mimecast

RISK RADAR

RILEVAMENTO | ANALISI | AZIONE

# RAPPORTO GLOBALE DI INTELLIGENCE SULLE MINACCE

LUGLIO-DICEMBRE 2024

# CONTENUTO.

# INTRODUZIONE.

01

Una solida intelligence sulle minacce è diventata cruciale per le aziende al fine di difendersi dalla crescente destrezza dei criminali informatici. Le aziende di tutte le dimensioni dovrebbero informarsi sulle ultime tendenze, monitorare le minacce che colpiscono il settore e i fornitori, rafforzare le difese e aggiornare i processi per evitare che le comunicazioni aziendali e le persone vengano usate contro di loro.

Nella seconda metà del 2024, Mimecast ha elaborato oltre 90 miliardi di punti dati per i suoi quasi 43.000 clienti, segnalando più di 5 miliardi di minacce durante un periodo di sei mesi. Il numero totale di interazioni protette ha superato di molte volte quel valore.
Gli strumenti di posta elettronica e collaborazione continuano a essere i canali attraverso i quali la maggior parte dei criminali informatici inizia a violare le aziende prese di mira, consentendo a Mimecast di rilevare e analizzare numerose minacce prima che diventino note.

**Nella seconda metà del 2024, Mimecast ha elaborato oltre 90 miliardi di punti dati per i suoi quasi 43.000 clienti, segnalando più di 5 miliardi di minacce durante un periodo di sei mesi.**

Per il report H2 2024 Global Threat Intelligence, Mimecast ha raccolto dati dai suoi sistemi che proteggono decine di milioni di utenti, fornito le informazioni dettagliate dei suoi analisti di intelligence e integrato informazioni di intelligence open source sulle minacce più recenti. Il report include l'analisi dell'attività delle minacce, statistiche che rivelano le tendenze degli attacchi e una serie di raccomandazioni per le piccole e grandi imprese per proteggere i dipendenti e ridurre l'impatto degli utenti a rischio.

Ti invitiamo a consultare il nostro report dedicato alla threat intelligenze del secondo semestre 2024 e prevediamo di condividere ulteriori approfondimenti in futuro.

# SINTESI.

**NELLA SECONDA METÀ DEL 2024, I CRIMINALI INFORMATICI HANNO UTILIZZATO SEMPRE PIÙ SERVIZI LEGITTIMI PER OFFUSCARE GLI ATTACCHI E TENTARE DI ELUDERE LE DIFESE.**

La tendenza dell'utilizzo di servizi legittimi (LOTS, Living Off Trusted Sites) per serrare attacchi implica che le aziende dovranno affidarsi a qualcosa di più dei semplici sistemi di reputazione e autenticazione per proteggersi dagli attacchi alla messaggistica e incentrati sulle persone. Inoltre, i criminali informatici sfruttano fornitori terzi, che si tratti di un fornitore di servizi o di un prodotto software, per infiltrarsi più facilmente in una rete.

02

**LA GEOPOLITICA HA FORNITO AI CRIMINALI INFOMATICI IL MOTIVO PER TENTARE COMPROMESSI PIÙ FREQUENTI NONCHÉ UNA RICCA FONTE DI ARGOMENTI PER CREARE GLI ATTACCHI.**

I gruppi al soldo dello stato hanno continuato a ricorrere ad attacchi informatici e allo spionaggio informatico per perseguire azioni confutabili contro i loro rivali. La Cina ha compromesso le infrastrutture statunitensi e canadesi[1], Iran e Israele hanno preso di mira le reciproche infrastrutture[2], e la Russia ha continuato a prendere di mira le aziende[3] europee e statunitensi dopo lo stallo dell'invasione dell'Ucraina.

1. Tunney, Catharine. "China 'compromised' Canadian government networks and stole valuable info: spy agency." CBC. 30 October 2024. https://www.cbc.ca/news/politics/cse-cyber-threats-china-1.7367719
2. Lemos, Robert. "As Geopolitical Tensions Mount, Iran's Cyber Operations Grow." Dark Reading. News article. 18 September 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow
3. Eddy, Nathan. "Ukraine-Russia Cyber Battles Tip Over Into the Real World." Dark Reading. News article. 3 October 2024. https://www.darkreading.com/cyberattacks-data-breaches/ukraine-russia-cyber-battles-tip-over-into-real-world

## LE TECNOLOGIE DI IA CONTINUANO A OFFRIRE VANTAGGI UNICI SIA AI DIFENSORI CHE AI CRIMINALI INOFMRATICI.

Gli analisti della sicurezza informatica possono analizzare più rapidamente i potenziali eventi legati alla sicurezza con l'aiuto degli assistenti IA, mentre chi è deputato a rispondere agli incidenti può utilizzare l'IA per bloccare e risolvere un attacco in modo più rapido e completo. Anche i criminali informatici ne stanno usufruendo: una ricerca di Mimecast  svolta[4] utilizzando l'analisi linguistica ha scoperto che circa il 12% delle email, inclusi gli attacchi di phishing, mostrava segni di essere stato scritto da modelli linguistici di grandi dimensioni (LLM). Audio e video deepfake sono stati utilizzati efficacemente per imitare i CEO e ordinare ai dipendenti di effettuare pagamenti fraudolenti sui conti dei criminali informatici.

## TUTTE QUESTE TENDENZE CONTINUERANNO NEL 2025.

Il numero di attacchi che hanno utilizzato il cloud in una certa misura è più che raddoppiato nel 2024, mentre la geopolitica si fa sempre più caotica, con Francia e Germania che affrontano le elezioni in Europa, il presidente degli Stati Uniti Donald Trump in carica per un secondo mandato non consecutivo e Russia e Cina che continuano a ostentare i loro eserciti sulla scena mondiale. Sia i ricercatori della sicurezza che i criminali informatici stanno sviluppando nuovi metodi per sfruttare i sistemi di IA, sfruttando le lacune della sicurezza o potenziando le strategie di attacco.

4. Lee, Evonne. "New Mimecast Threat Intelligence: How ChatGPT Upended Email." Mimecast Threat Intelligence Blog. 30 September 2024. https://www.mimecast.com/blog/how-chatgpt-upended-email/.

# PRINCIPALI CONCLUSIONI.

**Sebbene l'attività dei criminali informatici sia aumentata in base a quasi tutti i parametri, emergono alcune tendenze.**

03

OCTO

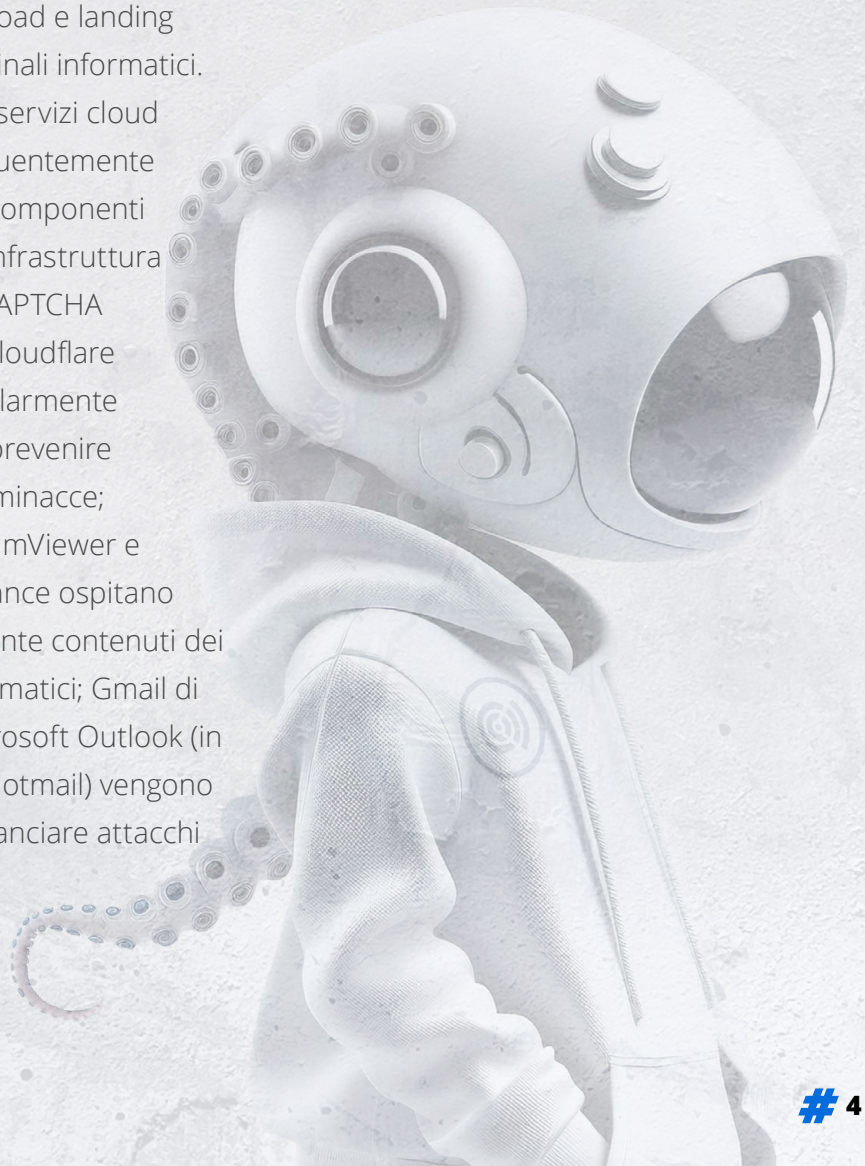
SPECIES

Maestri **dell'analisi** con un sistema nervoso altamente sviluppato e un cervello di grandi dimensioni. Eccellono nell'adattarsi al loro ambiente e nel superare le sfide, il che li rende dei veri e propri campioni nell'intelligence sulle minacce.

## P-1

### I CRIMINALI INFORMATICI UTILIZZANO SEMPRE PIÙ SPESSO SERVIZI LEGITTIMI (LOTS).

I servizi cloud di Microsoft, Google ed Evernote spesso ospitano payload e landing page dei criminali informatici. Tuttavia, altri servizi cloud vengono frequentemente utilizzati per componenti specifici dell'infrastruttura di attacco: i CAPTCHA Turnstyle di Cloudflare vengono regolarmente utilizzati per prevenire l'analisi delle minacce; DocuSign, TeamViewer e Wave Compliance ospitano inavvertitamente contenuti dei criminali informatici; Gmail di Google e Microsoft Outlook (in precedenza Hotmail) vengono utilizzati per lanciare attacchi di phishing.



## P-2

### LA GEOPOLITICA AUMENTA LA PROBABILITÀ DI ATTACCHI INFORMATICI.

Le elezioni francesi e tedesche, insieme alla continua incertezza legata alla guerra tra Russia e Ucraina, aumenteranno la tensione nella politica dell'Unione Europea. L'allontanamento da parte del governo degli Stati Uniti da normative prederminate potrebbe anche portare a un aumento dell'attività in ambito cyber. Gli esperti di business, politica e sicurezza informatica da tempo sottolineano che le tensioni geopolitiche e i rischi per la sicurezza informatica sono collegati. I due rischi principali identificati per il 2025 nel sondaggio annuale Systemic Risk Barometer condotto dalla società Depository Trust and Clearing Corporation sono il rischio geopolitico e il rischio informatico[5].

## P-3

### LE PRINCIPALI TECNOLOGIE DI AUTENTICAZIONE DELLE EMAIL HANNO AUMENTATO GLI OSTACOLI PER I CRIMINALI INFORMATICII, MENTRE L'IA HA SEMPLIFICATO LORO LA VITA,

Utilizzando servizi affidabili, i criminali informatici possono soddisfare i crescenti requisiti di autenticazione delle tecnologie email, come SPF, DKIM e DMARC, e apparire come provenienti da una fonte affidabile. Sebbene le tecnologie rendano i loro attacchi più complicati, i criminali informatici continuano a trovare servizi per superare i controlli di autenticazione e allineamento. Inoltre, la diffusione dei chatbot IA consente anche agli aspiranti criminali informatici di acquisire le competenze necessarie per perpetrare violazioni.

5. "Geopolitical and Cyber Risks Remain Top Threats to the Financial Services Sector in 2025." DTCC. 4 December 2024. https://www.dtcc.com/news/2024/december/04/geopolitical-and-cyber-risks-remain-top-threats-to-the-financial-services-sector-in-2025

## P-4

**I SETTORI ARTE, INTRATTENIMENTO E TEMPO LIBERO, SERVIZI LEGALI E MEDIA ED EDITORIAHANNO REGISTRATO IL MAGGIOR NUMERO DI MINACCE PER UTENTE NEL SECONDO SEMESTRE DEL 2024.**

Sono state osservate notevoli differenze nei profili di minaccia tra i vari settori., tra cui unamaggior quantità  di file dannosi che hanno preso di mira i settori dell'arte, dell'intrattenimento e del Tempo libero, mentre gli addetti al settore Media ed Editoria hanno riscontrato un numero maggiore di link dannosi. Gli attacchi di furto d'identità sono stati prevalenti per il settore software e SaaS.

