AGID | Agenzia per l'Italia Digitale

CERT-AGID
Computer Emergency Response Team

ANNO 2024

RAPPORTO DI RIEPILOGO

L'andamento delle campagne malevole trattate dal CERT-AGID

Report riepilogativo sulle tendenze delle campagne malevole analizzate dal CERT-AGID nel 2024

Questo report offre un quadro sintetico sui numeri delle principali campagne malevole osservate dal CERT-AGID nel corso del 2024 che hanno colpito soggetti pubblici e privati afferenti alla propria *constituency*.
Le informazioni qui presentate sono state raccolte tramite diverse fonti, tra le quali le segnalazioni spontanee provenienti da soggetti privati o Pubbliche Amministrazioni, le rilevazioni dei sistemi automatizzati del CERT-AGID impiegati a difesa proattiva della propria *constituency*, le analisi dettagliate di campioni di malware e le indagini sugli incidenti trattati.

Analisi delle tendenze generali

Dall'analisi delle tendenze generali riscontrate nel periodo considerato, si sono contraddistinte, nel vasto panorama delle minacce informatiche, le seguenti:

- **aumento delle campagne via caselle PEC compromesse**: l'utilizzo di caselle di Posta Elettronica Certificata (PEC) compromesse è triplicato rispetto all'anno precedente, con un picco di attività registrato nella seconda metà del 2024. Questo vettore, sempre ambito dagli attori malevoli, consente di rendere più verosimili le campagne di phishing e permette di aumentare la distribuzione di malware come **Vidar**;
- **incremento dell'uso di bot Telegram come C2:** quest'anno si è registrato un significativo aumento dell'utilizzo improprio di bot Telegram come server di Command and Control (C2) per attività di phishing e distribuzione di malware. Questa strategia permette agli attori malevoli di gestire con un buon grado di anonimato le comunicazioni con i sistemi compromessi;
- **crescita della registrazione di domini potenzialmente ingannevoli**: durante il 2024 sono stati registrati numerosi domini che richiamano il nome di soggetti noti come **INPS, Agenzia delle Entrate e Polizia di Stato**. Sebbene alcuni siano stati realmente utilizzati per campagne di phishing e altre truffe, la maggior parte di essi è rimasta inattiva o è attualmente in vendita;
- **prevalenza degli Infostealer tra i software malevoli**: gli infostealer hanno rappresentato la categoria di malware più diffusa, veicolati principalmente tramite archivi compressi di tipo ZIP e RAR. Questi formati continuano a essere i vettori iniziali più usati, spesso contenenti script o eseguibili utili ad avviare la catena di infezione;
- **incremento delle minacce per sistemi Android**: le campagne malevole rivolte ai

dispositivi mobili hanno registrato un notevole aumento rispetto all'anno precedente. Malware come Irata e SpyNote sono stati diffusi tramite smishing e file APK malevoli, con lo scopo principale di rubare credenziali bancarie e codici OTP, eseguendo transazioni fraudolente in tempo reale.

