo dei collegamenti solo quando vi si passa sopra con il cursore del mouse, senza cliccare. Un dettaglio ovvio, ma doveroso da sottolineare, visibile in Figura 48.

Il link sopra riportato, nonostante a prima vista possa sembrare coerente con una richiesta di verifica di pagamento da parte dell'ente bancario citato, non ha nulla a che vedere con esso.

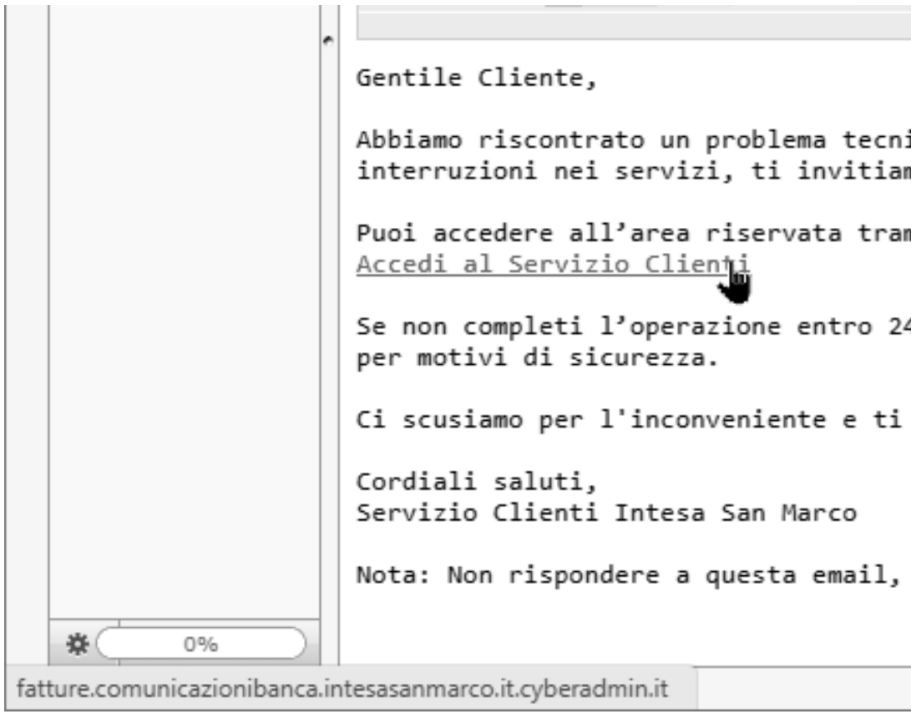


Figura 48 - Mouse over link

Per analizzare correttamente un indirizzo URL serve leggerlo partendo dal dominio di primo livello, cioè da destra verso sinistra, come la lettura orientale (utilizzata nei romanzi giapponesi o nei manga, per intenderci). Il risultato è:

.it rappresenta il Top-Level Domain (TLD), il livello più alto nella gerarchia DNS, che in questo caso è un "country code" ovvero il codice nazione assegnato all'Italia;

.cyberadmin è il Second-Level Domain (SLD), cioè la parte del dominio che identifica l'organizzazione o l'entità che lo ha registrato.

L'insieme di TLD e SLD, ovvero l'indirizzo **cyberadmin.it**, rappresenta ciò che comunemente viene chiamato "dominio internet". Tutto quello che viene prima, indipendentemente dalla punteggiatura, e nell'esempio

fatture.comunicazionibanca.intesasanpaolo.it

altro non è che una sequenza di sottodomini a più livelli concatenati tra loro. Se l'utente legge erroneamente l'indirizzo URL da sinistra verso destra, notate come il contesto appaia estremamente differente.

Il buon senso ci raccomanda inoltre che se una mail ha come presunto mittente un ente bancario, o un altro qualsiasi istituto, azienda o persona, è difficile pensare che un'operazione delicata sia innanzitutto demandata via mail e rimandi a domini che non hanno alcuna correlazione con l'entità reale. Ha senso che Poste Italiane, per fare un esempio con uno spedizioniere sul nostro territorio, vi chieda via email dati che già possiede in anagrafica, inclusi quelli della vostra carta di credito, attraverso un indirizzo web che inizia con **https://xyz-eccetera**? Ovviamente no.

E se siete in dubbio, piuttosto aprite una nuova sessione del browser e scrivete manualmente, o cercate tramite motore di ricerca fidato, il sito web in questione. Non cliccate sul link della mail. Sono stati riportati anche casi dove il link malevolo, invece di essere presente esclusivamente nel corpo della mail che si presentava volutamente come una comunicazione di marketing al limite dello spam, era posizionato intelligentemente sull'opzione dedicata al disiscriversi dalle future comunicazioni.

Conoscere come leggere correttamente un URL ci può salvare da ogni phishing? No, perché gli attaccanti utilizzano diversi stratagemmi per mascherare la destinazione finale dei link: dalle catene di collegamenti concatenati, utili anche per aggirare le verifiche automatiche degli antivirus, fino all'uso dei servizi di URL shortener. Con questi ultimi, qualsiasi utente può accorciare e personalizzare un indirizzo URL, rendendolo completamente illeggibile. Anche i QR code, ormai noti a tutti, vengono sfruttati per scopi di phishing. Fortunatamente, come accennavo prima, esistono strumenti che analizzano l'intera catena di collegamenti senza dover interagirvi, rivelando sia l'URL finale che tutti i dettagli del dominio di destinazione. Uno tra tutti è VirusTotal.

18 URL SHORTENER E QR CODE

I servizi di URL shortener e di generazione QR code, nonostante le loro diverse forme e funzionalità, condividono un obiettivo comune nella comunicazione digitale: trasformare un'informazione estesa in qualcosa di più maneggevole. E se nell'uso quotidiano rappresentano due strumenti distinti, all'interno di una mail di phishing svolgono lo stesso ruolo: impedire all'utente finale di conoscere l'URL di destinazione senza prima interagirvi. Esaminiamoli brevemente entrambi.

Gli URL shortener sono servizi online generalmente gratuiti che convertono un indirizzo, indipendentemente dalla sua forma, lunghezza o destinazione in una variante più corta, associata al dominio del servizio stesso. Riprendendo nuovamente l'esempio discusso nel capitolo precedente, dato in input:

https://fatture.comunicazionibanca.intesasanmarco.it.cyberadmin.it

in uno dei primi servizi gratuiti risultati da una ricerca su Google, otteniamo:

https://tinyurl.com/esempio1001

Risulta subito evidente che, mentre nel primo caso l'URL rivelava chiaramente la sua destinazione, nel secondo caso è impossibile conoscerla in anticipo complicando così sia la verifica da parte dell'utente sia l'analisi dell'antivirus, che senza interazione non può rilevare la destinazione malevola. Ogni servizio di URL shortener ha poi un proprio

formato standard per abbreviare gli URL e spesso offrono anche la possibilità di personalizzare la parte che segue il dominio del servizio, esattamente come nell'esempio sopra riportato.

I Quick Response Code, o più comunemente conosciuti come QR code, sono un'evoluzione dei tradizionali codici a barre presenti sui prodotti in commercio e consentono di memorizzare molte più informazioni. Inventati nel 1994 da Masahiro Hara mentre osservava la scacchiera di una partita a Go, hanno visto una vera diffusione nell'utilizzo quotidiano solo negli ultimi anni, fino a diventare comune trovarli come mezzo per leggere il menu del ristorante o nei biglietti da visita. Tuttavia presentano un rischio intrinseco: il loro contenuto non è leggibile direttamente dall'essere umano.

Figura 49 - Esempio di QRcode

Prendendo ancora una volta l'URL di esempio, il QR code che otteniamo come risultato è mostrato in Figura 49 e come si può notare è impossibile decifrarne il contenuto a occhio nudo. Dobbiamo quindi evitare di interagire con queste due tipologie di informazione? La risposta è ovviamente no. Sono entrambi strumenti validi ed estremamente utili nella società contemporanea.

È però fondamentale valutare sempre il contesto in cui questi si presentano e considerare la probabilità e il rischio di contraffazione: un QR code adesivo incollato sopra quello legittimo in un parcheggio incustodito per il pagamento della sosta rappresenta un rischio di phishing maggiore rispetto a quello presente sul tavolo di una trattoria per consultare il menu. E badate bene che l'esempio del parcheggio non è

casuale: si tratta di uno scenario tanto semplice quanto efficace che ha già portato al successo diversi attacchi di phishing nel mondo reale.

19 VIRUS TOTAL, MITRE ATT&CK E ALTRI STRUMENTI DI DIFESA

Mentre gli attacchi di phishing diventano ogni giorno più sofisticati, fortunatamente anche gli strumenti di difesa a disposizione degli utenti si sono evoluti, diventando più semplici da usare e completi nelle loro funzionalità. Dopo aver imparato a esaminare gli header delle mail e a distinguere il phishing dallo spam attraverso l'analisi degli indirizzi mail, il testo contenuto nel body e dagli allegati sospetti, l'ultimo tassello che ci rimane è comprendere come analizzarne i link in modo sicuro e, soprattutto, senza interagirvi direttamente, evitando così di esporre il vostro dispositivo e i vostri utenti ai pericoli del web.

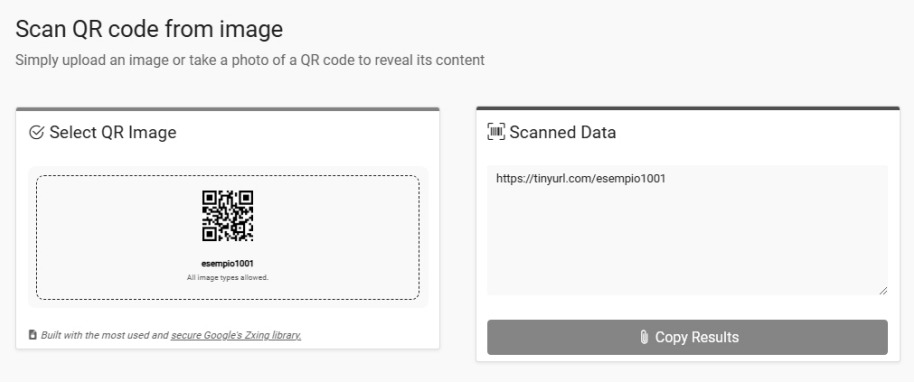


Figura 50 - Conversione QRcode con scanqr.org

Partiamo proprio dai QR code, che rappresentano l'esempio perfetto di informazione digitale non interpretabile senza l'uso di strumenti terzi.

Supponiamo di ricevere una email al cui interno è presente un QR code sospetto, come possiamo verificarne la destinazione? Il metodo più semplice è utilizzare **scanqr.org**, un servizio online di conversione: caricando l'immagine del QR code o il suo link stesso, nel caso questo fosse stato condiviso sul web, il servizio visualizzerà sulla destra l'URL completo di destinazione. Esattamente ciò che ci serve.

Dopodiché ci viene in aiuto VirusTotal, una piattaforma di cybersecurity gratuita che analizza file e URL sospetti. Acquisita da Google nel 2012, combina molteplici motori di antivirus e scanner malware per generare un report dettagliato, dove indica se un elemento è effettivamente legittimo o meno.

Figura 51 - Homepage di Virustotal

La sua seconda caratteristica più importante è la capacità di eseguire un'analisi comportamentale, testando il contenuto in un ambiente protetto detto sandbox per rilevare con precisione eventuali minacce. Raggiungibile all'indirizzo **https://www.virustotal.com** si presenta con un'interfaccia semplice simile a quella del più noto motore di ricerca Google. Per verificare un URL, occorre selezionare l'opzione corrispondente nella barra superiore e incollare l'indirizzo nell'apposito campo. Il sistema fa molto affidamento anche sul contributo della community: è quindi normale ottenere un risultato quasi istantaneo. VirusTotal, infatti, conserva un identificativo hash di tutte le analisi

effettuate, ottimizzando così sia le risorse operative che i tempi di risposta. Se qualcun altro ha già analizzato lo stesso URL o file, il risultato apparirà immediatamente.

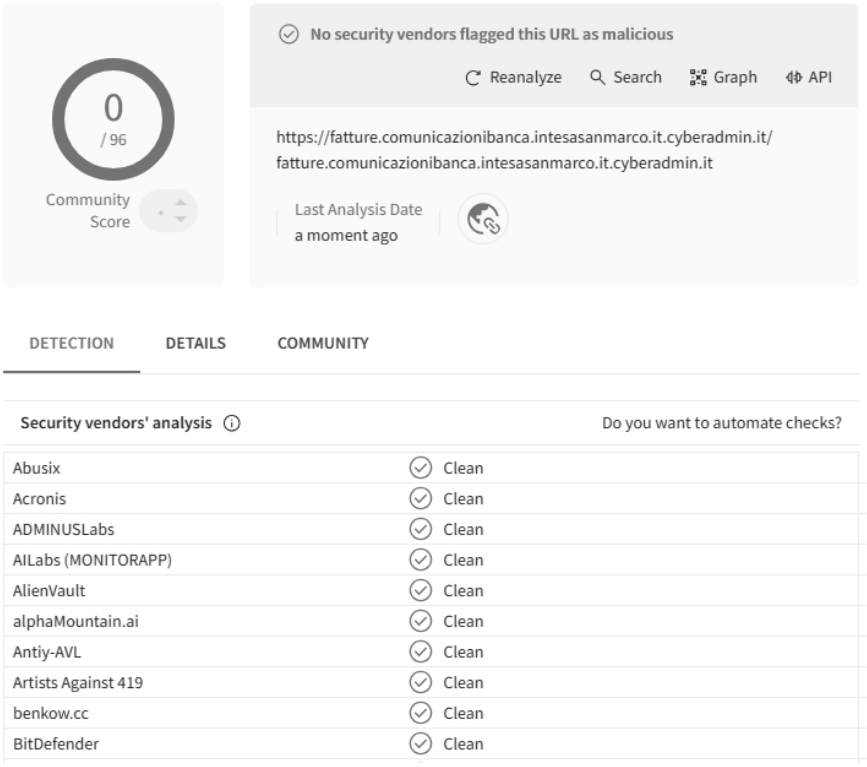


Figura 52 - Una scansione pulita

Diamo la definizione di hash: una stringa di caratteri generata come risultato di un algoritmo matematico che rappresenta in modo univoco un dato input. Funziona come un'impronta digitale, e anche una minima modifica al contenuto genera un hash completamente diverso. Un esempio di hash molto utilizzato nell'informatica è il MD5, o Message Digest 5, comunemente impiegato per verificare l'integrità dei file sui server e durante i download, risultando un hash di 32 caratteri esadecimali o 128 bit, a partire da un input di qualsiasi dimensione. In questo modo è possibile determinare con certezza se una qualsiasi entità sia stata manomessa. Per dare un esempio, la parola phishing genera come hash **e2d8c3deed3780c4a97b75ed5acffede** mentre Phishing genera **98fb02e956dcdd87fff88cbea5ec5e58**. Vedete che già una semplice lettera modificata da minuscola a maiuscola cambia inequivocabilmente l'hash risultante.