## P-5

**GLI ESSERI UMANI CONTINUANO AD ESSERE IL PRINCIPALE PUNTO DEBOLE NELLA MAGGIOR PARTE DELLE VIOLAZIONI.**

La maggior parte delle violazioni è resa possibile da un collaboratore interno che intraprende un'azione che a sua volta consente ai criminali informatici di accedere a risorse sensibili o protette. L'edizione 2024 del report annuale Data Breach Investigations  (DBIR) ha rilevato che oltre due terzi (68%) delle violazioni avvenute nel 2023[6] avevano "un fattore umano non dannoso". Un sondaggio del 2024 su 1.000 dipendenti ha rilevato che un terzo (34%) temeva di rappresentare una vulnerabilità sfruttabile dai criminali informatici, anche se la maggior parte (86%) si considerava esperta di sicurezza informatica[7]. Più della metà degli intervistati teme di perdere il lavoro qualora esponesse la propria azienda a un attacco informatico

6. Verizon Data Breach Investigations Report, 2024
   https://www.verizon.com/business/resources/reports/dbir/#takeaways
7. Why AI fuels cybersecurity anxiety, particularly for younger employees
   https://www.ey.com/en_us/consulting/human-risk-in-cybersecurity

04

# THE THREAT LANDSCAPE



## BAT

### SPECIES

**Rilevare** le minacce è il loro mestiere. Utilizzando l'ecolocalizzazione, emettono suoni ad alta frequenza che rimbalzano sugli oggetti, dando loro una mappa dettagliata dell'ambiente circostante. Questo li aiuta a evitare gli ostacoli, anche in completa oscurità.

04
.1

# IL PANORAMA DELLE MINACCE IN GRAFICI.

Il panorama delle minacce nella seconda metà del 2024 ha evidenziato un crescente utilizzo da parte dei criminali informatici dei servizi cloud rivolti ai consumatori e alle aziende come metodo per evitare il rilevamento. Di conseguenza, diversi importanti servizi cloud sono stati utilizzati per ospitare i contenuti dei criminali informatici e i link continuano ad essere utilizzati come meccanismo per la distribuzione di payload.

Nella seconda metà del 2024, i criminali informatici hanno concentrato l'attenzione sui settori Arte, intrattenimento e tempo libero, Servizi legali e Software e SaaS. Si tratta di un cambiamento rispetto alla prima metà del 2024, quando i settori Bancario, Viaggi e ospitalità e Arte e intrattenimento occupavano i primi posti nell'elenco degli obiettivi. Mentre ogni settore ha subito un numero significativo di attacchi di email inviate in massa da fonti di bassa reputazione, i criminali informatici hanno preso di mira il settore Arte e intrattenimento con un maggior numero di attacchi tramite file dannosi, mentre il settore Servizi legali ha subito più attacchi tramite il furto d'identità.

Ecco come si presenta il panorama delle minacce, secondo i dati.

W 41°24'12.2 "
E 23°44'54.4"
PE-3 NVGT B

## ABUSO DEI SERVIZI CLOUD
## #01

I criminali informatici stanno sfruttando sempre più i servizi legittimi (LOTS) nel tentativo di eludere le difese basate sull'identificazione degli attacchi individuando codice, risorse e servizi online non affidabili. Sebbene alcuni dei servizi scelti dai criminali informatici per ospitare l'infrastruttura d siano scelte ovvie (Google Docs, Evernote.com, Dropbox DocSend, ecc.), altri servizi online sono meno noti, come il sito di pubblicazione interattiva Publuu, l'host di webinar online Wave Compliance e il sito di presentazioni Gamma.

I criminali informatici hanno inoltre utilizzato piattaforme specifiche per inviare email di phishing e diversi siti per ospitare il payload, spesso semplicemente un modulo web o un file con un link. Il sito di email marketing GetResponse, ad esempio, si è rivelato una fonte importante di email di phishing, anche se molte di queste possono non essere dannose, ma solo indesiderate. Sebbene i siti Adobe non siano i principali a ospitare i payload, almeno due siti vengono utilizzati dai criminali informatici per ospitare le landing page iniziali.

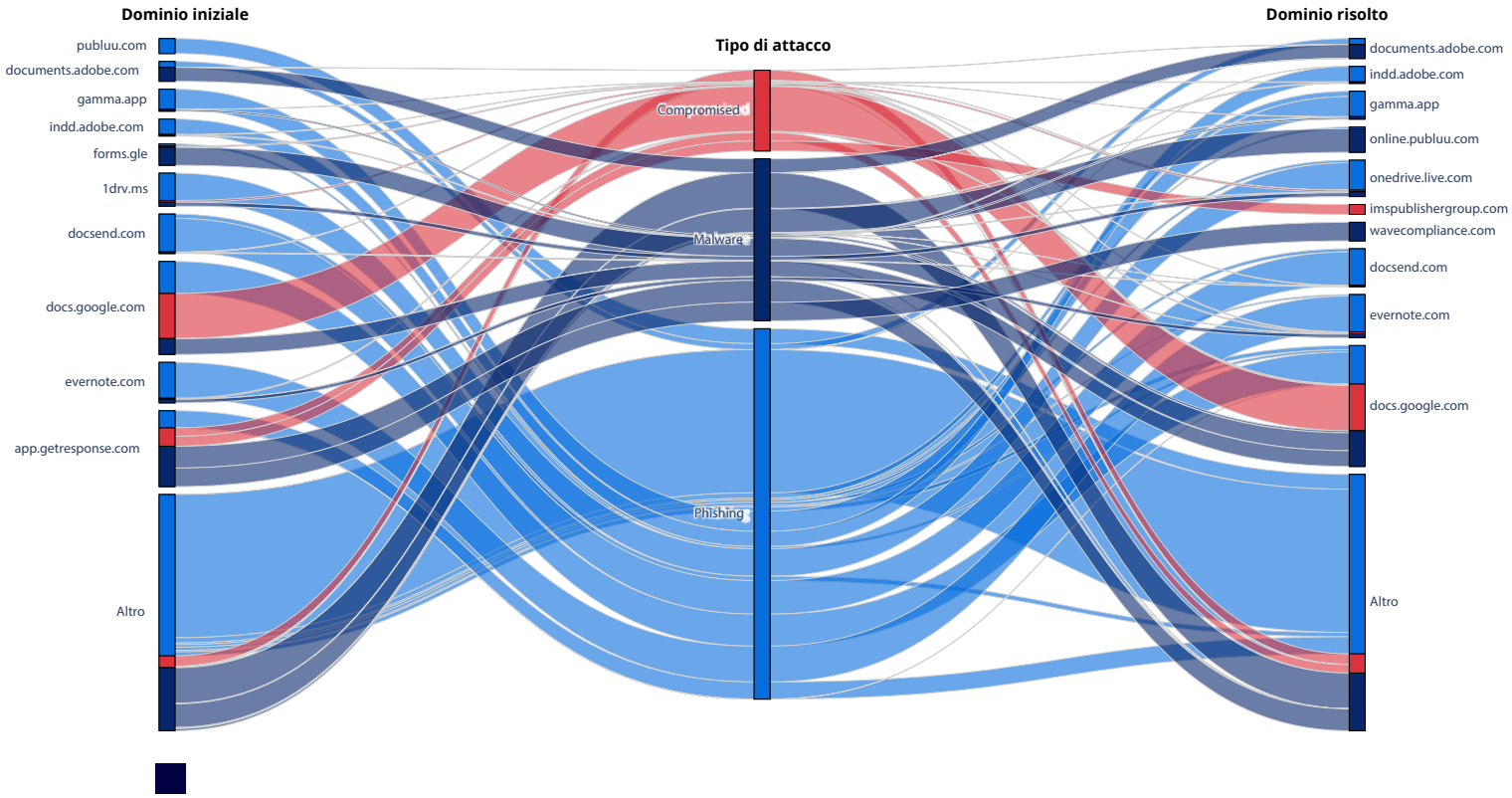



**Grafico 1:** La maggior parte dei domini iniziali corrisponde a domini finali simili, come la maggior parte degli attacchi che utilizzano Evernote inizialmente, ospitando anche un payload. Tuttavia, si riscontra una serie di eccezioni notevoli, in cui una piattaforma ospita la pagina di reindirizzamento iniziale (per esempio un grande volume di spam proveniente dal servizio di marketing GetResponse.com), e una seconda piattaforma che ospita la landing page, come il servizio di formazione e di webinar WaveCompliance.

## TPU PER TIPO DI ATTACCO
## #02

Sebbene lo spam continui a rappresentare la maggior parte dei messaggi bloccati da Mimecast nel secondo semestre del 2024, durante l'estate abbiamo rilevato un aumento dei messaggi email indesiderati. Sebbene tale impennata si sia attenuata entro la fine dell'anno, gli attacchi di phishing, che in genere includono un URL a un sito o servizio controllato dai criminali informatici, hanno registrato una crescita lenta nel corso del semestre.

---

**Mimecast classifica le attività dannose e indesiderate in base alla fase in cui avviene il rilevamento.**

**LO SPAM** intercetta le email inviate in massa provenienti da domini non attendibili e quelle che includono contenuti ampiamente diffusi..

**I MESSAGGI SOSPETTI** sono messaggi, file o URL potenzialmente dannosi; non vengono rilevati contenuti dannosi, ma sono presenti indicatori che dimostrano che il messaggio deve essere trattato con cautela, come se provenisse da un servizio comunemente utilizzato in modo improprio o da una fonte con una bassa reputazione.

**LA CATEGORIA INDESIDERATI** include i messaggi bloccati dall'utente.

**LE MINACCE DI PHISHING** sono progettate per indurre le vittime a rivelare informazioni sensibili, come credenziali o dati di pagamento. Includono link di phishing, BEC, furto d'identità o allegati html progettati per imitare le pagine di accesso.

**I MESSAGGI MALWARE** includono allegati rilevati come dannosi o link che portano al malware.

L'aumento significativo dello spam tra la prima e la seconda metà del 2024 è dovuto all'evoluzione del sistema di rilevamento e alla raccolta dati di Mimecast, non a una tendenza nel volume dello spam. L'aumento dei rilevamenti di spam si verifica perché Mimecast ha aggiunto lo spam trattenuto nel gateway ai dati di rilevamento, che possono essere configurati dall'amministratore, anziché solo le email respinte sicuramente dannose.

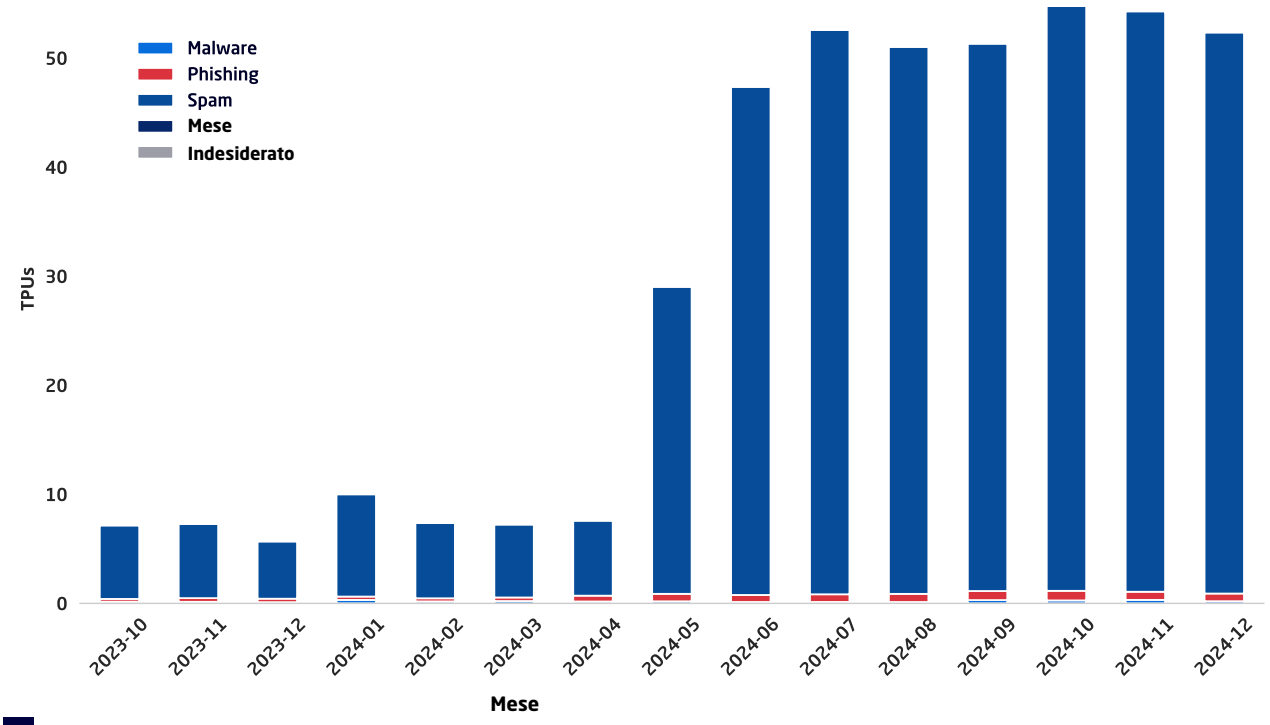



**Grafico 2a:** Il notevole aumento dei rilevamenti di spam segue l'integrazione dello spam trattenuto a livello di gateway, anziché basarsi esclusivamente sulle email respinte come spam; questo cambiamento

