REPORT 2026

CAMPAGNE MALWARE

TG Soft
Cyber Security Specialist
www.tgsoft.it

REPORT 2026

CAMPAGNE MALWARE

Autori

Nicola Miotti

Samuele Callegaro

Riccardo Badan

Michele Zuin

Gianfranco Tonello

Enrico Tonello

Sommario

Introduzione

Il seguente report, redatto dal C.R.A.M. di TG Soft, sintetizza tutte le campagne di MalSpam veicolate via email che sono state analizzate durante l'anno 2025.

Il C.R.A.M. di TG Soft rilascia settimanalmente un'analisi delle campagne di MalSpam veicolate in Italia e le rende disponibili nella sezione News del Sito di TG Soft.

Come negli anni scorsi anche nell'anno 2025 la maggioranza dei malware distribuiti appartengono alla famiglia degli **Info/Password Stealer** e dei **RAT**.

L'utilizzo quasi totale di queste tipologie di malware è dettato sicuramente dalla facilità di acquisto e distribuzione sul campo di tali strumenti da parte dei cybercriminali, che possono acquistare tali malware nel Dark Web come MaaS (Malware as-a-Service) con prezzi facilmente accessibili. Un'altra motivazione di questa tendenza è l'effettiva pericolosità di queste tipologie Malware che possono risultare alquanto sofisticate.

Questa tipologia di Malware viene utilizzata solitamente come primo punto di ingresso per evolversi poi diverse tipologie di attacchi che possono arrivare anche ad estendersi per tutta la rete/azienda, come nel caso di Ransomware/CryptoMalware o sfociare in attacchi MITM (Men in the Middle) per il dirottamento di Bonifici/denaro, ecc.

I Ransomware in particolare, se non mitigati con tecnologie efficaci come quelle presenti nella suite Vir.IT eXplorer PRO (vedi Vir.IT AntiRansomware protezione CryptoMalware) possono mettere in difficoltà l'intera azienda per periodi molto prolungati portando a gravi conseguenze economiche di mancata produzione e con alti di costo di ripristino.

L'evoluzione delle campagne vede un andamento altalenante nel corso dell'anno. L'andamento segue anche le festività principali come i periodi natalizi, pasquali ed estivi con un leggero calo in questi periodi legato alla minore attività produttiva del paese.

In generale il malware che è stato utilizzato maggiormente nelle campagne globali è stato il **FormBook**, un Info/Password Stealer facilmente reperibile che esfiltra dati e password dalle macchine colpite. I dati raccolti vengono esfiltrati tramite un Server di Command & Control (C2).

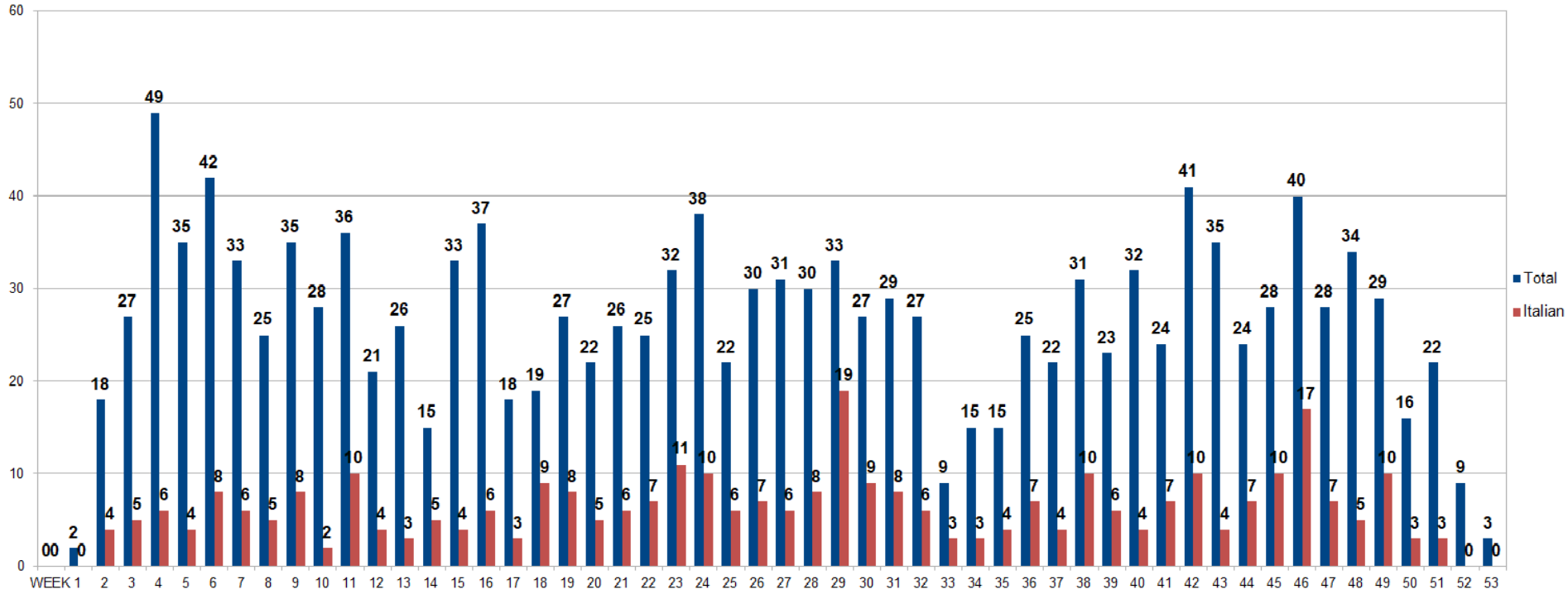
Per le campagne italiane invece il malware più utilizzato è stato l'**AgentTesla**, un Info/Password Stealer anch'esso, che esfiltra dati e password dalle macchine colpite principalmente tramite email, ma il malware prevede anche funzionalità di esfiltrazione via FTP o canali Telegram/Discord.

Vediamo in una piccola tabella di sintesi l'anno 2025 in breve, nelle pagine successive invece analizzeremo più nel dettaglio l'andamento delle campagne veicolate in Italia via email:

NUMERO CAMPAGNE GLOBALI VEICOLATE IN ITALIA ANALIZZATE	**1403**
NUMERO CAMPAGNE IN ITALIANO (scritte in lingua italiana) ANALIZZATE	**332 – 23,66%** rispetto alle campagne globali
PICCO MASSIMO DI CAMPAGNE GLOBALI SETTIMANALE	**49 – Week 04**
PICCO MASSIMO DI CAMPAGNE IN ITALIANO SETTIMANALE	**19 – Week 29**
LINGUAGGIO PIÙ UTILIZZATO	**SCRIPT – 31,25%** del totale
FAMIGLIA MALWARE PIÙ UTILIZZATA GLOBALMENTE	**FormBook**
FAMIGLIA MALWARE PIÙ UTILIZZATA NELLE CAMPAGNE IN ITALIANO	**AgentTesla**
NUMERO TOTALE DI TEMI	**19**
TEMA PIÙ UTILIZZATO NELLE CAMPAGNE IN ITALIANO	**Ordini**

La media generale calcolata sull'intero anno sulle campagne globali è di circa **27** campagne settimanali, mentre quella delle campagne scritte in italiano è di circa **6** campagne.

