Report riepilogativo sull'andamento delle campagne malevole che hanno interessato l'Italia nel 2023

03/01/2024

2023

Questo report offre un quadro sintetico sui numeri delle principali campagne malevole che hanno interessato l'Italia nel corso del 2023. Le informazioni qui presentate sono state raccolte dal CERT-AGID attraverso diverse fonti e metodologie, comprese le segnalazioni provenienti da enti privati o pubbliche amministrazioni, rilevazioni tramite sistemi automatizzati del CERT, analisi dettagliate di campioni di malware e indagini sugli incidenti trattati.

Analisi delle tendenze generali

L'analisi delle tendenze generali riscontrate nel periodo considerato ha evidenziato che:

- Nonostante il **ransomware** rimanga la minaccia più rilevante e ampiamente discussa anche nel 2023, si è riscontrato un singolo caso in Italia di ransomware (Knight) distribuito attraverso un loader veicolato tramite email. Le compromissioni da ransomware continuano ad essere realizzate manualmente, sfruttando accessi ai sistemi ottenuti mediante l'utilizzo di malware di tipo Infostealer o RAT.
- A fianco della costante diffusione degli Infostealer è stata osservata una crescita dell'uso illecito di **strumenti di controllo remoto** come *ScreenConnect* o *UltraVNC*, strumenti che presentano funzionalità molto simili al noto *TeamViewer*. Questi strumenti consentono di assumere il controllo delle macchine delle vittime, visualizzandone il contenuto del loro schermo ed interagendo con esso come farebbe un utente locale utilizzando mouse e tastiera.
- E' in forte crescita in Italia il trend di attacchi spyware con funzionalità di RAT, veicolati tramite campagne di smishing e finalizzati ad ottenere il controllo completo dei dispositivi **Android**.
- Si è registrata una costante diminuzione del numero di campagne malware condotte attraverso account compromessi di Posta Elettronica Certificata (**PEC**).
- Nel corso del 2023, **Telegram** ha consolidato la sua posizione di ecosistema predominante utilizzato dalle attività di cybercrime, come evidenziato dalla grande diffusione sui suoi canali della vendita e divulgazione di dati personali e aziendali rubati. Inoltre, ha assunto un ruolo predominante anche come luogo privilegiato per la rivendicazione di attacchi informatici e di compromissione, soprattutto da parte di collettivi filorussi e gang ransomware.

I dati riepilogativi del 2023

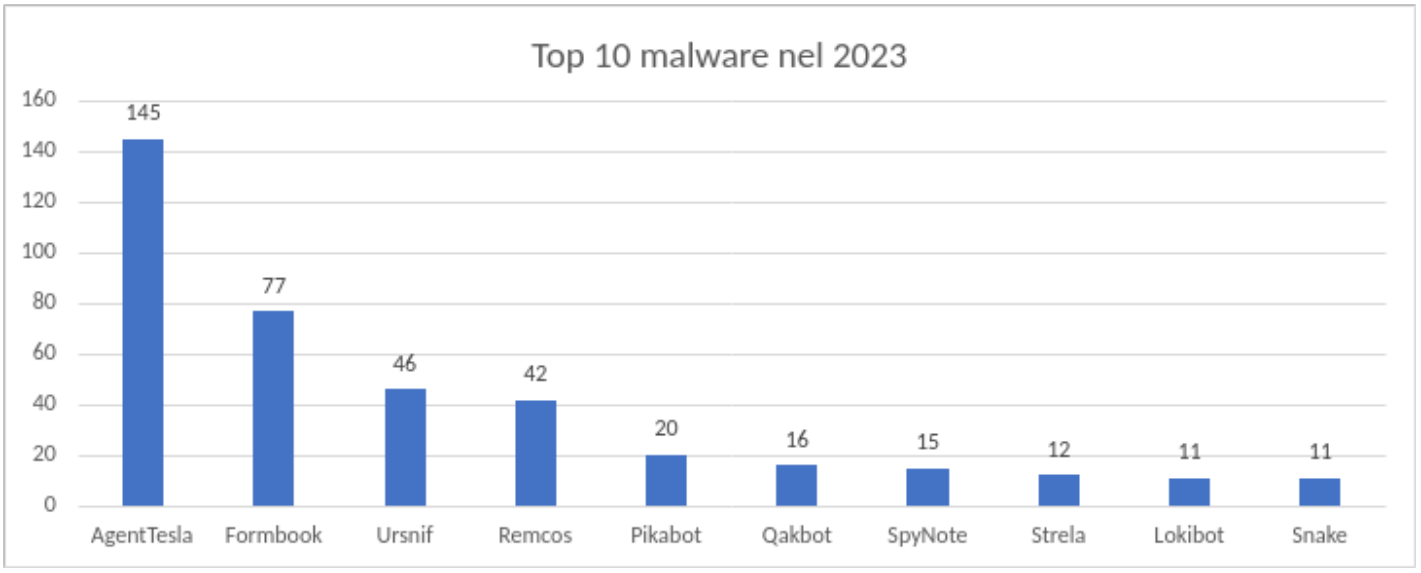
Nel corso del 2023, il CERT-AGID ha individuato e contrastato un totale di **1713** campagne malevole, condividendo con le sue organizzazioni accreditate un totale di **20,603** indicatori di compromissione (IoC).