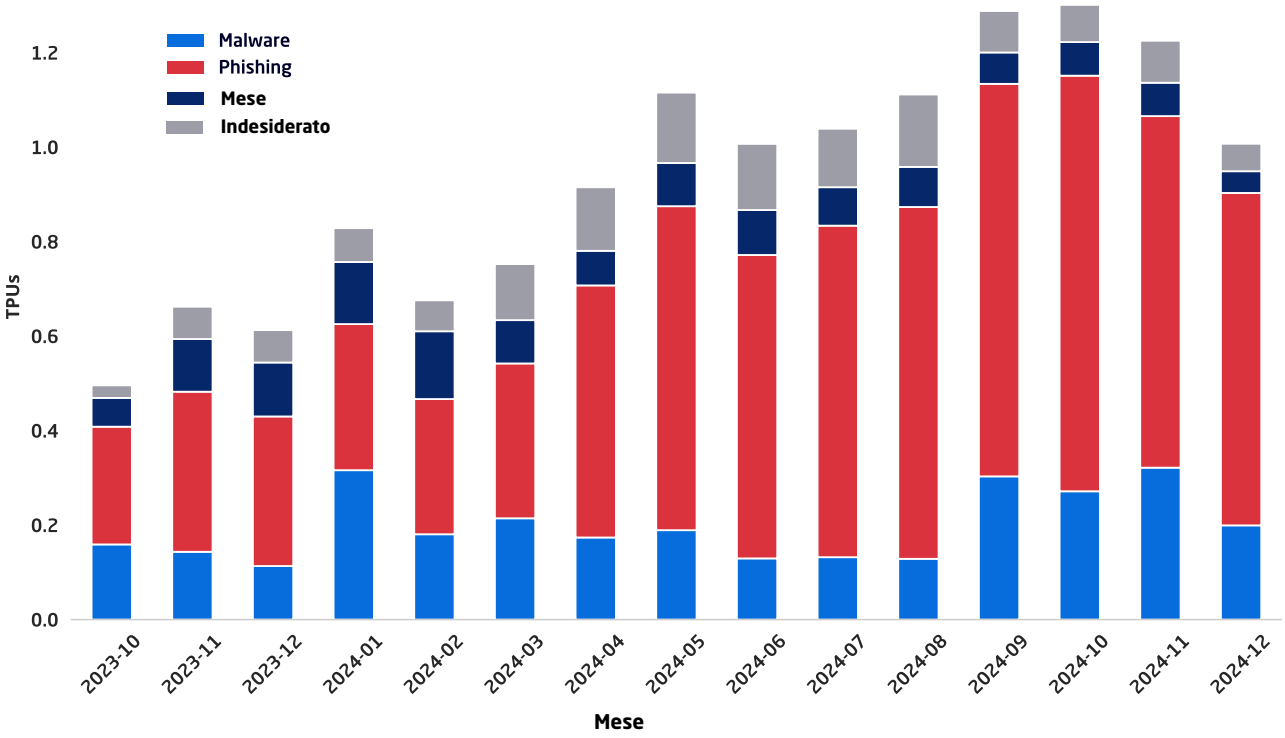



**Grafico 2b:** Rimuovendo l'enorme influenza dello spam, la serie di dati mostra un aumento de phishing nonché un'impennata degli attacchi di malware verso la fine della seconda metà del 2024. Nel dicembre 2024, il rilevamento di malware nell'Africa subsahariana è aumentato del 42,14%, un incremento significativo rispetto all'anno precedente, causato dall'instabilità politica e dall'aumento dell'attività cibernetica. Inoltre, la regione sta assistendo a un aumento degli attacchi ransomware, sempre più opportunistici, spesso sfruttando le vulnerabilità e diffusi come infezioni secondarie, indicando una tendenza preoccupante nel panorama delle minacce.

## PRINCIPALI SETTORI COLPITI PER TPU

## #03

I criminali informatici tendono a utilizzare diversi tipi di attacchi per colpire vari settori, conferendo a ciascun settore un profilo di minaccia unico. Il settore Arte, intrattenimento e tempo libero (il settore più attaccato dopo la rimozione della grande quantità di spam) ha riscontrato il maggior numero di minacce per utente (TPU), laddove la maggior parte degli attacchi è costituita da email e messaggi con payload dannosi.

I settori dei servizi professionali, Servizi legali, Media ed editoria sono al secondo posto in termini di intensità delle minacce, con quasi 9 TPU ciascuno. I criminali informatici hanno preso di mira il settore dei Servizi legali con un numero maggiore di attacchi di furto d'identità, mentre il settore Media ed editoria ha riscontrato un numero elevato di URL dannosi.

Ogni settore si trova ad affrontare un volume significativo di spam e minacce che vengono rilevate poiché i criminali informatici utilizzano infrastrutture a bassa reputazione. Nell'ambito dell'analisi, Mimecast ha rimosso i messaggi email inviati in massa (rilevati come spam o a bassa reputazione) che corrispondevano rispettivamente a 17 TPU e 5 TPU.

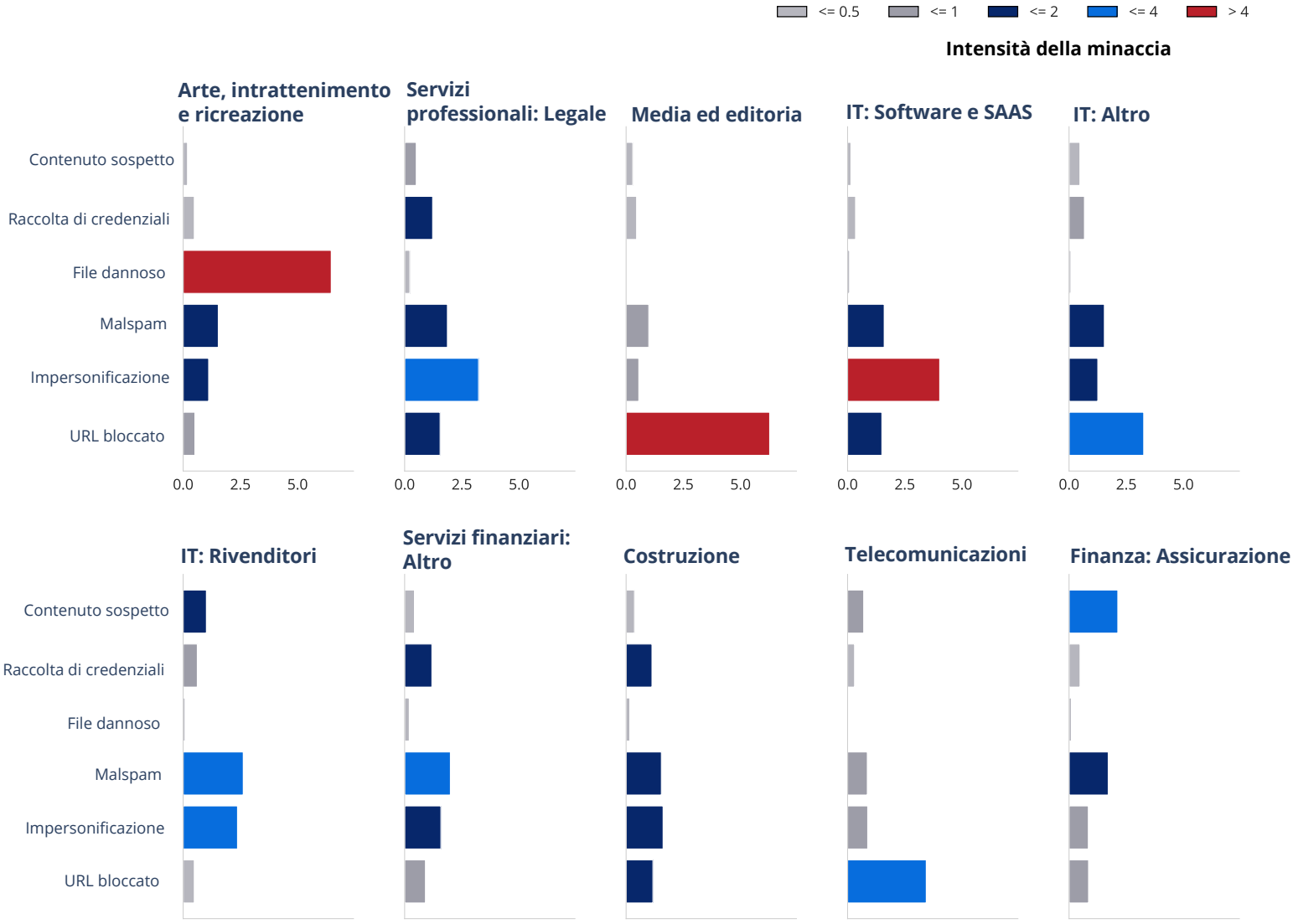



**Grafico 3 :** Il profilo di minaccia per i 10 settori principali, escludendo le categorie Spam e Bassa reputazione poiché tendono a sovraccaricare i dati. I conteggi delle TPU (asse x) sono in formato logaritmico.

# GRUPPI DI MINACCE
# #04

L'attività di attribuzione delle minacce informatiche è intrinsecamente complessa, specialmente per quanto riguarda le tattiche miste utilizzate da molti criminali informatici e a seguito dell'aumento di modelli di cybercrime-as-a-service come RaaS (Ransomware-as-a-Service), PhaaS (Phishing-as-a-Service) e IAB (Initial Access Brokers). Questi servizi consentono a diversi criminali informatici di riutilizzare gli stessi strumenti e la stessa infrastruttura, portando al lancio di campagne simili da parte di gruppi completamente diversi. I criminali informatici spesso impiegano una combinazione di tecniche da diversi vettori di attacco e cambiano frequentemente i loro metodi, rendendo difficile individuare un singolo criminali o movente.

I metodi di attribuzione tradizionali, che si basano sull'infrastruttura o sulle firme del malware, sono sempre più inaffidabili. Mimecast si concentra invece sull'analisi delle Tattiche, Tecniche e Procedure (TTP) per classificare e referenziare sistematicamente gli attacchi. Monitorando il modo in cui operano i criminali informatici, raggruppiamo le minacce e identifichiamo i modelli delle campagne, anche quando i metodi di attribuzione tradizionali falliscono. Questo approccio fornisce una comprensione più chiara e affidabile delle funzionalità in evoluzione. Gli attacchi più prolifici con i nomi di attribuzione interni di Mimecast sono evidenziate di seguito insieme alle campagne correlate per descriverne i comportamenti e il potenziale impatto.