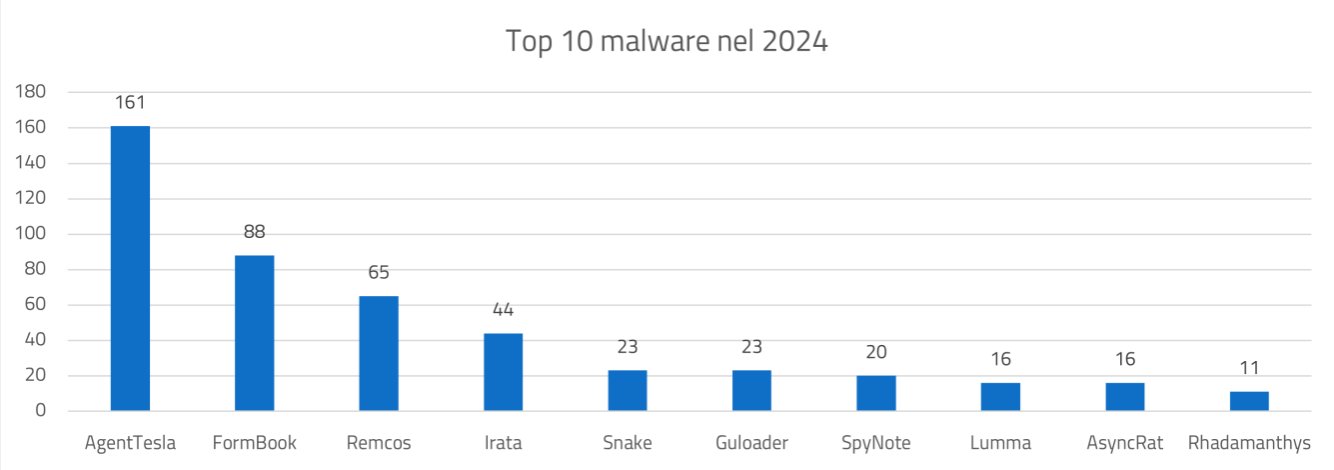
I dati riepilogativi del 2024

Nel corso del 2024, il CERT-AGID ha individuato e contrastato un totale di **1.767** campagne malevole, condividendo con la sua constituency un totale di **19.939** Indicatori di Compromissione (IoC).

	Malware	**Phishing**
Famiglie rilevate / Brand coinvolti	69	113
Campagne censite	639	1.128
Indicatori di Compromissione (IoC) diramati	6.645	13.294

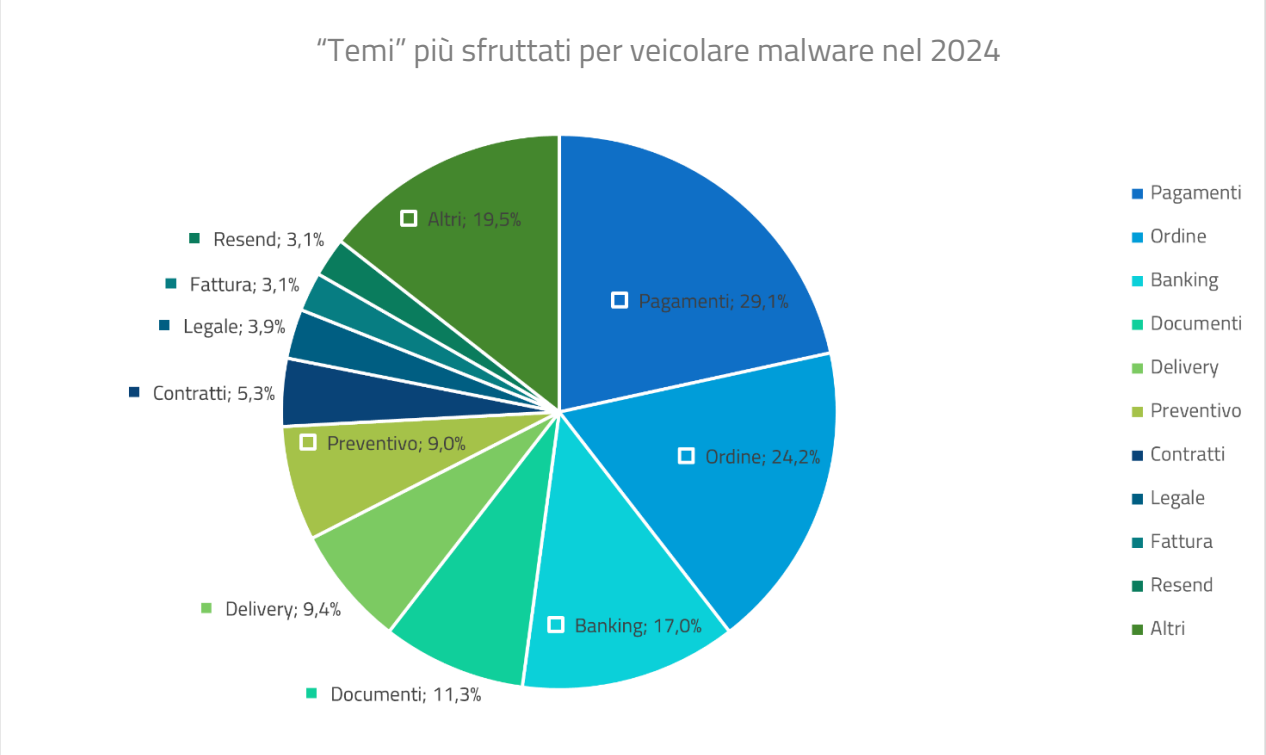
In totale sono state identificate **69 famiglie di malware.** Dei sample analizzati, circa il 67% rientra nella categoria degli Infostealer, mentre il restante 33% in quella dei RAT (Remote Access Trojan). Nel contesto di attacchi di phishing/smishing, che hanno coinvolto complessivamente **133 brand**, l'obiettivo principale è stato il furto di credenziali bancarie, di credenziali di accesso a webmail e, nel caso dello smishing ai danni di INPS, il furto di documenti di identità.

