AGID | Agenzia per l'Italia Digitale

CERT-AGID

REPORT 2025

Il riepilogo delle campagne malevole analizzate dal CERT-AGID nel 2025

Sommario

Report riepilogativo sulle tendenze delle campagne malevole analizzate dal CERT-AGID nel 2025

Il presente report intende fornire un quadro sintetico su statistiche e numeri relativi alle principali campagne malevole osservate dal CERT-AGID nel corso del 2025. L'analisi si concentra esclusivamente su attività che hanno interessato il territorio italiano, con particolare attenzione a quelle rivolte contro soggetti pubblici e privati afferenti alla propria *constituency*[1].

Basi informative di riferimento

Le informazioni qui presentate derivano da un insieme di fonti impiegate dal CERT-AGID nello svolgimento delle proprie attività: segnalazioni spontanee provenienti da soggetti privati e Pubbliche Amministrazioni, rilevazioni dei sistemi automatizzati interni a supporto della difesa proattiva della *constituency*, analisi di campioni di malware e attività di indagine sugli incidenti trattati.

Scenario delle minacce nel 2025

Nel corso del 2025 il CERT-AGID ha censito un totale di **3.620 campagne malevole**, condividendo con la propria constituency **51.530 Indicatori di Compromissione** (IoC). Nel periodo analizzato si è osservata una massiccia diffusione del phishing a tema **PagoPA** (328 campagne), basata su falsi solleciti di pagamento per presunte sanzioni stradali. Parallelamente, è aumentato in modo significativo l'abuso della **PEC** come vettore di campagne malevole (circa +80%, 103 eventi), impiegata sia per phishing, spesso mirato al furto di credenziali bancarie, sia per la distribuzione di malware, con **MintsLoader** tra le

[1] ai sensi del Piano Triennale per l'informatica nella PA 2024-2026, comprende le Pubbliche Amministrazioni e i Trust Services rientranti nel perimetro di competenza AgID, destinatari di attività di supporto proattivo in ambito sicurezza informatica, senza attribuzione di funzioni di gestione o coordinamento nazionale degli incidenti.

minacce più ricorrenti. Pur a fronte di una riduzione complessiva dello smishing rispetto al 2024 (circa -23%), cresce l'incidenza delle campagne SMS orientate alla distribuzione di malware. Si registra inoltre un incremento delle campagne basate sulla tecnica **ClickFix** (circa 70) e la conferma degli *infostealer* come tipologia di malware più diffusa. Le campagne rivolte a **dispositivi Android** risultano in aumento (circa +55%), con infezioni frequentemente innescate da smishing. Le esche usate per veicolare malware restano sostanzialmente in continuità con gli anni passati, con il tema "*Ordine*" al primo posto. Infine, sul versante dell'esposizione di dati, sono state rilevate **89 compromissioni** contenti informazioni di interesse per la *constituency*, derivate principalmente alla diffusione illecita di database.

Analisi delle tendenze generali

Dall'analisi delle tendenze generali riscontrate nel periodo considerato, si sono contraddistinti, nel vasto panorama delle minacce informatiche, i seguenti trend di maggiore impatto.

Comparsa massiva del phishing a tema PagoPA

Nel corso del 2025 è stata rilevata, per la prima volta, la diffusione su larga scala di campagne di phishing che sfruttano in modo fraudolento il nome di **PagoPA**[2]. L'esca è sempre rappresentata da false e-mail di sollecito di pagamento per **presunte sanzioni stradali** che reindirizzano verso pagine contraffatte finalizzate alla raccolta di dati personali e degli estremi delle carte di pagamento. Le prime evidenze sono state registrate a fine marzo 2025, con una marcata intensificazione a partire da maggio, per un **totale di 328 campagne censite** nel corso dell'anno (9%).

[2] https://cert-agid.gov.it/tag/pagopa/

Incremento dello sfruttamento di caselle PEC

L'uso della Posta Elettronica Certificata come vettore per campagne malevole, sia di phishing che malware, è **quasi raddoppiato** rispetto al 2024. Vengono sfruttate soprattutto caselle legittime compromesse, ma è stato anche osservato l'uso di indirizzi malevoli registrati ad hoc, prontamente dismessi a seguito di segnalazione ai gestori PEC. I principali dati quantitativi e la ripartizione per finalità sono riportati nella sezione "Canali di diffusione delle campagne malevole".