Operazione di minaccia a

## TO1014

**Osservato per la prima volta: 2020**

### OBIETTIVO

FURTO DI INFORMAZIONI E SPIONAGGIO

### MIRATO

NORD AMERICA
EUROPA
MEDIO ORIENTE

**Settore**

AVIAZIONE
AEROSPAZIALE
TRASPORTI

OCT 2024

**Ultime campagne**

Operazione di minaccia a

## TO1003

**Osservato per la prima volta: 2018**

### OBIETTIVO

DATA THEFT

### MIRATO

PREVALENTEMENTE AMERICANO

**Settore**

IT
ISTRUZIONE

OCT 2024

**Ultime campagne**

Operazione di minaccia a

## TO3010

**Osservato per la prima volta: 2018**

### OBIETTIVO

CREDENTIAL FOR DISTRIBUTION

### MIRATO

SUDAFRICA

**Settore**

TUTTI

NOV 2024

**Ultime campagne**

Operazione di minaccia a

## TO5004

**Osservato per la prima volta: 2024**

### OBIETTIVO

FINANCIAL

CAMPAIGN INFO

### MIRATO

PRINCIPALMENTE
REGNO UNITO
AMERICANO

**Settore**

PRODUZIONE
IMMOBILIARE
VENDITA AL DETTAGLIO

DEC 2024

**Ultime campagne**

Operazione di minaccia a

## TO3028

**Osservato per la prima volta: 2018**

### OBIETTIVO

RACCOLTA DI CREDENZIALI

CAMPAIGN INFO

### MIRATO

GLOBALE

**Settore**

TUTTI

**Ultime campagne**

Operazione di minaccia a

## TO3001

**Osservato per la prima volta: 2023**

### OBIETTIVO

FURTO DI CREDENZIALI E DATI

### MIRATO

AUSTRALIA

**Settore**

PRINCIPALMENTE ISTRUZIONE

**Ultime campagne**

Operazione di minaccia a

## TO5005

**Osservato per la prima volta: 2020**

### OBIETTIVO

FINANZIARIO

### MIRATO

GLOBALE

**Settore**

TUTTI

**Ultime campagne**

Operazione di minaccia a

## TO3022

**Osservato per la prima volta: 2021**

### OBIETTIVO

RACCOLTA DI CREDENZIALI

### MIRATO

PRINCIPALMENTE REGNO UNITO

**Settore**

TUTTI

**Ultime campagne**

## GRAFICO - PRINCIPALI VULNERABILITÀ NEL TEMPO

# 05

Mentre la maggior parte degli attacchi che tentano di sfruttare le vulnerabilità software si è concentrata su due vulnerabilità molto diffuse (CVE-2017-0199 e CVE-2022-42889), i criminali informatici hanno tentato di sfruttare 89 vulnerabilità software diverse nella seconda metà del 2024. Confrontando le prime 10 vulnerabilità rilevate da Mimecast come parte di un'email o fornite come link, sette hanno un punteggio EPSS (Exploitability Prediction Scoring System) di almeno 0,88, che equivale a una probabilità dell'88% di sfruttamento entro i 30 giorni successivi, mentre due vulnerabilità, entrambe scoperte nel 2024, non sono ancora state registrate come sfruttate.

La mappatura mostra anche la divergenza tra il punteggio EPSS e il punteggio CVSS (Common Vulnerability Scoring System), che tende a correlarsi con la gravità finale dello sfruttamento.

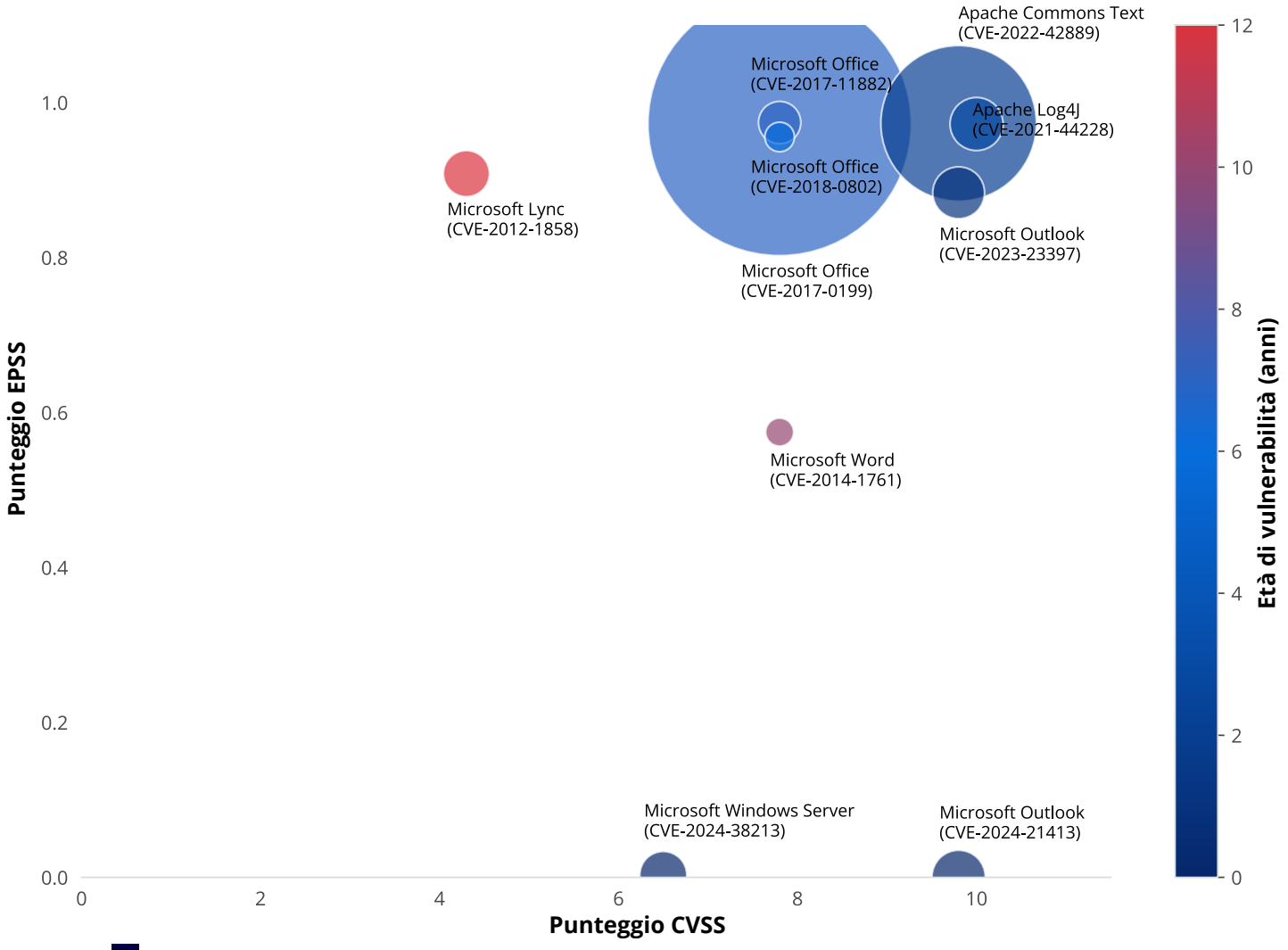



**Grafico 4:** Le prime 10 vulnerabilità rilevate nei messaggi, confrontate in base ai punteggi EPSS e CVSS. Due vulnerabilità diffuse esistono da almeno 10 anni. Dati EPSS raccolti al 15 gennaio 2025.

# PRINCIPALI MINACCE E CAMPAGNE.

04.2

01
SPOOFING APERTO

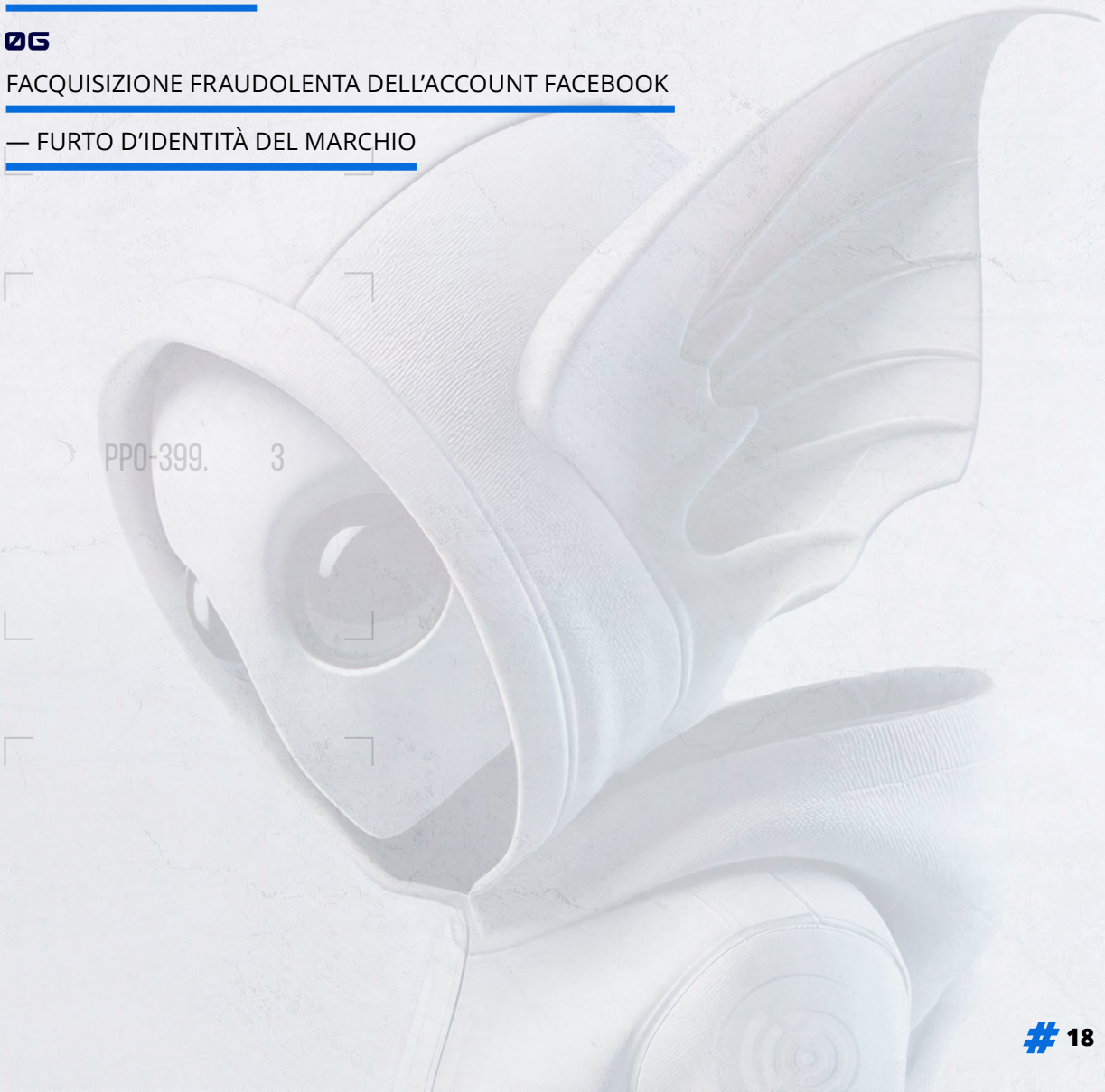
02
VIOLAZIONE DEL COPYRIGHT/NOTIFICA DI ABBONAMENTO

03
COPIA E INCOLLA LINK — TRUFFA PAGAMENTI

04
TRUFFA BEC MIRATA CON DEEPFAKE AUDIOE

05
MANCATA CONSEGNA

06
FACQUISIZIONE FRAUDOLENTA DELL'ACCOUNT FACEBOOK
— FURTO D'IDENTITÀ DEL MARCHIO



# #01 SPOOFING APERTO

**TECNICA** Router consumer compromessi fungono da proxy per l'invio di email di phishing contraffatte attraverso i servizi email dei fornitori di servizi Internet

**SERVIZI UTILIZZATI** Zimbra, MagicMail

**OBIETTIVI** Globale, tutti i settori

READ ARTICLE

**Sfruttamento del router del fornitore di servizi Internet dell'utente finale a causa di vulnerabilità o password inefficaci**

**Configurazione del router per essere utilizzato come proxy**

**Email di phishing inoltrate attraverso i server email dei fornitori di servizi Internet**

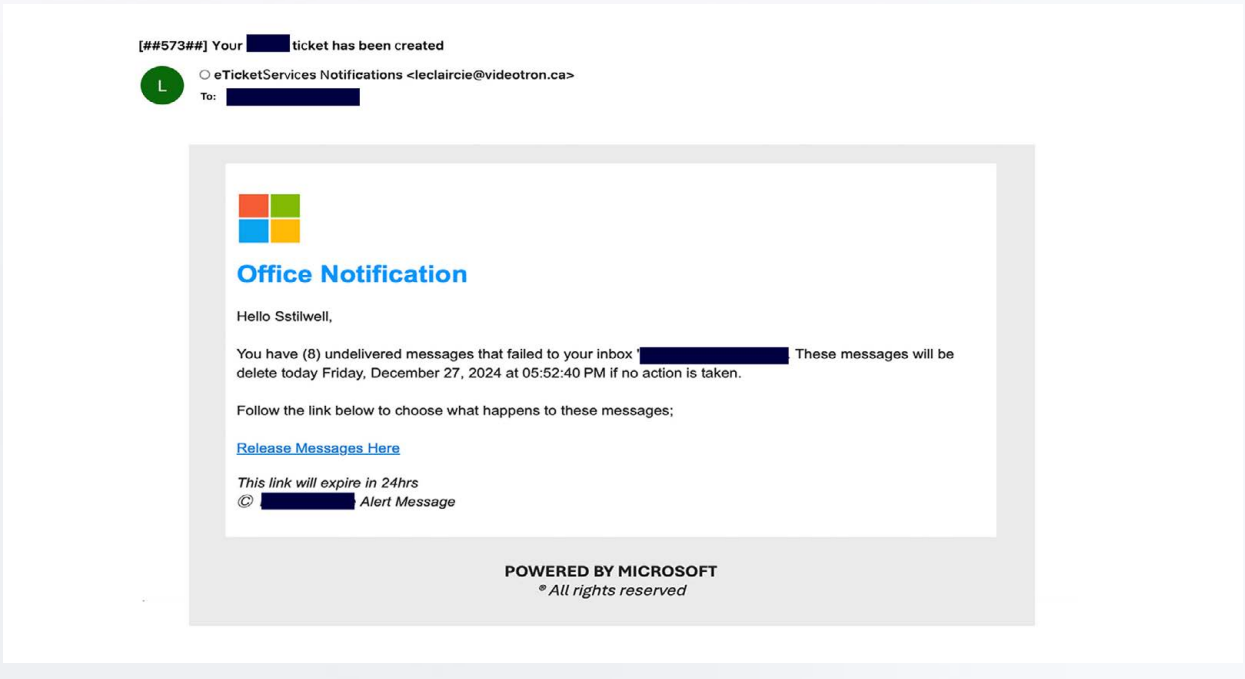
**Collegamenti dannosi ospitati su vari servizi cloud**

**Richiesta di nome utente e password di Microsoft 365**

**Raccolta delle credenziali e reindirizzamento dell'utente alla pagina di accesso autentica di Microsoft 365**

I criminali informatici sfruttano i router compromessi dei consumatori come proxy per inviare campagne di phishing delle credenziali d'accesso su larga scala attraverso i servizi email dei fornitori di servizi Internet, oscurando la loro infrastruttura e eludendo l'autenticazione delle email. Sfruttando i fornitori di servizi Internetcon un'autenticazione debole o addirittura assente delle email in uscita, i criminali informatici ottengono funzionalità di distribuzione ad alto volume e di spoofing dei mittenti senza restrizioni.