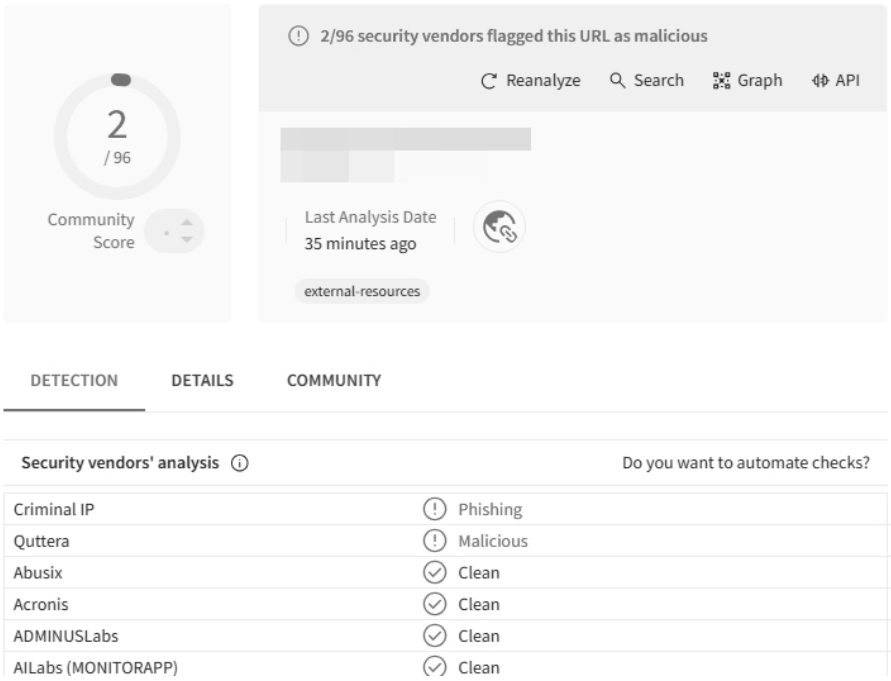


Figura 53 - Una scansione malevola

Se invece desiderate che venga effettuata una nuova analisi completa, ignorando i valori in cache, cliccate su “Reanalyze” per richiedere una nuova scansione, ma in questo caso dovrete armarvi di pazienza. Se la scansione non rileva elementi malevoli, la pagina dei risultati si colorerà di verde, e il punteggio di rischio virus resterà ancorato sullo zero di novantasei punti massimi, come mostrato in Figura 52. In caso contrario, la pagina mostrerà risultati arancioni e rossi di diversa gravità in base al contenuto rilevato, e il punteggio aumenterà di conseguenza, visibile in Figura 53.

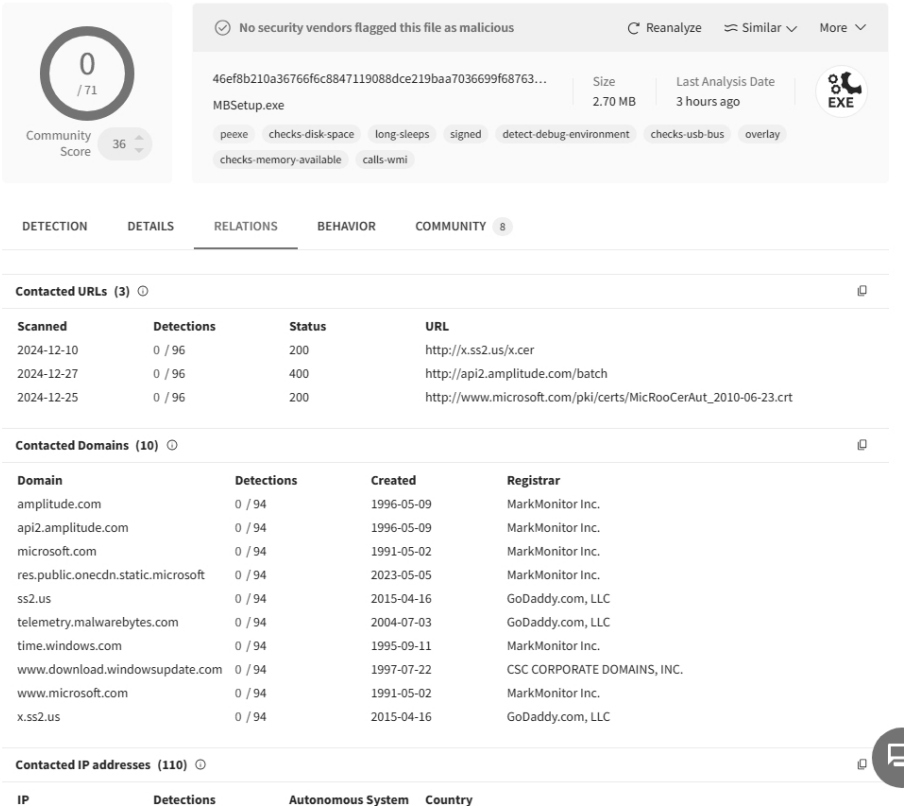


Figura 54 - Analisi file, scheda Relations

All’interno della pagina risultati, due sono le aree di principale interesse:

- “Detection”, che mostra il riepilogo della scansione tra punteggio totale e valutazione dei singoli strumenti di analisi, tra cui nomi importanti come Bitdefender, Sophos e Kaspersky.

- “Details”, che elenca una serie di dettagli cruciali, tra cui l’indirizzo di destinazione finale della catena di link in “Final URL”, quando è stata la prima scansione su quell’elemento nella storia del servizio in “History”, l’IP pubblico che ha risposto alla richiesta web in “Serving IP Address”, e l’elenco dei valori degli “Headers” come il nome del sito, le date di pubblicazione e aggiornamento, il motore di gestione, la descrizione e la lingua utilizzata.

Se è vero che possono verificarsi dei falsi positivi, specialmente nel caso degli URL abbreviati, quando più vendor segnalano una possibilità, con

un’indicazione rossa di malware o arancione di phishing, è molto probabile che l’elemento analizzato sia effettivamente malevolo. Prestate perciò attenzione.

Abbiamo già parlato di come VirusTotal permetta anche l’upload di file ed eseguibili dal proprio dispositivo, seguendo le stesse modalità di analisi viste in precedenza. Troverete due aggiunte. Saranno infatti a disposizione dell’utente due nuove aree di interesse:

- “Relations”, vedi Figura 54, mostra dettagli estremamente interessanti sugli indirizzi IP pubblici, gli URL relativi e i domini di terze parti richiamati dal file in apertura; i file figli generati nel caso di un eseguibile e la lista di file scaricati direttamente sul dispositivo con un relativo grafico concettuale di facile lettura;

- “Behavior”, mostra invece il comportamento del file o applicazione quando questo viene eseguito nella sandbox protetta di VirusTotal, descrivendo ogni fase delle sue azioni secondo il framework MITRE ATT&CK, standard riconosciuto a livello mondiale per l’analisi delle fasi di una minaccia. Si ottiene così la lista dei processi, delle chiavi di registro modificate, dei pacchetti di codice scaricato presso quale indirizzo Internet, i comandi eseguiti e quali servizi messi in esecuzione.

Occorre dedicare qualche parola sul MITRE ATT&CK [13], dove lo schema è riportato in Figura 55. E anche se l’argomento può sembrare inizialmente complesso, ne esamineremo soltanto gli aspetti fondamentali in modo semplice e chiaro.

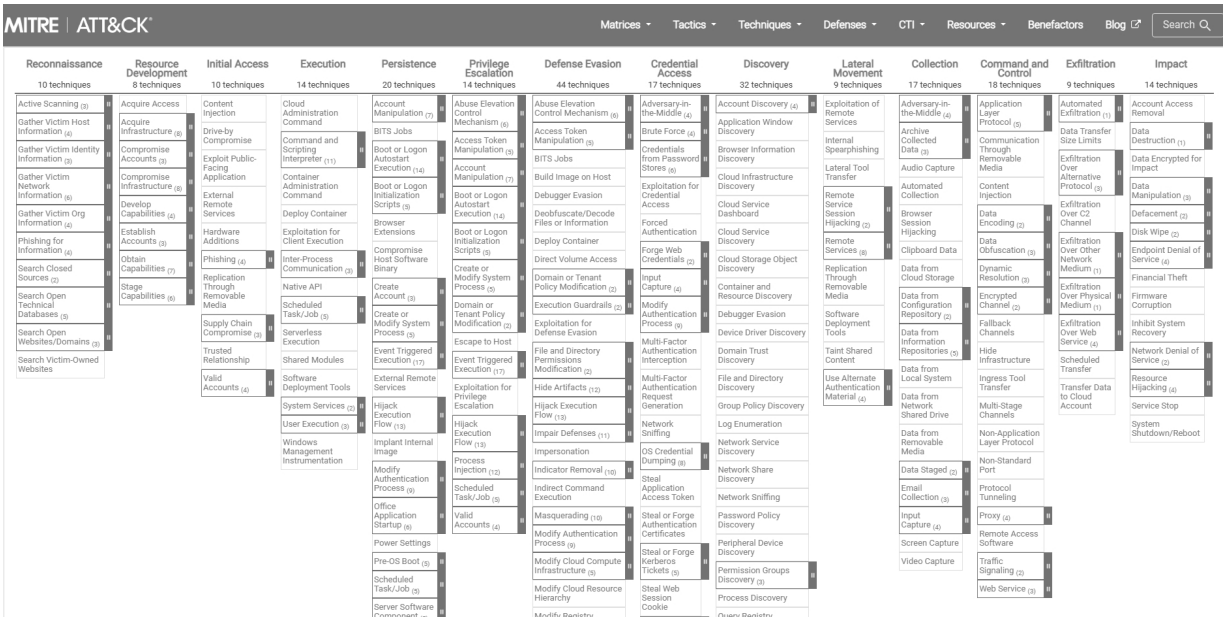


Figura 55 - MITRE ATT&CK Framework

La MITRE Corporation è una organizzazione senza scopo di lucro fondata nel 1958 e dedicata alla ricerca e sviluppo in ambito tecnologico, ed è conosciuta appunto per il suo ATTA&CK Framework. Acronimo di Adversarial Tactics, Techniques and Common Knowledge. Fornisce una mappa dettagliata delle tattiche, tecniche e procedure utilizzate dai threat actor durante le fasi di un attacco, dividendole in categorie aggiornate regolarmente, offrendo un quadro completo e in continua evoluzione delle minacce legate alla cybersecurity, e in particolare a quelle che potenzialmente mirano al settore di riferimento dell'individuo o dell'azienda. È proprio analizzando le tattiche e le tecniche tipicamente utilizzate dagli attaccanti che le aziende possono valutare l'impatto delle minacce sui propri sistemi di difesa e pianificare contromisure mirate per colmare tutte le vulnerabilità identificate. Le tattiche rappresentano il motivo o la finalità di una determinata azione. Le tecniche illustrano il metodo con cui l'obiettivo viene conseguito attraverso tale azione. Per semplificare, la tattica spiega perché l'attaccante desidera ottenere delle credenziali, mentre le tecniche descrivono i vari modi in cui le credenziali possono essere sottratte. Le informazioni ottenute sono estremamente complesse e la loro analisi è raccomandata solo agli esperti del settore. Per tutti gli altri utenti è sufficiente considerare il punteggio globale mostrato da Virus Total e agire di conseguenza.

Figura 56 - URL2PNG

Esistono inoltre altri diversi strumenti decisamente utili, che elencherò in una lista non esaustiva e non ordinata per importanza:

- **url2png.com**, permette di creare uno screenshot dell'indirizzo web indicato, consentendo di visualizzare il contenuto come immagine in totale sicurezza, visibile in Figura 56;

- **urlvoid.com**, verifica la reputazione di un dominio internet attraverso diverse fonti di cybersecurity e blacklist, fornendo una panoramica completa sulla sicurezza del sito, inclusi registrante e altre informazioni tecniche;

- **phishtank.org**, una piattaforma basata sulla community che permette agli utenti di segnalare e verificare tentativi di phishing, mantenendo un database aggiornato e accessibile a tutti;

- **checkshorturl.com**, strumento specifico per l'analisi degli URL abbreviati che ne mostra il formato originale completo e fornisce uno screenshot del sito di destinazione;

- **hybrid-analysis.com**, esamina nel dettaglio il comportamento di file caricati attraverso analisi statiche e dinamiche, fornendo così informazioni approfondite sulle potenziali minacce negli allegati delle email;

- **opentip.kaspersky.com**, consente di caricare file sospetti e fornisce una valutazione dettagliata della loro sicurezza attraverso l'uso combinato di tecnologie antivirus avanzate e analisi comportamentale;
- **urlscan.io**, esegue una scansione completa del sito web, catturando screenshot e monitorando le richieste di rete analizzandone i pacchetti transitati.

Il mio consiglio è di usarli a seconda della situazione.

20 SMISHING E VISHING

Oggi portiamo in tasca un vero e proprio computer portatile, qualcosa di impensabile fino a 18 anni fa, prima del lancio del primo iPhone. Gli smartphone non si limitano più a semplici interazioni vocali o brevi messaggi, ma permettono operazioni complesse e, aspetto molto interessante per chi si cela dietro il phishing, transazioni finanziarie. Sono così diventati un bersaglio sempre più frequente di attacchi, con varianti di malware e ransomware create appositamente per i due sistemi operativi principali: Android e iOS. Tralasciando il phishing via mail, di cui gli smartphone sono anch'essi vittima, concentriamoci sulle due operazioni principali che un telefono offre: chiamare e mandare messaggi. Queste due modalità di comunicazione portano a due diversi tipi di attacchi: smishing e vishing.

Lo smishing è la combinazione dei termini "short message service", che conoscete tutti con il diminutivo SMS, e "phishing", e come è facile intuire è la forma di phishing che avviene tramite messaggi di testo. Generalmente ne esistono di due tipi: quello che punta a instaurare una conversazione con la vittima e quello che lo reindirizza subito verso un sito malevolo. Nel primo caso si svolge principalmente attraverso applicazioni di messaggistica istantanea quali WhatsApp e Telegram, ma anche Instagram, Facebook e Linkedin. I truffatori creano un profilo falso o ne rubano uno esistente attraverso le modalità già descritte nei precedenti capitoli e prendono di mira tutti i contatti collegati al profilo compromesso. Avviano così conversazioni in cui, attraverso affinate tecniche manipolative, una persona fisica o un programma con risposte preconfigurate automatiche cercano di convincere il malcapitato a compiere determinate azioni sul proprio dispositivo, dalla procedura di

recupero password, richiedendo il codice PIN e condividendolo poi nella chat, all'invio di documenti e dati sensibili grazie a false promesse di colloqui di lavoro o guadagni facili. E una volta ottenuto illegalmente l'accesso al nuovo account della vittima, che nel frattempo viene completamente tagliata fuori, il ciclo si ripete nuovamente su tutti i contatti presenti. Un esempio reale è mostrato in Figura 57.

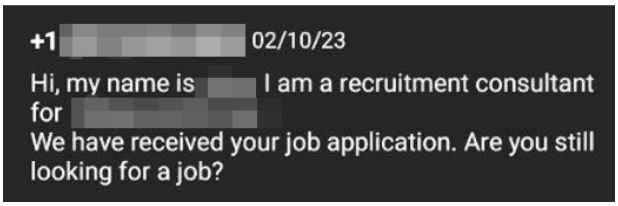


Figura 57 - Smishing con interazione diretta

Nel secondo caso invece la comunicazione è asincrona e non c'è un monitoraggio diretto dell'interazione tra vittima e l'esca, rendendo questa forma molto simile al phishing tradizionale via email. L'SMS contiene di solito un messaggio che comunica, come oramai sapete bene, un'urgenza e include un link verso siti esterni per risolvere il presunto problema. Naturalmente la pagina web di destinazione non ha nulla a che fare con quella legittima, e richiede l'inserimento di informazioni personali e dati di pagamento. Altro esempio reale in Figura 58.