	Malware	**Phishing**
Famiglie rilevate / Brand coinvolti	54	68
Campagne censite	510	1203
Indicatori (IoC) diramati	17827	2776

In totale sono state identificate **54 famiglie di malware**, di cui il 78% rientranti nella categoria Infostealer e il restante 22% in quella RAT (Remote Access Trojan). Nel contesto di attacchi di phishing/smishing, che hanno coinvolto

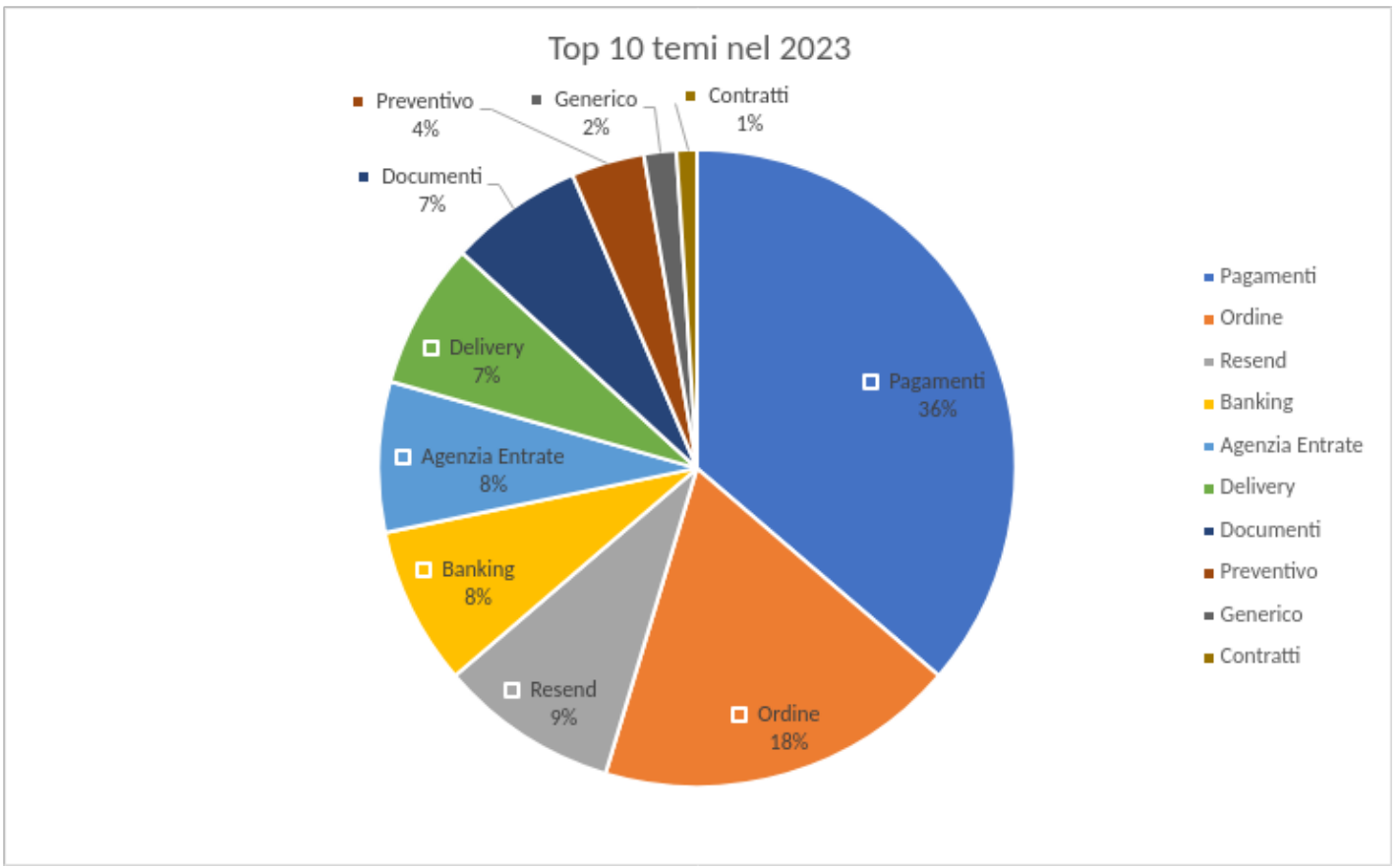
complessivamente **68 brand**, l'obiettivo principale è stato il furto di credenziali bancarie, di credenziali di accesso a webmail, e nel caso dello smishing verso INPS, il furto di documenti di identità.