I fornitori di servizi Internet interessati identificati dalla nostra indagine utilizzano soluzioni email come Zimbra e MagicMail e sembrano non disporre di misure antispam in uscita efficaci. La combinazione di autenticazione inadeguata e controlli di sicurezza insufficienti consente ai criminali informatici di conseguire tassi di invio elevati e mantenere campagne spam su larga scala senza interruzioni significative.



# #02 VIOLAZIONE DEL COPYRIGHT/NOTIFICA DI ABBONAMENTO

**TECNICA** Rubare l'identità di studi legali con un'esca di avviso di violazione di copyright per il furto di informazioni

**SERVIZI UTILIZZATI** Gmail, Mail Merge

**OBIETTIVI** Globali, ma principalmente con sede nel Regno Unito – settori della vendita al dettaglio, all'ingrosso, dei viaggi e dell'ospitalità

READ ARTICLE

**Email di phishing inviata tramite servizio di mail merge**

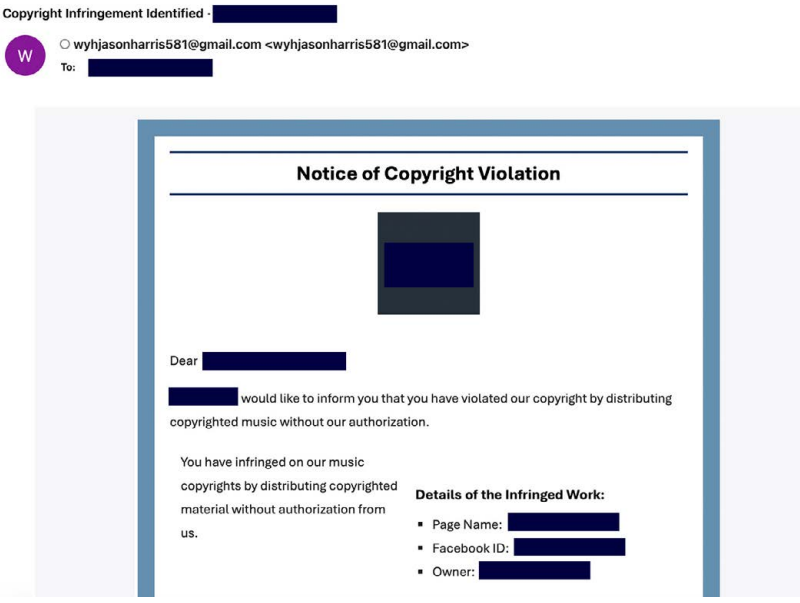
**Link ai contenuti ospitati su Dropbox**

**Download del file zip contenente il file eseguibile**

**Il file eseguibile scarica un infostealer da Github**

**Esfiltrazione dei dati sensibili**

Le email dannose inviate tramite Gmail attraverso un servizio di mail-merge si spacciano per studi legali rispettabili e affermano che le aziende stanno violando i diritti d'autore. L'email contiene un link diretto o un reindirizzamento a Dropbox, che porta al download di un file zip contenente un eseguibile. L'obiettivo delle campagne è utilizzare vari software infostealer per rubare informazioni sensibili dai computer infetti, come credenziali d'accesso e dettagli finanziari.


Copyright Infringement Identified - [redacted]

W wyhjasonharris581@gmail.com <wyhjasonharris581@gmail.com>

To: [redacted]

**Notice of Copyright Violation**

[redacted]

Dear [redacted]

[redacted] would like to inform you that you have violated our copyright by distributing copyrighted music without our authorization.

You have infringed on our music copyrights by distributing copyrighted material without authorization from us.

**Details of the Infringed Work:**

- Page Name: [redacted]
- Facebook ID: [redacted]
- Owner: [redacted]

# #03 COPIA E INCOLLA LINK — TRUFFA PAGAMENTI

**TECNICA** Convincere gli utenti a copiare e incollare un collegamento per eludere le difese

**SERVIZI UTILIZZATI** Amazon Simple Email Service, mailer Python

**DESTINATARI:** principalmente USA - manifatturiero, vendita al dettaglio, servizi legali

READ ARTICLE

**Email di phishing tramite AWS utilizzando il mailer Python**

**All'utente viene richiesto di incollare un URL falsato nel browser**

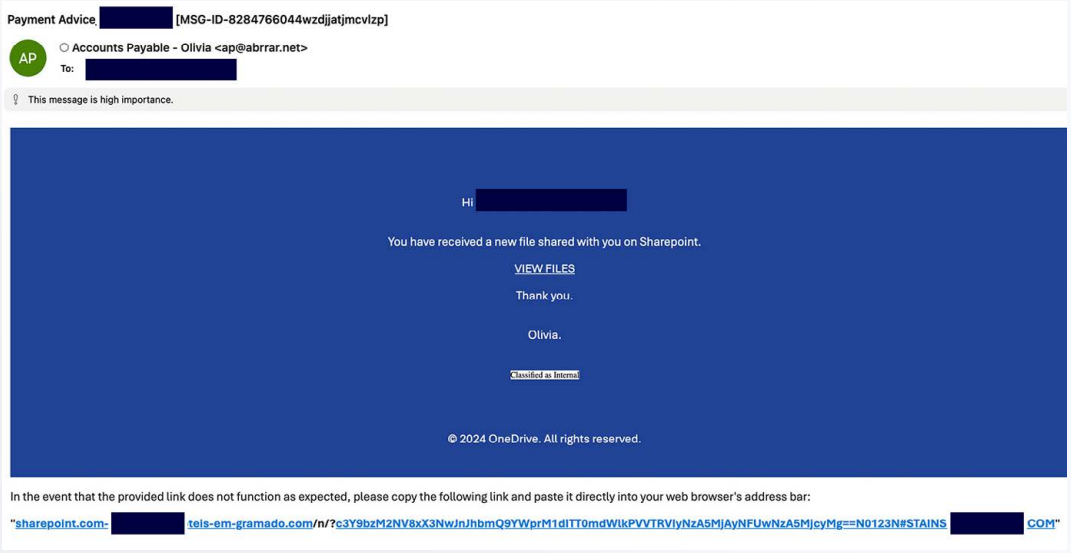
**Reindirizzamento verso un file condiviso ospitato su un falso sito SharePoint**

**Richiesto il nome utente e la password di M365**

**Carta di credito utilizzata o venduta sul mercato nero**

Nel tentativo di eludere i software e i servizi di rilevamento, i criminali informatici cercano di convincere gli utenti a copiare da un'email i link falsati (in cui generalmente manca il prefisso "http://") e incollarli nel browser. Le esche analizzate da Mimecast generalmente includevano un tasto con un link non funzionante e un testo con qualche variante del seguente tenore: "Se il link non funziona, copia e incolla il link qui sotto".

Questa tecnica si aggiunge ad altri metodi di offuscamento, come l'uso di codici QR per rendere i collegamenti illeggibili agli esseri umani e l'uso di tattiche intimidatorie abbinate a numeri di telefono per indurre le vittime a contattare un call center gestito dal criminale informatico. L'obiettivo delle campagne attuali che utilizzano questo attacco è generalmente quello di raccogliere le credenziali d'accesso della vittima.



# #04 TRUFFA BEC MIRATA CON DEEPFAKE AUDIO

**TECNICA** Deepfake audio, violazione dell'email aziendale (BEC)

**SERVIZI UTILIZZATI** Adobe Sign, DocuSign

**OBIETTIVI** Globali - prevalentemente i settori finanziari

READ ARTICLE

**Email BEC tramite Docusign o AdobeSign**

**L'utente firma l'NDA**

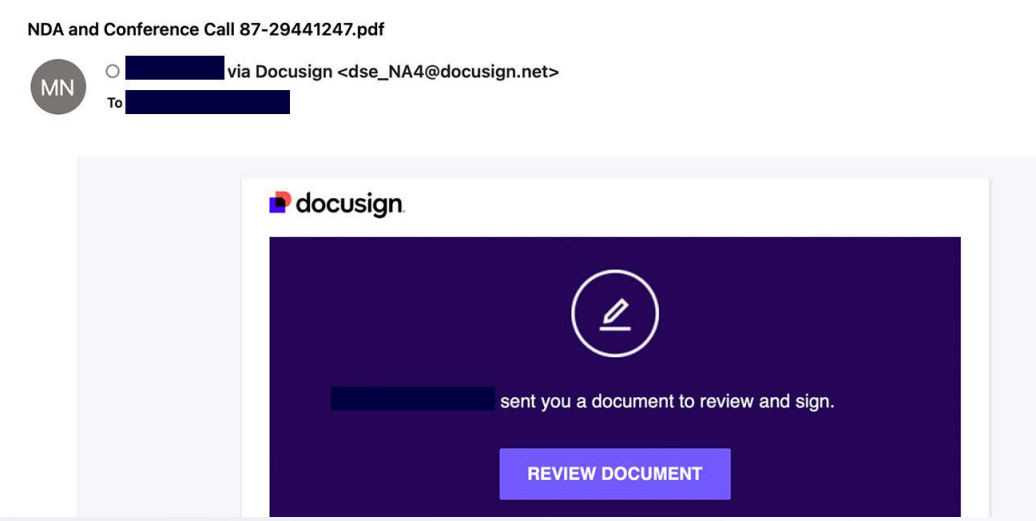
**L'utente chiama un numero falso per la verifica dell'NDA**

**L'interazione tramite email porta a una fattura sda pagare**

**Deepfake audio di un dirigente che conferma il pagamento**

**Pagamento effettuato sul conto bancario del criminale informatico**

I dipendenti nei settori bancario, assicurativo e di altri settori finanziari sono presi di mira da email di spear-phishing che sembrano provenire da uno studio legale e vengono inviati utilizzando un servizio affidabile come DocuSign e Adobe Sign. I messaggi mirati chiedono al dipendente di firmare un accordo di non divulgazione (NDA) e di chiamare un numero apparentemente di uno studio legale, ma che in realtà è controllato dal criminale informatico. Quest'ultimo si spaccia per lo studio legale utilizzando tecniche di deepfake audio per mascherare la voce e invia un'email da un dominio da lui controllato che sembra simile a quello dello studio legale imitato. Infine, il criminale informatico invia una fattura che sembra provenire dallo studio legale e dà seguito con una telefonata deepfake nella quale si finge il CEO dell'azienda o un altro dirigente.