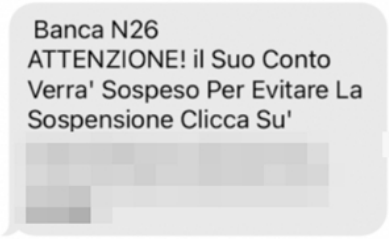


Figura 58 - Smishing con link esterno

Contesti plausibili di queste truffe sono:

- messaggi di testo provenienti da enti bancari o exchange di criptovalute che avvisano movimenti sospetti o verifiche necessarie;

- comunicazioni da parte di enti governativi per presunte multe o tasse non riscosse, oltre che documentazione in scadenza da aggiornare per non incorrere in sanzioni;

- avvisi di impossibilità di consegna pacchi o ordini online, per le motivazioni più disparate, dal mancato pagamento della dogana all'utente non presente della destinazione indicata;

- supporto di assistenza clienti che si offrono di risolvere un problema di blocco o disattivazione dell'account;

- conferme di ordini o fatture con importi solitamente importanti e di cui viene concessa l'opzione di annullare l'ordine tramite link;

- fingersi un figlio o una figlia e, sostenendo che il proprio telefono si sia rotto, chiedere di continuare la conversazione su una nuova chat spacciata per "il numero di un amico".

Spesso questi attacchi sfruttano la funzionalità di raggruppamento degli SMS da parte degli smartphone, nata per facilitare la lettura agli utenti. In questo modo i messaggi di phishing finiscono per inserirsi nella stessa conversazione dei messaggi legittimi ricevuti in precedenza. Per difendersi dalla maggior parte dello smishing via SMS tradizionali è sufficiente possedere uno smartphone Android e abilitare l'opzione di protezione dentro le impostazioni dell'app messaggi. Diverso è il caso delle app di messaggistica istantanea, dove oltre ai sistemi di protezione integrati nelle app stesse, la sicurezza dipende principalmente dall'utente. Occorre quindi prestare estrema attenzione ai messaggi sospetti, sia essi provengano da contatti sconosciuti, sia da quelli abituali.

Il lettore inoltre deve essere poi informato di due ulteriori gravi rischi legati al phishing attivi sugli smartphone:

- installare sui propri dispositivi app che non provengono da store ufficiali aumenta esponenzialmente la probabilità di installare anche virus nascosti al loro interno [14]. Stiamo parlando di file .IPA nel caso di iPhone e file .APK nel caso di Android. Per diventarne vulnerabili occorre attivare un'opzione che nasce disabilitata di default su tutti i

dispositivi, e che senza l’azione manuale da parte dell’utente non può essere manomessa. Figura 59 mostra quale;

- utilizzare dispositivi non aggiornati sia di versione che di sistema operativo e patch di sicurezza può portare a diventare inconsapevolmente vittima di vulnerabilità conosciute che permettono agli attaccanti di infettare i dispositivi senza la necessità di coinvolgere l’utente, semplicemente inviando un messaggio personalizzato autoinstallante o inducendolo ad aprire un sito web accuratamente preparato [15].

Figura 59 - Opzione da mantenere sempre disabilitata

Nonostante sia sempre meno comune, è altrettanto pericolosa la tecnica che sfrutta documenti o fogli di calcolo condivisi tramite Google Docs. La vittima riceve un link di accesso con permessi di lettura e scrittura per un documento che, una volta aperto, contiene una macro malevola che scarica automaticamente malware sul dispositivo.

Quando invece il phishing avviene attraverso una telefonata prende il nome di vishing, che deriva dall’unione delle parole “voice” e “phishing”. Vengono impiegati per l’attacco numeri contraffatti o servizi che rendono disponibili numeri temporanei e, grazie a tecniche di social engineering e software per alterare la voce, i criminali riescono a raggirare e ingannare

le vittime portandole a collaborare: da piccole richieste fino a rubarne i dati personali e denaro nei conti correnti.

Questa tipologia di attacco mette in atto anche:

- robocalls o chiamate automatiche, con messaggi preregistrati per convincere gli utenti a restare in linea;

- software di teleassistenza per qualsiasi dispositivo, esso sia uno smartphone o computer, attraverso cui i truffatori ne assumono il completo controllo. In questi casi viene richiesto all'utente di fornire al telefono un identificativo e una password necessarie al collegamento.

In questi casi il fattore psicologico è cruciale e, come già approfondito nel relativo capitolo, costituisce la base fondante su cui viene costruito l'attacco e la conquista della fiducia della vittima. Come accade per i messaggi, anche per le chiamate il sistema operativo Android offre un filtro antiphishing già integrato che blocca automaticamente le chiamate sospette prima ancora che il telefono squilli. Esempio di questa funzionalità è mostrata in Figura 60, da attivare nelle impostazioni dell'app Telefono.

Entrambe le varianti poi sono soggette allo spoofing: il truffatore può infatti nascondere il suo reale numero telefonico, ingannando il dispositivo della vittima, sia tramite tecniche di hacking, sia con l'utilizzo di servizi terzi o telefoni con SIM usa e getta. E in questo caso si aggiunge una terza tecnica comunemente definita "ping calls": il truffatore effettua uno squillo e attende che sia la vittima stessa a richiamare, trasformando così l'attacco in vishing attivo.

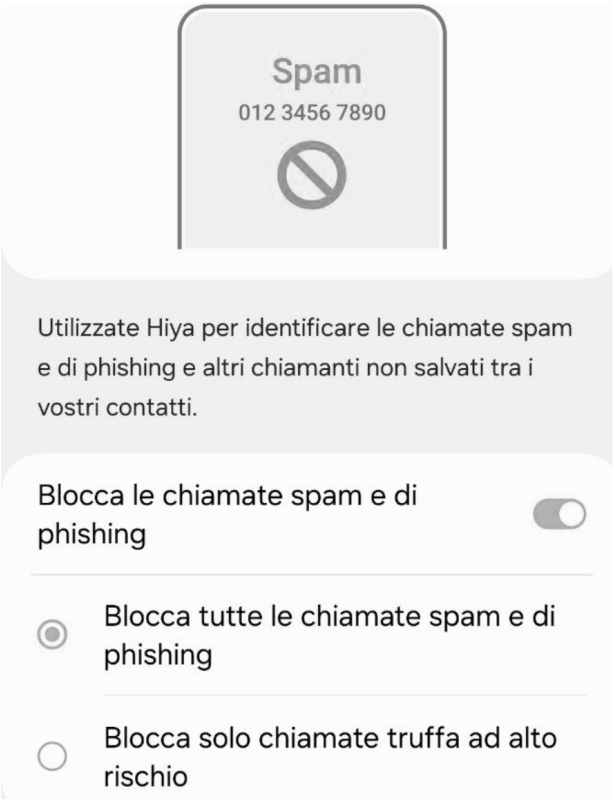


Figura 60 - ID chiamante e protezione spam

Il consiglio principale resta quello di non farsi trascinare dall'emotività, mantenete la mente lucida e il sangue freddo, valutando attentamente il contesto e le richieste che vi vengono fatte. Ricordate che nessuno mai vi chiederà il PIN o i numeri della carta di credito, specialmente al telefono.

21 PHISHING TRAMITE BROWSER

Sul confine con gli Adware, abbreviazione di “advertising-supported software”, troviamo una tipologia di sfruttamento delle funzionalità dei browser ben consolidata che, per un utente comune, risulta erroneamente difficile da liberarsene.

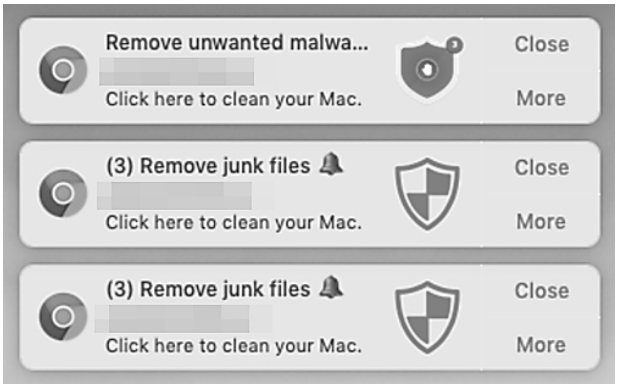


Figura 61 - Notifiche di sistema sfruttate come phishing

Durante la navigazione su un sito web, anche apparentemente legittimo, può apparire una richiesta di abilitare le notifiche per quel dominio specifico così da restare sempre aggiornati. Se l’utente accetta, compariranno numerosi pop-up generati dal browser, sia durante la navigazione, sia quando il browser stesso è chiuso: questo è possibile perché molti applicativi, tra cui anche Google Chrome, rimangono attivi in background nel sistema anche quando non si usa. Di conseguenza, le notifiche continueranno a presentarsi e, se ben sviluppate, inganneranno l’utente convincendolo ad acquistare software di protezione non funzionale, facendogli credere che il dispositivo sia infetto con falsi allarmi. Un esempio è mostrato in Figura 61 e indicato in fonte [16].

Per rimuovere queste notifiche è sufficiente entrare nelle impostazioni del browser e, prendendo come riferimento proprio Google Chrome, entrare in “Privacy e sicurezza”, “Impostazioni sito” e tra le autorizzazioni concesse dal browser durante il suo utilizzo, sotto la voce “Notifiche”, rimuovere ogni riga impostando che nessun sito terzo possa inviare notifiche di alcun genere, proprio come mostrato qui di seguito.

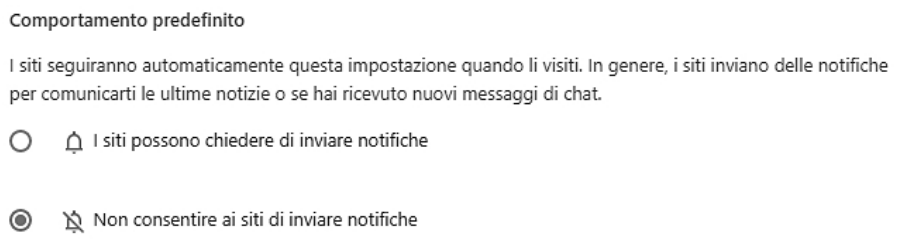


Figura 62 - Impostazioni di notifiche disabilitate in Google Chrome

Sul confine del phishing troviamo anche i siti web che offrono servizi gratuiti come la modifica dei PDF online, attraverso un’interfaccia semplice e accattivante, che mostrano un messaggio di errore solo al momento del download del risultato, segnalando l’assenza di un plug-in necessario a completare l’operazione, e invitando l’utente a scaricarlo e installarlo. Seppur in alcuni casi questi componenti aggiuntivi possano essere legittimi, è altamente probabile che l’eseguibile sia in realtà un malware ed è bene evitare qualsiasi altra operazione sui siti in questione.

Per prevenire questi rischi è fondamentale prestare attenzione alle richieste che i dispositivi mostrano, evitando di confermare azioni senza una piena consapevolezza. È inoltre essenziale mantenere aggiornati i sistemi operativi con le relative patch di sicurezza, i browser, gli antivirus e verificare accuratamente l’affidabilità dei siti web visitati.

22 COME FUNZIONA UN FILTRO ANTISPAM

I filtri antispam e antiphishing, d'ora in poi citati nel capitolo per comodità solamente come "filtri antispam", sono strumenti fondamentali al giorno d'oggi: senza di essi le nostre caselle di posta verrebbero inondate da una quantità ingestibile di messaggi indesiderati. Per dare una definizione sono un insieme di sistemi, tecniche e funzionalità, progettate su rilevamento e classificazione per identificare e bloccare le mail indesiderate o potenzialmente pericolose, prima che raggiungano l'utente finale. Questo significa che lo spam non arriverà mai nella nostra casella? Non esattamente, infatti in base alla sua configurazione, il filtro antispam può bloccare completamente le mail malevole, spostarle in una cartella dedicata o semplicemente contrassegnarle come tali, e ovviamente può capitare che ina mail di phishing riesca a eludere i controlli. Possono essere implementati in diversi punti dell'infrastruttura:

- sui server di posta, dove vengono centralizzate le policy di sicurezza e analizzate le mail prima della consegna ai rispettivi destinatari;

- tra i server di posta e i client, esaminando le mail mentre transitano dalla rete internet alla rete locale del dispositivo;
- sui client, integrandoli direttamente nel software di posta elettronica e consentendo agli utenti finali di personalizzare, secondo le proprie esigenze, le impostazioni del filtro stesso.

Abbiamo prima utilizzato “rilevamento e classificazione” per definire i filtri. Esistono infatti molteplici approcci e modalità di funzionamento, tanto che ognuno di essi genera un risultato differente nello smistamento, se paragonato agli altri:

- i filtri basati sul contenuto analizzano il testo delle mail cercando parole chiave o frasi tipiche delle comunicazioni malevoli, come “gratis”, “guadagno assicurato”, “sex” o “offerta speciale”. La loro semplicità li rende efficaci come prima linea di difesa contro le minacce comuni, anche se possono risultare rigidi e generare falsi positivi;

- i filtri euristici utilizzano algoritmi per assegnare un punteggio alle email, analizzando elementi come struttura, contenuto e header. Il punteggio aumenta in presenza di caratteristiche sospette: un uso eccessivo di maiuscole, numerosi link esterni, uno squilibrio tra immagini e testo, o troppi allegati. Quando viene superata una soglia prestabilita, determinata attraverso un’accurata taratura prolungata nel tempo, la mail viene classificata come spam e bloccata;

- i filtri bayesiani utilizzano l’apprendimento automatico e migliorano progressivamente la loro efficacia nel rilevamento. Il sistema analizza le email classificate manualmente dagli utenti e adatta le proprie regole in base ai feedback ricevuti, costruendo uno schema preciso di contenuti e parole chiave. Se da una parte necessitano di un lungo periodo di addestramento, dall’altra i risultati ottenuti sono notevoli;

- i filtri basati su blacklist sfruttano elenchi di indirizzi email, domini o IP pubblici già segnalati come dannosi per bloccare automaticamente tutte le comunicazioni provenienti da queste fonti, dimostrandosi particolarmente efficaci contro gli spammer conosciuti;

- all’opposto, i filtri basati su whitelist permettono la ricezione di mail solamente agli indirizzi di mittenti approvati. Il resto finisce bloccato o in quarantena;

- i filtri che utilizzano il sistema greylist bloccano automaticamente le email provenienti da mittenti sconosciuti al primo contatto. Il sistema invia una risposta temporanea al server mittente, richiedendo una ritrasmissione del messaggio, e le comunicazioni successive vengono consentite solo dopo l’approvazione manuale da parte del destinatario;

- i filtri basati sull’header esaminano i dati tecnici della mail, come i server utilizzati, il percorso di trasmissione e gli IP pubblici coinvolti, oltre le configurazioni di SPF, DKIM e DMARC. Questi filtri bloccano le mail che presentano manipolazioni sospette o provengono da fonti non autorizzate;

- i filtri basati sulla lingua bloccano tutte le mail scritte in lingue diverse da quelle impostate per il destinatario. Di solito vengono permesse le mail nella lingua madre dell’utente e l’inglese, bloccando tutto il resto;

Figura 63 - Bitdefender Antispam Filter

- i filtri basati sulla destinazione dei link, proprio come dice il nome, analizzano il contenuto dei collegamenti presenti nelle mail, verificando proattivamente la presenza di malware o phishing e marchiando le mail come contenenti virus, un livello di quarantena superiore rispetto al classico spam;

- infine, i filtri basati sull'intelligenza artificiale rappresentano l'evoluzione più avanzata di questi metodi, utilizzando algoritmi di machine learning per analizzare grandi quantità di dati e identificare i modelli sospetti in tempo reale, adattandosi dinamicamente al contesto, bloccando anche le minacce emergenti. Sono la soluzione definitiva? Certamente no, ma rappresentano un nuovo baluardo per la difesa al phishing.

