REPORT 2025

CAMPAGNE MALWARE

TG Soft
Cyber Security Specialist
www.tgsoft.it

REPORT 2025

CAMPAGNE MALWARE

Autori

Radu Breabin

Michele Zuin

Nicola Miotti

Samuele Callegaro

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 2024.

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.

Nell'anno 2024 la maggioranza dei malware utilizzati appartengono alla famiglia degli **Info/Password Stealer** e dei **RAT** con rare e sporadiche eccezioni.

Questa tendenza di crescita nell'utilizzo di queste tipologie di malware è dettata sia dalla facilità di accesso a tali strumenti da parte dei cybercriminali che acquistano questi servizi nel dark web come MaaS (Malware as-a-Service) a prezzi facilmente accessibili sia dall'effettiva pericolosità di questa tipologia di Malware che in determinate famiglie risultano essere particolarmente sofisticati.

L'utilizzo di tali Malware permette un accesso preliminare alle macchine/servizi colpiti portando poi ad un'evoluzione dell'attacco che si estende a tutta la rete/azienda che spesso culmina con la distribuzione di Ransomware CryptoMalware oppure con il dirottamento mediante attacchi MITM di Bonifici per il furto del 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 ginocchio l'intera azienda per giorni/settimane/mesi portando anche a gravi conseguenze economiche di mancata produzione e di costo di ripristino.

Numericamente il numero di campagne segue l'andamento delle attività produttive del paese, con un aumento delle campagne nella parte iniziale dell'anno per assestarsi e poi diminuire nella parte finale. L'andamento delle campagne rispecchia anche le festività principali con un calo nei periodi natalizi, pasquali e durante il periodo delle ferie estive.

I malware che hanno colpito storicamente l'Italia come ad esempio l'**Ursnif** non è stato veicolato nell'anno analizzato come anche l'**Emotet** che ha colpito l'utenza italiana dal 2020 attraverso campagne che utilizzano la tecnica del "reply-chain" per rendere i messaggi molto più credibili e quindi aumentare l'efficacia dell'attacco, ha effettuato solo qualche settimana di attività di MalSpam nel 2023 per passare ad un periodo di assenza definitiva.

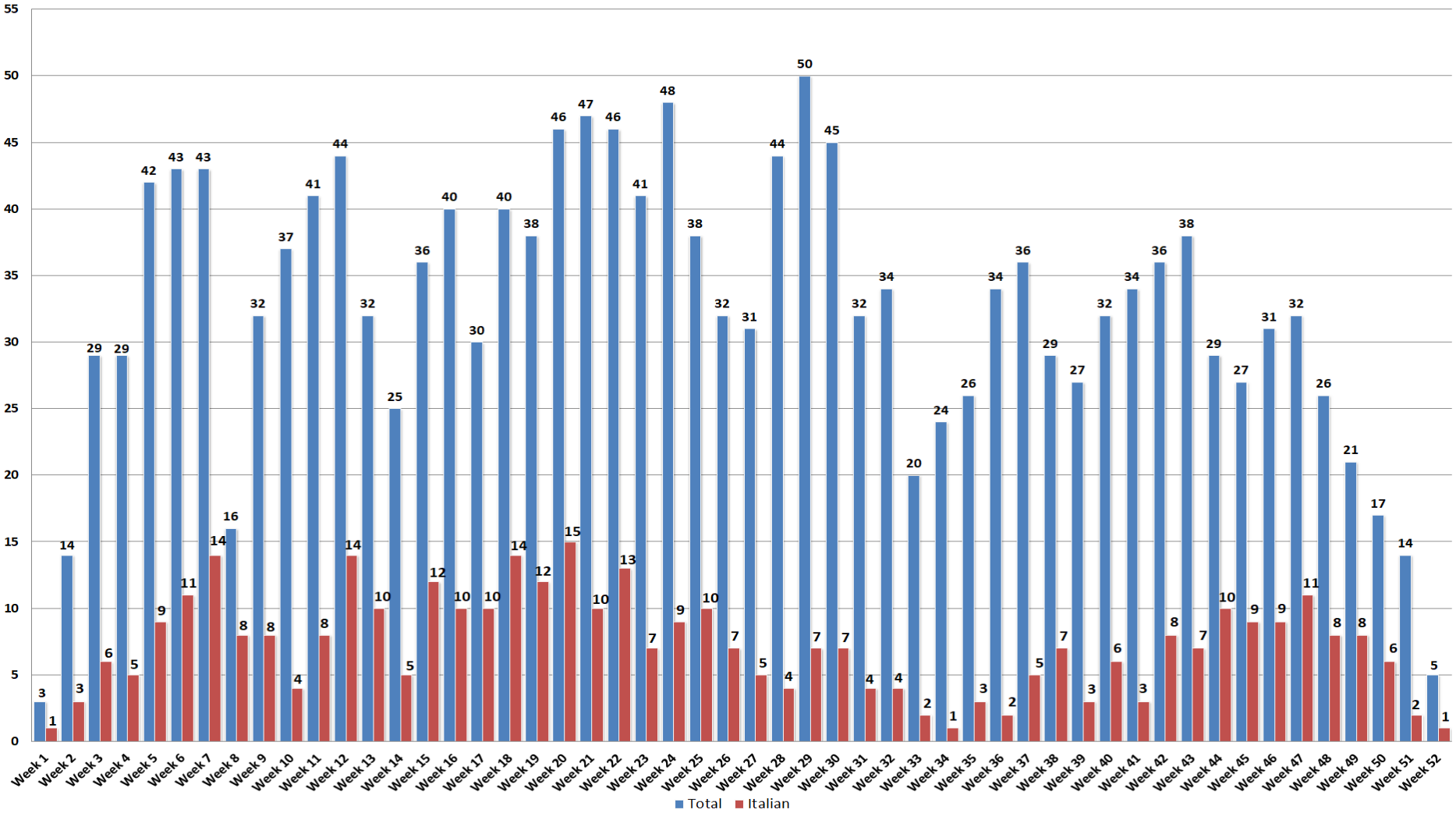
Una delle novità di quest'anno è stata l'intercettazione di due attacchi mirati a società ed entità governative italiane da parte di un cyber-attore cinese che sfruttano una variante del **Rat 9002** in modalità diskless. Altre varianti sono state nel tempo denominate come **Rat 3102**. Le due varianti sono notoriamente collegate all'**APT17**, un gruppo cyber-criminale cinese noto per: "l'Operazione Aurora (attribuito al governo cinese)", "l'Operazione Ephemeral Hydra" e per attacchi mirati a società ed entità governative.

In generale il malware che è stato utilizzato principalmente per colpire sia attraverso campagne globali che scritte in italiano è stato **AgentTesla**, un Info/Password Stealer facilmente reperibile che esfiltra dati e password dalle macchine colpite. Generalmente i dati raccolti vengono esfiltrati via email ma il malware prevede funzionalità di esfiltrazione anche via FTP e canali Telegram.