I 10 malware che hanno maggiormente interessato il Paese



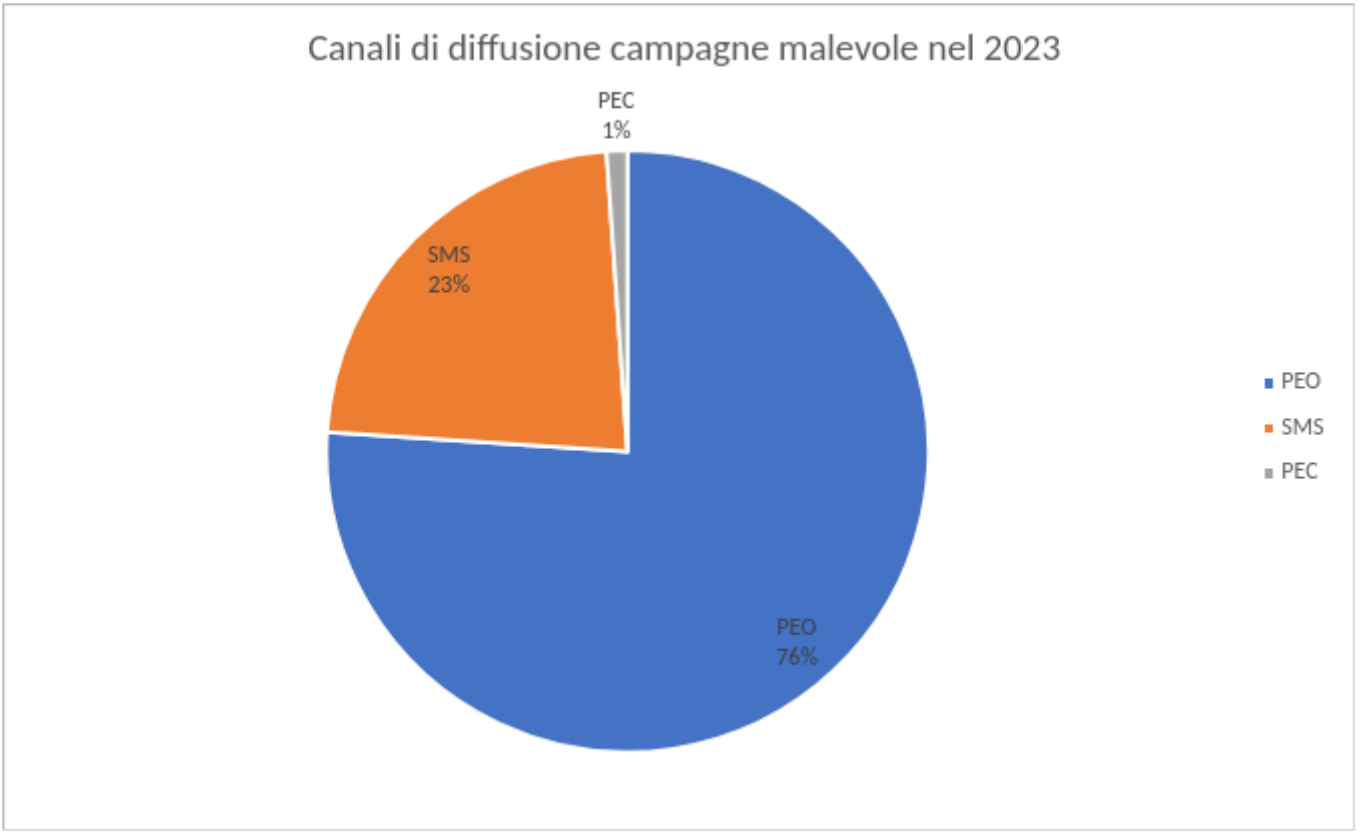
Nel corso del 2023, **AgentTesla** si è affermato come il malware più diffuso in Italia, seguito da *Formbook* e *Ursnif*. Tra i primi dieci, troviamo anche SpyNote, noto spyware progettato per dispositivi Android.