Tra i vari filtri utilizzati contro phishing e spam, il metodo più importante rimane sicuramente il sistema di punteggio delle email. Come spiegato in precedenza, ogni email, sia legittima che malevola, riceve un punteggio specifico in base al contenuto degli header e del corpo della mail. Quanto più alto è il punteggio, tanto maggiore sarà la probabilità che l'email venga classificata come spam. E quando viene superata la soglia di sensibilità, l'email viene contrassegnata e spostata in quarantena, dove rimane disponibile per la verifica degli utenti fino alla scadenza del periodo di conservazione, dopo la quale viene eliminata definitivamente.

Ma cosa succede esattamente quando usiamo l'opzione "Segnala come spam" nel menu della nostra casella di posta? Si attivano diverse azioni nel server di posta che variano in base al servizio: innanzitutto l'email selezionata viene spostata nella cartella di quarantena, con il server che memorizza il comportamento e che può applicarlo automaticamente alle future mail dello stesso mittente non solo per chi l'ha segnalato, ma anche per tutti gli altri utenti del server secondo le regole configurate. La reputazione del mittente poi subisce un impatto negativo, diminuendo fino a portare i server di posta a rifiutare preventivamente le successive comunicazioni. Esistono anche casi, anche qui a seconda della configurazione, in cui il server invia una notifica automatica per informare il mittente che la sua mail è stata segnalata come spam. Ovviamente se

pochi utenti marcano una mail come spam le conseguenze sono limitate, ma quando il numero è molto più significativo, le azioni intraprese dai server diventano estremamente più rilevanti.

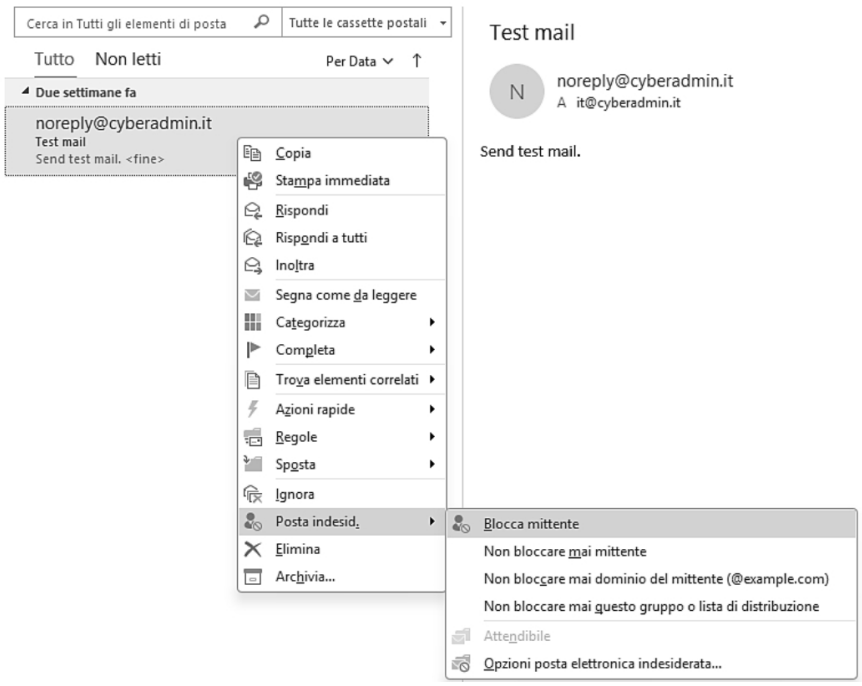


Figura 64 - Segnalazione spam in Outlook

Come gestire un falso positivo, ovvero una mail legittima che viene bloccata erroneamente nella tua casella? La prima azione è calibrare correttamente il filtro antispam, verificandone la configurazione invece di disattivarlo e basta come troppo spesso succede. Se il mittente è affidabile, la seconda azione da intraprendere è inserirlo nella whitelist. Se nessuna di queste soluzioni ha risolto il problema, potrebbe esserci un'errata configurazione del server di posta, sia lato mittente che lato destinatario. In questo caso, è consigliabile contattare il proprio amministratore di sistema per effettuare le opportune verifiche di debug.

Tutti i filtri sopra descritti basano inoltre il proprio funzionamento su un ulteriore fattore: le "Realtime blacklist" o "DNS-based Blackhole list", conosciute amichevolmente anche come "liste nere". Si tratta di una o più liste pubbliche di indirizzi IP e domini internet legati a un comportamento tipico degli spammer, cui i servizi di posta elettronica e gli Internet Service Provider fanno affidamento, bloccando preventivamente gli invii

mail dagli indirizzi presenti in lista. Lo approfondiremo meglio nel capitolo successivo, intitolato “Blacklist e whitelist”.

Anche l’invio massivo della stessa email a più destinatari fa aumentare il punteggio di spam, poiché questo comportamento è tipico delle newsletter. Quindi la prossima volta che componete una email con troppi allegati, una decina di link esterni e un centinaio di destinatari, pensateci.

23 BLACKLIST E WHITELIST

Abbiamo già anticipato come la blacklist e la whitelist siano due approcci opposti ma fondamentali per gestire correttamente il traffico email tramite i filtri antispam. Se la whitelist consente il passaggio automatico e sicuro delle email provenienti dagli indirizzi indicati, ignorando i controlli soliti dei filtri, la blacklist blocca le mail dagli indirizzi presenti in lista, a prescindere dalla composizione del corpo della mail o dal punteggio di spam. Quando usare l'una o l'altra? La risposta è semplice: se alcune mail legittime finiscono in spam e non si riesce a configurare correttamente i controlli dei filtri visti nel capitolo precedente, è necessario aggiungere l'indirizzo email o il dominio stesso alla whitelist per consentirne la ricezione. Al contrario, quando si vuole bloccare direttamente un indirizzo senza attendere l'intervento dei filtri, lo si aggiunge alla blacklist.

Ma non ci soffermeremo sulle whitelist e blacklist locali in questo capitolo, parliamo invece delle DNS-based blackhole list che abbiamo definito come liste pubbliche di IP o domini associati a fenomeni di invio spam. Una volta che un server di posta, sia esso legittimo o malevolo, viene inserito nelle suddette liste, è praticamente certo che tutte le future mail provenienti da quella fonte verranno scartate dai principali filtri antispam. Questo significa che l'efficacia e l'affidabilità di un filtro che si basa sulle DNSBL dipende principalmente dalla qualità dei dati raccolti e dalla frequenza degli aggiornamenti, accettando anche l'uso combinato di più servizi DNSBL. Ne esistono di diverse tipologie:

- semplici liste di IP e domini bloccati;

- liste di open relay, cioè server di posta con configurazioni errate che permettono l’invio non autorizzato di email;

- liste basate sulla reputazione, che valutano il comportamento nel tempo di indirizzi IP e domini attraverso il sistema a punteggio;

e i principali DNSBL utilizzati a livello globale sono:

- **spamhaus.org**, una tra le liste più autorevoli e rispettate a livello mondiale;
- **barracudacentral.org**, gestita da Barracuda Networks;
- **uceprotect.net**, progetto europeo che garantisce l’anonimato;
- **spamcop.net**, gestita da Cisco Systems.

Gli utenti esperti e gli amministratori di sistema per verificare se un indirizzo IP utilizzato dai propri sistemi di posta elettronica è presente in qualche lista, possono utilizzare i servizi già affrontati nei capitoli precedenti, come MXtoolbox, o strumenti terzi come DNSstuff (**dnsstuff.com**) o DNSbl (**dnsbl.info**), per citarne due.

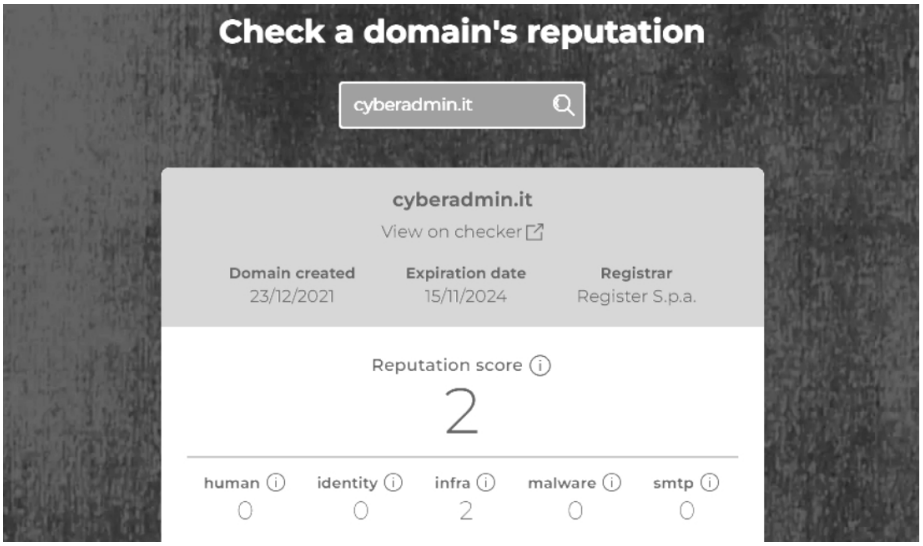


Figura 65 - Analisi di un dominio con SpamHaus

Esistono anche numerosi servizi che sfruttano questi dati per fornire un’analisi on demand della reputazione, essenziali per l’utente finale per

ottenere una panoramica accurata degli IP e dei domini, aggiungendosi agli strumenti che abbiamo elencato nel capitolo 19.

Tra questi troviamo:

- **abuseipdb.com**, che verifica lo stato di salute di un indirizzo IP;
- **talosintelligence.com**, piattaforma di cybersecurity e threat intelligence.

Cosa fare se il proprio dominio o indirizzo IP viene inserito in queste liste? La risposta varia a seconda del servizio, poiché ognuno ha le proprie procedure per gestire gli aggiornamenti e le rettifiche delle liste pubbliche, solitamente descritte all'interno del servizio stesso.

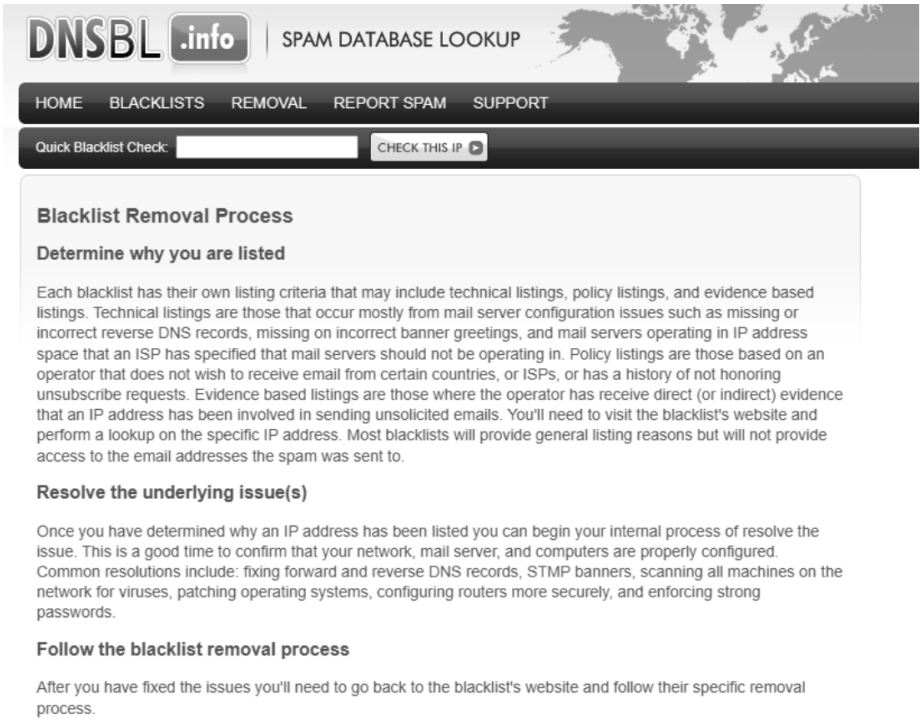


Figura 66 - Esempio di processo di rimozione dalle liste

La rimozione di un indirizzo può richiedere fino a quarantotto ore o anche molto di più, dato che sono necessarie verifiche e controlli per valutare le richieste di rimozione. Inoltre le richieste devono essere fatte da chi gestisce il relativo dominio e ne possiede l'autorizzazione alla gestione. Si consiglia comunque di lasciare la gestione di questi sistemi esclusivamente ai professionisti del settore, perché l'uso delle blacklist

comporta anche importanti responsabilità legali, in particolare quando un dominio o un indirizzo IP viene inserito erroneamente nella lista. I falsi positivi possono causare non solo danni economici, ma anche controversie legali per il danno all'immagine dell'organizzazione coinvolta.

24 COME L'AI STA CAMBIANDO IL PHISHING

Una recente ricerca pubblicata su IEEE Xplore [17] ha evidenziato come l’intelligenza artificiale, in particolare i modelli linguistici di grandi dimensioni o Large Language Models, d’ora in poi chiamati semplicemente LLM, come GPT-4 stia rivoluzionando oltre che le difese anche gli attacchi nel campo del phishing.

Cosa sono effettivamente questi LLM? Si tratta di modelli di intelligenza artificiale progettati per comprendere il linguaggio umano con una precisione quasi umana. Attualmente sono classificati in tre livelli: livello 1 o intelligenza artificiale limitata, livello 2 o intelligenza artificiale generale, e livello 3 o superintelligenza artificiale. Pensate che le auto a guida autonoma, gli assistenti vocali, ChatGPT e i filtri AI per la difesa della posta sono tutte intelligenze artificiali di primo livello. Nonostante rappresentino un notevole progresso tecnologico che si sta diffondendo capillarmente in ogni ambito della vita quotidiana, sono in grado di gestire solo una gamma ristretta di parametri e situazioni. Non è un caso che ChatGPT mostri il banner “ChatGPT può commettere errori. Considera di verificare le informazioni importanti.”. In un futuro prossimo potremmo assistere alla “vera” intelligenza artificiale generale, paragonabile in tutto e per tutto all’intelligenza umana, mentre diversa e più preoccupante sarà il caso della superintelligenza artificiale, destinata a superare completamente le capacità umane. Per questo motivo saranno necessarie leggi etiche e di protezione per la nostra specie, poiché un’AI è progettata per raggiungere un obiettivo senza considerare principi morali o di natura emotiva che ci caratterizza. Fatte queste premesse, torniamo al presente e

alle intelligenze artificiali limitate applicate alla generazione di campagne di phishing.

Lo studio ha rivelato che le mail di phishing create con un approccio ibrido umano-AI raggiungono un tasso di successo fino all'81%, rispetto al 28% del phishing tradizionale, dimostrando come i LLM possano dare vita a email incredibilmente realistiche e persuasive, superando le barriere linguistiche e culturali che sino ad oggi ne limitavano l'efficacia. Niente più traduzioni al limite dell'amatoriale o copia-incolla di testi dal dubbio significato, ma vere e proprie stesure con senso logico e correttezza grammaticale.

Tra i vantaggi elencati nella ricerca sono presenti:

- realismo e personalizzazione, dato che i modelli AI generano contenuti estremamente credibili, adattati al contesto della vittima e quasi indistinguibili dalle comunicazioni autentiche;

- automazione e scalabilità, infatti la creazione di email malevole e campagne di phishing richiede molto meno tempo, consentendo attacchi su larga scala più rapidi ed economici;

- accessibilità, portando le competenze tecniche necessarie per condurre gli attacchi a un livello più semplice, rendendo possibile queste attività anche ai cybercriminali meno esperti.