Vediamo in una piccola tabella di sintesi l'anno 2024 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	**1687**
NUMERO CAMPAGNE IN ITALIANO (scritte in lingua italiana) ANALIZZATE	**377 – 22,34%** rispetto alle campagne globali
PICCO MASSIMO DI CAMPAGNE GLOBALI SETTIMANALE	**50 – Week 29**
PICCO MASSIMO DI CAMPAGNE IN ITALIANO SETTIMANALE	**15 – Week 20**
LINGUAGGIO PIU' UTILIZZATO	**MSIL (C# .NET) – 36,22%** del totale
FAMIGLIA MALWARE PIU' UTILIZZATA GLOBALMENTE	**AgentTesla**
FAMIGLIA MALWARE PIU' UTILIZZATA NELLE CAMPAGNE IN ITALIANO	**AgentTesla**
NUMERO TOTALE DI TEMI	**24**
TEMA PIU' UTILIZZATO NELLE CAMPAGNE IN ITALIANO	**Ordini**

Grafico andamento delle campagne settimanali nel 2024



Dal grafico si può notare l'andamento delle campagne suddivise nelle varie settimane (Week) dell'anno 2024.

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	07/01
Week_02	08/01	14/01
Week_03	15/01	21/01
Week_04	22/01	28/01

In totale nell'anno 2024 sono state monitorate **1687** campagne globali mentre le campagne scritte in italiano sono state **377**.

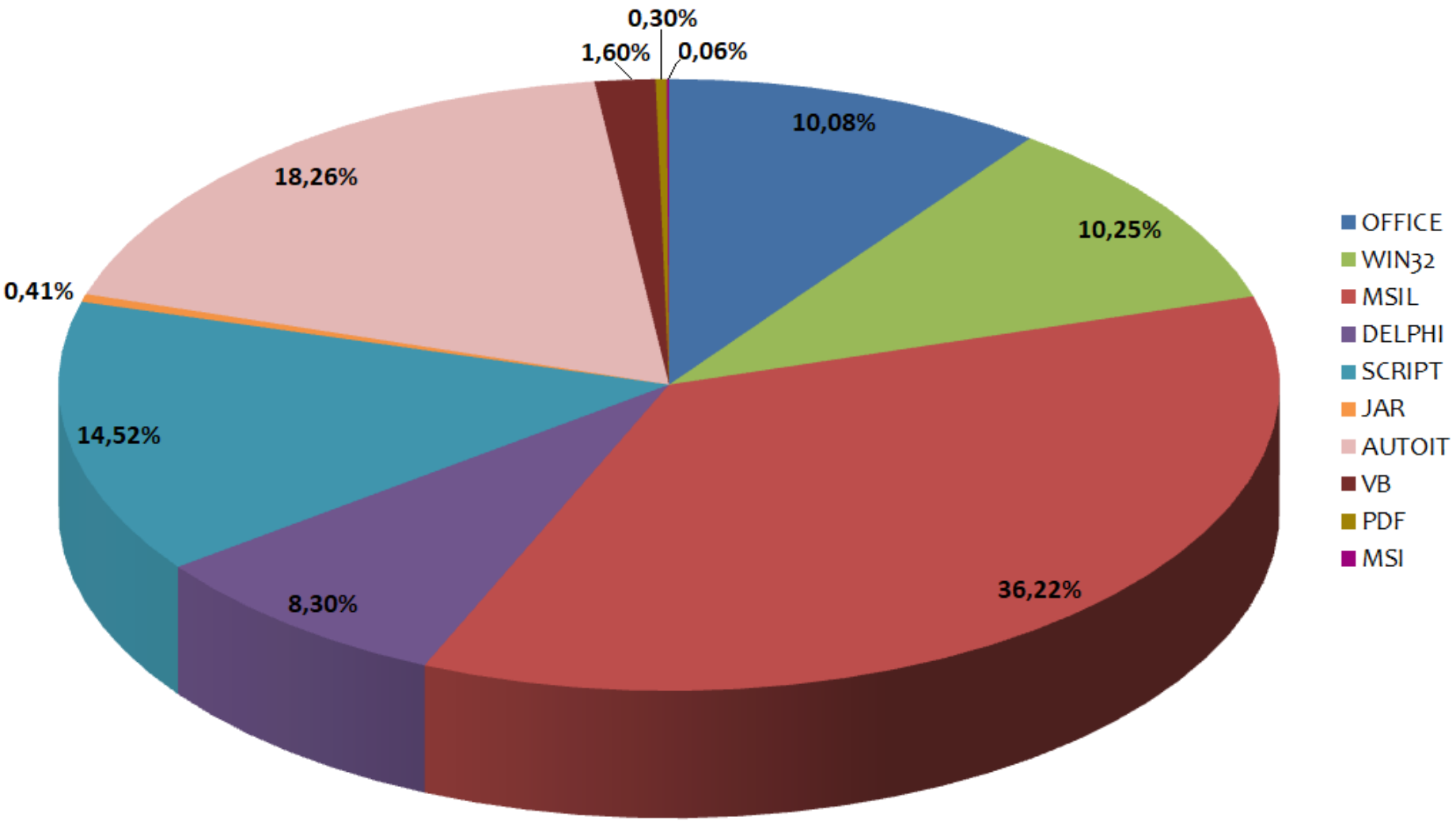
Il trend generale mostra una quantità maggiore di campagne nella parte iniziale dell'anno con una riduzione nella parte finale.

Dal grafico si può notare che anche le campagne di MalSpam seguono l'andamento delle regolari attività dell'utenza media con un calo nei periodi festivi ed un forte aumento nei periodi di maggiore produttività dove gli utenti sono più facilmente target delle campagne malevole.

La settimana con il maggior numero di campagne globali è stata la Week 29 che ha registrato **50** campagne, mente la settimana che ha registrato il maggior numero di campagne scritte in italiano è stata la Week 20 con **15** campagne.

La media generale calcolata sull'intero anno sulle campagne globali è di circa **32** campagne settimanali mentre quella delle campagne scritte in italiano è di circa **7** campagne.

Grafico sulle tipologie di linguaggio utilizzate nel 2024



Dal grafico analizziamo le tipologie di linguaggio utilizzate per sviluppare i malware veicolati nell'anno 2024.

Come si può vedere il linguaggio **MSIL** (C# .NET) è il linguaggio maggiormente utilizzato per creare i malware veicolati durante l'anno con ben il 36,22%.

Al secondo posto troviamo i file eseguibili **AutoIT** che rappresentano il 18,26%.

Sul terzo posto si posizionano i linguaggi di scripting con il 14,52%, questa famiglia comprende gli script come JavaScript, VBScript, PowerShell, i link, WSF, BAT, etc.

Al quarto posto troviamo i file Win32 che raggruppano tutti i sample eseguibili con vari linguaggi compilati come il C, C++, ecc. che rappresentano il 10,25%.