Smishing come vettore per la distribuzione di malware

Seppur in calo, **persistono le campagne veicolate via SMS**: nel 2025, a fronte di una diminuzione complessiva nel ricorso allo smishing, come sopra già evidenziato, con circa un quarto di casi in meno rispetto all'anno precedente, **cresce l'incidenza delle campagne orientate alla distribuzione di malware**. Sul fronte phishing permane l'abuso di denominazioni riconducibili a enti o servizi di interesse pubblico. I dettagli sui volumi e sugli argomenti sfruttati sono trattati nel seguito del report.

Diffusione di campagne basate su ClickFix

Si è osservata una forte crescita di campagne malware che adottano la tecnica **ClickFix**[3], una modalità di ingegneria sociale che, spesso attraverso un finto *CAPTCHA* o istruzioni operative, induce l'utente a eseguire manualmente comandi sul proprio sistema con l'effetto di avviare il download e l'esecuzione di codice malevolo. Il ricorso a esecuzioni "manuali" rende questo approccio particolarmente efficace nell'eludere controlli automatici. La prima campagna ClickFix osservata in Italia è stata segnalata dal CERT-AGID nel gennaio 2025, a conferma di una rapida adozione della tecnica anche nel contesto nazionale. Nell'arco del 2025 sono state censite circa **70 campagne riconducibili**

[3] https://cert-agid.gov.it/tag/clickfix/

a questa tecnica, impiegata specialmente per la diffusione di **AsycRat**, **Lumma Stealer** e **XWorm**.

Crescente utilizzo dell'intelligenza artificiale per fini malevoli

Si sta assistendo a una progressiva integrazione dell'IA all'interno dell'ecosistema criminale, sia come abilitatore di nuove capacità operative sia come ulteriore leva nelle dinamiche estorsive. In particolare, in contesti riconducibili ad attività ransomware, l'IA viene esplicitamente richiamata come possibile destinazione di riutilizzo dei dati sottratti, introducendo una nuova minaccia estorsiva basata sull'impiego dei dataleak per finalità di addestramento di modelli[4], utilizzata come ulteriore elemento di pressione sulle vittime oltre alla più consolidata divulgazione pubblica. Parallelamente, l'IA trova oggi un impiego diffuso e pragmatico nella creazione di campagne di phishing e smishing, consentendo la generazione di messaggi linguisticamente corretti, contestualizzati e adattati al pubblico di riferimento, riducendo l'efficacia delle tradizionali euristiche di rilevamento basate su errori formali. Tali strumenti favoriscono inoltre una maggiore scalabilità delle campagne, una rapida variazione dei template e un più agevole allineamento ai temi di attualità, contribuendo a un generale aumento della credibilità delle comunicazioni fraudolente.

L'attenzione crescente verso questi scenari emergenti è riflessa anche dalle attività di analisi tecnica rivolte alle amministrazioni, come le pubblicazioni del CERT-AGID dedicate ai profili di rischio connessi all'adozione di soluzioni di intelligenza artificiale nei sistemi della PA, con particolare riferimento alle implicazioni di sicurezza[5] e alla necessità di un approccio preventivo.

[4] https://cert-agid.gov.it/news/la-criminalita-digitale-si-evolve-gruppo-ransomware-minaccia-di-usare-i-dati-rubati-per-addestrare-ia/
[5] Paper del CERT-AgID - https://www.agid.gov.it/it/ambiti-intervento/sicurezza

Prevalenza degli infostealer tra i software malevoli

Anche nel 2025 gli *infostealer* si sono confermati la tipologia di malware più ricorrente. Si tratta di codici malevoli progettati per sottrarre informazioni dall'endpoint della vittima (ad esempio credenziali, cookie di sessione o token, documenti sensibili, ecc…) e trasferirle agli attori malevoli per abusi o rivendita. La loro diffusione è avvenuta principalmente tramite archivi compressi, che restano fra i vettori iniziali più utilizzati perché possono "incapsulare" script o eseguibili riducendo la probabilità di una rilevazione precoce.

I dati riepilogativi del 2025

Nel corso del 2025, il CERT-AGID ha individuato e contrastato un totale di **3620** campagne malevole, condividendo con la sua constituency[6] **51.530** Indicatori di Compromissione (IoC).