Grafico andamento delle campagne settimanali nel 2025

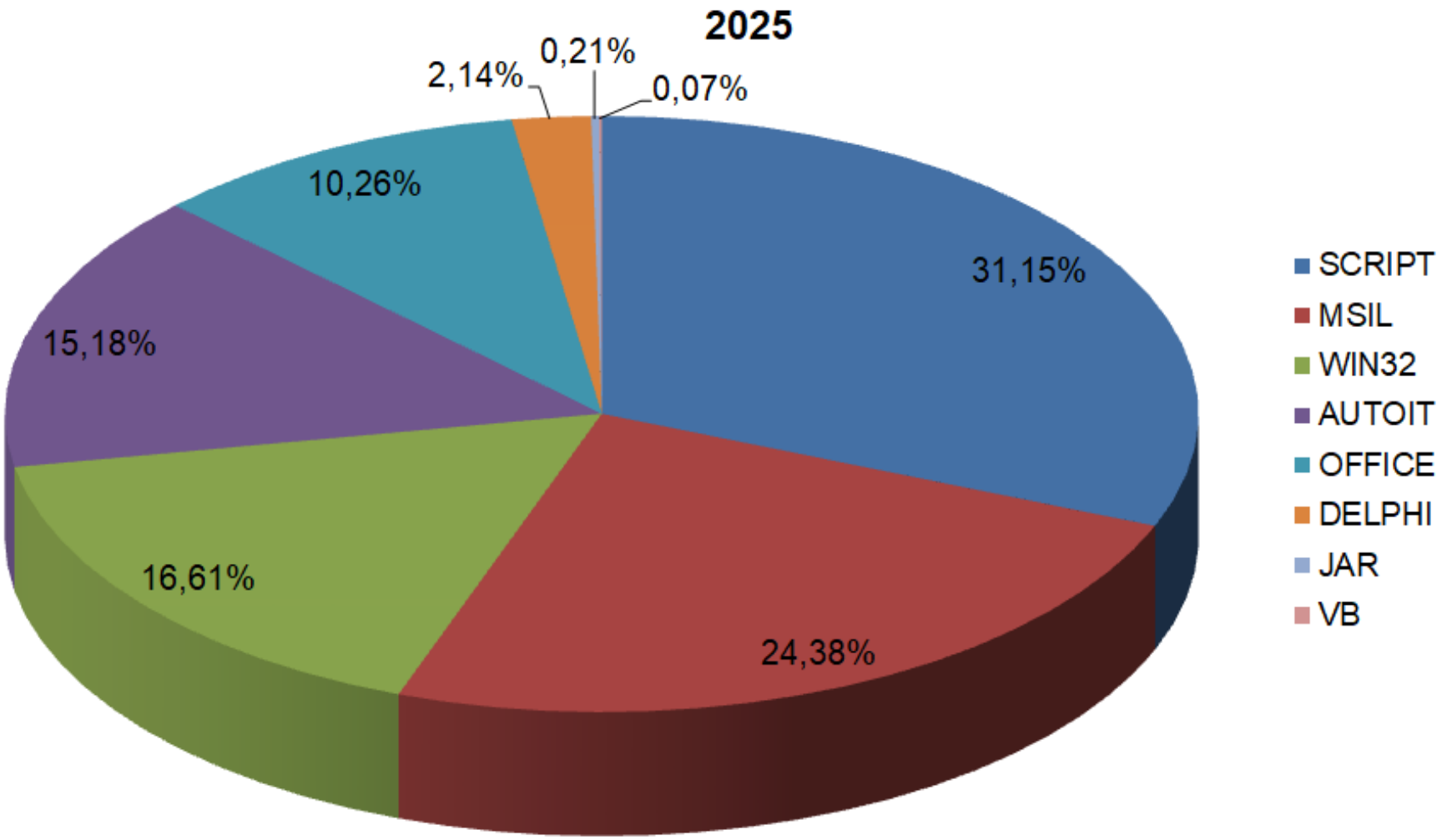


Dal grafico si può notare l'andamento delle campagne suddivise nelle varie settimane (Week) dell'anno 2025. La barra di colore blu indica il numero totale di campagne veicolate via email in Italia in ogni settimana, invece quella di colore rosso riguarda le campagne scritte in lingua italiana (con target Italia).

Per poter capire come sono suddivise le varie settimane (Week) di seguito riportiamo una piccola tabella di esempio che indica la suddivisione dei periodi presi in considerazione:

Settimana	dal	al
Week_01	01/01	05/01
Week_02	06/01	12/01
Week_03	13/01	19/01
Week_04	20/01	26/01

Grafico sulle tipologie di linguaggio utilizzate nel 2025



Dal grafico vediamo le tipologie di linguaggio utilizzati per sviluppare i malware veicolati nell'anno 2025.

Come si può vedere lo **Scripting** (JavaScript, VBScript, PowerShell, i link, WSF, BAT, etc.) è il linguaggio maggiormente utilizzato per i malware veicolati durante l'anno con ben il 31,15%.

Al secondo posto troviamo i file eseguibili **MSIL (C# .NET)** che rappresentano il 24,38%.

Sul terzo posto si classifica il linguaggio **WIN32** con il 16,61%, che raggruppa tutti i sample eseguibili creati con vari linguaggi compilati come il C, C++, ecc.

Al quarto posto si posizionano i file **AutoIT** che rappresentano il 15,18%.

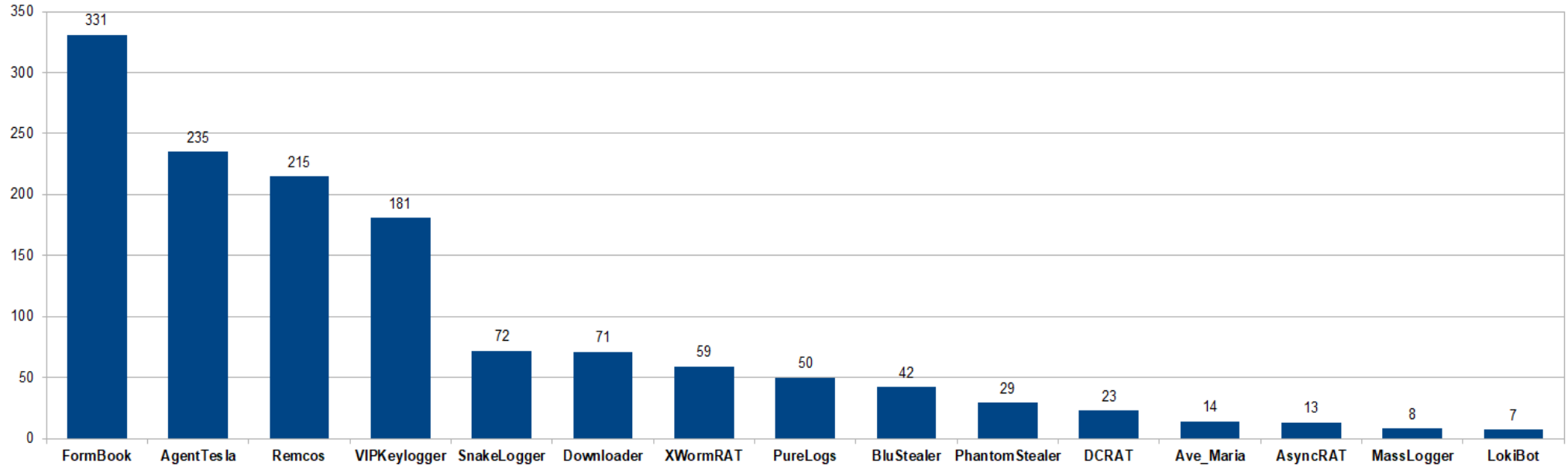
Il 10,26% dei malware veicolati sono rappresentati da documenti di **Microsoft Office** (Word, Excel, PowerPoint, etc.), essi generalmente utilizzano macro malevole o exploit per infettare il PC della vittima.