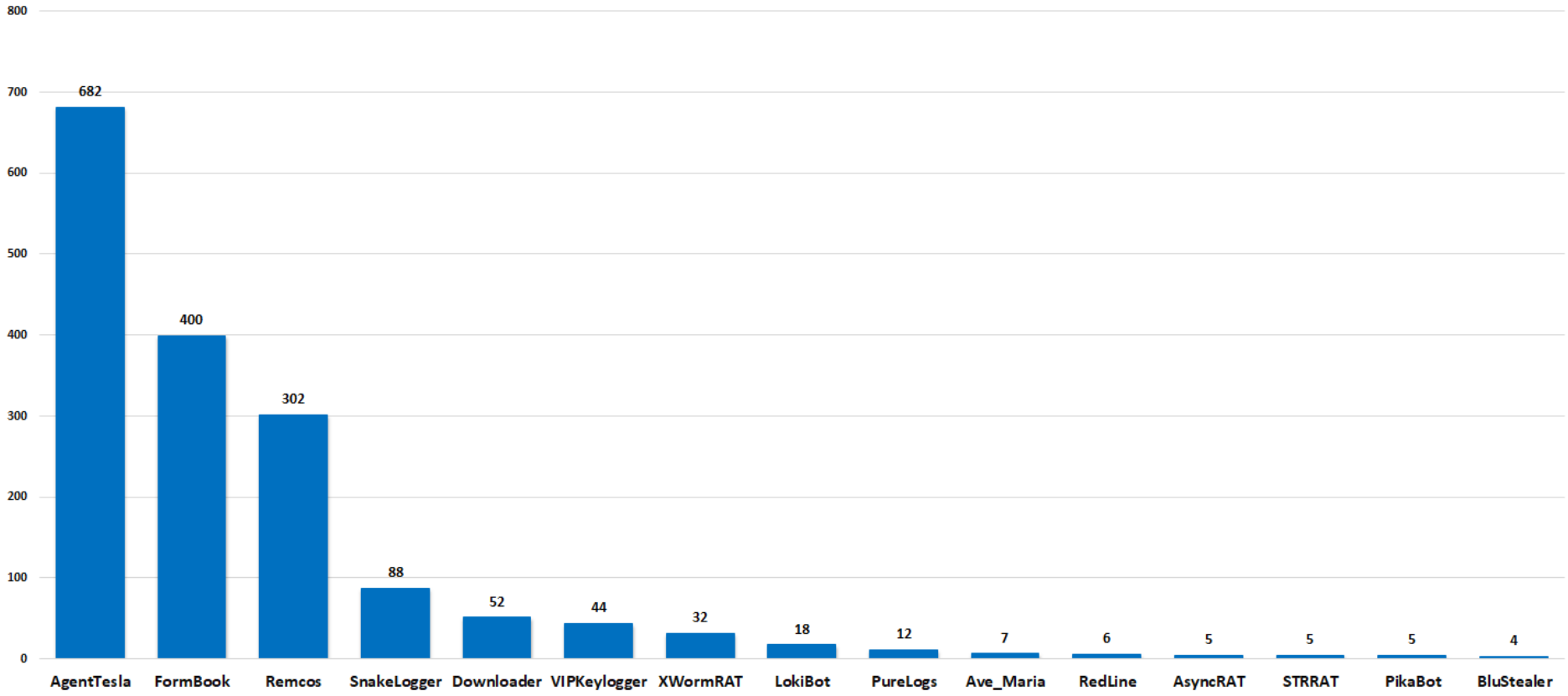
Il 10,08% dei malware veicolati sono rappresentati da documenti di Microsoft Office (Word, Excel, PowerPoint, etc.), i documenti di Office generalmente utilizzano macro malevole per infettare il PC della vittima.

Il linguaggio di programmazione Delphi è utilizzato nel 8,30% dei sample mentre il resto dei sample è rappresentato in minoranza da PDF, JAR (Java), MSI (pacchetti di installazione) e VB (Visual Basic).

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

LINGUAGGIO	NUMERO CAMPAGNE
MSIL	611
AUTOIT	308
SCRIPT	245
WIN32	173
OFFICE	170
DELPHI	140
VB	27
JAR	7
PDF	5
MSI	1

Famiglie malware globali analizzate nel 2024



Nel grafico vediamo le prime 15 famiglie malware veicolate globalmente nell'anno 2024, in totale sono state analizzate 31 famiglie di malware.

Come si può notare il malware più utilizzato è stato **AgentTesla** con il **FormBook** al secondo posto e **Remcos** al terzo.

Abbiamo rilevato un notevole aumento di una nuova famiglia malware chiamata **VIPKeylogger** il quale condivide molte caratteristiche e concetti con la famiglia malware chiamata SnakeLogger. Si tratta sempre di un **Info/Password Stealer** il quale è stato rilevato per la prima volta nel secondo semestre dell'anno 2024.

Più in generale la maggior parte dei malware utilizzati 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.

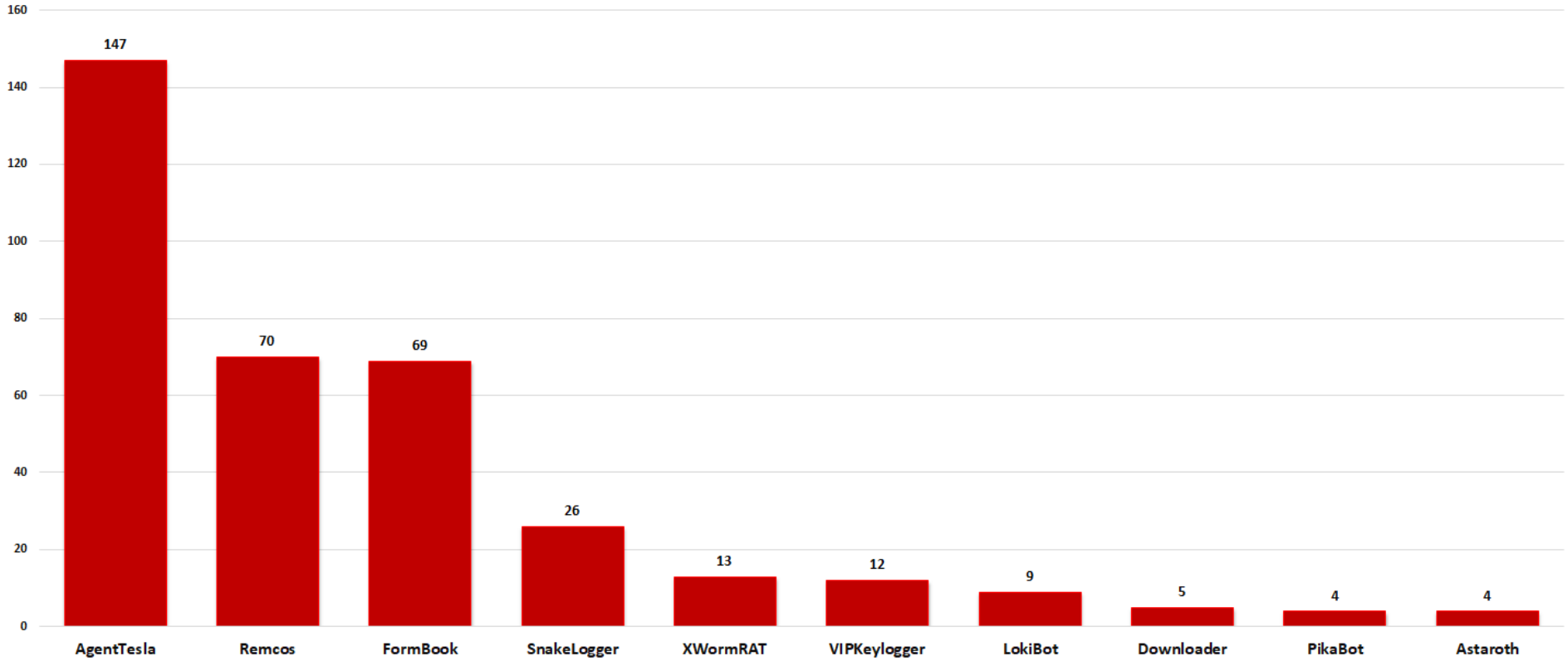
Gli **Info/Password Stealer** sono infatti una minaccia grave, in quanto sono spesso il punto iniziale di attacchi molto più sofisticati che prevedono l'utilizzo di Ransomware/CryptoMalware per la cifratura dei dati degli utenti con successiva richiesta di riscatto. Questi attacchi se non mitigati con tecnologie specifiche come quelle presenti nella suite Vir.IT eXplorer PRO possono mettere in ginocchio per settimane/mesi 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
AgentTesla	682	AzoRult	3
FormBook	400	DanaBot	3
Remcos	302	MintStealer	2
SnakeLogger	88	StormKitty	2
Downloader	52	Adwind	1
VIPKeylogger	44	VidarStealer	1
XWormRAT	32	DarkVisionRAT	1
LokiBot	18	NetSupportRAT	1
PureLogs	12	WikiLoader	1
Ave_Maria	7	WSHRAT	1
RedLine	6	RAT3102	1
AsyncRAT	5	Obj3ctivity	1
STRRAT	5	BlackWorm	1
PikaBot	5	LuminosityRAT	1
BluStealer	4	RAT	1
Astaroth	4		