	Malware	**Phishing**
Famiglie rilevate	90	—
Brand coinvolti	—	153
Campagne censite	1698	1922
Indicatori di Compromissione (IoC) diramati	38798	12732

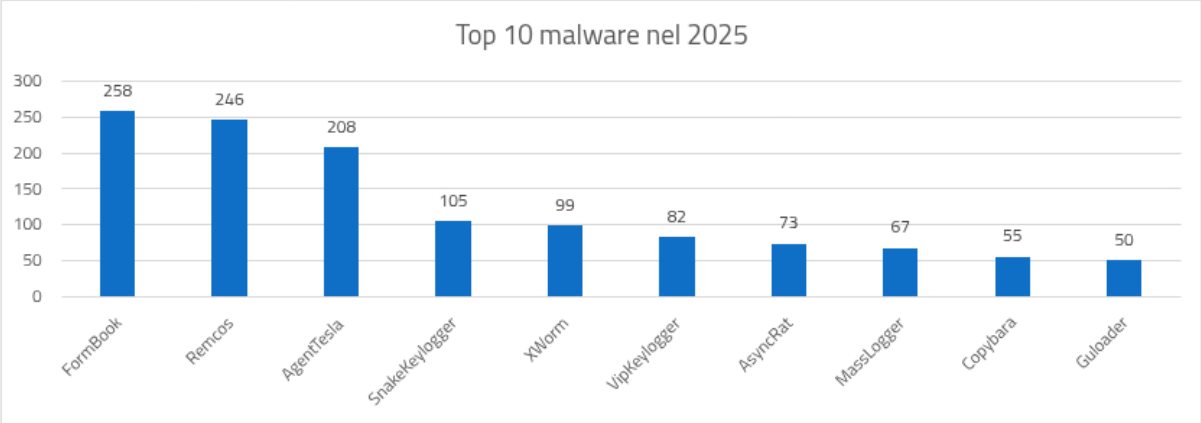
In totale sono state identificate **90 famiglie malware**. Dei campioni analizzati, circa il 60% rientra nella categoria degli *infostealer*, mentre un ulteriore 30% in quella dei *RAT* (*Remote Access Trojan*). La restante parte è costituita da *loader*, *dropper* e strumenti di accesso remoto legittimi ma sfruttati in maniera impropria.

Nel contesto di attacchi di phishing e smishing, che hanno coinvolto complessivamente **153 brand**, l'obiettivo principale è stato il furto di credenziali bancarie, di credenziali di

[6] https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/

accesso a webmail e, come nel caso delle campagne di phishing ai danni di **PagoPA**, il furto di dati di carte elettroniche di pagamento.

I 10 malware più diffusi in Italia



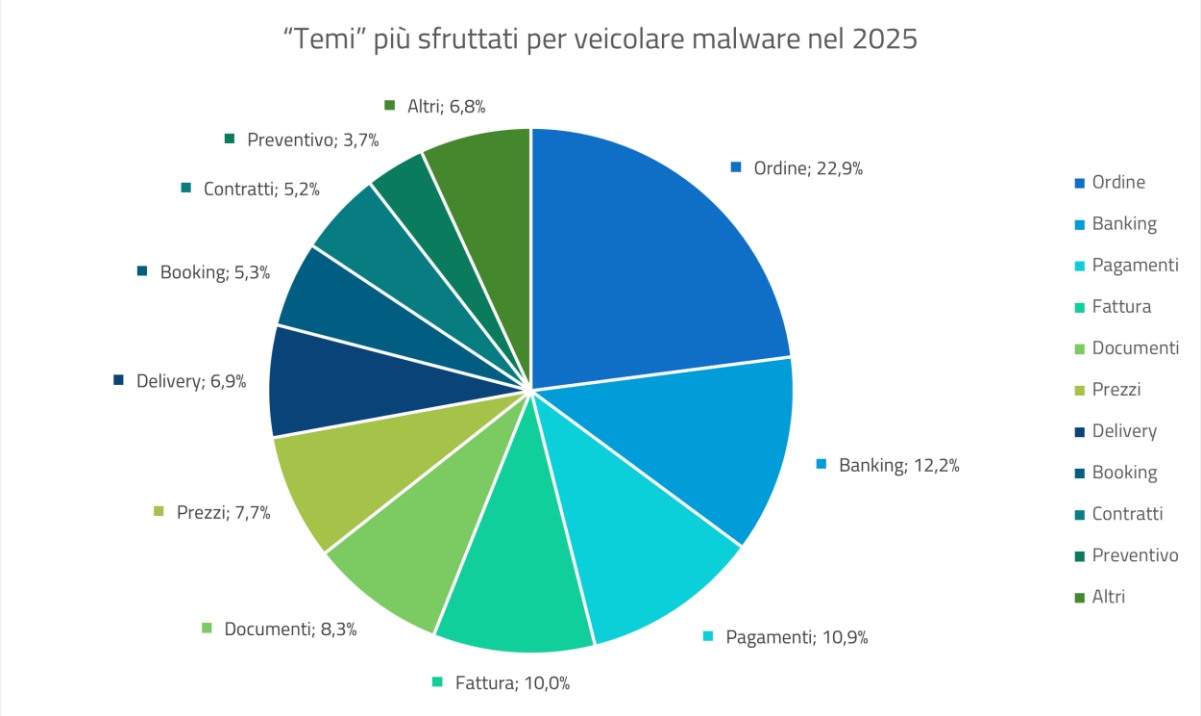
Nel corso del 2025, **FormBook** è stato il malware più diffuso in Italia, seguito a breve distanza da **Remcos** e **AgentTesla**. In generale, la maggior parte dei malware riscontrati è costituita da poche famiglie di *infostealer*, *keylogger* e *RAT,* di cui molti realizzabili tramite *builder* e servizi *Malware-as-a-Service* facilmente reperibili e quindi alla portata anche dei criminali meno capaci tecnicamente.