Il linguaggio di programmazione **Delphi** è utilizzato nel 2,14% dei sample mentre il resto dei sample è rappresentato in minoranza da JAR (file di Java) e VB (Visual Basic).

Di seguito una tabella con il numero di campagne divise per linguaggio:

LINGUAGGIO	NUMERO CAMPAGNE
SCRIPT	437
MSIL	342
WIN32	233
AUTOIT	213
OFFICE	144
DELPHI	30
JAR	3
VB	1

Famiglie malware globali analizzate nel 2025



Nel grafico vediamo le prime 15 famiglie malware veicolate globalmente nell'anno 2025, in totale sono state analizzate 38 famiglie di malware. Come si può notare il malware più utilizzato è stato il **FormBook**, con **AgentTesla** al secondo posto e il **Remcos** al terzo.

Abbiamo rilevato un notevole aumento della nuova famiglia malware, **VIPKeylogger**, si tratta di un **Info/Password Stealer** il quale è stato rilevato per la prima volta nel secondo semestre dell'anno 2024.

Si è notato anche l'ingresso del **Phantom Stealer** che dalla sua prima rilevazione, durante il mese di maggio 2025, ha mostrato un continuo trend di crescita. Questo malware è un **Info/Password Stealer** che è similare al malware **AgentTesla**. L'esfiltrazione dei dati avviene solitamente tramite mail con un server SMTP ma si sono visti anche esempi con BOT su Telegram.

La maggior parte dei malware rilevati appartengono alla macro famiglia degli **Info/Password Stealer**. Questo dimostra un forte interesse da parte dei cybercriminali verso i dati e le password delle vittime.

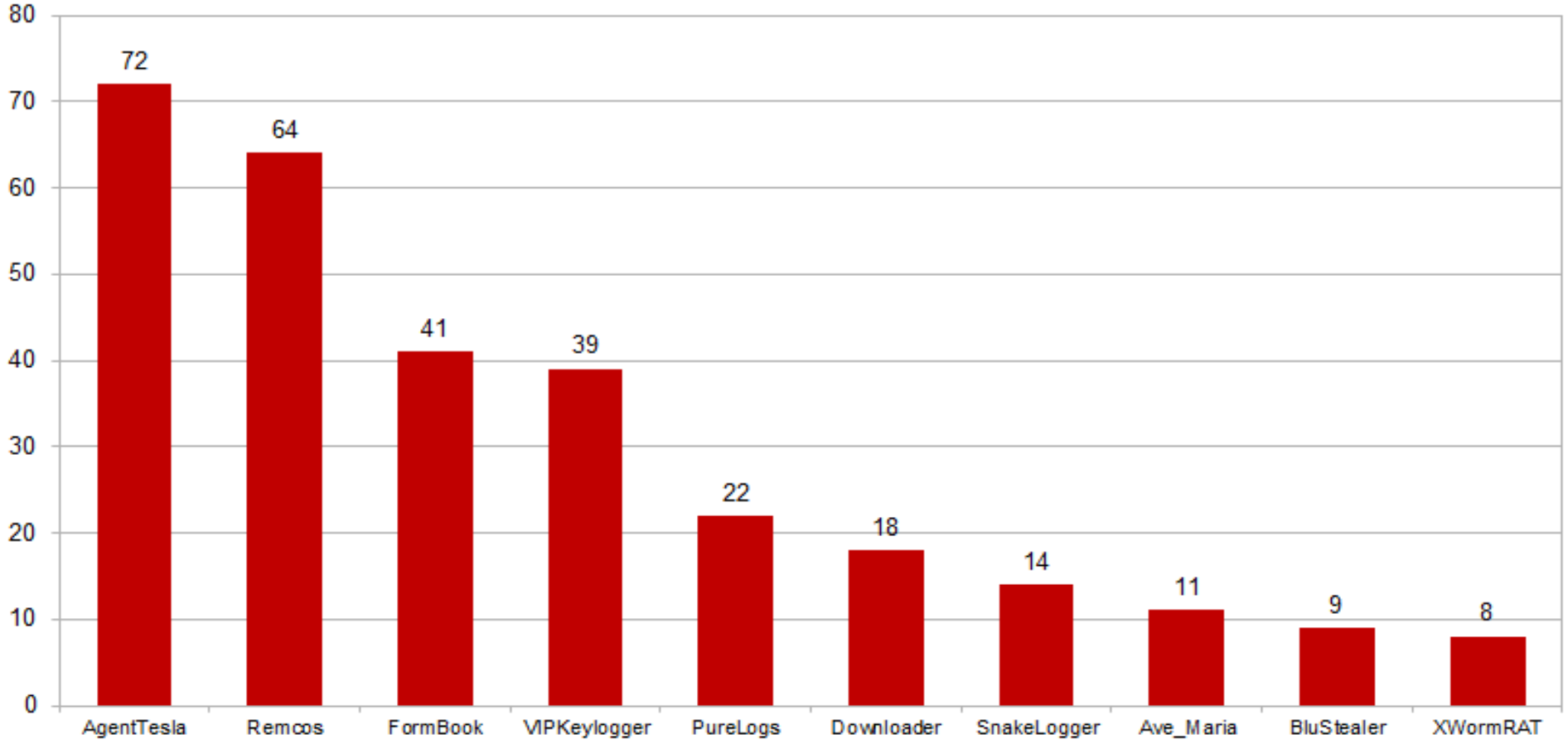
Gli **Info/Password Stealer** sono infatti una minaccia grave, in quanto sono spesso il punto iniziale di attacchi molto più sofisticati e pericolosi, che prevedono l'utilizzo di Ransomware/CryptoMalware per la cifratura dei dati degli utenti con successiva richiesta di riscatto. Questi attacchi se non mitigati con tecnologie specifiche come quelle presenti nella suite Vir.IT eXplorer PRO possono mettere in ginocchio intere aziende.

Un'altra macro famiglia molto utilizzata durante l'anno è quella dei **RAT** (Remote Access Trojan), questi malware permettono di prendere il controllo completo del PC della vittima generando quindi un pericoloso punto di accesso dall'esterno alla rete informatica della vittima.

Di seguito la tabella riepilogativa di tutte le famiglie analizzate con il relativo numero di campagne:

FAMIGLIA	NUMERO CAMPAGNE	FAMIGLIA	NUMERO CAMPAGNE
FormBook	331	DarkVisionRAT	3
AgentTesla	235	STRRAT	3
Remcos	215	RAT	3
VIPKeylogger	181	LummaStealer	3
SnakeLogger	72	Rhadamanthys	2
Downloader	71	RedLine	2
XWormRAT	59	Neshta	2
PureLogs	50	BabylonRAT	2
BluStealer	42	NetWire	1
Phantom Stealer	29	VidarStealer	1
DCRAT	23	StormKitty	1
Ave_Maria	14	SmokeLoader	1
AsynchRAT	13	Stealc	1
MassLogger	8	ClickFix	1
LokiBot	7	ScreenConnect	1
VenomRAT	7	DeerStealer	1
MintsLoader	7	Phorpiex	1
QuasarRAT	4	KatzStealer	1
MSIL Logger	4	KoiStealer	1