I 10 temi più sfruttati per veicolare malware



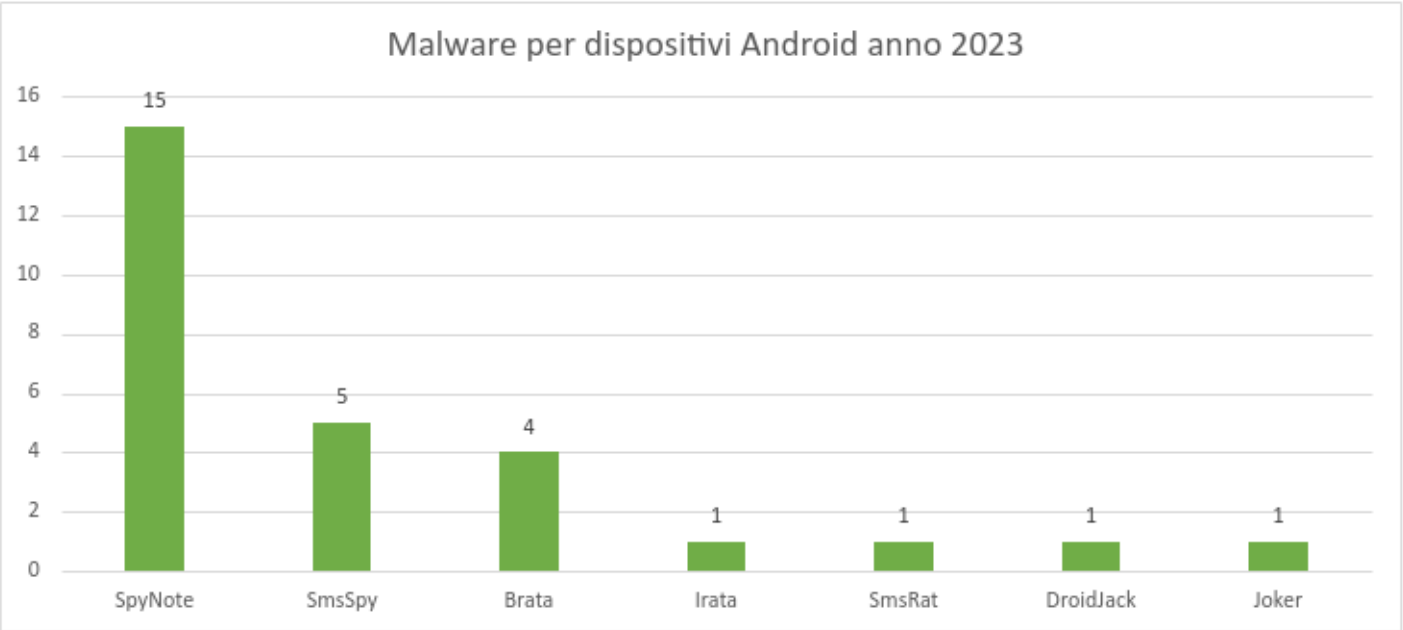
I temi principali sfruttati sono rimasti invariati rispetto agli anni precedenti, salvo che per il tema "*Agenzia Entrate*", che è stato impiegato prevalentemente nelle campagne **Ursnif** e successivamente replicato per veicolare i malware *Remcos*, *SystemBC*, *Purelogs*, *Mekotio* e *DroidJack*.

Canali di diffusione delle campagne malevole



Si è notata una significativa diminuzione delle campagne malevole veicolate attraverso account compromessi di Posta Elettronica Certificata (PEC) ma si registra parallelamente un notevole aumento dello smishing. Quest'ultimo consiste nell'invio massivo di SMS con comunicazioni ingannevoli, spesso simulando di provenire da noti "Istituti bancari" e contenenti link verso risorse malevole, quali pagine di phishing o malware per dispositivi mobili. In questo contesto, il canale più utilizzato rimane comunque la Posta Elettronica Ordinaria (PEO).