Famiglie malware in italiano analizzate nel 2024



Nel grafico vediamo le prime 10 famiglie malware scritte in italiano che sono state analizzate nell'anno 2024, in totale sono state rilevate 20 famiglie di malware.

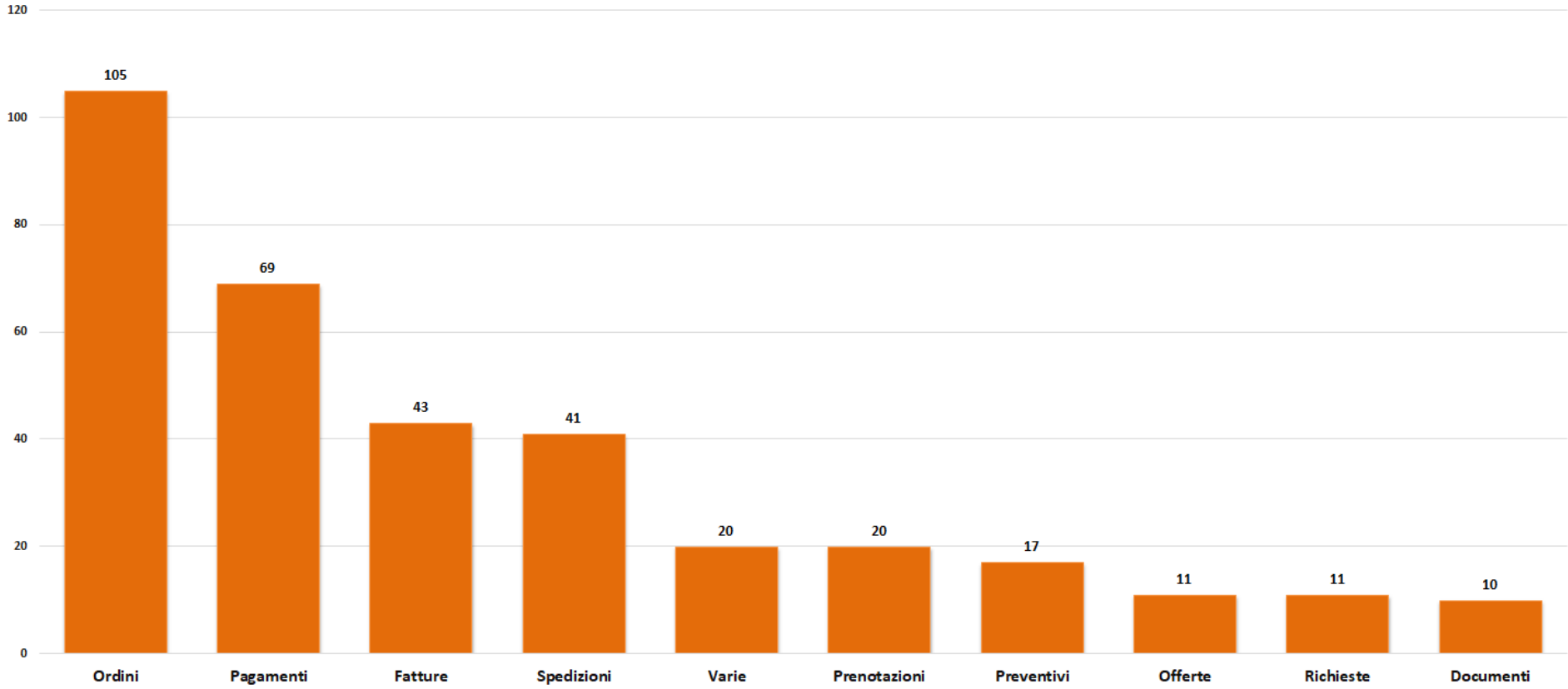
Rispecchiano le famiglie globali anche in quelle scritte in italiano il malware più utilizzato è **AgentTesla** con il **Remcos** al secondo posto e **FormBook** al terzo.

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	147	PureLogs	3
Remcos	70	DanaBot	3
FormBook	69	STRRAT	2
SnakeLogger	26	MintStealer	2
XWormRAT	13	BluStealer	2
VIPKeylogger	12	VidarStealer	1
LokiBot	9	RAT3012	1
Downloader	5	DarkVisionRAT	1
PikaBot	5	AsyncRAT	1
Astaroth	4	Adwind	1

Temi utilizzati nelle campagne malware in italiano analizzate nel 2024



Nel grafico analizziamo i primi 10 temi utilizzati nelle email di MalSpam con target italiano (scritte in lingua italiana), in totale sono stati rilevati 24 temi.

Al primo posto troviamo il tema "**Ordini**" con 105 campagne, subito al secondo posto con 69 campagne vi è il tema "**Pagamenti**", al terzo posto più distaccato vi è il tema "**Fatture**".