Famiglie malware in italiano analizzate nel 2025



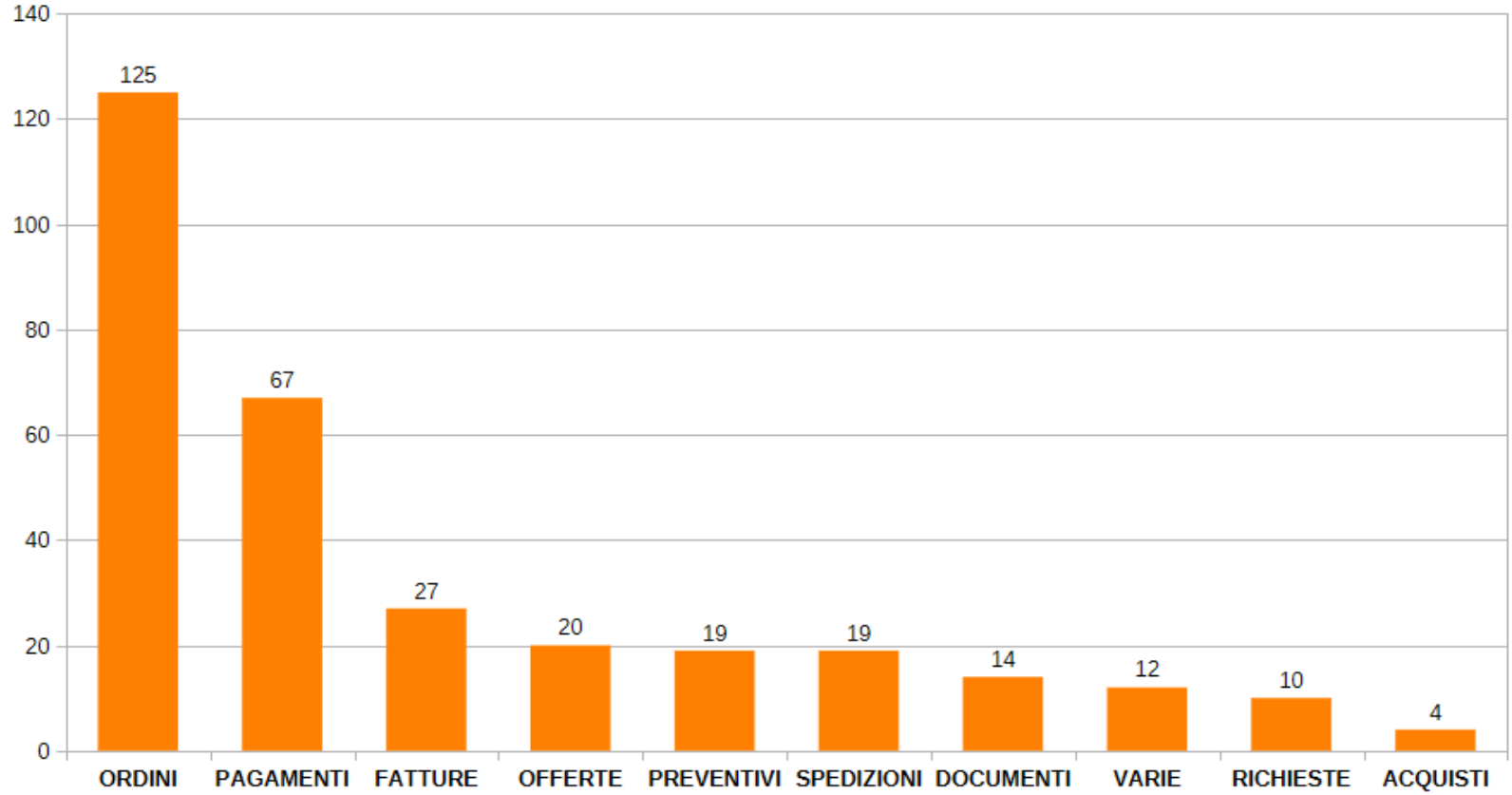
Nel grafico vediamo le prime 10 famiglie malware utilizzate nelle campagne di MalSpam scritte in lingua italiana che sono state analizzate nell'anno 2025, in totale sono state rilevate 25 famiglie di malware.

Nelle campagne scritte in italiano quest'anno il più utilizzato è l'**AgentTesla** con il **Remcos** al secondo posto e il **FormBook** al terzo.

Anche nelle campagne scritte in italiano, in generale la maggior parte dei malware utilizzati appartengono alla macro famiglia degli **Info/Password Stealer** e dei **RAT**. Di seguito la tabella riepilogativa di tutte le famiglie analizzate con il relativo numero di campagne:

FAMIGLIA	NUMERO CAMPAGNE	FAMIGLIA	NUMERO CAMPAGNE
AgentTesla	72	AsynchRAT	3
Remcos	64	STRRAT	2
FormBook	41	BabylonRAT	2
VIPKeylogger	39	DCRAT	2
PureLogs	22	Rhadamanthys	1
Downloader	18	VIdarStealer	1
SnakeLogger	14	StormKitty	1
Ave_Maria	11	VenomRAT	1
BluStealer	9	Stealc	1
XWormRAT	8	QuasarRAT	1
MintsLoader	7	MassLogger	1
Phantom Stealer	7	KatzStealer	1
LokiBot	3		

Temi utilizzati nelle campagne malware in italiano analizzate nel 2025



Nel grafico vediamo i primi 10 Temi utilizzati nelle email di MalSpam con target italiano (scritte in lingua italiana), in totale sono stati rilevati **19** temi.

I temi sono dei macro argomenti che rappresentano il contesto comunicativo rilevato nelle mail delle campagne con target italiano.

Al primo posto troviamo il tema "**Ordini**" con 125 campagne, al secondo posto con 67 campagne vi è il tema "**Pagamenti**", al terzo posto più distaccato con 27 campagne, vi è il tema "**Fatture**".

Il tema "**Varie**" indica email con temi generici e non particolarmente personalizzate o in alcuni casi email che contengono spezzoni di messaggi reali precedentemente rubati.

In generale i temi utilizzati coprono una vasta gamma di ambiti partendo da quelli più generici arrivando a temi più specifici o governativi.

Di seguito la tabella con tutti i temi riscontrati e la relativa quantità:

TEMA	NUMERO CAMPAGNE
ORDINI	125
PAGAMENTI	67
FATTURE	27
OFFERTE	20
PREVENTIVI	19
SPEDIZIONI	19
DOCUMENTI	14
VARIE-REPLY-CHAIN	12
RICHIESTE	10
ACQUISTI	4
PRENOTAZIONI	3
AVVISI	2
CONTRATTI	2
PRODOTTI	2
RICEVUTE	2
COMUNICAZIONI	1
ORDINANZE	1
PREAVVISI	1
PREZZI	1