Malware per dispositivi mobili basati su sistemi Android



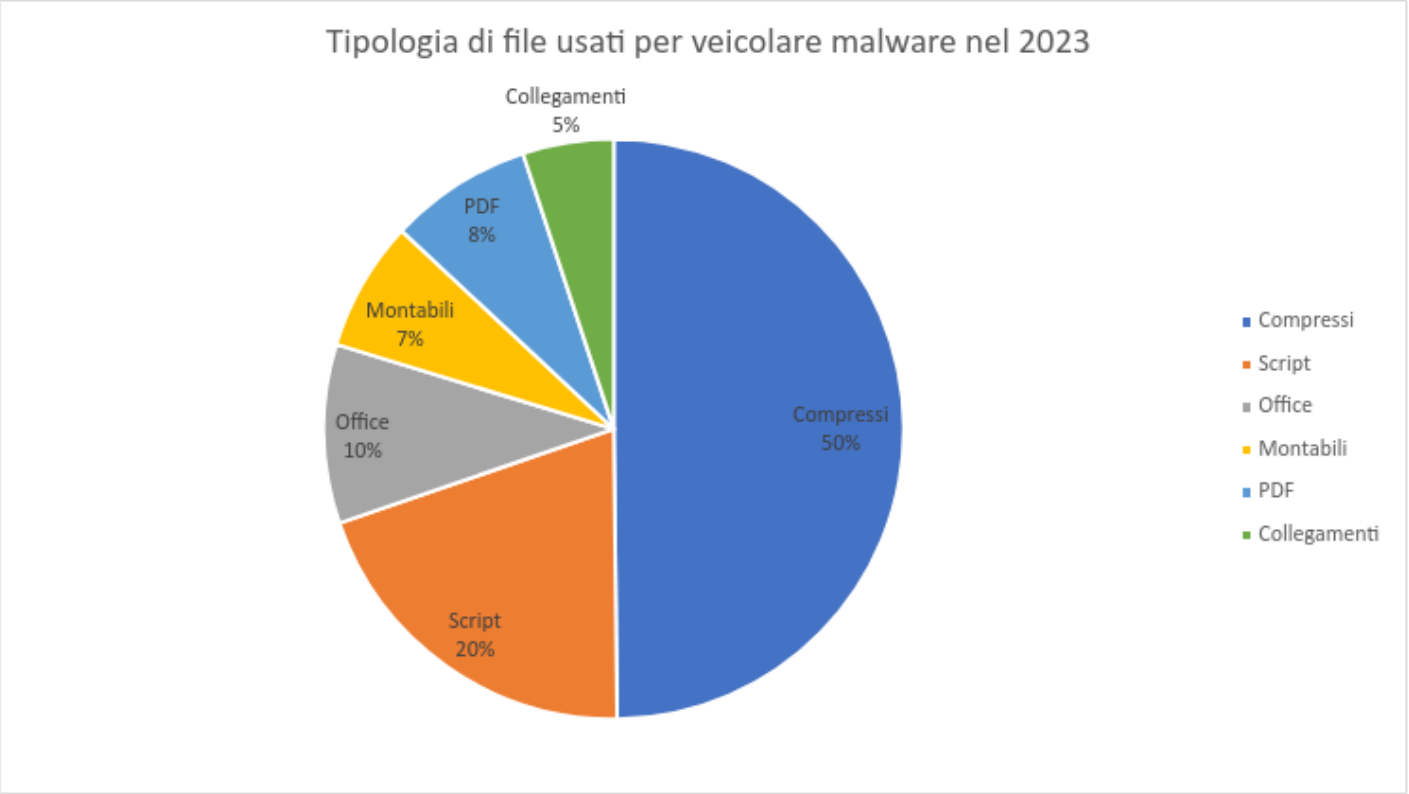
Nel corso del 2023, sono state individuate **29 campagne** malevole mirate a compromettere dispositivi mobili basati su sistemi Android.

Tra i vari malware identificati, **SpyNote** emerge come il più diffuso, con la registrazione di tre varianti nel corso dell'anno. Tutti i campioni analizzati si sono rivelati versioni riviste di malware originariamente concepiti come banking trojan e mirati al furto di denaro attraverso l'abuso delle operazioni di home banking. La maggior parte degli attori malevoli insiste nello sfruttamento di queste campagne di smishing, impersonando istituti bancari e inducendo le vittime a installare falsi aggiornamenti o nuove app.

L'app dannosa viene scaricata attraverso un link contenuto nel SMS che punta ad un file APK ospitato su un dominio di solito registrato ad-hoc.

La funzionalità predominante di queste applicazioni malevole è la lettura degli SMS, finalizzata a intercettare i codici inviati dalla banca come secondo fattore di autenticazione.

Tipologie di file utilizzati per veicolare malware



Il formato di file adoperato più frequentemente nelle campagne malevole è senza dubbio quello compresso, con un enfasi particolare sui file .**ZIP**. Questi ultimi, a loro volta, sono utilizzati per contenere documenti MS Office, file immagine montabili, script, e soprattutto nel secondo semestre, **PDF** con link a script o collegamenti a risorse condivise.

Taggato **2023**