# #05 MANCATA CONSEGNA

**TECNICA** Sfruttare servizi affidabili (LOTS)

**SERVIZI UTILIZZATI** Bucket S3 su AWS per ospitare file HTML

**OBIETTIVI** Regno Unito – enti senza scopo di lucro e edilizia popolare

READ ARTICLE

**Email di phishing tramite il fornitore di servizi Internet Biglobe**

**Reindirizzamento al file HTML ospitato su AWS**

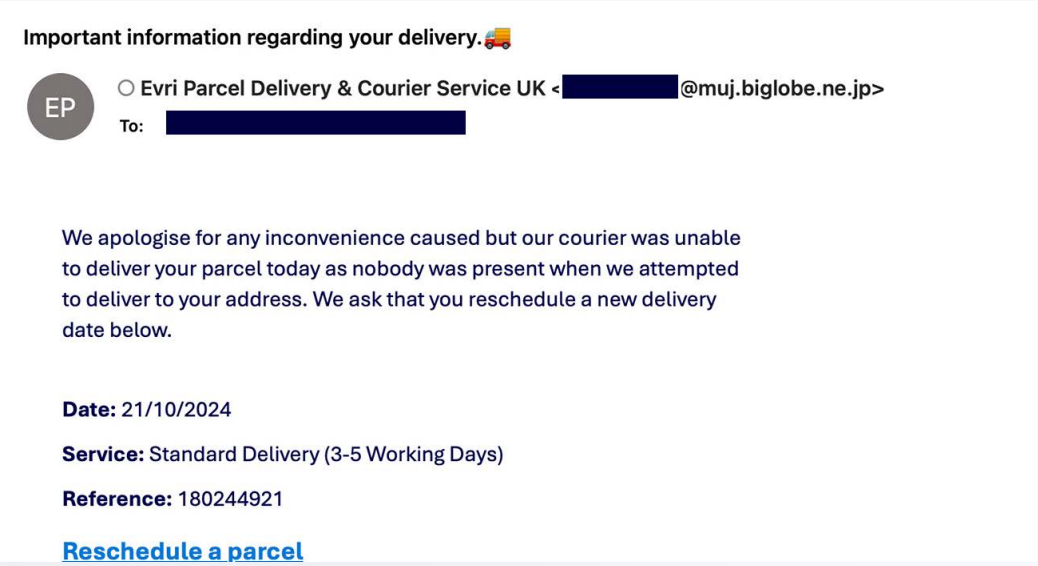
**Il file HTML imita la pagina di mancata consegna di EVRI**

**Forniti dati personali e informazioni della carta di credito per aggiornare la consegna**

**Carta di credito utilizzata o venduta sul mercato nero**

I messaggi inviati tramite BIGLOBE, un servizio giapponese spesso sfruttato dai criminali informatici, prendono di mira le gli enti senza scopo di lucro e per l'edilizia popolare nel Regno Unito con messaggi che segnalano una mancata consegna.

Esistono molti fornitori di servizi Internet in Asia che hanno permesso (o non sono consapevoli) di un abuso significativo delle reti. Gli attori delle minacce sfruttano questa situazione e altri fornitori di servizi Internet acquistando account autenticati tramite mercati clandestini, ottenendo così un accesso legittimo all'infrastruttura e consentendo di inviare email dannose che eludono la maggior parte dei protocolli di autenticazione delle email.



Important information regarding your delivery.🚚

EP

Evri Parcel Delivery & Courier Service UK <[redacted]@muj.biglobe.ne.jp>

To: [redacted]

We apologise for any inconvenience caused but our courier was unable to deliver your parcel today as nobody was present when we attempted to deliver to your address. We ask that you reschedule a new delivery date below.

**Date:** 21/10/2024

**Service:** Standard Delivery (3-5 Working Days)

**Reference:** 180244921

Reschedule a parcel

# #06 ACQUISIZIONE FRAUDOLENTA DELL'ACCOUNT FACEBOOK - FURTO D'IDENTITÀ DEL MARCHIO

**TECNICA** Esca legata alle opportunità di impiego sui social media che imita marchi come Victoria's Secret, Red Bull e Coca-Cola

**SERVIZIO UTILIZZATO** Recruitee

**DESTINATARI** Principalmente Regno Unito e Stati Uniti, prevalentemente i settori dei Media, dell'Editoria e della Vendita al dettaglio

READ ARTICLE

**Email di phishing inviata tramite il CMS Recruitee**

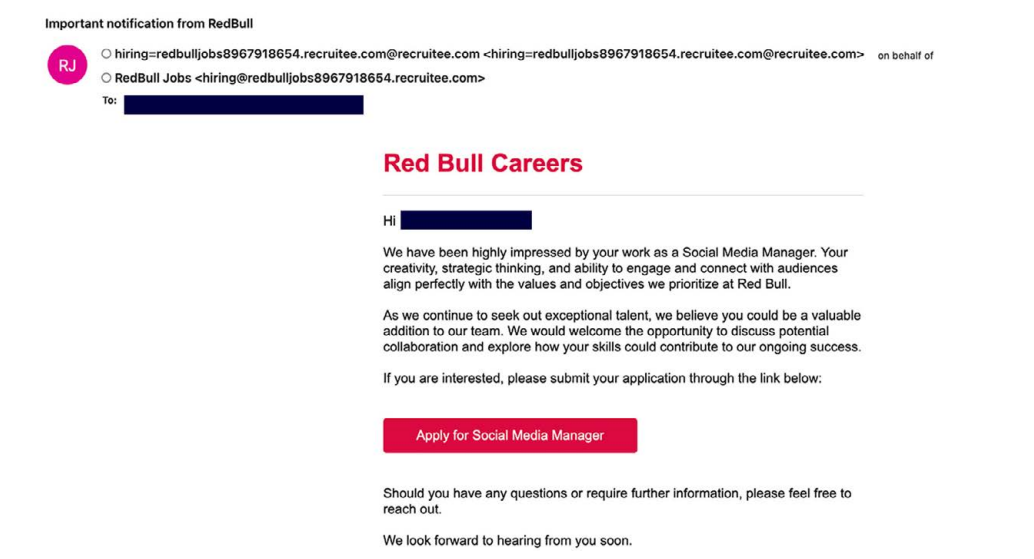
**Pagina di registrazione su un dominio simile del marchio imitato**

**Accesso tramite una pagina Facebook fasulla per inviare il modulo di richiesta**

**Richiesti i codici MFA per completare la richiesta**

**Le credenziali di Facebook ottenute vengono condivise tramite un logger di Telegram**

Una recente campagna di phishing ha sfruttato Recruitee, un sistema di gestione dei contenuti (CMS, Content Management System) legittimo di selezione e assunzione del personale di terze parti, per inviare email di offerte di lavoro fraudolente.
I criminali informatici registrano domini simili che imitano marchi noti per conferire credibilità alla truffa. Le pagine di phishing utilizzano i test CAPTCHA e il filtraggio IP per impedire il rilevamento automatico e mirano a raccogliere le credenziali d'accesso di Facebook.


Important notification from RedBull

RJ

hiring=redbulljobs8967918654.recruitee.com@recruitee.com <hiring=redbulljobs8967918654.recruitee.com@recruitee.com> on behalf of

RedBull Jobs <hiring@redbulljobs8967918654.recruitee.com>

To: [redacted]

Red Bull Careers

Hi [redacted]

We have been highly impressed by your work as a Social Media Manager. Your creativity, strategic thinking, and ability to engage and connect with audiences align perfectly with the values and objectives we prioritize at Red Bull.

As we continue to seek out exceptional talent, we believe you could be a valuable addition to our team. We would welcome the opportunity to discuss potential collaboration and explore how your skills could contribute to our ongoing success.

If you are interested, please submit your application through the link below:

Apply for Social Media Manager

Should you have any questions or require further information, please feel free to reach out.

We look forward to hearing from you soon.

04
.3

# MIMECAST RISK RADAR.

## I CRIMINALI INFORMATICI UTILIZZANO SEMPRE PIÙ SPESSO SERVIZI ATTENDIBILI (LOTS)

Dai provider di posta elettronica legittimi ai siti di condivisione file e ai servizi di hosting di webinar, i criminali informatici utilizzano sempre più servizi affidabili per eludere le difese che si basano sulla reputazione e sulla fiducia. Gli attacchi sfruttano comunemente i principali provider di email, come Gmail di Google e Outlook di Microsoft (in precedenza Hotmail), mentre i link nelle email terminano portano su un servizio di hosting legittimo, come Google Docs, Evernote, o i servizi OneDrive e SharePoint di Microsoft.

Mentre i servizi legittimi sono in grado di scoraggiare gli abusi, i criminali informatici si rivolgono anche verso obiettivi più piccoli. Le principali campagne tracciate da Mimecast, ad esempio, hanno utilizzato fornitori come Airtable, Publuu e WaveCompliance.

## I RISCHI GEOPOLITICI AUMENTANO

Con l'aumento delle tensioni geopolitiche a livello globale, il panorama delle minacce sta cambiando. Criminali informatici sono diventati più attivi, sfruttando il dominio cibernetico per la raccolta di intelligence, compromettendo le risorse delle nazioni rivali e generando profitti. La percezione della mancanza di conseguenze concrete per le operazioni informatiche ha spinto le nazioni ad ampliare le operazioni e i criminali informatici a condurre attacchi più audaci.

Tuttavia, le forze dell'ordine hanno ottenuto successi sempre maggiori nel contrastare l'infrastruttura dei criminali informatici, mentre gli sforzi dei difensori rendono più rari gli obiettivi facili da violare. A seguito dell'invasione dell'Ucraina da parte della Russia, entrambi i paesi hanno esaurito le loro scorte di exploit zero-day e n-day, portando a un picco (vedi Figura 5) che da allora si è attenuato. Nel 2024, il numero totale di vulnerabilità sfruttate segnalate attraverso il catalogo Known Exploited Vulnerability (KEV) ha mantenuto un tasso costante, ma basso.

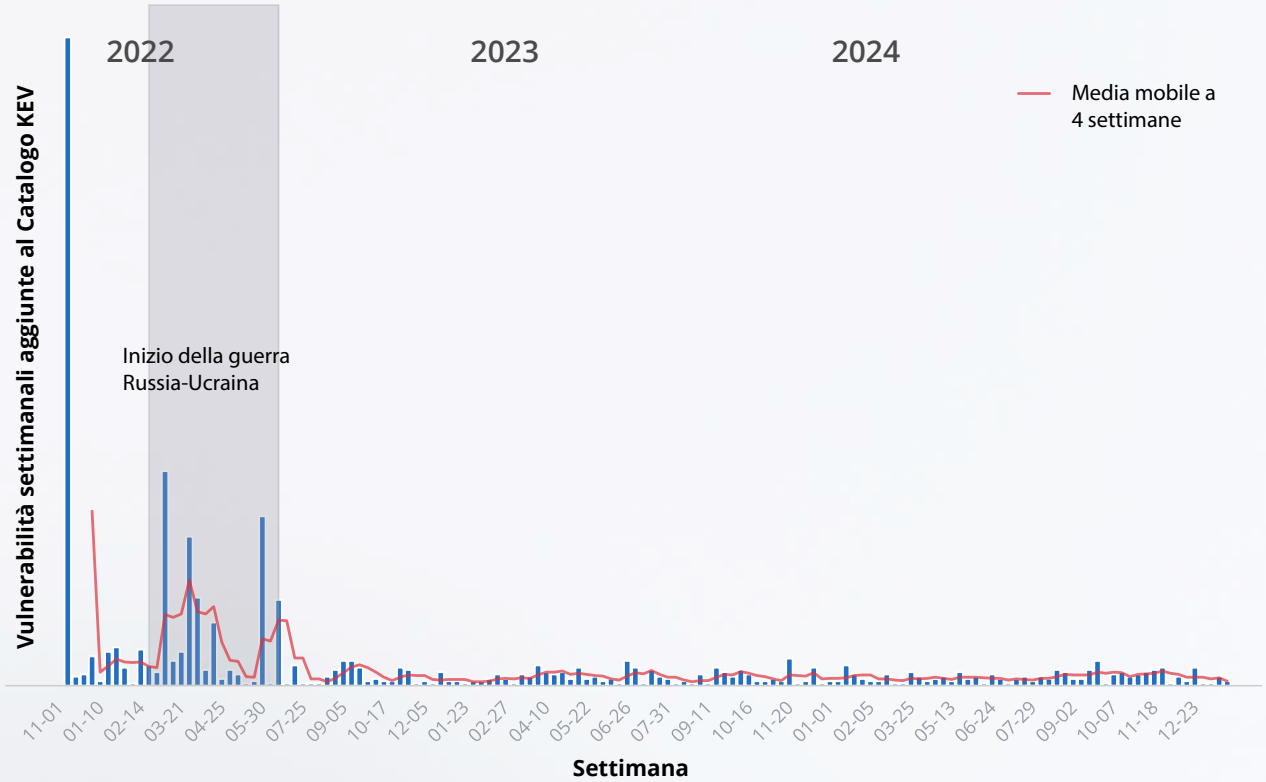



**Figura 5:** Dalla metà del 2022 fino alla fine del 2024, la CISA ha aggiunto circa 4 vulnerabilità a settimana al catalogo KEV, secondo i dati raccolti dalla Cybersecurity and Infrastructure Security Agency (CISA). I dati mostrano un forte picco nel momento in cui l'elenco è stato pubblicato per la prima volta, seguito da un'attività significativa durante i primi mesi dell'invasione russa dell'Ucraina.

Mentre la geopolitica ha causato un aumento del livello delle minacce informatiche, gli eventi globali offrono anche ai cirminali informatici, concentrati sulla vulnerabilità dell'elemento umano, una maggiore varietà di esche.