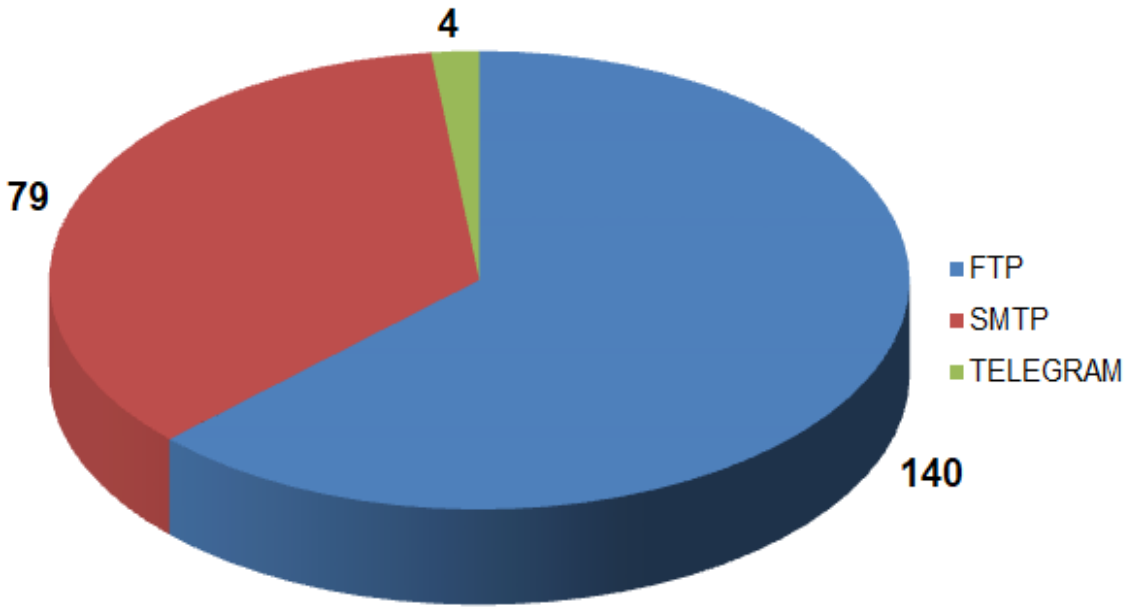
AgentTesla

Di seguito entriamo nel dettaglio del malware che è arrivato al secondo posto come distribuzione globale nel 2025 e al primo posto per quanto riguarda le campagne in lingua italiana: l'**AgentTesla,** malware che appartiene alla famiglia dei Info/Password Stealer.

I metodi principali di esfiltrazione dati che abbiamo rilevato nell'anno 2025 sono stati i seguenti 3:

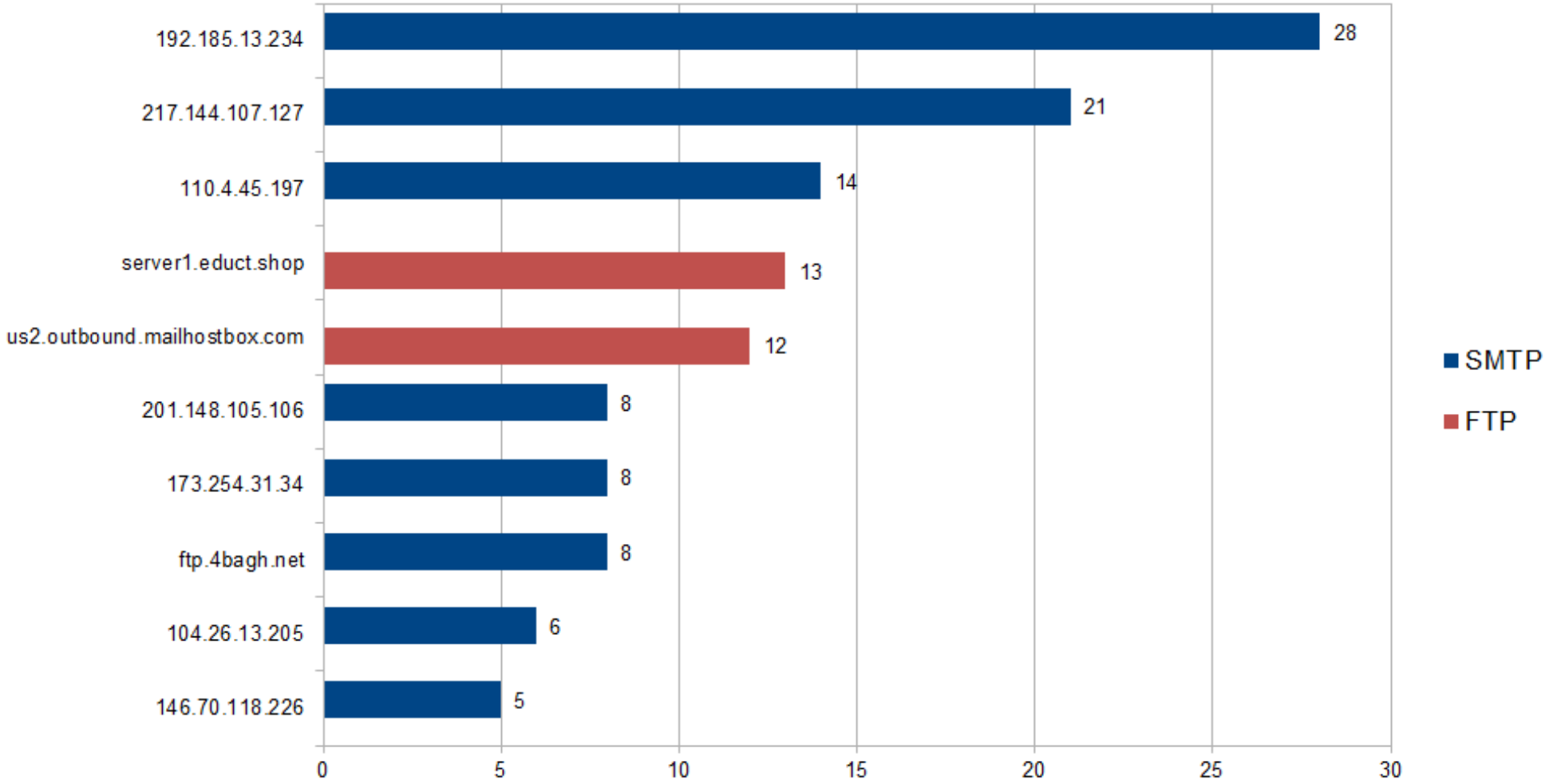
- **SMTP** (Simple Mail Transfer Protocol) - il quale rappresenta l'esfiltrazione tramite l'invio di posta elettronica ed è stato il più utilizzato nell'anno 2025 con un numero totale di **140** sample.
- **FTP** (File Transfer Protocol) - è il protocollo standard utilizzato per il trasferimento i file da un client ad un server, questo metodo è stato rilevato per un numero totale di **79** sample.
- **Telegram** - una delle più note piattaforme di messaggistica internazionale, viene spesso abusata dai malware per l'esfiltrazione dei dati rubati. Nella maggior parte dei casi l'esfiltrazione avviene tramite un BOT creato dai malviventi, al quale vengono inviati i dati sotto forma di un archivio compresso. Questo metodo è stato rilevato per un numero totale di **4** campagne.

Negli anni passati è stato rilevato anche l'uso di **Discord** come metodo di esfiltrazione. Si tratta sempre di una delle più note piattaforme internazionali di messaggistica e VoIP la quale anche essa viene utilizzata come metodo di esfiltrazione tramite un BOT creato dai malviventi, un metodo molto simile a quello sopra citato di Telegram.



NB: Non è stato possibile estrarre il metodo di esfiltrazione da tutte le campagne classificate.