I 10 malware più diffusi in Italia



Nel corso del 2024, **AgentTesla** si è affermato come il malware più diffuso in Italia, seguito da **Formbook** e **Remcos.** Appena fuori dai primi dieci, con 10 eventi, troviamo anche Vidar, un Malware-as-a-Service appartenente alla categoria degli Infostealer, veicolato tramite indirizzi **PEC** compromessi.

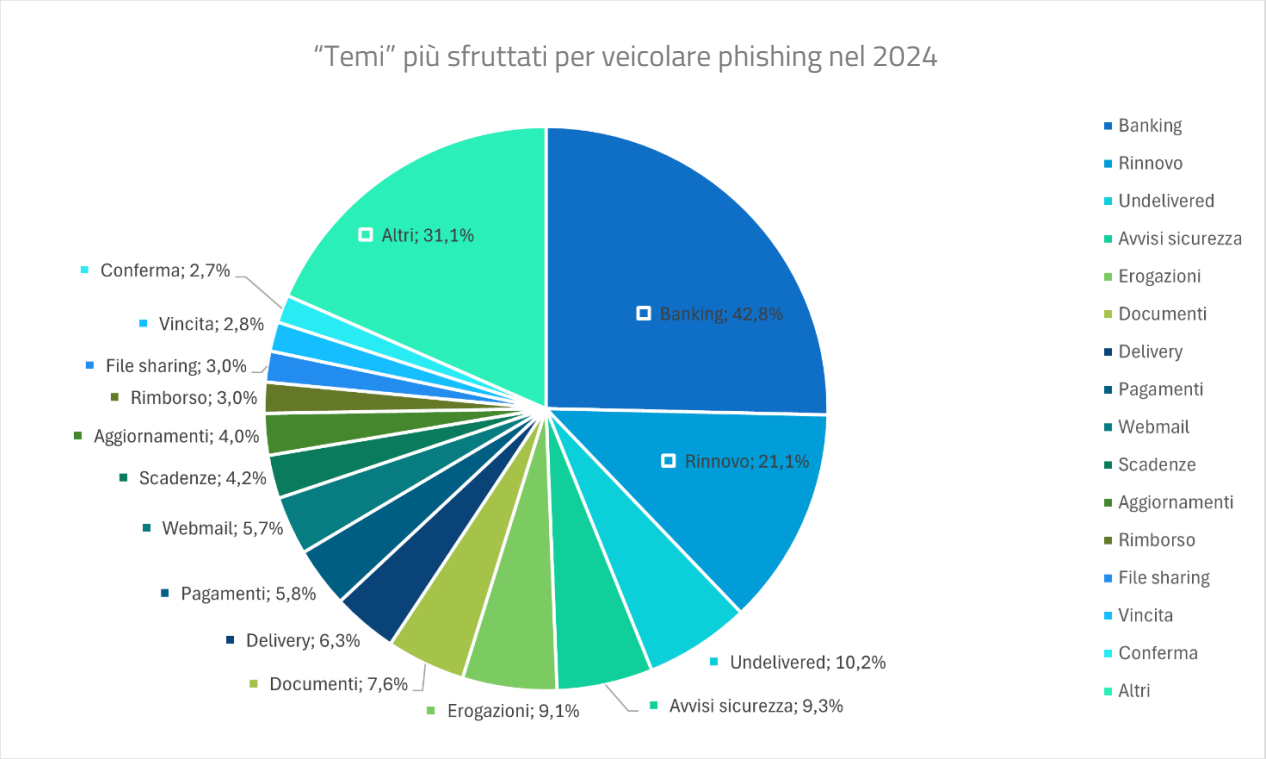
I 10 "temi" più sfruttati per veicolare malware