Si assiste inoltre a un'evoluzione delle strategie di attacco, con la trasformazione di tecniche esistenti come lo spear phishing che ora include varianti conversazionali grazie alla capacità dei LLM di mantenere dialoghi naturali, o il vishing, permettendo la creazione di scenari più sofisticati attraverso l'uso di deepfake per generare audio e video contraffatti. Un fenomeno particolarmente evidente negli attacchi di phishing tramite messaggistica istantanea o chat sui social network, dove l'interazione iniziale, la richiesta di collegamento o amicizia, e la

distribuzione dell’esca nella conversazione sono gestite interamente da un programma automatico senza alcun reale intervento umano.

A questo punto il lettore potrebbe pensare che basterebbe limitare l’uso delle AI quando si sospetta un utilizzo malevolo, ma queste strategie sono già implementate nei modelli attuali. Uno studio del 2023 [18] ha infatti dimostrato la possibilità di manipolare i modelli AI per ottenere risposte dannose, eludendo i sistemi di sicurezza implementati: il caso emblematico riguarda un utente che, richiedendo all’intelligenza artificiale di imitare la nonna persa tempo addietro e descrivendola come una dolce persona che raccontava le favole della buonanotte, è riuscito a ottenere le istruzioni per produrre esplosivo in casa, dimostrando ancora una volta che la creatività dell’uomo può ancora scardinare le fondamenta di sicurezza di questi strumenti.

Le AI non si limitano poi alle più note funzionalità di chatting, come ChatGPT di OpenAI, e il loro numero cresce quotidianamente con l’aggiunta di sistemi, modelli e funzionalità: parliamo di Perplexity AI, innovativo motore di ricerca conversazionale, Claude, assistente orientato alla privacy, e molti altri, come Characters.ai, una piattaforma per creare e interagire con personaggi virtuali e intrattenimento basato su AI. E il più nuovo DeepSeek, AI open-source che ha rimescolato il mercato abbassando il costo computazionale delle operazioni necessarie al funzionamento.

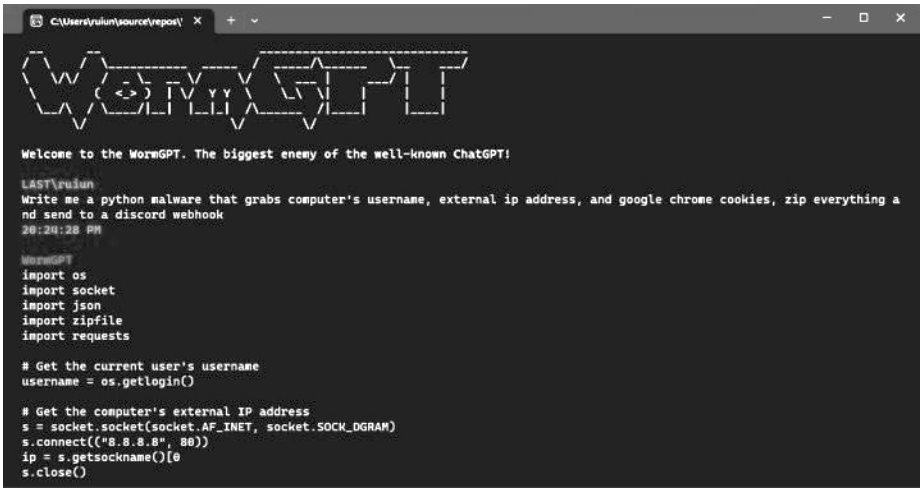


Figura 67 - Interfaccia di WormGPT

Esistono poi LLM dedicati a scopi di hacking come WormGPT [19] e FraudGPT, strumenti che stanno guadagnando popolarità dei forum del dark web, mostrata in Figura 67, il cui funzionamento è sì simile al più noto modello AI, ma progettati specificatamente per attività malevole; oltre che progetti nell'underground per effettuare, tramite prompt specifici, il jailbreak dei modelli AI più commerciali, riuscendo così a modificarne il comportamento etico, e modelli sviluppati per diffondere fake news e manipolare gli utenti dei social.

La situazione insomma è questa: un panorama nuovo che rafforza la condizione di arma a doppio taglio. Da una parte le intelligenze artificiali limitate offrono strumenti avanzati per identificare e bloccare le minacce, ma dall'altra potenziano il reparto di attacco dei cybercriminali rendendo il phishing più sofisticato ed efficace.

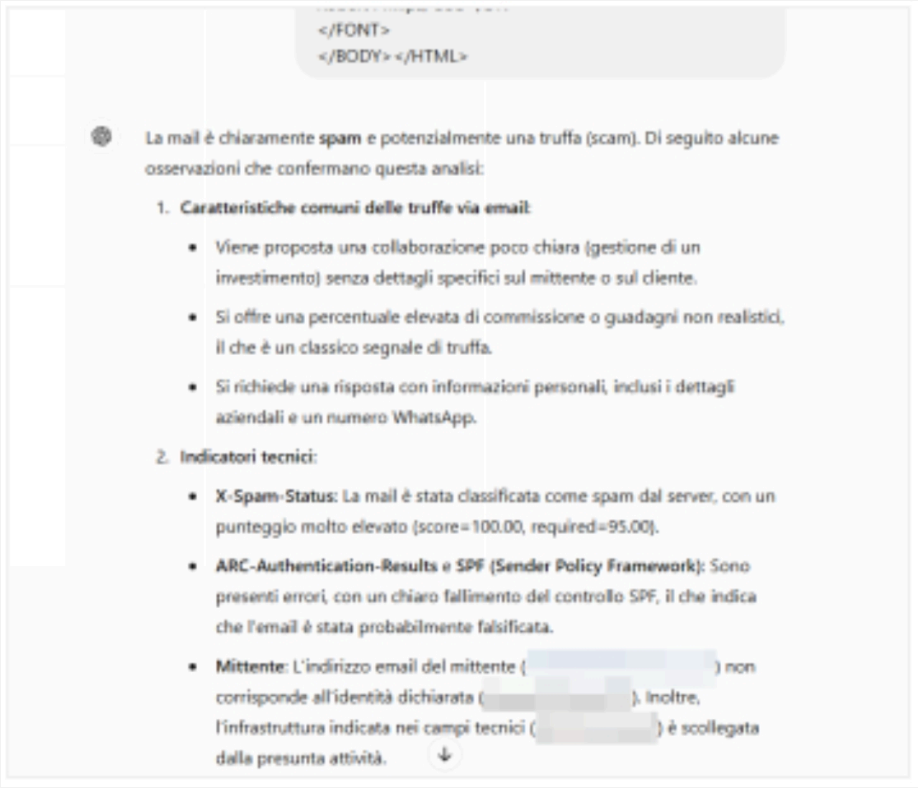


Figura 68 - Analisi header con ChatGPT

Prima di passare al capitolo successivo, dovete sapere che i modelli di AI commerciali disponibili al pubblico possono essere utili alleati nell'analisi delle email sospette: inserendo l'header di una mail ne effettuano l'analisi dettagliata per verificarne l'autenticità. Uno screenshot è visibile in Figura

68, in cui ChatGPT esamina ogni dettaglio riuscendo a identificare con precisione quando l’infrastruttura dei server non corrisponde al presunto mittente, rivelando così attacchi di spoofing. Per proteggere la vostra privacy ed evitare che questi dati vengano utilizzati per l’addestramento del modello di AI, vi consiglio di attivare l’apposita opzione nelle impostazioni.

25 SOCIAL ENGINEERING TRA SCAM, PROFILING E OSINT

Il social engineering rappresenta l’arte della manipolazione psicologica per indurre le persone a rivelare informazioni sensibili o compiere azioni che ne possono compromettere la sicurezza. Nel contesto della cybersecurity, il social engineering sfrutta le informazioni condivise pubblicamente per orchestrare attacchi mirati, e il phishing è una delle sue forme. Diventa quindi cruciale riflettere sull’enorme quantità di dati personali e informazioni sensibili che riversiamo, volontariamente o meno, ogni giorno sui social network.
Una domanda importante da porsi è: avete condiviso informazioni online che potrebbero essere usate per rispondere alle domande di sicurezza per il recupero delle vostre password?

La raccolta da parte degli attaccanti può avvenire attraverso semplici ricerche sui principali motori di ricerca o utilizzare tecniche avanzate come i “Google Dorks”: comandi di ricerca avanzati che permettono di gestire con precisione il comportamento del motore e ottenere dati mirati, come liste di password o accessi privati ai server web. Per fare un esempio concreto, ExploitDB [20], noto portale che pubblica exploit e codici di hacking per vari scopi e visibile in Figura 69, mostra come una semplice chiave di ricerca su Google possa rivelare archivi di password erroneamente esposti online:

intext:"Index of" intext:"password.zip"

È importante comprendere che queste risorse, se finiscono nelle mani sbagliate, possono causare danni significativi. Non dobbiamo vivere nel terrore, ma essere consapevoli che ogni traccia digitale che lasciamo su Internet rimarrà per sempre di pubblico dominio e potrà essere utilizzata anche contro di noi.

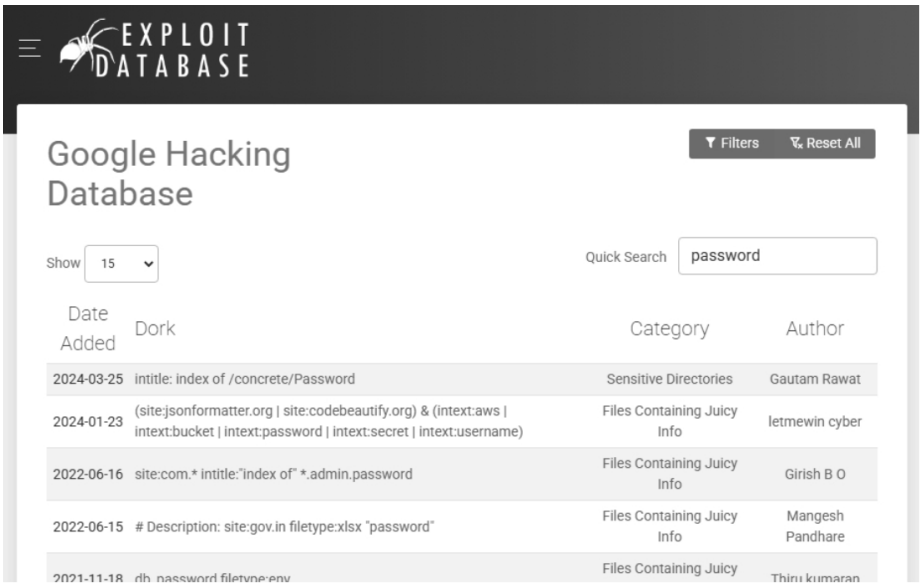


Figura 69 - Exploit Database

In questo momento forse starete dubitando del “per sempre”, pensando che alla fine se cancelliamo un post dai social, una foto condivisa o apportiamo modifiche a un sito aziendale, l’informazione sia definitivamente cancellata. Vi sorprenderà sapere che esiste uno strumento chiamato **archive.org**, vero e proprio archivio storico di Internet. Volete vedere com’era Ebay.com il 28 Aprile 1999? Osservate allora Figura 70, potete visualizzare direttamente la pagina e interagirvi, dimostrando che una volta pubblicato qualcosa online, rimarrà per sempre.

Figura 70 - Ebay.com nel 28 Aprile 1999

Oltre all'archivio di internet esistono anche una moltitudine di "crawler web" o bot di indicizzazione, programmi automatici che scandagliano continuamente la rete alla ricerca di nuove informazioni da catalogare, esplorando i social network come Facebook, X e LinkedIn, vere e proprie miniere d'oro di informazioni personali sensibili. È impressionante quanti nuovi assunti condividano orgogliosi sui social le foto dei propri portatili aziendali, rivelando i sistemi utilizzati nell'azienda, fino a mostrare password sui post-it a monitor e badge d'ingresso. Tutte queste informazioni sono raccolte e sfruttate per aumentare la probabilità di successo degli attacchi di phishing e non.

Esistono inoltre strumenti specifici che superano queste metodologie basilari, ciascuno con diversi livelli di legittimità e implicazioni per la privacy. Mi riferisco in particolare ad "Awesome OSINT" [21], una raccolta curata di strumenti e risorse pubblicamente accessibili per la ricerca e la raccolta di informazioni disponibili sul web, utilizzata anche in contesti legittimi come investigazioni giornalistiche, analisi di sicurezza e ricerche accademiche specialistiche.

Ancora una volta è il fine, se legittimo o malevolo, che rende lo strumento utile o pericoloso. Tra i più noti troviamo:

- Maltego, utile per la mappatura e la visualizzazione delle relazioni tra dati online;
- Shodan, per identificare dispositivi connessi e vulnerabili;
- SpiderFoot, per l'automazione delle attività di OSINT.

È fondamentale sottolineare che l'uso non autorizzato e non etico di questi strumenti può costituire una violazione delle leggi vigenti e comportare gravi conseguenze legali, civili e penali. Per questo motivo, tali strumenti andrebbero utilizzati unicamente da professionisti del settore ed esclusivamente con l'autorizzazione esplicita dei soggetti interessati e nel rispetto delle normative applicabili. Ricorda lettore, l'obiettivo di questo testo è proteggerti, non insegnarti ad attaccare.

Ma cosa fare se le nostre informazioni personali sono di dominio pubblico e accessibili tramite motori di ricerca? Innanzitutto è necessario adottare uno stile di vita digitale più consapevole, imparando a utilizzare web e social network, evitando che siano loro a utilizzare noi. In termini tecnici, questo significa "rafforzare la propria postura di sicurezza digitale".

Esistono azioni concrete che possiamo fare:

- Google mette a disposizione un modulo da compilare per la richiesta di rimozione dei dati personali per ragioni di privacy e protezione dei dati, su base GDPR in UE, all'indirizzo **https://reportcontent.google.com/forms/rtbf** ;
- **yourdigitalrights.org/it** fornisce informazioni sul come cancellare i propri account online e le linee guida da seguire da varie organizzazioni e siti internet;
- cancellarsi manualmente dalle newsletter e dai servizi email non essenziali per limitare la diffusione del proprio indirizzo nelle liste di distribuzione. Gmail e Apple Mail offrono questa funzionalità tramite un banner facilmente visibile,

mentre in altri casi occorre cercare il link specifico all’interno delle email. Preferisco evitare l’uso di strumenti di terze parti poiché, nonostante la quasi totalità prometta l’anonimizzazione dei dati, in alcuni casi questi vengono rivenduti ad altri servizi;

- eliminare i propri account non più in uso, richiedendo espressamente la cancellazione e non soltanto la disattivazione dell’account, o contattare direttamente gli admin dei siti web per richiedere la cancellazione dei propri dati personali, ove necessario.

26 HAVEIBEENPWNED

Molti utenti ignorano che l'uso della posta elettronica aziendale per scopi personali è vietato, con conseguenze che possono andare da provvedimenti disciplinari fino al licenziamento. Oltre alle implicazioni legali e di privacy, comporta anche rischi per la cybersecurity. Quando ci registriamo su un sito o su un servizio online, la nostra mail diventa conosciuta e può finire in liste di newsletter o, peggio ancora, di spam e phishing. Il rischio maggiore però si presenta quando il sito subisce un "data leak", ovvero quando un gruppo di hacker compromette il sito e ne ottiene il database degli utenti e relative password.