Di seguito vediamo la **TOP10** dei server **SMTP/FTP** utilizzati dal malware di AgentTesla:

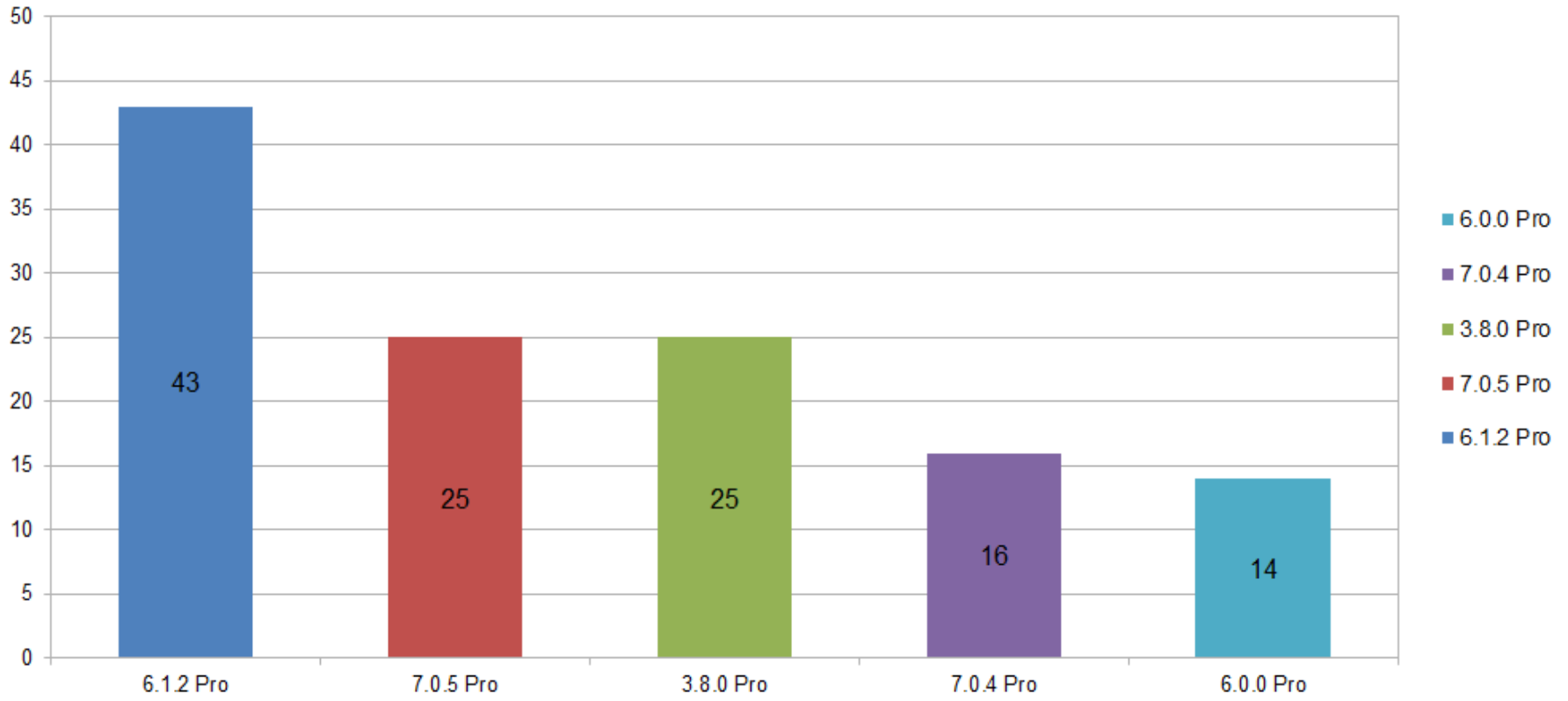


Remcos

Un'altra analisi approfondita è stata realizzata nei confronti del malware **Remcos** il quale appartiene alla macro-famiglia dei RAT (Remote Access Trojan). Questo malware si è posizionato al terzo posto tra i malware veicolati globalmente nell'anno 2025 e al secondo posto nelle campagne scritte in lingua italiana.

La versione **6.1.2 Pro** (per "Pro" si intende la versione Professional pertanto acquistata con tutte le funzionalità disponibili) è la Build più diffusa, con **43** campagne rilevate.

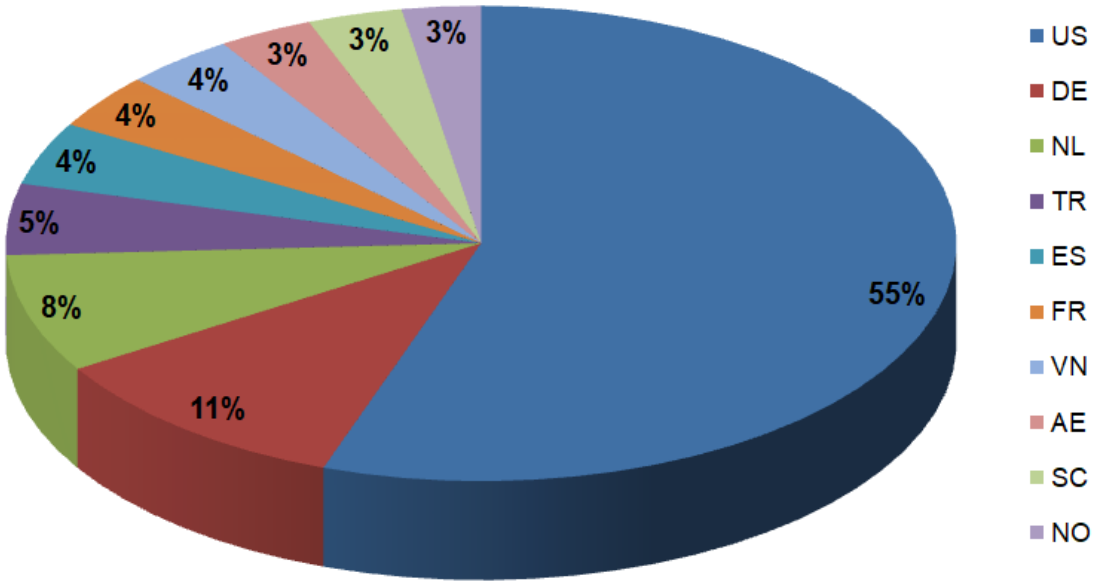
Dal grafico vediamo la **TOP 5** delle versioni più utilizzate per il malware **Remcos**:



Abbiamo analizzato anche i vari dati che compongo la Build Professional del Remcos, la licenza più utilizzata è stata: “**2E83F9960FC53638552B52D7DF6F58A5**” con **11** utilizzi su 215 campagne analizzate.

Il “MUTEX”, che è una stringa che il Threat Actor assegna una volta completata la configurazione della Build, più diffusa nel 2025 è la stringa "**chrome-JPTHQD**".

TOP 10 MUTEX	
MUTEX	**NUMERO DI CAMPAGNE**
chrome-JPTHQD	5
Rmc-0DM30N	4
Rmc-P941XE	4
Rmc-QWEW4X	4
syserms-HERNG3	4
uerusaoie-1EMHVJ	4
weweasawswsa-8QOGEH	3
Rmc-4UZES8	3
Rmc-GGCIP4	3
Rmc-PNQJCE	3