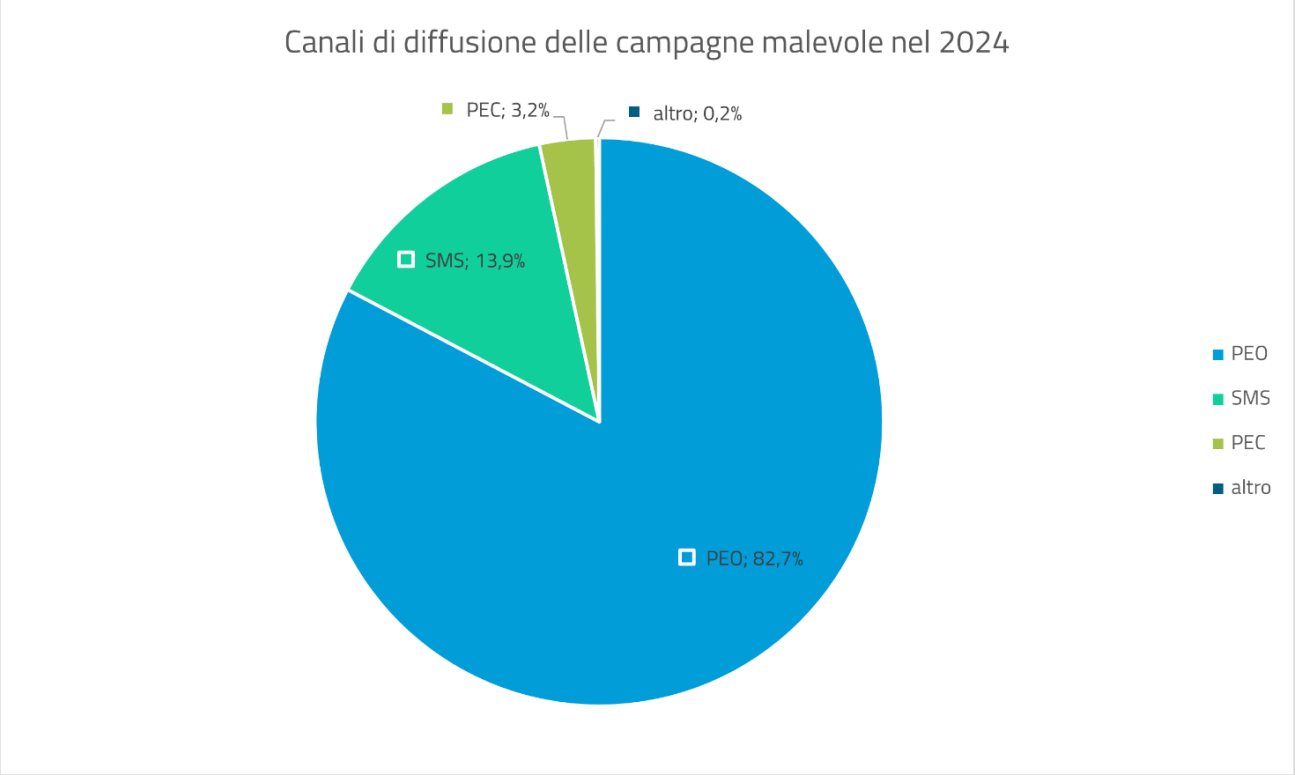
I principali "temi" sfruttati rimangono simili a quelli degli anni precedenti. Particolarmente ricorrente è stato il tema "Pagamenti", utilizzato in ben **141** campagne. I malware più frequentemente diffusi mediante tale argomento sono stati i seguenti:

Malware	**Numero di campagne**
AgentTesla	32
Formbook	26
Remcos	18
Astaroth	10
Vidar	10
Snake	9
Xworm	5

Degno di nota, anche se non rientra tra i primi dieci "temi" descritti, è stato il sofisticato tentativo di frode ai danni di utenti dell'Agenzia delle Entrate, finalizzato a infettare le vittime con un malware di tipo **keylogger**.



Canali di diffusione delle campagne malevole

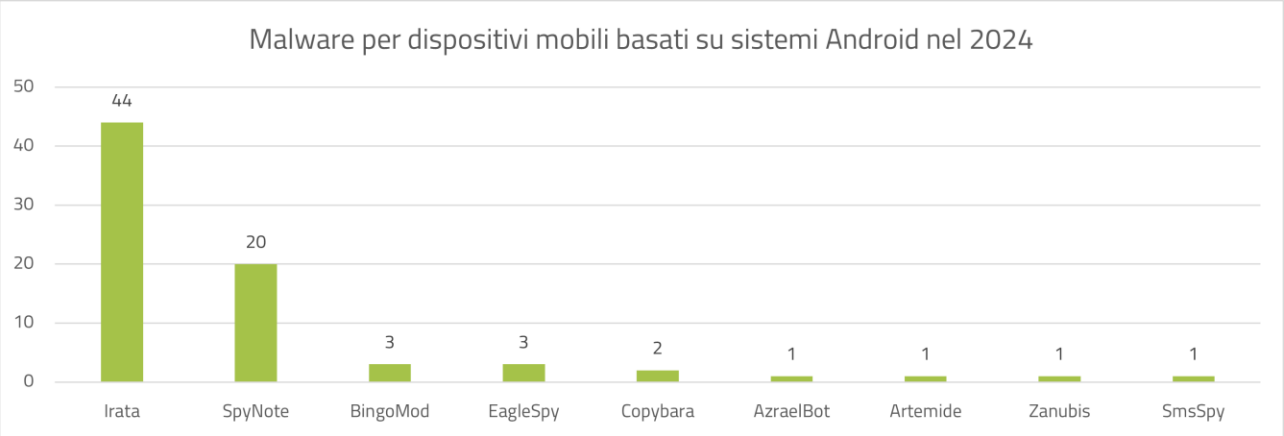


Rispetto all'anno precedente è più che **triplicato** il numero delle campagne malevole diffuse attraverso caselle di Posta Elettronica Certificata (PEC) compromesse, con un picco significativo riscontrato nella seconda metà dell'anno. Questa modalità di invio è stata sfruttata per **57** campagne totali, di cui 12 finalizzate alla distribuzione di malware e 45 destinate ad attività di phishing. Quest'ultimo ha avuto come tema principale il settore bancario, con un'attenzione particolare nei riguardi dei clienti di **Intesa Sanpaolo**. Un numero considerevole di email malevole ha colpito, inoltre, anche gli utenti di Aruba. Nei casi di malspam via PEC, come già accennato, è stato Vidar il protagonista di diverse ondate.

Contestualmente, si è registrata una **riduzione di circa il 37%** nell'utilizzo dello **smishing**, ossia dell'invio massivo di SMS fraudolenti che imitano comunicazioni provenienti da istituti bancari, servizi postali come **Poste italiane**, **INPS** o altri enti legittimi e contenenti link a risorse malevole come pagine di phishing o di download malware per dispositivi mobili.

In definitiva, il canale complessivamente più utilizzato rimane comunque quello della **Posta Elettronica Ordinaria** (PEO), sfruttato per veicolare numerose tipologie di phishing e malware.