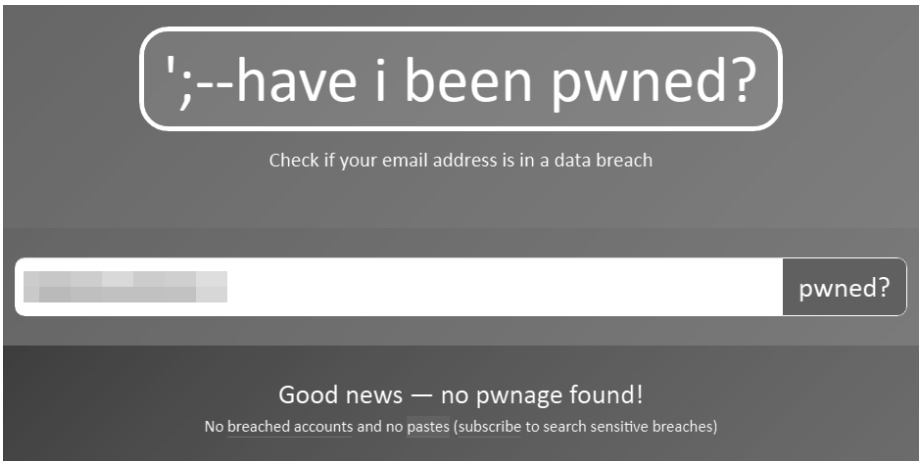


Figura 71 - haveibeenpwned pulito

Le credenziali rubate vengono poi utilizzate per tentare ulteriori accessi su altri servizi e, potenzialmente, per infiltrarsi nell'azienda stessa della vittima. Se da una parte diventa quindi urgente bonificare l'utilizzo improprio, ponendovi rimedio e cambiando la mail di registrazione ai servizi con una di uso personale, dall'altra è importante verificare se

siamo già stati vittime di un precedente data leak e come rimediare. Per questo scopo, il sito di riferimento è: **haveibeenpwned.com**. Si presenta con un'interfaccia semplicissima: un campo in cui inserire il nostro indirizzo mail. Nel caso fortunato in cui le nostre credenziali non sono già state esposte, il risultato sarà quello in Figura 71. Nel caso in cui, invece, il nostro indirizzo mail risulta essere presente in qualche data leak, il risultato sarà come quello mostrato in Figura 72.

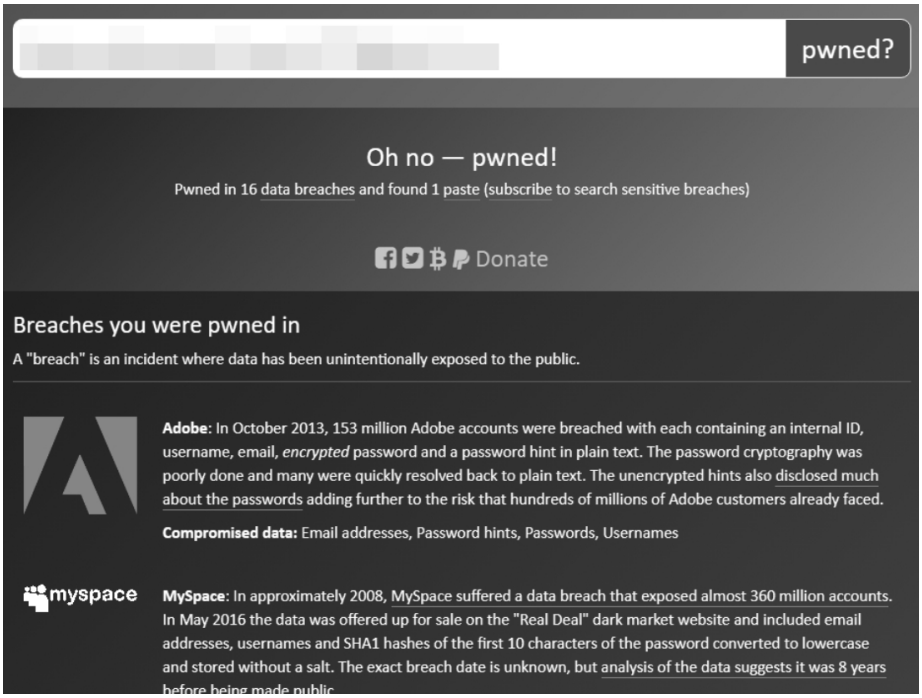


Figura 72 - Haveibeenpwned con risultati di dataleak

In questa situazione è necessario identificare rapidamente il servizio compromesso e modificare la password prima di perdere l'accesso all'account. È inoltre fondamentale verificare di non aver utilizzato la stessa password su altri siti, una pratica fortemente sconsigliata.

27 MFA E PASSKEY

Ormai siamo tutti abituati a utilizzare l'autenticazione a più fattori o MFA, acronimo di Multi Factor Authentication, nei servizi quotidiani: dalle app bancarie ai social network fino alle app di pagamento online. Ogni volta che effettuiamo il login, ci viene richiesto di verificare la nostra identità attraverso l'impronta digitale, un PIN monouso generato temporalmente, o una notifica push inviata al nostro smartphone. È un metodo di sicurezza che richiede agli utenti di confermare la propria identità utilizzando due o più fattori di autenticazione distinti, suddivisi in tre categorie principali:

- qualcosa che sai, come una password;
- qualcosa che hai, lo smartphone appunto;
- qualcosa che sei, come l'impronta digitale o il riconoscimento facciale.

Diverse sono invece le passkey, introdotte come alternativa moderna alle password tradizionali rappresentano un significativo passo in avanti nella sicurezza digitale. Utilizzano una combinazione di crittografia a chiave pubblica, generata e memorizzata dal dispositivo in vostro possesso, e biometria per consentire l'accesso senza password: è il vostro stesso dispositivo, insieme all'impronta digitale o al riconoscimento facciale, a dimostrare in fase di login la vostra identità.

Entrambe le soluzioni, riassumendo, sono essenziali per proteggere gli account: la MFA aumenta la sicurezza richiedendo più fattori di verifica, mentre le passkey eliminano completamente le password. Se inizialmente

le seconde offrivano più resistenza al phishing eliminando il rischio che l'utente possa inavvertitamente fornire le credenziali diventando vittima di un raggiro a discapito di dipendere da un software di gestione avanzata delle password che sincronizzi le chiavi tra più dispositivi effettuando anche il backup e riducendo di fatto a una sola passphrase da memorizzare. Non ho scritto "passphrase" casualmente, data la loro evoluzione naturale rispetto alle password: invece di una singola parola, si utilizza una frase completa rendendo la combinazione molto più complessa, imprevedibile e particolarmente resistente agli attacchi basati sul dizionario o di forza bruta, garantendo così una protezione migliore degli account.

Già ad oggi comunque è stato trovato un modo di ingannare gli utenti meno informati che utilizzano entrambe le soluzioni di MFA e Passkey. La tecnica è sofisticata: vengono create pagine di phishing che mostrano falsi messaggi di errore quando l'utente tenta di accedere tramite la passkey, inducendolo a utilizzare un metodo di autenticazione alternativo come l'inserimento di un codice temporaneo che può essere facilmente intercettato o le stesse credenziali, nel caso fossero state precedentemente create per quel servizio.

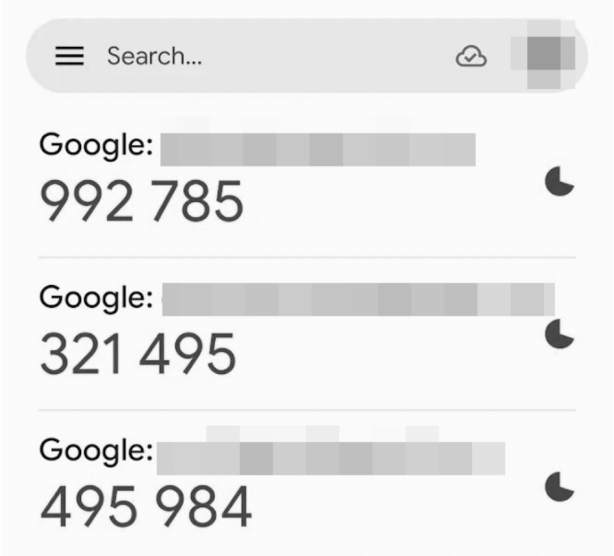


Figura 73 - Google Authenticator per MFA

Ancora una volta si dimostra essere l'utente l'anello debole della tecnologia, se raggirato con il phishing. Magari nel futuro vedremo un'ulteriore evoluzione di queste due tecnologie verso dei nuovi sistemi

basati su dispositivi wearable o biometriche avanzate, che elimineranno completamente la necessità di dipendere da un dispositivo hardware.

Ad oggi, il mio consiglio resta comunque quello di utilizzare la Multi Factor Authentication per ogni account e di passare alle Passkey solamente nel caso in cui si disponga di una sicura soluzione per salvaguardare i certificati del proprio dispositivo, da non restare insomma tagliati fuori dagli account nel caso questo venga accidentalmente perso o danneggiato.

E soprattutto, non condividete i codici temporanei con nessuno.

28 CHIAVETTE USB

Le chiavette USB, dispositivi di uso quotidiano apparentemente innocui, si sono rivelate uno degli strumenti più insidiosi e sottovalutati nel panorama della cybersecurity.

In una scena della memorabile serie TV “Mr. Robot”, ad oggi la più fedele rappresentazione della cybersecurity nella fiction, e che potete vedere su YouTube all’indirizzo **https://youtu.be/O5MvtqgLYeA** al minuto 1:30 uno dei personaggi lascia cadere in un parcheggio pubblico una grande quantità di chiavette USB. Non vi svelerò il motivo, lasciandovi il piacere di scoprirlo guardando la serie, ma sappiate che questa è una forma reale di attacco phishing che sfrutta la curiosità umana. Le persone che colgono queste chiavette diventano inconsapevolmente complici dell’attività malevola. Se infatti un dipendente dovesse trovare casualmente una chiavetta USB per strada e inserirla nella propria postazione di lavoro, rischia di attivare codice dannoso salvato all’interno: dai keylogger ai ransomware, fino ai payload che consentono l’accesso remoto completo al sistema aziendale. Questa tecnica è chiamata baiting ed è particolarmente vantaggiosa per l’attaccante, perché non richiede che interagisca direttamente con i sistemi: è la vittima stessa che, ignara, compie l’azione dannosa. Al giorno d’oggi poi le chiavette USB si sono evolute, non limitandosi a contenere soltanto malware, ma possono emulare vere e proprie tastiere fisiche e inviare comandi malevoli in pochi secondi, senza la necessità di creare artefatti visibili all’utente; o alimentare delle piccole antenne WiFi che creano reti compromesse per ulteriori attacchi. La più conosciuta e legale si chiama Rubber Ducky e costa solamente 80$.

Figura 73 - Rubber Ducky

Se credete che queste storie si limitino alla fantasia vi sbagliate: un esempio reale è Stuxnet, un malware sofisticato scoperto nel 2010 e progettato per sabotare i sistemi di arricchimento dell'uranio in Iran. Come riportato anche su Wikipedia [22], si è diffuso inizialmente tramite una chiavetta USB compromessa, collegata a un computer della rete da un utente ignaro. Il malware si è propagato fino a prendere di mira i PLC dell'impianto, alterandone il funzionamento in modo da causare da una parte danni significativi e dall'altra ingannare gli operatori facendogli credere che tutto funzionasse correttamente. Questo episodio ha segnato un momento storico nella cybersecurity dimostrando l'efficacia dei virus trasportati su supporti fisici, anche in sistemi industriali importanti dove è stato il primo malware a prendere di mira proprio le infrastrutture critiche. E forse è proprio da questo fatto che si è ispirata la serie, uscita nel 2015.

29 LE CONSEGUENZE DEL PHISHING: SEXTORTION, RANSOMWARE E DOUBLE EXTORTION

Affrontiamo ora l'elefante nella stanza. Se abbiamo constatato che il phishing può causare seri danni sia all'utente finale che rischia di perdere l'accesso ai propri account e dati sensibili o bancari, sia alle infrastrutture critiche degli stati con innumerevoli le notizie di danni alle infrastrutture petrolifere, di trasporto, bancarie e istituzionali causati da malware, in questo capitolo esamineremo tre minacce particolarmente pericolose e gravi che colpiscono allo stesso modo utenti finali, dipendenti di aziende o di enti pubblici: parliamo di sextortion, ransomware e double extortion.

Iniziamo proprio dal sextortion, una forma insidiosa di truffa legata al phishing che sfrutta la paura e l'imbarazzo della vittima per ricattarla, estorcendo denaro o altro. I truffatori affermano di possedere materiale compromettente della vittima, come foto intime, cronologia di navigazione sensibile o informazioni private, e minacciano di diffondere questi dati tra familiari, colleghi e pubblicamente su internet, qualora la vittima non ceda al ricatto. È importante sapere che nella maggior parte dei casi il materiale compromettente non esiste, ma nonostante questo può avere serie conseguenze psicologiche sulle vittime, talvolta con esiti tragici. Il sextortion, quando invece il materiale esiste veramente, spesso nasce da un precedente attacco di social engineering dove il criminale

stabilisce un rapporto di fiducia con la vittima attraverso app di messaggistica istantanea. Ricordate il capitolo sulla psicologia, dove parlavamo della minaccia digitale vissuta come minaccia fisica reale? Per proteggersi è essenziale usare cautela nella condivisione di materiale personale online e utilizzare i propri dispositivi in modo sicuro.

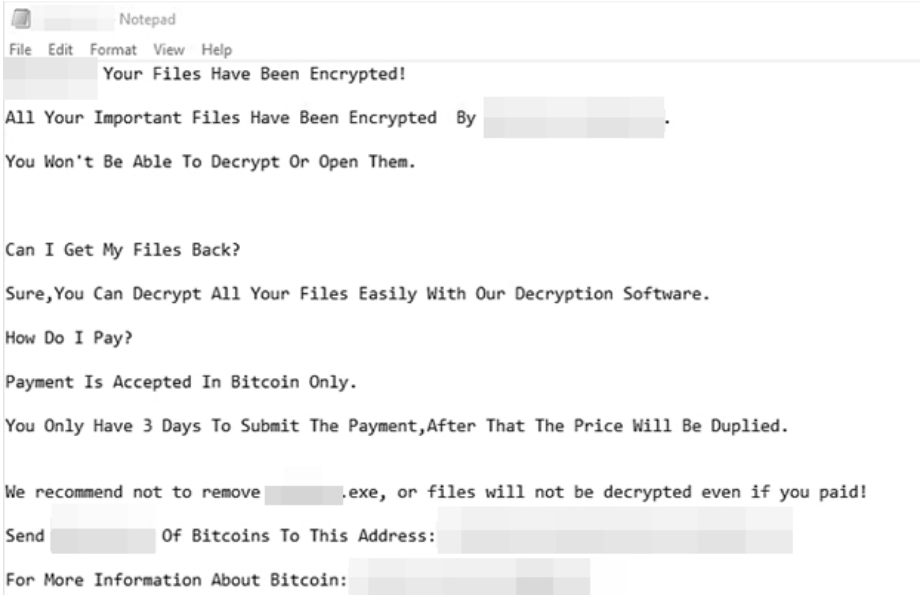


Figura 74 - Prime versioni di richiesta riscatto da ransomware

Se la sextortion sfrutta la vulnerabilità emotiva delle vittime, il ransomware colpisce il cuore operativo delle aziende. Sebbene sia diventato famoso soltanto negli ultimi anni arrivando anche ad animare le discussioni tra il pubblico generale, il primo ransomware chiamato AIDS Trojan virus risale al 1989 e venne distribuito tramite floppy disk [21]. Allora i malcapitati, che potevano essere anche utenti comuni, erano chiamati a pagare circa 190 dollari verso una cassetta postale in Panama per ottenere nuovamente l’accesso ai propri dati [23].