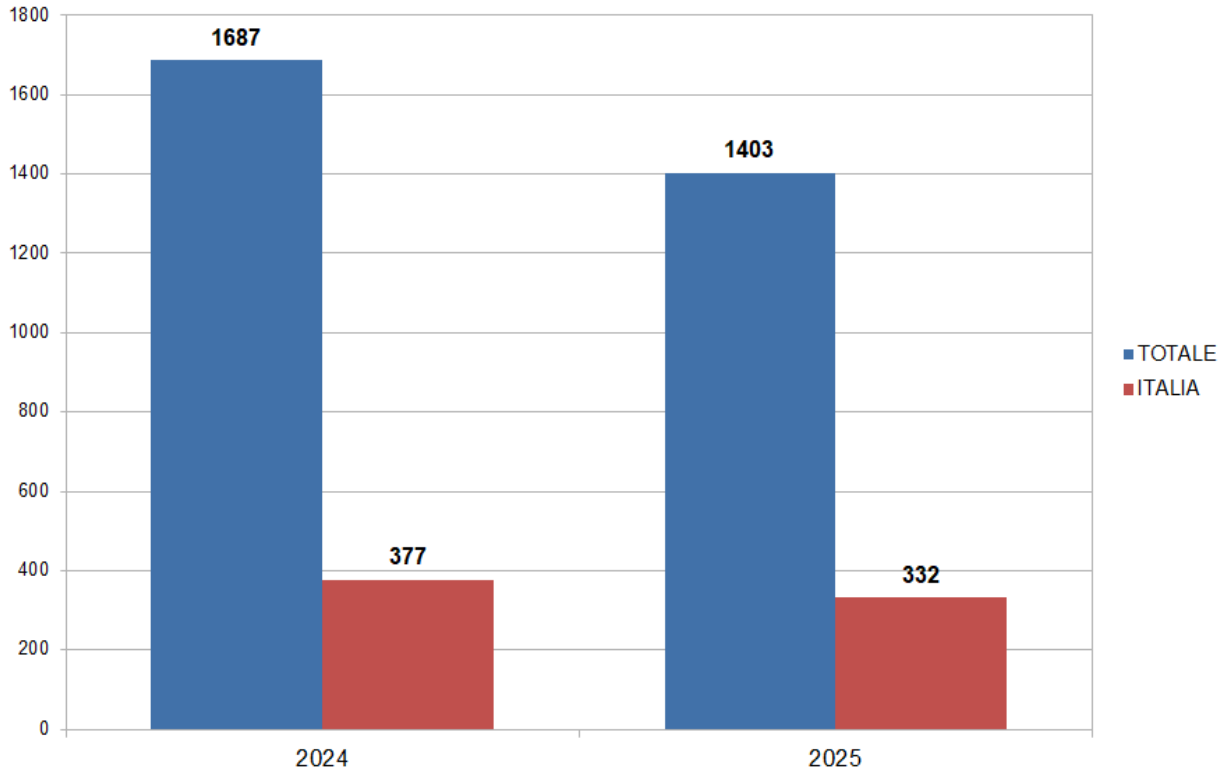


TOP10 C2

Per la parte di esfiltrazione dei dati, dalle analisi effettuate sulla attività di traffico dati, abbiamo rilevati i 10 paesi più utilizzati dove risiedono i server di Command & Control (C2). Nel grafico a torta si può notare che la percentuale più alta è quella degli Stati Uniti d'America, esso è il paese dove abbiamo il maggior numero di server C2 con 50 indirizzi IP diversi. Al secondo posto troviamo la Germania (sigla DE) con 13 indirizzi. Per quanto riguarda invece il terzo posto, si tratta dei Paesi Bassi (sigla NL) con 15 indirizzi IP.

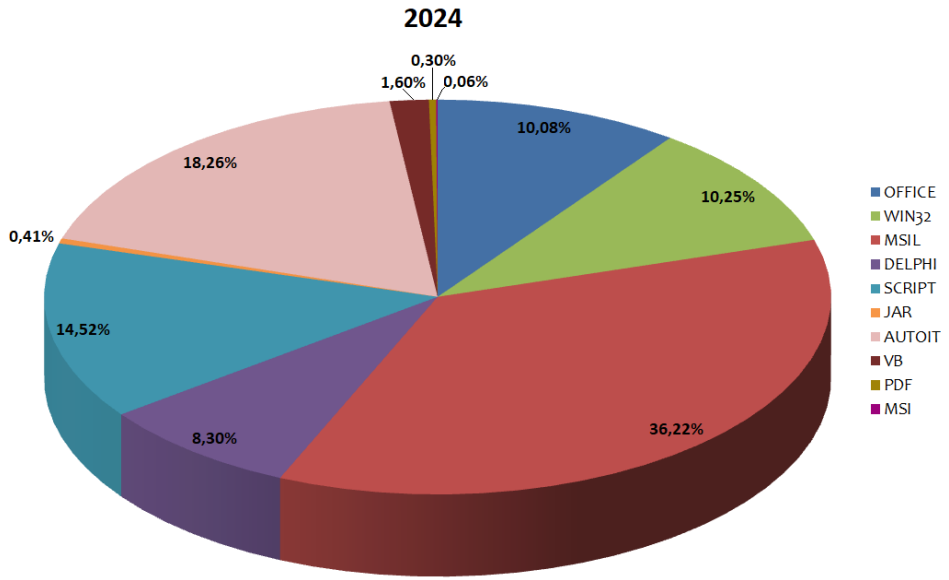
Confronto delle campagne malware analizzate nel 2024/2025

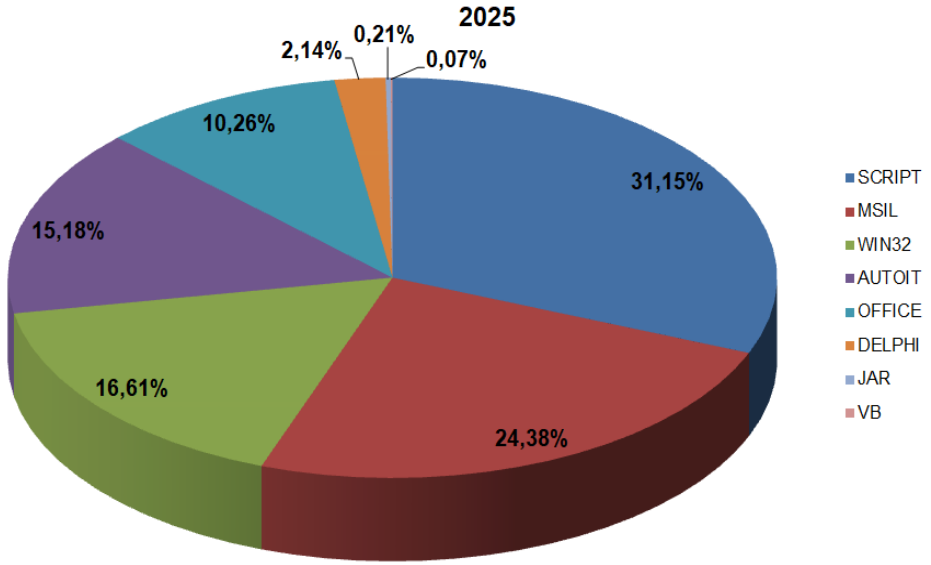
Facendo una comparazione con l'anno 2024, possiamo notare che il 2025 ha avuto una diminuzione di 284 campagne globali (-16,83%) e di 45 campagne scritte in lingua italiana (-11,93%).



Questo trend di diminuzione del numero di campagne è sicuramente dovuto dalle importanti attività di contrasto messe in atto dalle forze di polizia nazionali ed internazionali che hanno portato allo smantellamento di svariate Botnet utilizzate per la diffusione massiva di Malware, basta pensare al take-down da parte di un gruppo interforze di Emotet e lo smantellamento delle reti criminali di QakBot, IcedID, ecc.

Per quanto riguarda le tipologie di linguaggio utilizzate, nel 2025 abbiamo rilevato una forte diminuzione del linguaggio **MSIL** (C# .NET) del 11.84% rispetto all'anno 2024, e un notevole aumento del 16,73% del linguaggio di **Scripting**.





Restano invariate le prime 3 famiglie che hanno dominato in entrambi gli anni, più precisamente quelle delle macro famiglie dei Info/Password Stealer che sono **FormBook, AgentTesla** e quelli delle macro famiglie dei RAT che è **Remcos**, anche se in ordine differente rispetto all'anno 2024.

Un'altra somiglianza importante riguarda i temi utilizzati nelle email di MalSpam con target italiano (scritte in lingua italiana), dominano anche quest'anno i seguenti temi: **Ordini, Pagamenti** e **Fatture**.