Il tema "**Varie**" indica email di risposta a reali conversazioni precedentemente rubate e sfruttate dai CyberCriminali per aumentare la credibilità del messaggio inviato e per ingannare più facilmente la vittima.

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

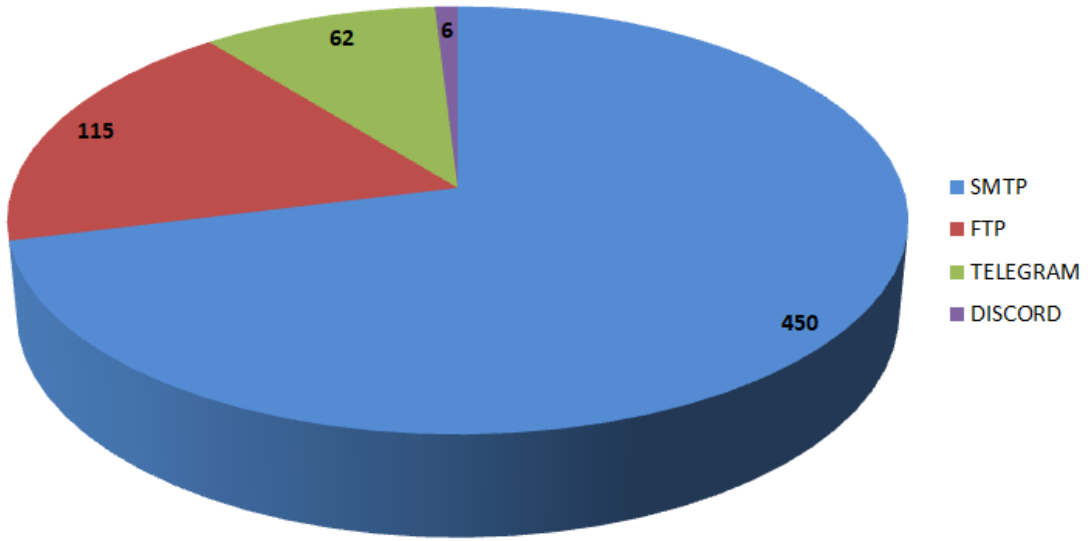
Di seguito la tabella con tutti i temi riscontrati e la relativa quantità:

TEMA	NUMERO CAMPAGNE	TEMA	NUMERO CAMPAGNE
ORDINI	105	CONTRATTI	4
PAGAMENTI	69	ACQUISTI	4
FATTURE	43	PROMOZIONI	2
SPEDIZIONI	41	COMUNICAZIONI	2
VARIE-REPLY-CHAIN	20	OPERAZIONI	2
PRENOTAZIONI	20	PROGETTI	1
PREVENTIVI	17	PREZZI	1
OFFERTE	11	POLIZZE	1
RICHIESTE	11	AVVISI	1
DOCUMENTI	10	TRANSAZIONI	1
GIACENZE	5	RIMBORSI	1
AGENZIA DELLE ENTRATE	4	MINISTERO DELLA GIUSTIZIA	1

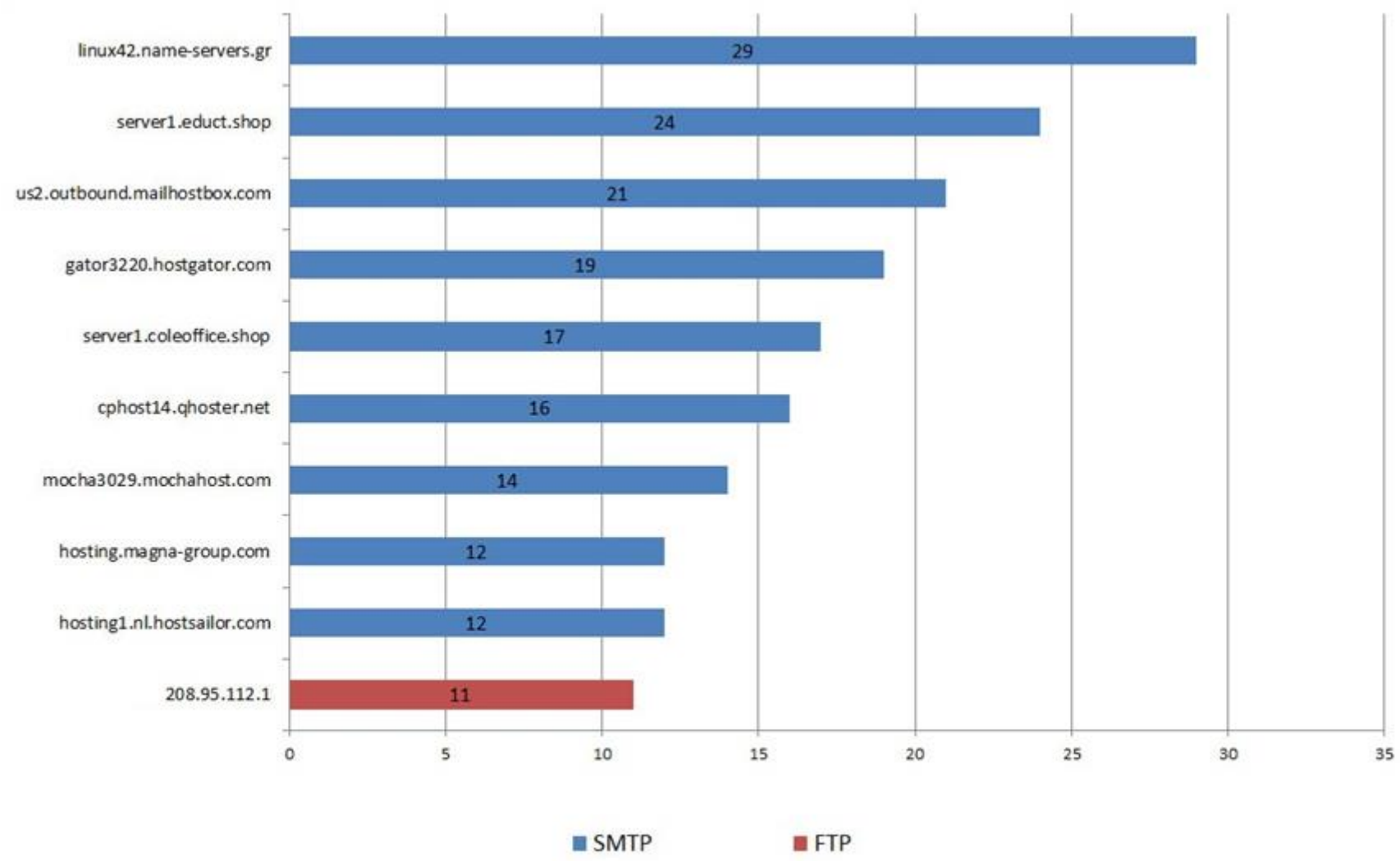
AgentTesla

Abbiamo realizzato un'analisi più approfondita dell'**AgentTesla**, il malware che appartiene alla famiglia dei Info/Password Stealer per capire meglio i suoi principali metodi di esfiltrazione dati e degli host che sono stati usati più frequentemente. I metodi principali di esfiltrazione dati che abbiamo rilevato nell'anno 2024 sono stati i seguenti 4:

- **SMTP** (Simple Mail Transfer Protocol) - il quale rappresenta l'esfiltrazione tramite i server di posta elettronica ed è stato il più diffuso nell'anno 2024 con un numero totale di **450** sample.
- **FTP** (File Transfer Protocol) - è il protocollo più famoso che viene utilizzato per trasferire i file da un server a un client il quale è stato rilevato per un numero totale di **115** sample.
- **Telegram** - una delle più note piattaforme di messagistica internazionale utilizzata dal 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 **62** campagne.
- **Discord** - si tratta sempre di una delle più note piattaforme internazionali di messagistica 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. In questo caso Discord è stato rilevato per un numero totale di **6** campagne.