Un elemento di interesse è l'ulteriore consolidamento di catene di infezione "a più stadi", nelle quali l'installazione del *payload* finale è frequentemente preceduta da passaggi intermedi di ingegneria sociale o da componenti "ponte" progettate per aumentare la probabilità di esecuzione e ridurre l'efficacia dei controlli automatici. In questa logica si inseriscono, ad esempio, le citate campagne basate su **ClickFix**, che inducono la vittima a eseguire manualmente comandi dannosi, abilitando l'avvio della compromissione; oppure l'impiego di *loader* e *dropper*, utilizzati per predisporre l'ambiente, effettuare controlli, scaricare componenti aggiuntivi e distribuire *payload* differenti in funzione del bersaglio o

del contesto operativo. Fra questi ultimi vi è ad esempio **MintsLoader**[7], spesso veicolato tramite indirizzi **PEC** compromessi.

Concludono il panorama, diversi malware e varianti meno frequenti, come ad esempio alcuni loader specializzati, RAT legacy e **strumenti di accesso remoto[8] usati impropriamente**.

I 10 "temi" più sfruttati per veicolare malware e phishing

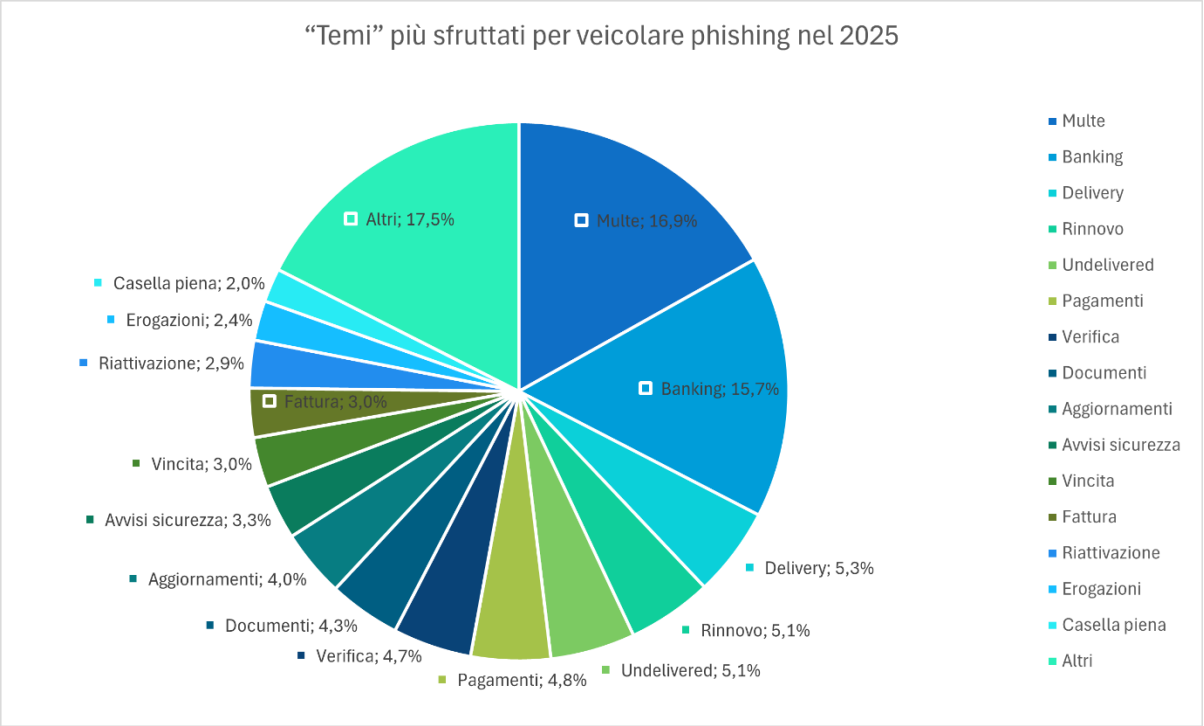