**Le principali esche geopolitiche individuate da Mimecast sono le seguenti:**

**01**
CHINA-TAIWAN

**02**
CINA-MAR CINESE MERIDIONALE

**03**
CINA-CAVO TAGLIATO

**04**
GUERRA RUSSIA-UCRAINA

**05**
CONFLITTO ISRAELE-GAZA

**06**
LEGISLAZIONE DELL'UNIONE

**07**
ELEZIONI RUSSIA-STATI UNITI

**08**
ELEZIONI IRAN-USA

**09**
EVENTI METEOROLOGICI NEGLI STATI UNITI

## INDUSTRIE MAGGIORMENTE ATTACCATE

I settori maggiormente esposti a minacce significative includono quello dell'Arte, intrattenimento e tempo libero, che ha registrato più di 10 minacce per utente (TPU), e i settori dei servizi professionali: Legale e Media e Editoria, con quasi 9 TPU.

La maggior parte dei settori ha osservato differenze nel profilo di minaccia. Il settore Arte, Intrattenimento e Tempo libero ha registrato una percentuale molto maggiore di attacchi tramite file dannosi, mentre i dipendenti degli studi legali hanno subito un numero significativo di attacchi di furto d'identità. I criminali informatici hanno preso di mira i lavoratori del settore Media e Editoria principalmente con link dannosi, mentre il settore Software e SaaS ha dovuto affrontare numerosi attacchi di furto d'identità.

Nell'ambito dell'analisi, Mimecast ha rimosso i messaggi email inviati in massa (rilevati come spam o a bassa reputazione) che corrispondevano rispettivamente a 17 TPU e 5 TPU.

| | | |
|---|---|---|
| 01 | ARTE, SPETTACOLO E RICREATIVO | 10.322010 TPU |
| 02 | LEGALE | 8.613564 TPU |
| 03 | MEDIA ED EDITORIA | 8.622578 TPU |

# CRONOLOGIA DEI PRINCIPALI EVENTI

04.2

**GIU.**
10 MILIARDI DI PASSWORD TRAPELATE

**SET.**
PIATTAFORME DI TRADING CRIPTO ASIATICHE COLPITE DA FURTI

**OTT.**
AUMENTANO LE PREOCCUPAZIONI PER SALT TYPHOON

**NOV.**
"FALSI LAVORATORI" IRANIANI MIRANO A INDUSTRIE SENSIBILI

**DIC.**
IL TESORO DEGLI STATI UNITI HACKERATO TRAMITE TERZE PARTI
GLI SVILUPPATORI DI PHISHING COMPROMETTONO L'ESTENSIONE DEL BROWSER

## GIU.

### 10 MILIARDI DI PASSWORD TRAPELATE

**VULNERABILITÀ** Riutilizzo di password
**IMPATTO** Attacchi di credential stuffing e forza bruta

Scoperta di RockYou2024, la più grande fuga di password della storia, pari a 9.948.575.739 password in chiaro univoche. Questo file enorme, pubblicato su un forum di hacking, solleva notevoli preoccupazioni, poiché include password accumulate negli ultimi due decenni, esponendo potenzialmente molti utenti ad attacchi di credential stuffing e ad altre minacce informatiche.

## SET.

### PIATTAFORME DI TRADING CRIPTO ASIATICHE COLPITE DA FURTI

**VULNERABILITÀ** Violazioni della rete
**IMPATTO** Più di 70 milioni di dollari in perdite

A settembre, gli attacchi a due piattaforme di trading di criptovalute, BingX con sede a Singapore e Indodax con sede in Indonesia, hanno comportato enormi perdite in seguito a violazioni separate. Indodax, con sede a Giacarta, si è impegnata a risarcire gli utenti dopo una perdita di 22 milioni di dollari, mentre BingX ha dichiarato una perdita di 44 milioni di dollari. Negli Stati Uniti, il Dipartimento di Giustizia ha anche annunciato l'arresto di due persone legate al furto di 230 milioni di dollari in criptovalute ai danni di un cittadino statunitense.

### VIOLAZIONE DI INTERNET ARCHIVE

**VULNERABILITÀ** Sconosciuta
**IMPATTO** Informazioni su 31 milioni di account univoci esposte

L'organizzazione Internet Archive ha subito diverse violazioni nell'arco di 22 giorni. Intorno al 28 settembre, un crimininale informatico ha sottratto il file del database della Wayback Machine di Internet Archive, compromettendo nomi utente, indirizzi email e password crittografate. Sebbene il fondatore del sito abbia dichiarato di aver ripulito i sistemi e aggiornato la sicurezza, in ottobre si sono verificati molteplici attacchi denial-of-service e una seconda violazione.

## OTT.

### AUMENTANO LE PREOCCUPAZIONI PER SALT TYPHOON

**VULNERABILITÀ** Infiltrazione nei sistemi di telecomunicazione statunitensi
**IMPACT** Gruppi cinesi ottengono un ampio accesso alle comunicazioni

Salt Typhoon, il gruppo criminale al soldo dello Stato cinese, ha ottenuto l'accesso a informazioni altamente sensibili su cittadini e funzionari governativi statunitensi violando i principali fornitori di telecomunicazioni e servizi Internet degli Stati Uniti, tra cui Verizon e AT&T. Secondo quanto riferito, sono stati colpiti ben nove diversi provider, anche tramite l'accesso all' infrastruttura di intercettazione autorizzata dal tribunale presso alcuni provider, in quello che è stato definito un "fallimento del controspionaggio di altissimo livello".

## NOV.

### "FALSI LAVORATORI" IRANIANI MIRANO A INDUSTRIE SENSIBILI

**VULNERABILITÀ** Social engineering, abuso di LinkedIn

**IMPATTO** Ai settori aerospaziale, aeronautica e difesa in Israele e negli Emirati Arabi Uniti; anche Turchia, India e Albania tra i possibili obiettivi

Hacker iraniani sospettati hanno utilizzato falsi siti web di agenzie di collocamento per spacciarsi per addetti alla selezione di candidati su LinkedIn, contattando aziende del settore aerospaziale, della difesa e dell'aviazione in Israele, Emirati Arabi Uniti, Turchia, India e Albania. Gli hacker si sono spacciati per addetti alla selezione su LinkedIn per distribuire malware alle vittime tramite false offerte di lavoro lucrative per spiare gli obiettivi e rubare dati sensibili a partire dal 2023. Il malware e le tattiche utilizzate sono simili a quelle di un gruppo di hacker nordcoreani che ha preso di mira i fondi delle criptovalute negoziati in borsa.

## DIC.

### IL TESORO DEGLI STATI UNITI HACKERATO TRAMITE TERZE PARTI

**VULNERABILITÀ** Fornitore terzo, ruolo critico del software di sicurezza

**IMPATTO** I criminali informatici hanno ottenuto accesso a dati non classificati su

Il Dipartimento del Tesoro degli Stati Uniti ha annunciato che una violazione del fornitore di soluzioni di sicurezza delle identità BeyondTrust ha colpito a cascata anche i suoi sistemi, portando all'esposizione di diverse workstation e dati non classificati. Mentre le indagini proseguono, gli Stati Uniti hanno indicato un gruppo di hacker al soldo della Cina che, secondo quanto riferito, ha ottenuto l'accesso a una chiave API utilizzata per il supporto remoto. BeyondTrust non ha ancora rivelato come i criminali informatici abbiano ottenuto l'accesso alla chiave.

### GLI SVILUPPATORI DI PHISHING COMPROMETTONO L'ESTENSIONE DEL BROWSER

**VULNERABILITÀ** attacco di spear-phishing che porta a autorizzazioni elevate sulle estensioni di Chrome

**IMPATTO** Raccolta di informazioni da parte di estensioni dannose delle credenziali e delle informazioni degli utenti

I gruppi di di criminali informatici hanno violato più di 30 estensioni del browser nell'ultimo anno inviando email di spear phishing che sembrano provenire da Google alla persona o al gruppo di contatto per le estensioni del browser Chrome prese di mira. Agli sviluppatori che fanno clic sull'email viene chiesto di concedere privilegi a un'applicazione dal nome innocuo. In realtà danno ai criminali informatici la possibilità di sostituire l'estensione con un'applicazione dannosa. La società di sicurezza dei dati Cyberhaven ha segnalato per la prima volta queste tattiche a dicembre, dopo che uno dei suoi sviluppatori è caduto vittima dell'attacco e ha concesso le autorizzazioni all'applicazione "Privacy Policy Extension". Fino a 2,6 milioni di utenti potrebbero essere stati colpiti dall'attacco.

# RACCOMAN-DAZIONI

05

MINACCIA SPECIFICA

BEST PRACTICE E CONSIGLI

PASSAGGI PER I CLIENTI MIMECAST

**CROW**

**SPECIES**

Noti per le loro capacità di problem-solving e insegnamento. Sempre **educativi** e attivi. Il tuo punto di riferimento per le strategie di mitigazione del rischio di sicurezza informatica.

# THREAT-SPECIFIC COUNTERMEASURES.

05.1

**Le aziende dovrebbero intraprendere azioni specifiche per rafforzare le proprie difese e scoraggiare gli attacchi rendendoli più onerosi per i criminali informatici.**

## GESTIONE DEI RISCHI LEGATI ALLE PERSONE

Le aziende dovrebbero implementare un framework di gestione dei rischi legati alle persone che allinei gli obiettivi di sicurezza con quelli aziendali. Mappando i fattori di rischio legati alle persone e i potenziali esiti avversi, le aziende possono sviluppare un sistema di risposta a più livelli che distingue tra errori non intenzionali e azioni dolose. Le principali preoccupazioni sono la perdita di proprietà intellettuale o di altre informazioni strategiche, l'esfiltrazione di dati sensibili e l'uso improprio delle risorse aziendali.

Le aziende dovrebbero incorporare sia i nudge per rafforzare i comportamenti positivi che le misure correttive in un approccio graduale. Per raggiungere questi obiettivi, è fondamentale istituire gruppi di lavoro interfunzionali per garantire il sostegno delle parti interessate e una gestione efficace del cambiamento, mantenendo canali di comunicazione chiari con la leadership in merito alle metriche di rischio, ai potenziali incidenti e alle strategie di mitigazione.

## FORNIRE FORMAZIONE DI SENSIBILIZZAZIONE

Nel complesso panorama odierno, in cui le tensioni geopolitiche si manifestano frequentemente come minacce informatiche, una formazione di sensibilizzazione completa diventa essenziale. Il personale deve essere istruito non solo sui rischi informatici generali, ma anche su come gli eventi globali possano influenzare le campagne di phishing, le minacce interne e i tentativi di social engineering che prendono di mira la loro azienda. Implementando solidi programmi di formazione di sensibilizzazione alla sicurezza informatica e piattaforme di gestione dei rischi legati alle persone per proteggere gli utenti, le aziende possono rafforzare il proprio firewall umano sia contro gli attacchi informatici convenzionali sia contro quelli motivati da ragioni geopolitiche. Questo approccio alla sicurezza incentrato sulle persone aiuta il personale a identificare e rispondere efficacemente alle minacce, che provengano da email, social media, strumenti di collaborazione o altri vettori che sfruttano la psicologia umana.

## IMPORRE MAGGIORE SICUREZZA ALLE TERZE PARTI

Gli attacchi contro le aziende del settore manifatturiero, dei trasporti, stoccaggio e consegna, oltre alla vendita al dettaglio e all'ingrosso rappresentano un rischio significativo di violazione della supply chain da parte di terzi. Le aziende dovrebbero rivedere gli accordi sul livello di servizio per stabilire livelli minimi di sicurezza dei dati e di sicurezza informatica e trovare modi per monitorare più da vicino i loro fornitori, ad esempio utilizzando servizi di valutazione esterni e sottoponendo le acquisizioni a controlli più rigorosi.

## BLOCCARE LE IMMAGINI NEI MESSAGGI DI POSTA ELETTRONICA

I criminali informatici utilizzano sempre più tipi di file basati su immagini per introdurre esche di phishing e codice dannoso, eludendo il rilevamento. L'analisi di Mimecast ha identificato criminali informatici che utilizzano anche la crittografia e testi in lingue straniere all'interno delle immagini per evitare di essere rilevati. Le aziende dovrebbero configurare i client di posta elettronica per impedire il caricamento delle immagini nei messaggi e isolare le immagini che gli utenti segnalano esplicitamente. Nota: gli utenti di CyberGraph dovrebbero utilizzare siti affidabili per garantire che i banner vengano caricati correttamente.