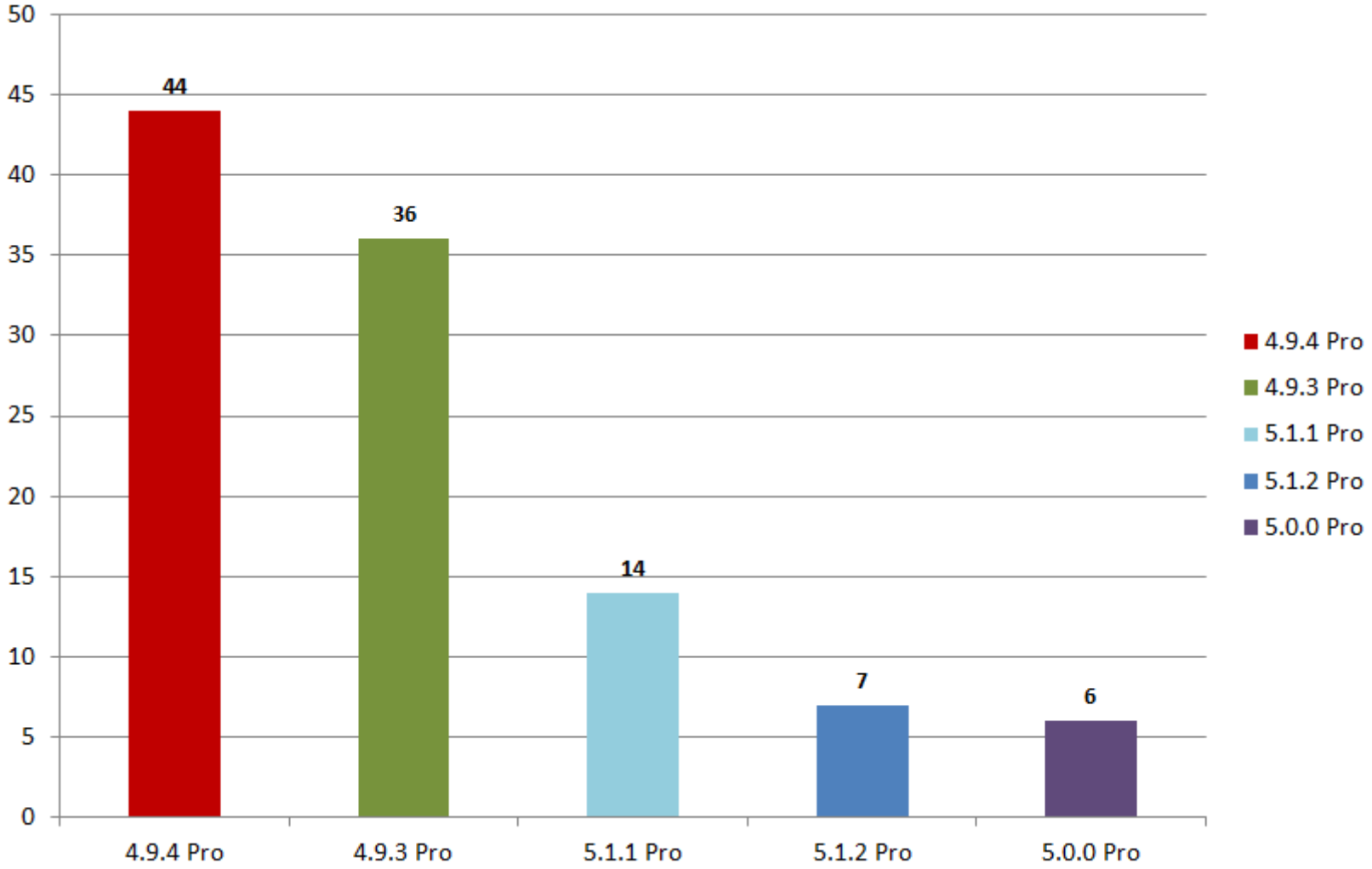


Di seguito vediamo il **TOP10** dei server **SMTP/FTP** utilizzati dal malware di AgentTesla:



Remcos

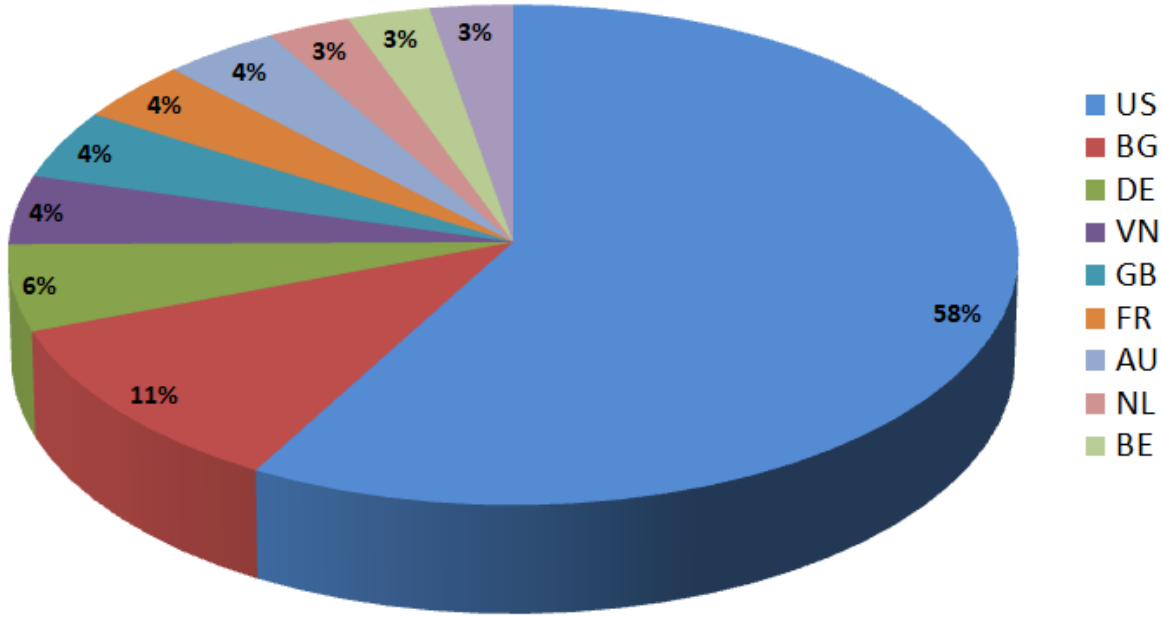
Un'altra analisi approfondita è stata realizzata nei confronti del malware **Remcos** il quale appartiene alla macro-famiglia dei RAT (Remote Access Trojan), come abbiamo già evidenziato sopra, questo malware si è posizionato al terzo posto tra i malware veicolati globalmente nell'anno 2024. La build più diffusa è stata la versione 4.9.4 Pro (per "Pro" si intende la versione professional acquistata con tutte le funzionalità disponibili) con 44 campagne rilevate.