I temi sfruttati per veicolare malware non mostrano discontinuità rilevanti rispetto agli anni passati. Quello più ricorrente è risultato "*Ordine*", utilizzato come esca in **382** campagne complessive. Tale argomento ha distanziato in misura significativa il secondo tema per frequenza, "*Banking*", che è stato impiegato in 203 campagne nel corso dell'anno.

[7] https://cert-agid.gov.it/tag/mintsloader/
[8] https://cert-agid.gov.it/news/campagna-malware-abusa-di-strumenti-di-rmm-legittimi-tramite-falsa-condivisione-di-documenti/

I malware più frequentemente diffusi mediante tale argomento sono stati i seguenti:

Malware	Numero di campagne
Formbook[9]	75
AgentTesla	72
Remcos[10]	55
SnakeKeylogger	35
VipKeylogger	25
MassLogger	19
Xworm[11]	17



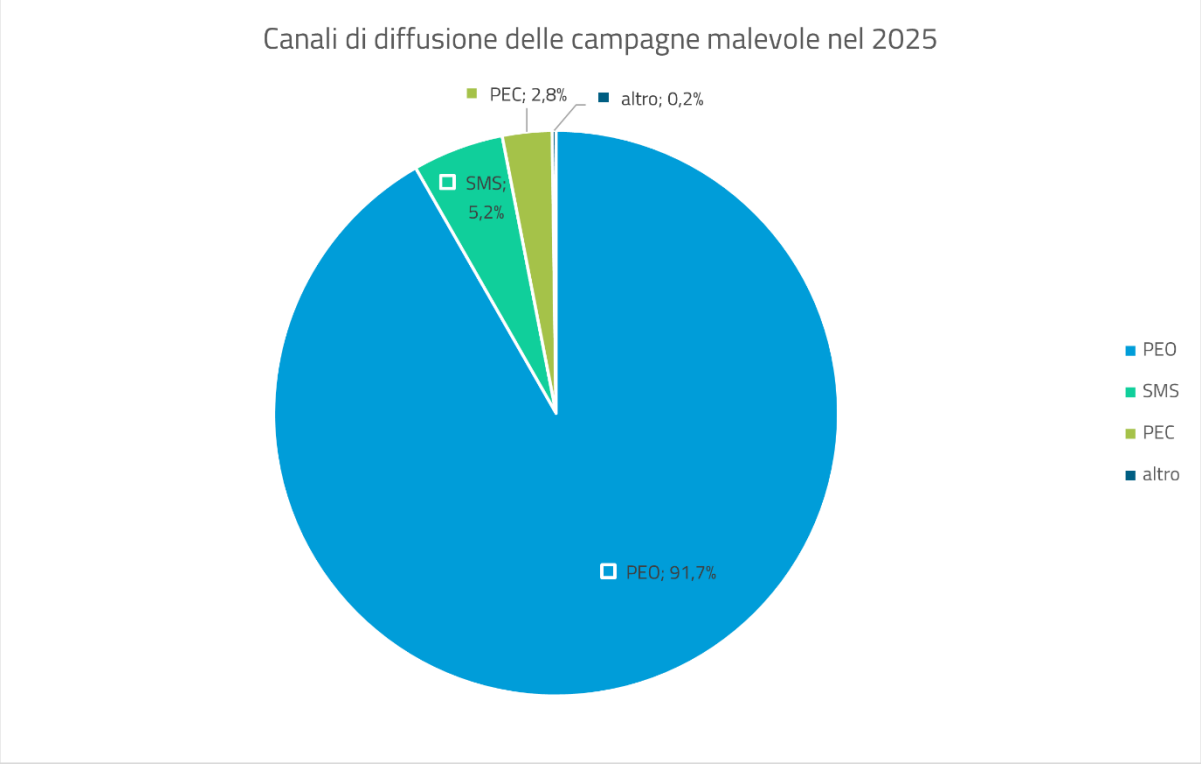
[9] https://cert-agid.gov.it/news/false-comunicazioni-riguardanti-il-politecnico-di-milano-usate-per-veicolare-formbook/
[10] https://cert-agid.gov.it/news/analisi-di-remcos-rat-diffuso-in-italia-con-campagna-clickfix-a-tema-gls/
[11] https://cert-agid.gov.it/news/xworm-e-katz-stealer-distribuiti-tramite-spazio-di-storage-di-posta-elettronica/