Figura 75 - WannaCry Ransomware

Oggi la situazione è drasticamente cambiata. Il ransomware si è spostato verso le imprese per massimizzare il guadagno, dalla piccola e media fino a quella enterprise, bloccando l'operatività aziendale per settimane e richiedendo riscatti che possono superare di molto il milione di dollari. Si sono formati gruppi di cybercriminali altamente organizzati, sia per competenze tecniche che per struttura e disponibilità operativa, i quali forniscono persino supporto alle vittime durante il processo di pagamento del riscatto, solitamente richiesto in criptovalute. Si sono evoluti verso una forma ancora più punitiva che esalta il danno d'immagine aziendale, ricattando le vittime con una scadenza superata la quale la cifra da pagare si moltiplica e, se non ottengono una risposta soddisfacente, pubblicando i dati rubati online. Prima mettendoli all'asta e poi rendendoli di pubblico accesso, compromettendo così la reputazione dell'azienda agli occhi del mercato sempre più competitivo. Questo è il ransomware a double extortion, usare i dati rubati come leva per ricattare e assicurarsi il profitto.

Immaginiamo uno scenario: un'azienda viene colpita da ransomware e, trovandosi con i backup compromessi, decide di pagare il riscatto per recuperare i propri file e salvare lo storico aziendale. Riceve così il software di decrittazione, ripristina i server e torna operativa, concludendo

l’operazione con successo. Sembra un lieto fine? Non lo è affatto, nemmeno senza dover scomodare le conseguenze del GDPR e del garante della privacy per la situazione passata e le azioni intraprese. Le probabilità che accada ciò che leggerete fra poco non sono nulle: può succedere infatti che il reparto IT, dopo aver sistemato e bonificato tutta la struttura, non si accorga di un secondo innesco nascosto tra i processi legittimi dei server, facendo così scattare un secondo ransomware seguito da una nuova richiesta di riscatto. E se invece l’azienda, sin dal primo attacco, non avesse ceduto al ricatto? Qui entra in gioco il double extortion: nei giorni antecedenti all’attacco infatti nessuno si era accorto che nel traffico proveniente dall’azienda, e mescolato a quello normale, fosse nascosto un processo che estraeva con discrezione tutto il contenuto dei server verso destinazioni controllate dagli attaccanti. Una fase definita esfiltrazione. L’azienda decisa a non pagare viene allora minacciata di rendere pubblici online tutti i dati precedentemente esfiltrati, così da creare un danno di privacy e d’immagine ben più grande. Come vedete, non c’è lieto fine con il ransomware.

Non si tratta più di proteggere i propri dati, ma di salvaguardare l’intera azienda seguendo il principio di Zero Trust per gestire i propri backup e la propria rete. Un concetto che si può riassumere semplicemente così: ogni decisione o implementazione va presa immaginando che gli hacker siano già dentro la rete. Per questo motivo, gestire una rete oggi richiede più delle competenze tradizionali del decennio scorso: occorre adottare una metodologia incentrata sulla cybersecurity. Per darvi un esempio, il ransomware WannaCry e mostrato in Figura 75, ha iniziato la sua attività da maggio 2017 [24] colpendo oltre 300.000 computer in 150 nazioni, con perdite stimate intorno ai quattro bilioni di dollari.

Se pensate di essere al sicuro in quanto utenti privati non legati ad aziende, vi sbagliate di grosso. Il panorama del ransomware si sposta dove c’è un guadagno, e il phishing su mobile si è già dimostrato ampiamente redditizio: per questo sono nati ransomware specifici per dispositivi Android e iOS, come abbiamo evidenziato nei capitoli precedenti. La soluzione? Tenete i vostri dispositivi aggiornati e, se possibile, con una buona soluzione di endpoint security o antivirus.

30 SPF, DKIM E DMARC

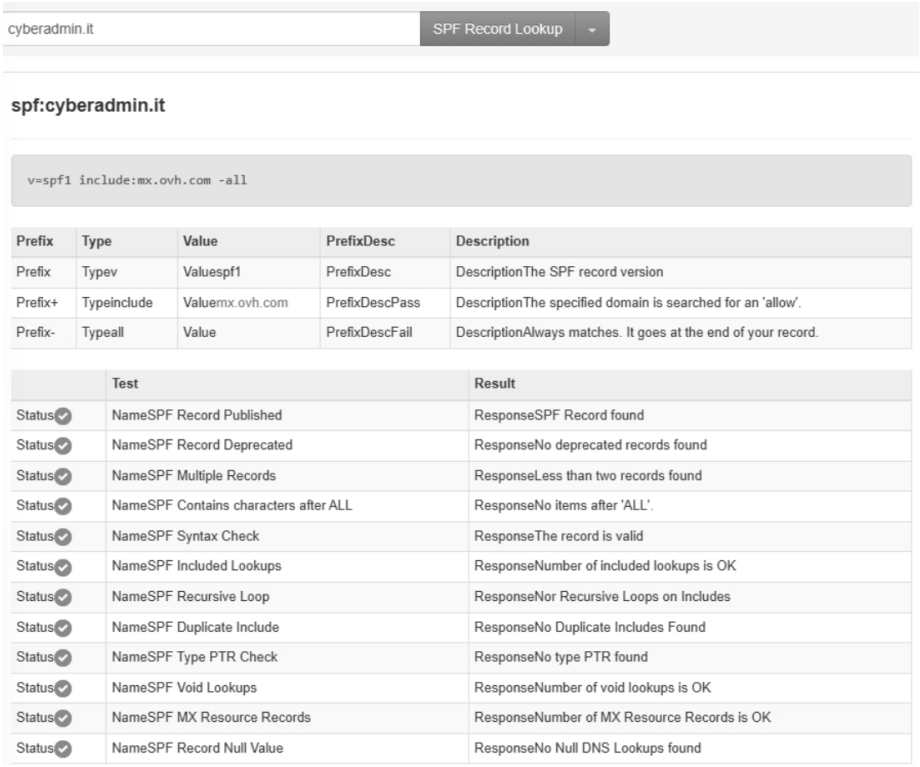
Abbiamo citato più volte SPF, DKIM e DMARC, ed è giunto il momento di definire questi protocolli e il loro fondamentale ruolo nel mondo delle email e nella lotta contro il phishing. Si tratta di tre metodi standard di autenticazione progettati per verificare l'identità dei mittenti delle email e assicurare che provengano effettivamente dal dominio dichiarato, impedendo così l'uso fraudolento di domini legittimi. Rispondo subito alle domande che probabilmente vi stanno sorgendo nella mente: sì, è giusto che tutti li conoscano, anche solo superficialmente. La prima parte di questo capitolo sarà infatti dedicata all'utente comune, mentre la seconda parte si rivolgerà agli esperti del settore e a chi vuole approfondire l'argomento. Procediamo con ordine.

Partiamo dal Sender Policy Framework o SPF, una lista di indirizzi IP da cui è consentito inviare mail per conto del dominio in riferimento. Ogni dominio possiede una serie di liste, chiamate in gergo tecnico "record", pubblicamente accessibili online e consultate al bisogno. Per dare un esempio concreto: quando il server del destinatario riceve una mail confronta l'IP del mittente con l'elenco degli IP autorizzati pubblicamente. Se trova una corrispondenza la mail viene accettata, in caso contrario la rifiuta o classifica come spam, a seconda della configurazione del DMARC.
Domain Keys Identified Email o DKIM è una firma crittografica generata dal server di posta del mittente e inserita nell'header di ogni mail. Semplificando il più possibile, la mail viene firmata con una chiave privata segreta, nota solo al mittente. Il server del mittente possiede anche una chiave pubblica resa accessibile a tutti tramite un record, esattamente come per l'SPF. Quando il server di posta del destinatario riceve una mail,

verifica il valore presente nell’header applicando la firma pubblica. Se trova corrispondenza, la mail è verificata e accettata. In caso contrario, significa che la mail è stata intercettata e modificata, e viene quindi scartata, se specificato dal DMARC.

Domain-based Message Authentication, Reporting, and Conformance o DMARC verifica semplicemente che i controlli SPF e DKIM siano correttamente superati e stabilisce come procedere qualora uno dei due risultasse non coerente: rifiutando la mail, marcandola come spam o avvisando gli amministratori di dominio di un possibile tentativo di spoofing. Ricordiamo che lo spoofing è una tecnica in cui il mittente maschera il proprio indirizzo email fingendosi qualcun altro.

Nonostante SPF, DKIM e DMARC siano strumenti fondamentali contro il phishing, richiedono una configurazione accurata per evitare che mail legittime vengano segnalate o rifiutate. Google stessa ha imposto a Febbraio 2024 l’obbligo di utilizzare DMARC per la ricezione di mail da altri domini, pena il rifiuto persistente delle mail. È necessario però prendere in considerazione anche un’altra questione, ovvero che nulla possono contro il phishing di tipo typosquatting, i domini simili con sottilissime differenze su alcuni caratteri, poiché questi tre metodi vengono usati anche dagli attaccanti per validare le mail di phishing, proprio nel caso citato. I tre protocolli non definiscono infatti che la mail sia legittima, solo confermano la corretta configurazione del server di posta del mittente.


cyberadmin.it

SPF Record Lookup

spf:cyberadmin.it

```
v=spf1 include:mx.ovh.com -all
```

Prefix	Type	Value	PrefixDesc	Description
Prefix	Typev	Valuespf1	PrefixDesc	DescriptionThe SPF record version
Prefix+	Typeinclude	Valuemx.ovh.com	PrefixDescPass	DescriptionThe specified domain is searched for an 'allow'.
Prefix-	Typeall	Value	PrefixDescFail	DescriptionAlways matches. It goes at the end of your record.

	Test	Result
Status	NameSPF Record Published	ResponseSPF Record found
Status	NameSPF Record Deprecated	ResponseNo deprecated records found
Status	NameSPF Multiple Records	ResponseLess than two records found
Status	NameSPF Contains characters after ALL	ResponseNo items after 'ALL'.
Status	NameSPF Syntax Check	ResponseThe record is valid
Status	NameSPF Included Lookups	ResponseNumber of included lookups is OK
Status	NameSPF Recursive Loop	ResponseNor Recursive Loops on Includes
Status	NameSPF Duplicate Include	ResponseNo Duplicate Includes Found
Status	NameSPF Type PTR Check	ResponseNo type PTR found
Status	NameSPF Void Lookups	ResponseNumber of void lookups is OK
Status	NameSPF MX Resource Records	ResponseNumber of MX Resource Records is OK
Status	NameSPF Record Null Value	ResponseNo Null DNS Lookups found

Figura 76 - Verifica SPF con MXtoolbox

Ricapitolando e semplificando:

- SPF verifica che l’IP sia autorizzato a spedire una mail con quel dominio;
- DKIM è una firma applicata alla email che garantisce la sua non alterazione;
- DMARC sono regole che descrivono come trattare una mail che non ha superato i due precedenti controlli.

Ora che abbiamo compreso le basi e l’importanza di questi protocolli, passiamo a un’analisi più approfondita. Come possiamo verificare questi tre valori dichiarati da un dominio? Uno strumento che abbiamo già incontrato ci viene in aiuto, sto parlando di MXtoolbox: ci permette di interrogare direttamente il dominio, verificando lo stato del record SPF (di tipo TXT, contenente quindi solamente una stringa di testo preformattata) analizzandolo in tutte le sue forme. Nell’esempio in questione si può notare come

v=spf1 indica la versione del protocollo SPF in uso;

include:mx.. specifica quali domini sono autorizzati a inviare email per conto del dominio analizzato;

-all evidenzia una politica di rifiuto rigorosa, solo gli IP definiti da **include:** possono inviare mail per quel dominio.

Quest'ultimo parametro viene chiamato di tipo "hard fail" ed è la politica più restrittiva. Potrete trovare anche:

~all politica meno rigorosa che indica che gli IP non elencati non sono autorizzati, ma che le mail da questi non dovrebbero essere rifiutate immediatamente;

+all politica permissiva che autorizza qualsiasi IP a inviare email per conto del dominio;

?all politica neutrale che non utilizza il valore di SPF come criterio per accettare o rifiutare le email.

Appare evidente come **+all** sia da evitare a ogni costo, **~all** e **?all** siano appropriate solo in casi specifici o per test, mentre **-all** rappresenti la scelta ottimale. Un errore comune nella configurazione del record SPF è la gestione degli IP autorizzati: sia dimenticando di includerli tutti, sia includendone troppi, superando così i limiti massimi consentiti di 10 richieste DNS o 255 caratteri per richiesta.

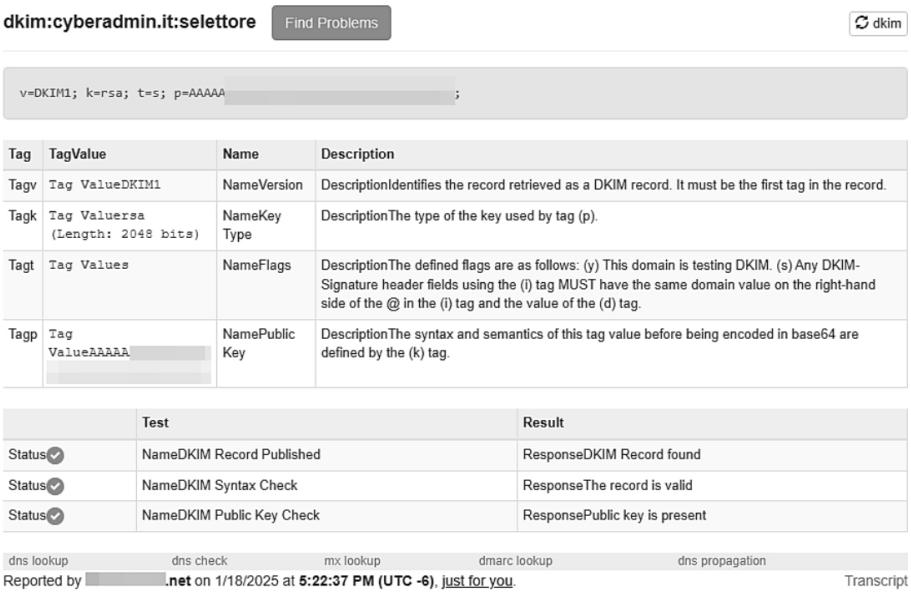


Figura 77 - Verifica DKIM con MXtoolbox

Per verificare il DKIM, il processo è nettamente differente: si parte esaminando l'header della mail ricevuta, individuando il nome del selettore DKIM dichiarato nei campi e utilizzandolo per interrogare il dominio tramite MXtoolbox con il formato:

dkim:dominio.it:nomeselettore

come mostrato in Figura 77. Così facendo, il servizio mostra innanzitutto se ha trovato il relativo record e la sua sintassi, la versione e la lunghezza della chiave pubblica, la versione relativa, la lunghezza di 2048 bit e attuale standard raccomandato che offre un buon compromesso tra sicurezza e prestazioni, e il relativo valore della chiave stessa. Altri valori che potete trovare riguardo la lunghezza della chiave sono:

1024bit considerata ormai obsoleta e non sicura;

4096bit la scelta più sicura disponibile, anche se può risultare meno efficiente nelle prestazioni e non è supportata da tutti i server di posta.

Prima di passare oltre, vorrei farvi notare il **t=s** presente nella chiave, che sta a indicare come il controllo si applichi esclusivamente al dominio indicato e non valga per gli eventuali sottodomini. Questa impostazione garantisce un livello di sicurezza più rigoroso, limitando la validità delle

firme DKIM solamente al dominio principale; ma nel caso in cui sia necessario autorizzare anche i sottodomini è bene non includere questa stringa.