Questo si spiega per il semplice motivo che la maggior parte delle email legittime che vengono inviate nelle attività quotidiane riguardano l'ambito lavorativo e quello relazionale, come gli ordini ed i relativi pagamenti e fatture. I CyberCriminali ovviamente cercano di simulare il più possibile queste attività così da tentare di ingannare il maggior numero di utenti.

Nella tabella sottostante possiamo vedere la comparazione delle famiglie tra il 2024 e il 2025, come si può notare alcune famiglie malware sono state presenti sia nel 2024 sia nel 2025 (colore azzurro), alcune sono state presenti solamente nel 2024 (colore rosso) mentre altre sono delle famiglie che sono state presenti solo nel 2025 (colore verde).

Malware storici come **Ursnif** ed **Emotet** non sono stati rilevati nel 2025, sostituiti da nuove famiglie come ad esempio il **Phantom Stealer**.

2024	2025
Adwind	
AgentTesla	AgentTesla
Astaroth	
AsynchRAT	AsynchRAT
Ave_Maria	Ave_Maria
AzoRult	
	BabylonRAT
BlackWorm	
BluStealer	BluStealer
	ClickFix
DanaBot	
DarkVisionRAT	DarkVisionRAT
	DCRAT
	DeerStealer
Downloader	Downloader
FormBook	FormBook
	Katz Stealer
	KoiStealer
LokiBot	LokiBot
	LummaStealer
LuminosityRAT	
	MassLogger
MintStealer	MintStealer
	MSIL Logger
NetSupportRAT	

2024	2025
	Neshta
	NetWire
Obj3ctivity	
	Phantom Stealer
PikaBot	
	Phorpiex
PureLogs	PureLogs
	QuasarRAT
RAT	RAT
RAT3102	
RedLine	RedLine
Remcos	Remcos
	Rhadamanthys
	ScreenConnect
	SmokeLoader
SnakeLogger	SnakeLogger
	Stealc
StormKitty	StormKitty
STRRAT	STRRAT
	VenomRAT
VidarStealer	VidarStealer
VIPKeylogger	VIPKeylogger
WikiLoader	
WSHRAT	
XWormRAT	XWormRAT

APT (Advanced Persistent Threat)

Anche nel 2025 il C.R.A.M (Centro Ricerca Anti-Malware) di TG Soft ha seguito il panorama mondiale degli **APT**.

Gli APT sono una tipologia di malware più sofisticata e con target mirati e specifici, spesso con attacchi sponsorizzati da stati. Con obiettivi che vanno dallo spionaggio al sabotaggio e alla guerra cibernetica.

Nel 2025 si è notata una persistente ed aumentata attività anche grazie all'instabile e fortemente degradato panorama geo-politico internazionale con vari conflitti che sono nati o si sono intensificati nel corso dell'anno e che vengono rispecchiati anche nel dominio cibernetico.

Spesso questa tipologia di attacchi utilizza tecniche specifiche e fa uso di vulnerabilità/exploit 0-day, persiste l'utilizzo di file MSC per la distribuzione di campagne malevole e anche l'uso di file LINK (.lnk).

Molto utilizzata anche la tecnica della *DLL Side Loading* che consiste nell'utilizzo di file eseguibili legittimi che caricano librerie malevole o modificate ad arte per eseguire funzioni o parti di codice malevolo.

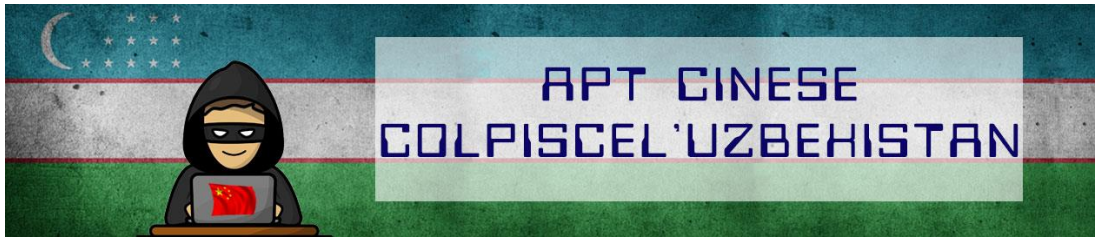
Il C.R.A.M (Centro Ricerca Anti-Malware) di TG Soft ha analizzato nel dettaglio l'attività di un gruppo **APT Cinese** che ha veicolato 3 campagne malware fortemente mirate con obiettivo gli enti governativi dell'**Uzbekistan**.

Le campagne sono state osservate l'11, il 12 e il 13 novembre 2025, tutte e 3 le email contenevano all'interno un file di **LINK** (.lnk) che esegue del codice PowerShell per estrarre una serie di file. Dopo l'estrazione viene aperto e mostrato il file di decoy e come ultimo passaggio viene eseguito un file eseguibile legittimo che con la tecnica della *DLL Side Loading* carica una libreria malevola.

La DLL malevola decifra quindi un file .DAT precedentemente estratto ed ottiene una **shellcode** a 64 bit che viene caricata ed eseguita in memoria. La **shellcode** è a sua volta cifrata con più layer, ogni layer estrae lo step successivo decifrandolo finché non ottiene il payload finale che è il beacon di **Cobalt Strike**.

I decoy utilizzati sono documenti riservati ed estremamente recenti rispetto alla data di distribuzione delle campagne facendo ipotizzare che il threat actor avesse già il controllo di alcuni sistemi da dove ha potuto esfiltrare i dati.

È possibile visionare l'intera analisi molto più dettagliata nell'articolo dedicato: [APT cinese mette nel mirino l'Uzbekistan]



Conclusioni

L’anno 2025, sebbene in calo rispetto all’anno 2024, è stato caratterizzato dalle famiglie degli **Info/Password Stealer** e dei **RAT** veicolate principalmente attraverso la posta elettronica ordinaria (**PEO**) e in alcuni casi mediante posta elettronica certificata (**PEC**).

Salendo dal secondo al primo posto, il malware più diffuso nel 2025 è stato il **FormBook**, dimostrando l’interesse sempre maggiore da parte della Cybercriminalità per dati (come le password) ed informazioni presenti nei dispositivi delle vittime, anche se l’**AgentTesla** che è stato per gli ultimi due anni nel primo gradino del podio, si classifica secondo quest’anno.

Il linguaggio più utilizzato nell’anno 2025 è stato lo **Scripting**, questo linguaggio è più di alto livello e permette quindi una implementazione di codice facilitata e che richiede minori conoscenze specifiche, a differenza di altri linguaggi che necessitano di capacità di programmazione più avanzate e conoscenze più sofisticate dei sistemi.

Per quanto riguarda i ransomware, il vettore maggiormente utilizzato negli attacchi ransomware anche nell’anno 2025 rimane l’accesso tramite **Remote Desktop (RDP)** esposto verso internet connesso all’uso improprio dell’utente Guest. Anche lo sfruttamento di vulnerabilità dei sistemi Firewall e/o VPN rimane uno dei principali vettori di accesso da parte dei cyber-criminali.

I temi predominanti sono stati **Ordini, Pagamenti** e **Fatture**, tutti e tre legati al fattore produttivo del paese mostrando in aclini casi tecniche di social engineering anche sofisticate.

Nel 2025 l’attività da parte degli **APT** (Advanced Persistent Threat) è aumentata soprattutto a causa del degradato panorama geo-politico internazionale che ha visto vari conflitti nascere ed altri che si sono evoluti o intensificati nel corso dell’anno, questi conflitti vengono rispecchiati anche nel dominio cibernetico come attacchi tra stati o ad entità strategiche.

TG Soft

Cyber Security Specialist

www.tgsoft.it