Per quanto riguarda le campagne di phishing, si osserva un'ampia varietà di temi impiegati. Le esche più comuni, che complessivamente rappresentano circa un terzo degli argomenti rilevati, sono costituite da:

- falsi avvisi di **sanzioni stradali non pagate**[12] che mirano a rubare dati personali e informazioni di carte di pagamento;
- **notifiche bancarie**, volte a sottrarre le credenziali di accesso degli utenti ai portali di *home banking*.

È importante sottolineare che, mentre i phishing ad argomento *"Banking"* sono sempre stati molto frequenti, la diffusione delle campagne a tema *"Multe"* rappresenta una significativa novità emersa nel 2025.

Canali di diffusione delle campagne malevole



[12] https://cert-agid.gov.it/tag/pagopa/

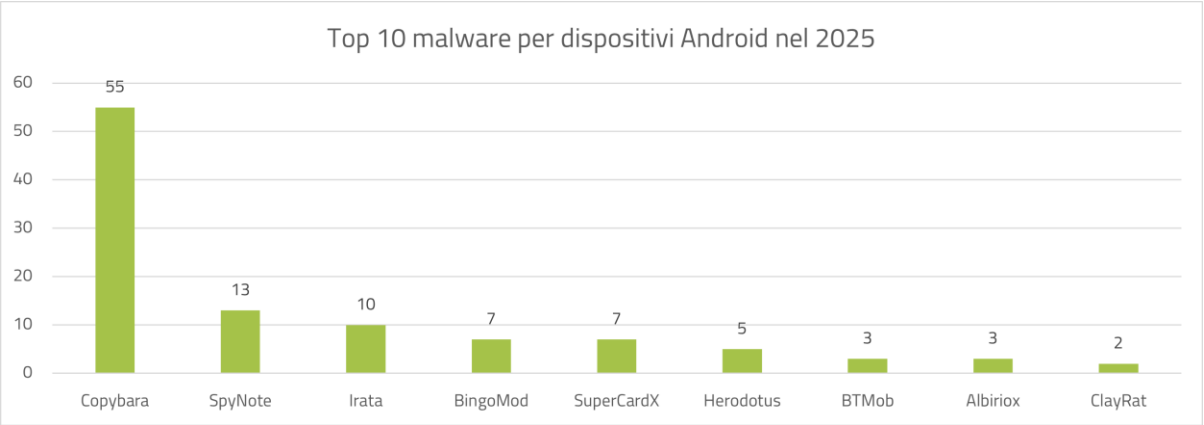
Il canale più sfruttato continua ad essere la **Posta Elettronica Ordinaria** (PEO), impiegata per diffondere vari tipi di phishing e malware.

Relativamente alle **PEC**, invece, è da notare che, rispetto all'anno precedente, il numero di campagne malevole che sfrutta la Posta Elettronica Certificata è **aumentato di circa l'80%**, per un totale di **103 eventi** registrati. In particolare, sono state individuate **77 campagne di phishing**, concentrate nella prima metà dell'anno e per lo più finalizzate a rubare credenziali bancarie[13], e **26 campagne volte a distribuire malware** come MintsLoader[14]. I phishing hanno avuto come obiettivo principale i clienti di **Intesa Sanpaolo** e **Aruba**, seguiti da altri istituti di credito.

A fronte della più volte evidenziata **riduzione dell'impiego dello smishing (di circa il 23%)**, si evidenzia l'**aumento dell'incidenza dello smishing orientato alla distribuzione di malware**, la cui quota passa da circa il 28% del totale nel 2024 a circa il 45% nel 2025. Sul fronte phishing, invece, anche se con dati migliori rispetto all'anno passato, permane l'abuso di denominazioni riconducibili a enti o servizi di interesse pubblico, con **INPS**[15] quale tema più ricorrente (59 campagne), seguito da **Autostrade per l'Italia**[16] (8) e **INAIL** (1).