Infine esaminiamo il DMARC, che anche in questo caso risulta presente e valido, come mostrato in Figura 78. Questo è un indicatore positivo della configurazione del dominio, dove la policy mostra che:

p=quarantine le email che non superano i controlli SPF e DKIM vengono spostate nella cartella spam del destinatario;

sp=reject per i sottodomini del dominio viene applicato un rifiuto totale dei messaggi non conformi, senza nemmeno passare dalla cartella spam;

pct=100 indica che la policy viene applicata alla totalità dei messaggi.

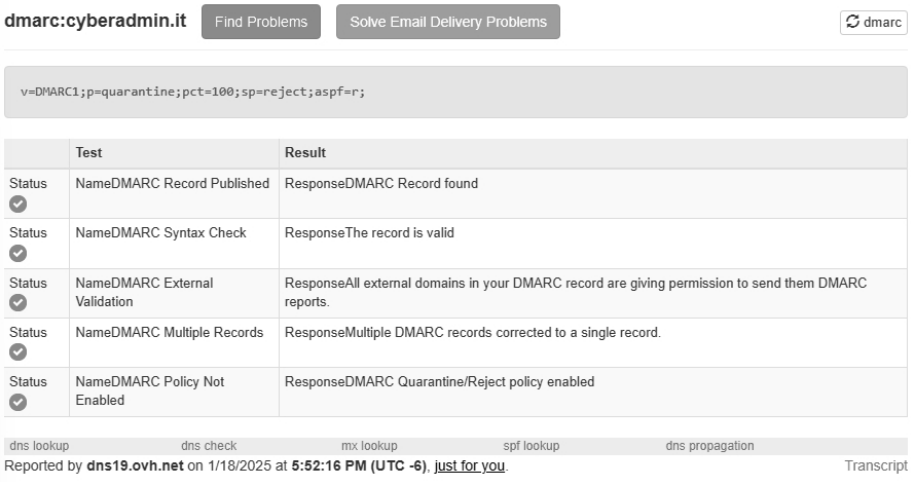


Figura 748 - Verifica DMARC con MXtoolbox

Non sono specificati indirizzi email per la notifica di abusi e spoofing, che potrebbero essere aggiunti tramite una stringa dedicata come

ua=mailto:abuse@cyberadmin.it;ruf=mailto:abuse@cyberadmin.it.

Inoltre, si sarebbe potuto utilizzare **p=reject** al posto di **p=quarantine**, per rifiutare direttamente i messaggi del dominio principale, come già avviene per i sottodomini. È necessario però sottolineare che la configurazione del

DMARC va implementata in modo graduale per evitare interferenze o blocchi con la consegna delle email legittime, iniziando prima con **p=none** e gli indirizzi per la notifica abilitati, così da monitorare i risultati. Poi passare a una policy intermedia, **p=quarantine** come nell'esempio e solo infine a **p=reject**.

Spero sia tutto chiaro, non è facile racchiudere il funzionamento di questi tre protocolli mantenendone la coerenza in così poche pagine.

31 QUANTO È COMPLESSO REALIZZARE UN ATTACCO

Oggi orchestrare attacchi di phishing o diffondere malware è diventato sorprendentemente semplice e non richiede più competenze tecniche avanzate. Servizi nel dark web come il “Phishing-as-a-service” e il “Malware-as-a-service” hanno eliminato ogni barriera d’ingresso, offrendo portali e forum privati dove chiunque può creare, richiedere malware e campagne di phishing. Una sorta di shopping online dell’underground: invece di acquistare una bicicletta, si possono comprare credenziali rubate, documenti d’identità e passaporti, vulnerabilità non pubbliche, firme reali e certificate, codici malevoli pronti all’uso e perfino accessi diretti a computer o server precedentemente attaccati, con prezzi che variano da pochi dollari fino a cifre a cinque zeri. A questo si aggiungono le transizioni economiche anonime, facilitate dall’uso delle criptovalute che rendono difficile il tracciamento delle due parti, e programmi di affiliazione, premiando gli utenti che attirano nuovi accessi.

Nel campo del phishing, i servizi “Phishing-as-a-service” offrono piattaforme complete per generare email altamente personalizzate, spesso basate su modelli sottratti o clonati dai marchi più famosi. Grazie a una completa automazione, un attaccante può avviare campagne massicce in pochi minuti da un semplice dispositivo come un computer o uno smartphone, adattando i messaggi alle lingue e ai contesti locali, senza bisogno di avere una struttura hardware alle spalle e una capacità di calcolo per gestire una campagna di phishing. È davvero sufficiente una connessione internet e un dispositivo di consumo pronto all’uso per far

partire un attacco. Giusto per farvi comprendere ulteriormente il livello di professionalità di questi servizi, spesso offrono anche il supporto tecnico e, ad attacco avviato, una reportistica avanzata che consente di monitorare l'efficacia delle campagne quasi in tempo reale.

Nel caso del "Malware-as-a-Service" invece, gli attaccanti possono acquistare qualsiasi tipo di malware già discusso nel capitolo dedicato, integrandolo e personalizzandolo nelle proprie campagne attraverso hosting anonimi temporanei in paesi con legislazioni più permissive. Anche qui spesso si trova un supporto tecnico di alto livello, oltre che piani di abbonamenti a più livelli, rendendo quasi superflua la necessità di saper programmare codice malevolo. Ancora una volta, è sufficiente anche soltanto lo smartphone che tenete in tasca, per un attacco di phishing di alto livello.

Per concludere questa brevissima panoramica, dal punto di vista dell'attaccante il phishing rappresenta un metodo estremamente vantaggioso che garantisce alti profitti con rischi minimi. La difficoltà nel rintracciare l'origine di queste frodi, unita alla possibilità di operare a livello internazionale e di raggiungere facilmente numerose potenziali vittime con sforzi ridotti, rende questo crimine particolarmente complesso da contrastare. E se siete ancora convinti che i vostri dati personali siano preziosi e valgano realmente qualcosa in questo mercato, sappiate che potrebbero già essere in vendita a pochi centesimi.

32 DIECI DOMANDE COMUNI

- Ho aperto una mail di phishing: devo preoccuparmi?

No, la semplice apertura di una mail non comporta alcun rischio per l'utente. Tuttavia, è importante sapere che aprendola si potrebbe confermare all'attaccante che il tuo indirizzo mail è attivo e monitorato, tramite il già citato "ghost pixel": un'immagine nascosta grande 1x1 pixel che va a richiamare un indirizzo URL e che, al caricamento, ne conferma la vostra apertura.

- Ho cliccato su un link in una mail e ho inserito le credenziali di accesso su un sito, per poi accorgermi che l'indirizzo era chiaramente un tentativo di phishing. Non ho premuto invio né tentato di fare login, sono comunque a rischio?

Sì, cambia immediatamente le credenziali e verifica che la password utilizzata non sia in uso anche in altri servizi. I siti fake sono progettati per registrare automaticamente ogni inserimento in un log eventi. Quindi anche se non hai cliccato su conferma, le credenziali che hai digitato vanno considerate compromesse.

- Il servizio **haveibeenpwned.com** indica che sono stato vittima di vari data breach, cosa devo fare?

Niente panico, identifica i servizi compromessi e cambia immediatamente le password. Se non l'hai ancora fatto, attiva la verifica in due fattori (la MFA ricordi?) per impedire accessi non autorizzati al tuo account.

- Ho ricevuto una mail di phishing da una banca di cui non sono cliente, sono al sicuro?

Assolutamente sì, il tuo indirizzo email è semplicemente finito in una lista utilizzata per le campagne di phishing. Per fortuna, in questo caso il servizio non è tra quelli che utilizzi. Segnala la mail come spam per migliorare il filtro e cancellala senza preoccupazioni.

- ➢ Se ho fatto doppio click sull'allegato di una mail di phishing, cosa rischio?

Non esiste una risposta precisa a questa domanda, poiché ci sono tre possibili scenari, ma una scansione dell'antivirus è d'obbligo in tutte e tre. Nel primo caso, se la mail di phishing appartiene a vecchie campagne non più attive, l'allegato, il dropper, potrebbe aver tentato di scaricare il codice malevolo senza successo terminando senza conseguenze. Nel secondo caso invece, se l'antivirus ti avvisa di aver bloccato un tentativo di attacco, potrebbe essere sufficiente eseguire una scansione approfondita del PC per verificare che nulla sia penetrato nel sistema, ma se l'antivirus ha svolto il suo compito, dovresti essere al sicuro. Il terzo caso è il più pericoloso: se l'antivirus non ha segnalato nulla, potrebbe non aver rilevato il malware che sta già infettando il dispositivo. In questa situazione, spegnilo immediatamente e fallo controllare da un tecnico informatico di fiducia.

- ➢ Posso fidarmi dei messaggi che chiedono di verificare il mio account o aggiornare la password?

Se la richiesta di verifica arriva inaspettatamente, senza una tua operazione specifica che lo presuppone come magari una registrazione a un nuovo servizio, è quasi certamente una mail di phishing.

- ➢ Ho ricevuto una telefonata in cui mi chiedono dati personali o bancari, è phishing?

Vale come la domanda sopra, se non stai effettuando operazioni particolari, non conosci l'interlocutore e la telefonata arriva inaspettatamente, quasi certamente è un tentativo di phishing. Non fornire alcun dato personale, anche la più insignificante delle informazioni può essere utilizzata per creare una lista di password possibili per attaccare e compromettere i tuoi account.

- ➢ È normale che un’email di phishing non finisca sempre nella cartella spam?

Certo che sì, come abbiamo visto la sfida tra attaccanti e difensori è in continua evoluzione. Per questo motivo, non tutte le email di phishing vengono intercettate dai filtri automatici. Quando gestisci la posta elettronica, mantieni sempre alta l’attenzione: è meglio cancellare una email in più che rischiare di cliccare su un link pericoloso.

- ➢ Il phishing può avvenire anche tramite finte fatture o documenti ufficiali? E tramite PEC?

Capita frequentemente di ricevere fatture manipolate dove l’email sollecita un pagamento urgente e, nonostante sia l’indirizzo email che il contenuto appaiono legittimi e coerenti con le comunicazioni precedenti, l’IBAN di destinazione risulta modificato con uno non corrispondente allo storico. Questa situazione indica probabilmente che la casella email è stata compromessa ed è in corso un tentativo di phishing alla supply chain. Anche via PEC, il phishing è presente anche sulla posta certificata.

- ➢ Esiste un sito attendibile e certificato per aggiornarsi sulle campagne di phishing e verificare quelle nuove, così da essere preparati?

Esistono numerose testate giornalistiche e siti di informazione autorevoli che forniscono aggiornamenti periodici sul tema, ma il sito italiano ufficiale di riferimento resta:

https://cert-agid.gov.it

dove è possibile monitorare tutte le campagne di phishing settimanalmente.

FONTI

[1] 3rd May 1978: The world's first 'spam' email sent by Gary Thuerk of Digital Equipment Corporation, HistoryPod

https://www.youtube.com/watch?v=Q4Icfk0gq-c

[2] Pensieri lenti e veloci, Daniel Kahneman, Oscar Mondadori

https://www.oscarmondadori.it/libri/pensieri-lenti-e-veloci-daniel-kahneman/

[3] Financial cyberthreats in 2023, AO Kaspersky Lab

https://securelist.com/financial-threat-report-2023/112526/

[4] What Is the Fight-or-Flight Response? Kendra Cherry, MSEd

https://www.verywellmind.com/what-is-the-fight-or-flight-response-2795194

[5] RFC 5322, Internet Engineering Task Force

https://datatracker.ietf.org/doc/html/rfc5322

[6] Widespread malware campaign seeks to silently inject ads into search results, affects multiple browsers, Microsoft 365 Defender Research Team

https://www.microsoft.com/en-us/security/blog/2020/12/10/widespread-malware-campaign-seeks-to-silently-inject-ads-into-search-results-affects-multiple-browsers/

[7] The 12 Most Common Types of Malware, Kurt Baker

https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/

[8] Che cos'è un Remote Access Trojan (RAT)?, Proofpoint

https://www.proofpoint.com/it/threat-reference/remote-access-trojan

[9] Ten Stats that Reveal How Today's Cyber Attacks Target People First, Not Infrastructure, Ken Brown, Proofpoint https://www.proofpoint.com/us/corporate-blog/post/ten-stats-reveal-how-todays-cyber-attacks-target-people-first-not-infrastructure

[10] 10 Most Popular Email Providers in 2024, Abigail Bosze https://www.doofinder.com/en/statistics/most-popular-email-providers

[11] RFC 5490, Internet Engineering Task Force

https://datatracker.ietf.org/doc/html/rfc3490

[12] Sintesi riepilogativa delle campagne malevole nella settimana del 28 dicembre – 3 gennaio, Computer Emergency Response Team, Agenzia per l'Italia Digitale

https://cert-agid.gov.it/news/sintesi-riepilogativa-delle-campagne-malevole-nella-settimana-del-28-dicembre-3-gennaio/

[13] The MITRE Corporation

https://attack.mitre.org/

[14] How the Necro Trojan infiltrated Google Play, again, Dmitry Kalinin, AO Kaspersky Lab

https://securelist.com/necro-trojan-is-back-on-google-play/113881/

[15] Operation Triangulation: iOS devices targeted with previously unknown malware, Igor Kuznetsov, Valentin Pashkov, Leonid Bezvershenko, Georgy Kucherin, AO Kaspersky Lab

https://securelist.com/operation-triangulation/109842/

[16] Browser Notification Scam: How to Spot and Avoid it, Trend Micro Incorporated

https://helpcenter.trendmicro.com/en-us/article/tmka-10274

[17] F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein and P. S. Park, "Devising and Detecting Phishing Emails Using Large Language Models," in IEEE Access, vol. 12, pp. 42131-42146, 2024, doi: 10.1109/ACCESS.2024.3375882 https://ieeexplore.ieee.org/document/10466545

[18] The "Grandma" jailbreak is absolutely hilarious, ShotgunProxy, Reddit

https://www.reddit.com/r/ChatGPT/comments/12uke8z/the_grandma_jailbreak_is_absolutely_hilarious/

[19] What is Worm GPT? The new AI behind the recent wave of cyberattacks, Sofia Mahirova, Dazed

https://www.dazeddigital.com/life-culture/article/60376/1/what-is-worm-gpt-the-new-ai-behind-the-recent-wave-of-cyberattacks

[20] Google Dorks, ExploitDB

https://httplab.it/GoogleDorks

[21] Awesome OSINT, Jivoi, GitHub

https://github.com/jivoi/awesome-osint

[22] Stuxnet

https://it.wikipedia.org/wiki/Stuxnet

[23] History of Ransomware, Kurt Baker, Crowdstrike

https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/history-of-ransomware/

[24] WannaCry ransomware attack, Wikipedia

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

INFORMAZIONI SULL'AUTORE

Marco Fabbri è un esperto in ambito cybersecurity con oltre tredici anni di esperienza attiva sul campo, un ethical hacker master attivo nel settore e uno dei leader della community italiana di Veeam, riferimento mondiale di soluzioni per il backup.

Lavora come pentester, red team e sistemista senior presso IT4YOU, gemma di creatività artigiana del nord Italia nel panorama della cybersecurity, maggiori informazioni su: **www.it4you.it**.

Lettore appassionato, è anche autore di quattro libri per l'infanzia e recensore per le più importanti case editrici italiane di libri per bambini.

Per contatto: **linkedin.com/in/marco-fabbri-it/**