Durante la nostra analisi abbiamo anche rilevato che la licenza del Remcos più utilizzata è stata: “**38CBE3E7CD1A6C11156346CAE4B39D90**” con **13** utilizzi su 207 campagne analizzate.

È stato anche notato che i mutex maggiormente diffusi nel 2024 sono stati "**Rmc-2OLA39**" e "**Rmc-999Z97**" con 6 apparizioni ciascuno, il “MUTEX” è la stringa che viene assegnata dal Threat Actor una volta terminata la configurazione della build, molto spesso esso viene anche utilizzato per risalire al numero di campagne diffuse da un certo attore.

TOP 10 MUTEX	
MUTEX	**NUMERO DI CAMPAGNE**
Rmc-2OLA39	6
Rmc-999Z97	6
Rmc-A49MY7	4
Rmc-7XHN5V	4
Rmc-WTDTSU	4
Rmc-BCCHC0	3
lakosegtst-I6VUY0	3
Rmc-TLPQMO	3
wewewowoswsa-2HIPIN	3
Rmc-ROE36P	3

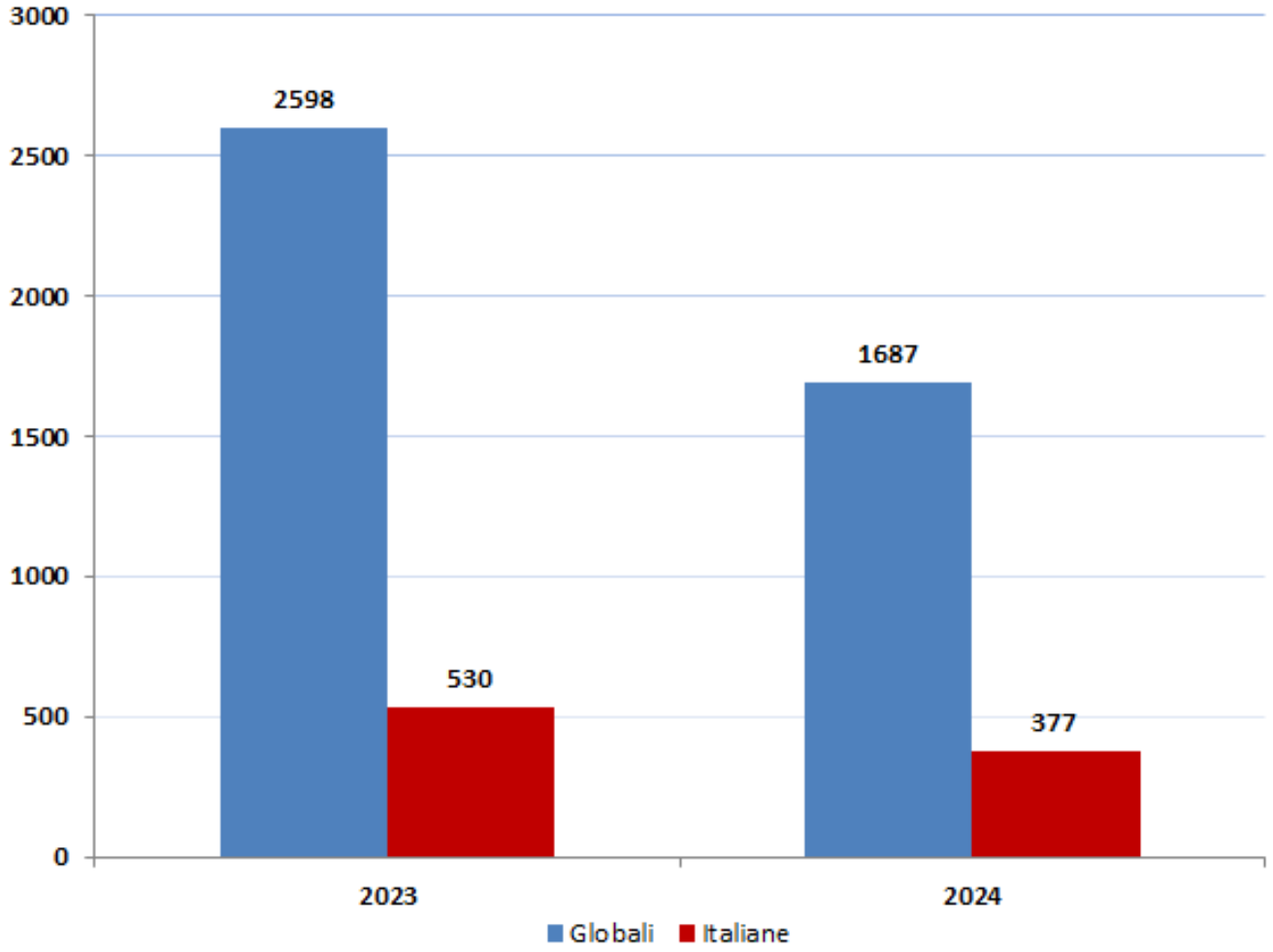


TOP10 C2

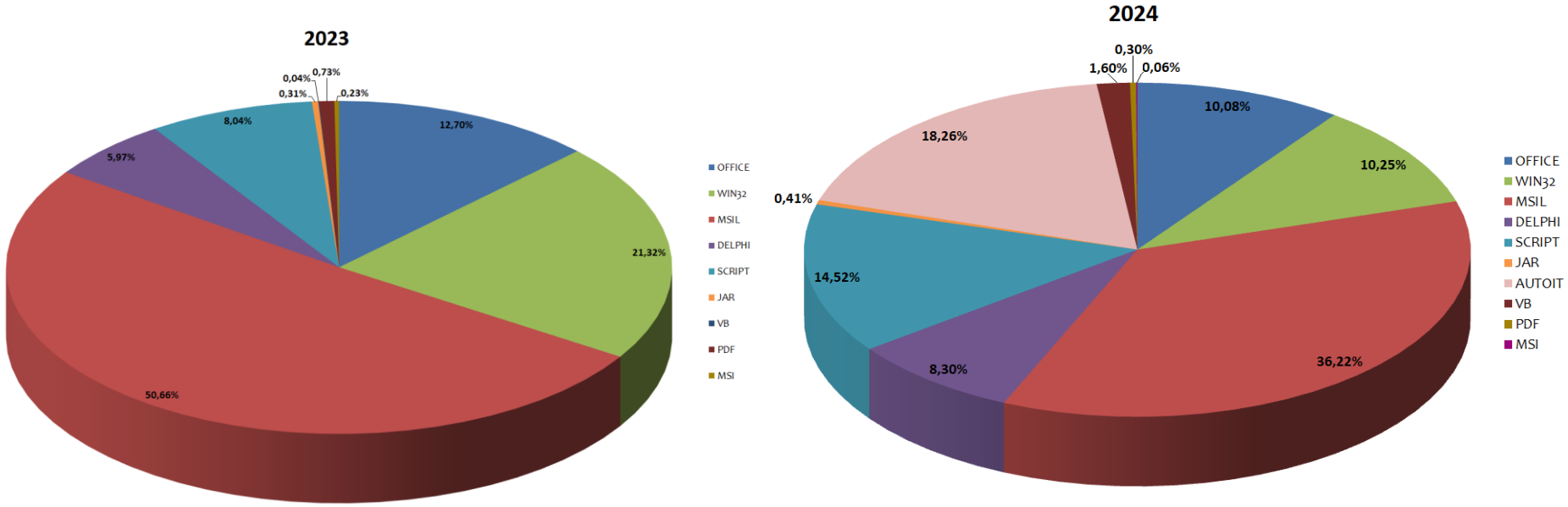
Dall'analisi del malware e delle sue attività per quanto riguarda il traffico, sono stati individuati i 10 paesi più utilizzati per ospitare i server di Comando e Controllo (C2). Come possiamo notare dal grafico a torta, la percentuale più alta è quella degli Stati Uniti d'America, esso è il paese dove abbiamo il maggior numero di server C2 con 46 indirizzi IP diversi su 105 in totale. Al secondo posto troviamo la Bulgaria con 15 indirizzi diversi su un totale di 20. Per quanto riguarda invece il terzo posto, si tratta della Germania (sigla DE) con 6 indirizzi IP diversi su un totale di 10.

Confronto delle campagne malware analizzate nel 2023/2024

Facendo una comparazione con l'anno 2023, possiamo notare che il 2024 ha avuto una flessione di ben 911 campagne globali e di 153 campagne italiane (scritte in lingua italiana) in meno rispetto all'anno 2023.



Per quanto riguarda le tipologie di linguaggio utilizzate, nel 2024 abbiamo rilevato una forte diminuzione del linguaggio MSIL (C# .NET) del 14.44% all'incirca rispetto all'anno 2023, e un notevole aumento del 18,26% del linguaggio di programmazione AutoIT, che però nel 2023 era inglobato nella famiglia Win32.



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 **AgentTesla, FormBook** e quelli delle macro famiglie dei RAT che è **Remcos**.

Un'altra somiglianza importante riguarda i temi utilizzati nelle email di MalSpam con target italiano (scritte in lingua italiana), e la comune predominanza dei seguenti temi: **Ordini, Pagamenti** e **Fatture**. Questo fatto si spiega per il semplice motivo che la maggior parte delle email che vengono inviate dai clienti e fornitori riguardano l'ambito lavorativo e quello relazionale, dove nella maggior parte dei casi si tratta proprio degli ordini e dalle attività che vengono effettuate su di essi, principalmente pagamenti e fatture.

Nella tabella sottostante possiamo vedere la comparazione delle famiglie, come si può notare alcune famiglie malware sono state presenti sia nel 2023 sia nel 2024 (colore azzurro), alcune non sono state presenti nel 2024 (colore rosso) mentre altre sono delle famiglie che non sono state presenti nel 2023 (colore verde).