[13] https://cert-agid.gov.it/news/caselle-pec-sempre-piu-usate-nel-phishing-per-le-frodi-bancarie/
[14] https://cert-agid.gov.it/tag/mintsloader/
[15] https://cert-agid.gov.it/tag/inps/
[16] https://cert-agid.gov.it/news/in-corso-uno-smishing-ai-danni-di-autostrade-per-litalia/

Malware per dispositivi mobili basati su sistemi Android

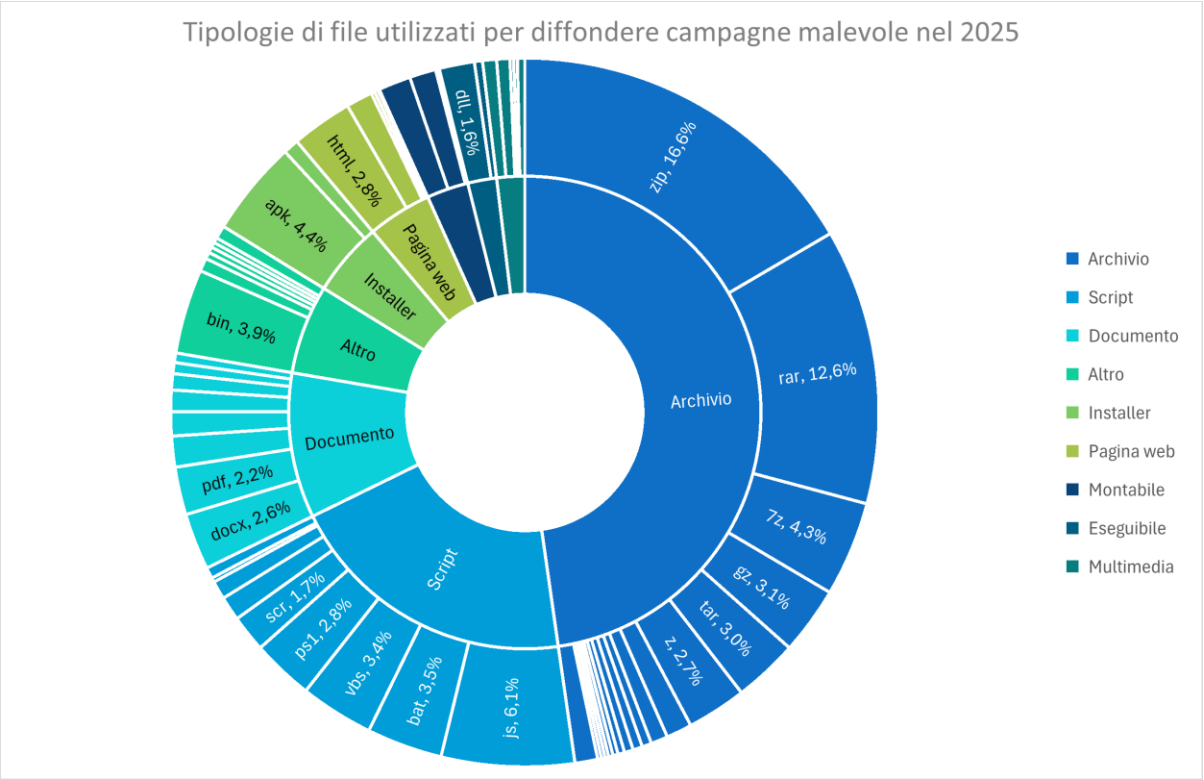


Nel 2025 il numero di campagne malware finalizzate a compromettere dispositivi mobili **Android** è aumentato in modo netto rispetto all'anno precedente (circa **+55%**). **Copybara** è risultata la famiglia più frequente, seguita a distanza da **Irata** e **SpyNote**, che erano state invece le più diffuse nel 2024.

Una quota rilevante di queste infezioni è stata veicolata tramite campagne di smishing, nelle quali gli attori malevoli inducono le vittime a installare falsi aggiornamenti o nuove applicazioni. Nella quasi totalità dei casi, i messaggi includono un link che rimanda al download del pacchetto APK dannoso e ne favorisce la successiva installazione.

Le applicazioni proposte come "da aggiornare" o "da installare" vengono spesso presentate come app bancarie, in modo da persuadere l'utente, data l'importanza del servizio, a procedere rapidamente con l'installazione.