## ANALIZZARE L'AMBIENTE ALLA RICERCA DI ERRORI DI CONFIGURAZIONE O PORTE APERTE VERSO L'ESTERNO

Le aziende dovrebbero analizzare regolarmente la propria infrastruttura per individuare percorsi noti che possono essere sfruttati, come porte di rete esterne aperte non sicure o ambienti cloud pubblici. Utilizzando strumenti come Cloud Security Posture Management, le aziende possono rapidamente individuare gli errori di configurazione nel cloud pubblico. Questa modalità garantisce che tutte le porte dei server accessibili pubblicamente siano chiuse o adeguatamente protette e sicure.

Ad esempio, Mimecast ha osservato un aumento continuo degli attacchi contro le porte RDP (Remote Desktop Protocol), che rappresentano l'80% delle violazioni ransomware andate a buon fine. I criminali informatici continueranno a cercare porte RDP aperte per prendere di mira le aziende.

## SEGMENTARE LA RETE E REGISTRARE IL TRAFFICO INTERNO

I criminali informatici, in particolare durante un attacco ransomware, possono spostarsi lateralmente in modo rapido attraverso una rete. Segmentare la rete interna e collocare le risorse critiche nelle proprie enclave può ridurre i danni causati dal ransomware e altri attacchi. Il monitoraggio del traffico interno, specialmente delle comunicazioni verso segmenti specifici, può portare a un rilevamento anticipato delle minacce.

## RAFFORZARE LE CREDENZIALI DEGLI UTENTI, IMPLEMENTARE L'AUTENTICAZIONE A PIÙ FATTORI

Molte minacce malware sfruttano le password comuni per infiltrarsi nelle reti. Gli attacchi recenti mettono in evidenza come password inefficaci contribuiscano alle violazioni. Rafforzare qualsiasi rete imponendo password efficaci, soprattutto per gli utenti con privilegi. Il team della sicurezza IT deve eliminare le password amministrative predefinite. La richiesta di autenticazione a più fattori può ridurre drasticamente la violazione di account o credenziali rubati.

05.2

# BEST PRACTICE E CONSIGLI.

## AVVISO APT40: TECNICHE OPERATIVE DEL MSS DELLA RPC IN AZIONE

8 Lug. 2024 LEGGERE >

**Organizzazioni: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK, BND e altre**

Le agenzie governative responsabili della sicurezza informatica e delle forze dell'ordine in Australia, Canada, Nuova Zelanda, Germania, Corea del Sud, Regno Unito e Stati Uniti hanno delineato le tattiche utilizzate il criminale informatico al soldo della Cina APT40 (noto anche come Gingham Typhoon), che ha ripetutamente preso di mira le reti australiane, così come le reti del settore governativo e privato nella regione. Il gruppo può rapidamente utilizzare, adattare e sfruttare il codice proof-of-concept per nuove vulnerabilità negli attacchi e distribuire tali strumenti nelle campagne.

## RILEVAMENTO E MITIGAZIONE DELLE VIOLAZIONI DI ACTIVE DIRECTORY

Set. 2024 LEGGERE >

**Organizzazioni: ASD, CISA, NSA, CCCS, NCSC-NZ, NCSC-UK**

Le agenzie di sicurezza informatica delle nazioni dell'alleanza Five Eyes descrivono 17 diverse tecniche per attaccare Microsoft Active Directory, le soluzioni di gestione delle identità e accesso più comuni utilizzate nelle aziende. Dato il suo ruolo cruciale nei processi di autenticazione e autorizzazione e la sua vulnerabilità dovuta a impostazioni predefinite inadeguate e alla complessità dell'installazione, i criminali informatici spesso prendono di mira Active Directory.

## CRIMINALI INFORMATICI MILITARI RUSSI PRENDONO DI MIRA LE INFRASTRUTTURE CRITICHE GLOBALI E DEGLI STATI UNITI

5 Set. 2024 LEGGERE >

**Organizzazioni: CISA, FBI, NSA**

Diversi gruppi di criminali informatici russi associati ad agenzie militari hanno preso di mira le agenzie governative ucraine e altri obiettivi alleati della NATO con il malware WhisperGate. I criminali informatici hanno utilizzato le vulnerabilità nei dispositivi di rete per ottenere l'accesso iniziale.

## PRINCIPALI VULNERABILITÀ SFRUTTATE REGOLARMENTE NEL 2023

12 Nov. 2024 LEGGERE >

**Organizzazioni: ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK**

Forse con un certo ritardo, le principali agenzie delle nazioni dell'alleanza Five Eyes (Australia, Canada, Nuova Zelanda, Regno Unito e Stati Uniti) hanno pubblicato informazioni sulle 15 principali vulnerabilità sfruttate abitualmente nel 2023. Undici delle 15 vulnerabilità sono state sfruttate in attacchi zero-day, rispetto a soli due attacchi zero-day della dozzina di vulnerabilità elencate nel 2022.

## RAFFORZARE LA RESILIENZA INFORMATICA: INFORMAZIONI DALLA VALUTAZIONE DEL RED TEAM DELLA CISA SU UN'AZIENDA DEL SETTORE DELLE INFRASTRUTTURE CRITICHE DEGLI STATI UNITI

21 Nov. 2024 LEGGERE >

**Organizzazioni: CISA**

La CISA (Cybersecurity and Infrastructure Security Agency) ha identificato significative vulnerabilità nella sicurezza informatica in un'azienda di infrastrutture critiche durante un'analisi del Red Team. Il team ha violato l'azienda utilizzando una web shell lasciata da una valutazione precedente, violando il suo dominio e i sistemi sensibili date le protezioni inadeguate della rete e il ritardo delle risposte.

## I CRIMINALI INFORMATICI AFFILIATI ALL'IRGC SFRUTTANO I DISPOSITIVI PLC IN DIVERSI SETTORI, INCLUSI GLI IMPIANTI DEI SISTEMI IDRICI E DELLE ACQUE REFLUE NEGLI STATI UNITI

18 Dic. 2024 LEGGERE >

**Organizzazioni: FBI, CISA, NSA, US EPA, INCD, CCCS, NCSC**

Le agenzie di intelligence e sicurezza informatica di Stati Uniti, Israele, Canada e Regno Unito hanno emesso un avviso aggiornato che descrive le attività informatiche dannose da parte di criminali informatici collegati al Corpo delle guardie della rivoluzione islamica (IRGC) dell'Iran, inclusi attacchi ai controllori logici programmabili (PLC) e alle infrastrutture critiche nel Regno Unito e in Israele.

# PASSAGGI PER I CLIENTI MIMECAST.

**Per proteggere i propri utenti dalle minacce descritte nel report, i clienti di Mimecast possono adottare misure di sicurezza specifiche e pratiche, con un livello di approfondimento tecnico medio.**

## GATEWAY CLOUD PER LA SICUREZZA DELL'EMAIL

1. Per ridurre il rischio che l'email venga utilizzata come vettore d'attacco dai criminali informatici, si consiglia di iutilizzare il single sign-on offerto dal proprio gestore delleidentità o sfruttare l'autenticazione a più fattori integrata di Mimecast.
2. Assicurarsi che le policy di autenticazione DNS rispettino i record DMARC. Una seconda policy applicata a un gruppo di policy con l'azione DMARC Fail impostata su Ignora/Mittenti gestiti e autorizzati, permetterà il recapito delle email legittime rifiutate o messe in quarantena a causa di errori DMARC.
3. Ottimizzare la protezione contro as per the best practice guidelines of two hits set to tag Subject/Body and include a separate C-Level/VIP policy based on name match with a hold for admin review. In addition, create another policy for any detections of three hits or more with the admin hold action.
4. Implementare la protezione contro le minacce BEC avanzate con tre policy: applicazione moderata per il rilevamento delle minacce, bypass del mittente per le fonti attendibili e bypass del destinatario per le esclusioni interne.
5. L'impostazione di una riscrittura efficace degli URL garantirà che tutti gli URL vengano analizzati al momento del clic; tenere in considerazione che qualsiasi elemento che sembri un URL verrà riscritto (ad esempio indirizzi IP e link interni).
6. Utilizzare le integrazioni predefinite con la maggior parte dei fornitori di soluzioni SIEM e XDR per garantire l'acquisizione e l'analisi dei log per l'applicazione delle policy di sicurezza.
7. Sfruttare l'intelligence sulle minacce "bring-your-own" per sfruttare qualsiasi feed di minacce di terze parti per il rifiuto automatico degli indicatori corrispondenti.
8. Gli utenti finali dovrebbero segnalare i messaggi potenzialmente dannosi ricevuti attraverso gli strumenti utente di Mimecast al SOC di Mimecast per un'analisi supplementare.

## SICUREZZA DELL'EMAIL INTEGRATA NEL CLOUD

1. Abilitare l'isolamento del browser per ridurre al minimo il rischio che gli utenti accedano a siti potenzialmente sospetti.
2. Personalizzare le regole di autorizzazione e blocco per specificare chi è autorizzato nel proprioambiente.
3. Esaminare i report settimanali per ottenere informazioni sulle minacce rilevate nel proprio ambiente.
4. Gli utenti finali dovrebbero segnalare i messaggi potenzialmente dannosi ricevuti attraverso gli strumenti utente di Mimecast al SOC di Mimecast per un'analisi aggiuntiva.

**Se non si è sicuri dell'effetto di una qualsiasi delle impostazioni proposte, contattare il proprio account manager Mimecast, il responsabile del successo dei clienti o prenotare una chiamata con l'assistenza Mimecast.**

# CONCLUSIONE.

Nella seconda metà del 2024, l'analisi delle minacce ha rivelato un'intensificazione delle campagne di disinformazione sofisticate e delle operazioni coordinate degli hacktivisti, in concomitanza con l'escalation delle tensioni geopolitiche che hanno permesso ai criminali informatici di sfruttare eventi globali per attacchi mirati. Queste tattiche evolute ora comprendono l'esfiltrazione sistematica dei dati, il dispiegamento mirato di ransomware e gli attacchi DDoS orchestrati, sfruttando le vulnerabilità legate alle persone attraverso campagne di social engineering sofisticate, incentrate sui principali sviluppi geopolitici, ponendo collettivamente rischi significativi per la continuità aziendale e la disponibilità dei sistemi.

L'identificazione delle attività dannose è diventata tecnicamente complessa poiché i criminali informatici abbinano azioni dannose con operazioni legittime, sfruttando anche servizi affidabili e binari di sistema comuni. I criminali informatici utilizzano sempre più strumenti legittimi del Red Team, rendendo estremamente difficile per i controlli di sicurezza distinguere tra attività legittime e non autorizzate.

Tutto questo richiede capacità di monitoraggio avanzate, inclusa l'analisi comportamentale avanzata e i sistemi di rilevamento delle anomalie.

In altre aree del panorama delle minacce, gli attacchi di social engineering mantengono tassi di successo elevati, evolvendosi tramite l'integrazione di tecnologie di intelligenza artificiale automatizzate. Le minacce persistenti avanzate ora utilizzano tecnologie deepfake sofisticate e contenuti generati dall'IA per lanciare attacchi mirati, complicando notevolmente i meccanismi tradizionali di rilevamento e prevenzione. La complessità tecnica di questi attacchi mette in risalto una ricerca e un'analisi dettagliata di social engineering dei modelli di comunicazione della supply chain.

La sicurezza perimetrale rimane una preoccupazione significativa, poiché i i criminali informatici che sfruttano costantemente le vulnerabilità nell'infrastruttura edge, tra cui appliance VPN, firewall e servizi esposti a Internet. Lo sfruttamento delle vulnerabilità zero-day combinato con l'implementazione ritardata delle patch crea finestre di vulnerabilità

prolungate, specialmente in ambienti ad alta disponibilità che richiedono test approfonditi delle patch. Questa sfida è amplificata dalle architetture di rete complesse e dall'espansione della superficie di attacco guidata dalla migrazione verso infrastrutture cloud e dall'evoluzione delle tecnologie operative. Le aziende devono disporre di funzionalità di risposta agli incidenti dedicate, tra cui strumenti forensi avanzati, sistemi di analisi della rete e meccanismi di rilevamento automatizzati.

## Vulnerabilità che potrebbero essere sfruttate quest'anno:

### VPN

Come evidenziato nella recente aggiunta della minaccia CVE 2025 0282 Ilvanti Connect Secure VN al catalogo delle Vulnerabilità Conosciute Sfruttabili (CISA).

### AUTENTICAZIONE

Osservata più recentemente nelle vulnerabilità che sfruttano il bypass tramite un percorso o canale alternativo e nel codice di autenticazione mancante.

### DENIAL OF SERVICE (DOS)

Un'attività dannosa sempre più popolare, progettata ad esempio per interrompere le operazioni aziendali, per esempio CVE 2024 3393 PAN OS Firewall Denial of Service

## RISORSE.

**DoS**
Translating Threat Intelligence into Practical Security Strategies

**Rapporto di ricerca**
Stato della sicurezza delle email e della collaborazione

## TI HUB.

Mimecast TI Hub

## Comunità.

Mimecast central

mimecast