Malware storici come **Ursnif**, **Emotet** e **sLoad** non sono stati rilevati nel 2024 sostituiti da nuove famiglie come ad esempio il **MintStealer.**

2023	2024
Adwind	Adwind
AgentTesla	AgentTesla
	Astaroth
AsyncRAT	AsyncRAT
Ave_Maria	Ave_Maria
AzoRult	AzoRult
	BlackWorm
BluStealer	BluStealer
Chaos	
CoinMiner	
	DanaBot
DarkVisionRAT	DarkVisionRAT
DCRAT	
Downloader	Downloader
Emotet	
FormBook	FormBook
Generic	
GomorrahStealer	
HawkEye	
LaplasClipper	
LokiBot	LokiBot
	LuminosityRAT
Mekotio	
	MintStealer
NanoCore	
NetSupportRAT	NetSupportRAT

2023	2024
NetWire	
njRAT	
	Obj3ctivity
PandoraRAT	
PikaBot	PikaBot
PovertyStealer	
PureLogs	PureLogs
QakBot	
QuasarRAT	
RAT	RAT
	RAT3102
	RedLine
Remcos	Remcos
Rhadamanthys	
sLoad	
SnakeLogger	SnakeLogger
	StormKitty
StrelaStealer	
STRRAT	STRRAT
Ursnif	
VidarStealer	VidarStealer
	VIPKeylogger
Vjw0rm	
	WikiLoader
WSHRAT	WSHRAT
XWormRAT	XWormRAT

Conclusioni

L’anno 2024, sebbene in calo rispetto all’anno 2023, 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**).

Seguendo il trend degli ultimi anni, anche nel 2024 il malware più diffuso è stato **AgentTesla**, dimostrando l’interesse da parte della Cybercriminalità per dati ed informazioni presenti nei dispositivi delle vittime.

Il linguaggio di compilazione di malware più utilizzato nell’anno 2024 è stato il **C# (MSIL/.Net)**, questo linguaggio è più di alto livello e permette quindi una più facile implementazione di codice con minori conoscenze specifiche, a differenza di altri linguaggi che richiedono capacità di programmazione più avanzate.

Per quanto riguarda i ransomware, il vettore maggiormente utilizzato negli attacchi ransomware anche nell’anno 2024 è l’accesso tramite **Remote Desktop (RDP)** esposto verso internet mostrando come l’RDP sia ancora un punto debole di molte reti aziendali e che se mal configurato/esposto può portare a conseguenze molto gravi.

I temi predominanti sono stati **Ordini, Pagamenti** e **Fatture**, tutti e tre legati al fattore produttivo del paese.

Per quanto riguarda gli **APT**, il 24 giugno e il 2 luglio 2024 sono stati osservati due attacchi mirati a società ed entità governative italiane da parte di un cyber-attore cinese che sfruttano una variante del **Rat 9002** in modalità diskless. Queste attività sono associate al gruppo APT17 noto anche con il nome "DeputyDog".

La prima campagna del 24 giugno 2024 ha sfruttato un documento di Office, mente la seconda campagna conteneva un link.
Entrambe le campagne invitavano la vittima ad installare un pacchetto di Skype for Business da un link di un dominio simil governativo italiano per veicolare una variante del **Rat 9002**.

Maggiori informazioni possono essere trovate all’articolo dedicato: Enti governativi ed aziende italiane nel mirino di un APT cinese

TG Soft
Cyber Security Specialist
www.tgsoft.it