Malware per dispositivi mobili basati su sistemi Android

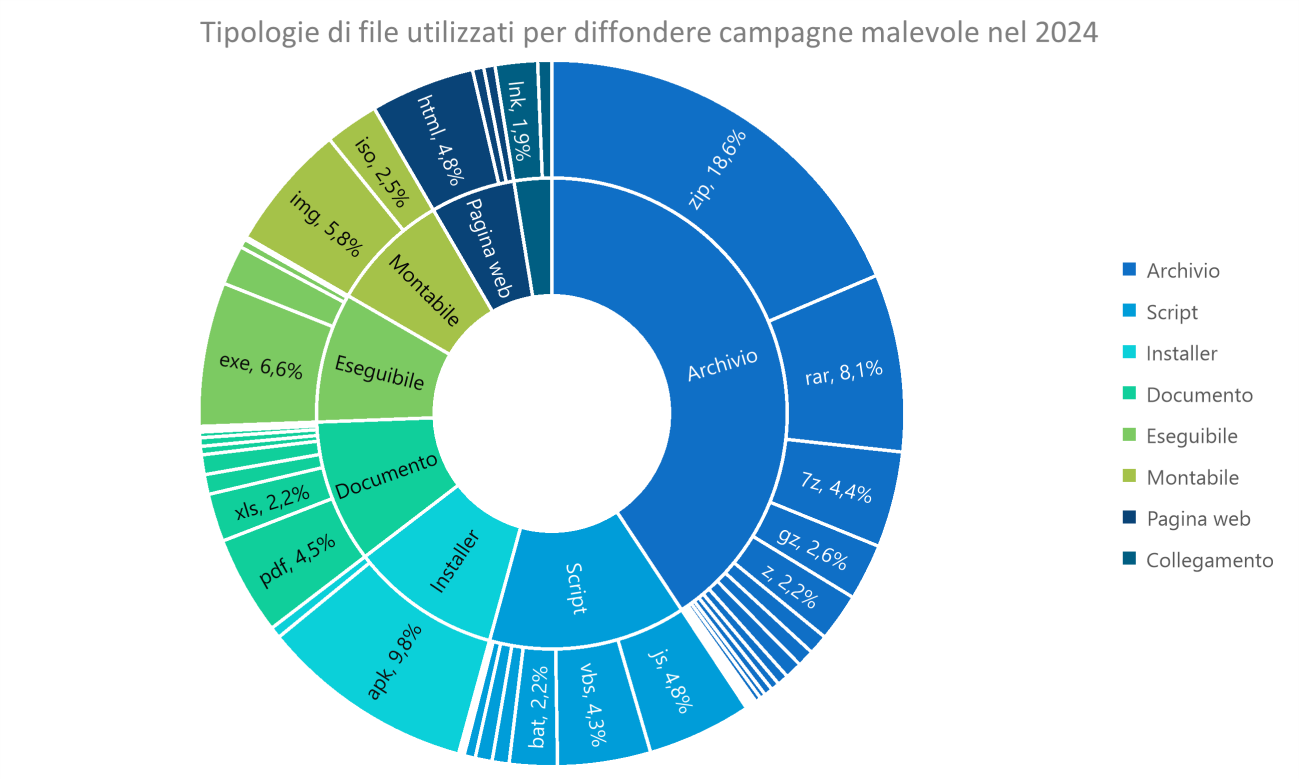


Nel corso del 2024 sono quasi **triplicate** le campagne malware mirate a compromettere dispositivi mobili basati su sistemi **Android**: ben 76 campagne malevole contro le 29 del precedente anno. Tra i diversi malware identificati, **Irata** è stata la famiglia più diffusa, seguita da **SpyNote** e da altri malware in misura inferiore.

La maggior parte di questi malware sono stati comunque veicolati tramite campagne di smishing, nelle quali gli attori malevoli tentano di indurre le vittime ad installare falsi aggiornamenti o nuove app. Nello specifico, i file APK vengono scaricati attraverso un link contenuto nel messaggio, che rimanda a un dominio di solito registrato e predisposto ad hoc.