Tipologie di file utilizzati per veicolare malware



Gli archivi compressi restano la tipologia più usata per diffondere malware, costituendo quasi la metà dei file malevoli rilevati. Gli attaccanti li impiegano inserendo al loro interno file pericolosi o collegamenti ad essi, allo scopo di tentare di superare i primi controlli di sicurezza dei server e-mail. I formati più comuni sono **ZIP** e **RAR**, che insieme rappresentano quasi il **30%** del totale, seguiti con distacco da **7Z**, **GZ**, **Z** e **TAR**. Vengono però impiegati anche formati più insoliti che comunque possono essere aperti da comuni programmi di gestione archivi.

Al secondo posto, con un'occorrenza del 20%, si rilevano file script in diversi formati, quali **JS**, **VBS**, **BAT** e **PS1**. Questa tipologia viene spesso usata in passaggi intermedi della catena di infezione e, come gli eseguibili **EXE**, possono anche essere direttamente avviati con un semplice doppio clic.

Anche **PDF**, **documenti di testo, fogli di calcolo e presentazioni** continuano a essere impiegati nelle campagne di phishing e nella diffusione di malware, rappresentando circa il 10% dei file. Queste tipologie possono includere link a risorse malevole o macro VBA. Molto spesso gli attaccanti ricorrono all'ingegneria sociale usando contenuti credibili per incrementare le aperture e l'efficacia degli attacchi.

Si osserva infine una costante utilizzo di file **APK**, impiegati per veicolare applicazioni dannose per sistemi Android e che da soli costituiscono il 4,4% di tutti i file malevoli rilevati.

Esposizione di dati trafugati

Le campagne malware basate su *infostealer*, insieme ad attacchi diretti a infrastrutture, hanno contribuito all'esfiltrazione e alla successiva diffusione di dati riferibili a utenze italiane, pubblicati per il download (gratuito o a pagamento) su diversi canali online, inclusi forum e gruppi social. Il monitoraggio del CERT-AGID si è concentrato prioritariamente su credenziali relative a caselle PEC e a servizi fiduciari e, più in generale, su account riconducibili a domini della Pubblica Amministrazione.

Nel complesso sono state rilevate **89 compromissioni**, prevalentemente riconducibili alla diffusione illecita di database appartenenti ad aziende private e a servizi commerciali. Tali archivi includevano comunque oltre 500.000 indirizzi e-mail riferibili a enti pubblici, insieme a numerosi dati personali. In poco più di tre quarti dei casi risultavano presenti anche password trafugate.

Sulla base delle evidenze raccolte, il CERT-AGID ha provveduto a informare, caso per caso, gli enti coinvolti e/o i gestori PEC interessati, con l'obiettivo di ridurre il rischio di riutilizzo improprio delle credenziali esposte.

Un caso di rilievo, per il quale il CERT-AGID ha lanciato per primo l'allarme in Italia, è rappresentato dall'attività di vendita illegale di documenti d'identità trafugati da **hotel operanti sul territorio italiano**[17]. Si è trattato di annunci che offrivano centinaia di migliaia di scansioni di documenti di riconoscimento di cittadini italiani e stranieri. Tali copie, acquisite in fase di check-in, sarebbero state sottratte tra giugno e luglio 2025 tramite accessi non autorizzati ai sistemi informatici di alcune strutture alberghiere.

L'incidente ha evidenziato un'accelerazione preoccupante nel mese di agosto 2025, con l'individuazione di un ulteriore stock di circa 17.000 elementi derivanti da una diversa unità ricettiva coinvolta. In quel periodo, l'attaccante ha rivendicato il controllo di oltre 70.000 documenti aggiuntivi prelevati da quattro ulteriori complessi turistici italiani, portando il conteggio totale delle entità alberghiere violate a dodici. Le operazioni si sono protratte con annunci sequenziali fino a circa metà estate 2025, delineando un approccio strutturato e iterativo alle violazioni.

Per altro verso, il CERT-AGID ha sollecitato le imprese del settore ospitaliero ad alzare i livelli di protezione cibernetica. In contemporanea, insieme alla Vigilanza dell'Agenzia per l'Italia Digitale, sono state diffuse comunicazioni ufficiali ai fornitori di meccanismi di riconoscimento digitale, come SPID e sigilli elettronici, invitandoli a potenziare i protocolli di verifica dei documenti.

[17] https://cert-agid.gov.it/news/in-vendita-documenti-di-identita-trafugati-da-hotel-italiani/