La funzionalità predominante di queste applicazioni malevole rimane sempre il furto di credenziali bancarie. Tuttavia, le attività svolte dal malware si sono differenziate: oltre al furto di credenziali, alcune varianti intercettano o richiedono il controllo degli SMS per accedere ai codici OTP (One-Time Password). Una volta ottenuto l'accesso a tali informazioni, gli attori malevoli eseguono così le transazioni in tempo reale, sfruttando gli SMS intercettati per completare il processo di autenticazione/autorizzazione.

Tipologie di file utilizzati per veicolare malware



I formati di file più frequentemente adoperati per veicolare malware rimangono gli archivi compressi, che costituiscono circa il **41%** dei file malevoli riscontrati e sono utilizzati per contenere al loro interno file pericolosi o collegamenti ad essi. Come quantità **spiccano i formati ZIP e RAR**, mentre è più occasionale l'utilizzo di altri formati, come **7Z**, **GZ**, **Z**, **XZ e TAR**.

Al secondo posto, per un totale di quasi il 14%, troviamo file script in diversi formati, quali **JS, VBS, BAT** e **PS1**, che, alla stessa stregua dei file eseguibili **EXE,** in molti casi possono essere lanciati anche semplicemente facendo un "doppio click" e permettono di eseguire comandi dannosi sul sistema, come il download e l'esecuzione di ulteriori malware, la modifica di configurazioni di sistema o l'esfiltrazione di dati.

Alcuni di questi formati rappresentano il vettore iniziale di una infezione. Altri, come i **PS1** (script di PowerShell) o gli **EXE** (file eseguibili), rappresentano invece i passi di infezione successivi e spesso il cosiddetto payload finale del malware. Questo significa che vengono scaricati o eseguiti dopo il download e l'attivazione del primo stadio dell'infezione, come ad esempio uno script malevolo (JS, VBS, BAT) contenuto generalmente all'interno di un archivio compresso come ad esempio ZIP o RAR.

Permane comunque l'uso di documenti contenenti link a file di script o altre risorse dannose, in particolare file **PDF**, documenti Excel, Word e altri formati della suite Office, per un totale di circa il 10% del totale.

Si nota, inoltre, una frequenza sempre maggiore d'utilizzo di file **APK** (9,8%) per l'istallazione di applicazioni dannose su sistemi Android.

Si osserva infine un modesto utilizzo (circa il 5%) di file **HTML** malevoli, che si presentano come finte pagine web e sono utilizzati per diffondere principalmente phishing di varia natura, come avvenuto per i casi di campagne che hanno sfruttato Outlook e DocuSign. Sono utilizzati anche file formato **LNK** che, come primo passo nella catena di compromissione, possono eseguire comandi o reindirizzare ad altre risorse, come file scaricabili o pagine web.

Esposizione di dati trafugati

Le campagne di malware che sfruttano codice di tipo Infostealer hanno portato a una preoccupante quantità di informazioni relative a utenze italiane esfiltrate, che sono state successivamente messe in vendita su diversi canali online.
L'attenzione del CERT-AGID è stata rivolta in particolare alle utenze di caselle PEC e di servizi fiduciari coinvolti e, più in generale, anche alle eventuali utenze appartenenti al dominio della Pubblica Amministrazione.
Complessivamente sono state individuate **34 compromissioni** di diversa natura, per lo più riguardanti diffusione illecita di database di aziende private e di servizi non istituzionali, che contenevano comunque più di 250.000 indirizzi e-mail appartenenti a enti pubblici insieme a numerosi dati personali e non. Di queste, poco meno della metà contenevano anche password trafugate illecitamente.

Il CERT-AGID ha, di volta in volta, informato ciascun ente o gestore PEC coinvolto riguardo alle informazioni raccolte, al fine di evitare l'uso improprio delle credenziali rubate e diffuse pubblicamente, provvedendo anche a tenere aggiornati **i Responsabili della Protezione dei Dati**, i singoli dipendenti e gli utenti delle Pubbliche Amministrazioni sulle possibili violazioni di dati personali da parte di terzi.