REPORT 2024

CAMPAGNE MALWARE

TG Soft
Cyber Security Specialist
www.tgsoft.it

REPORT 2024

CAMPAGNE MALWARE

Autori

Michele Zuin

Radu Breabin

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 2023.

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 2023 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.

Malware che colpiscono storicamente l'Italia come ad esempio l'**Ursnif** è stato veicolato anche nell'anno analizzato principalmente con tema governativo dell'Agenzia delle Entrate.

Il malware **Emotet** che ha colpito duramente 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 prolungata.

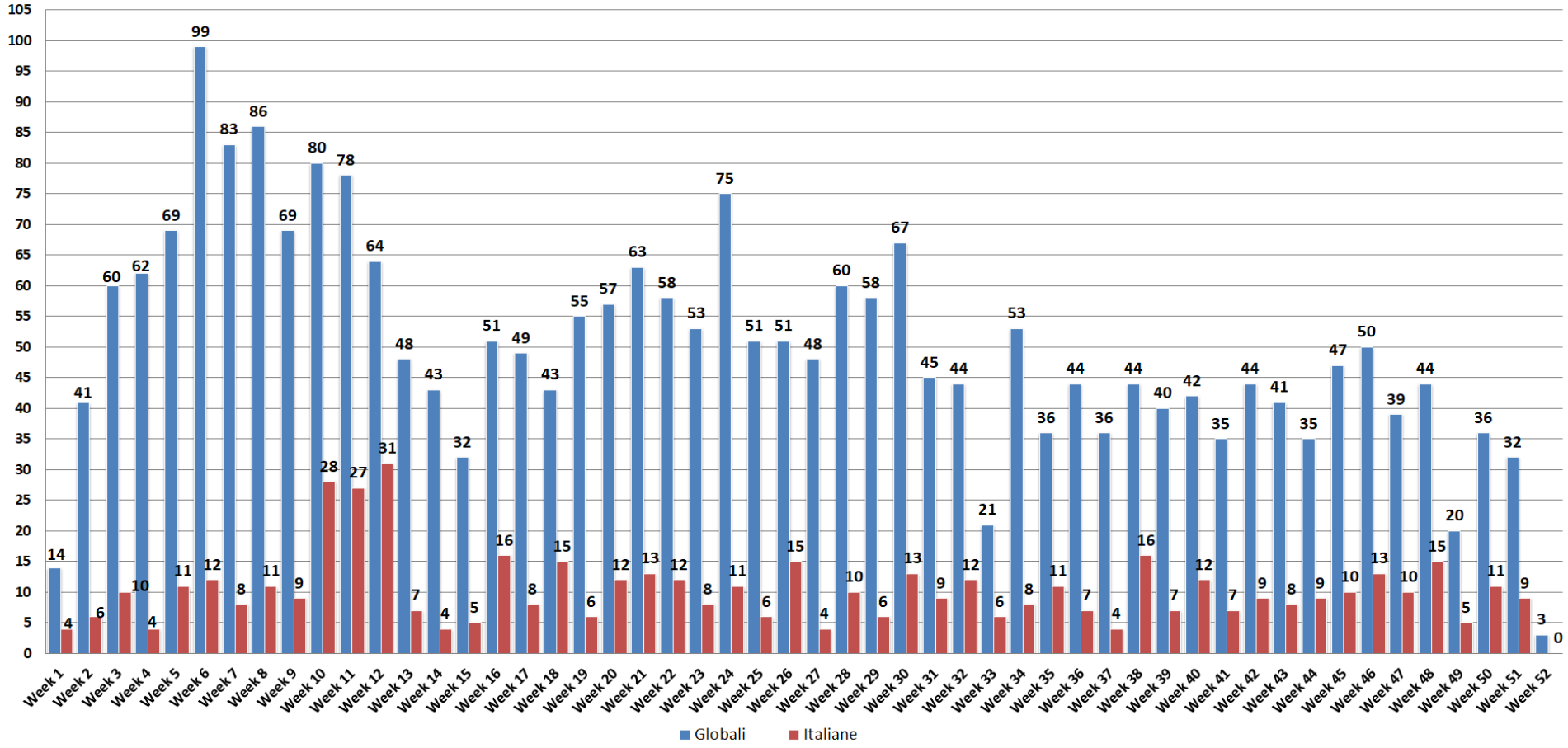
Presenti nell'anno anche i malware **PikaBot** e **QakBot** molto spesso utilizzati come vettore iniziale d'attacco per effettuare poi attività di spostamento laterale ed infettare il maggior numero di macchine possibili presenti in rete.

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 2023 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	**2598**
NUMERO CAMPAGNE IN ITALIANO (scritte in lingua italiana) ANALIZZATE	**530**
PICCO MASSIMO DI CAMPAGNE GLOBALI SETTIMANALE	**99 – Week 6**
PICCO MASSIMO DI CAMPAGNE IN ITALIANO SETTIMANALE	**31 – Week 12**
LINGUAGGIO PIU' UTILIZZATO	**MSIL (C# .NET) – 50,66%** del totale
NUMERO FAMIGLIE GLOBALI	**41**
NUMERO FAMIGLIE CAMPAGNE IN ITALIANO	**24**
FAMIGLIA MALWARE PIU' UTILIZZATA GLOBALMENTE	**AgentTesla**
FAMIGLIA MALWARE PIU' UTILIZZATA NELLE CAMPAGNE IN ITALIANO	**AgentTesla**
NUMERO TOTALE DI TEMI	**28**
TEMA PIU' UTILIZZATO NELLE CAMPAGNE IN ITALIANO	**Ordini**

Grafico andamento delle campagne settimanali nel 2023



Dal grafico si può notare l'andamento delle campagne suddivise nelle varie settimane (Week) dell'anno 2023.

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	02/01	08/01
Week_02	09/01	15/01
Week_03	16/01	22/01
Week_04	23/01	29/01

Il 01/01/2023 è censito nella Week52 dell'anno 2022 ma non ha registrato alcuna campagna.

In totale nell'anno 2023 sono state monitorate **2598** campagne globali mentre le campagne scritte in italiano sono state **530**.

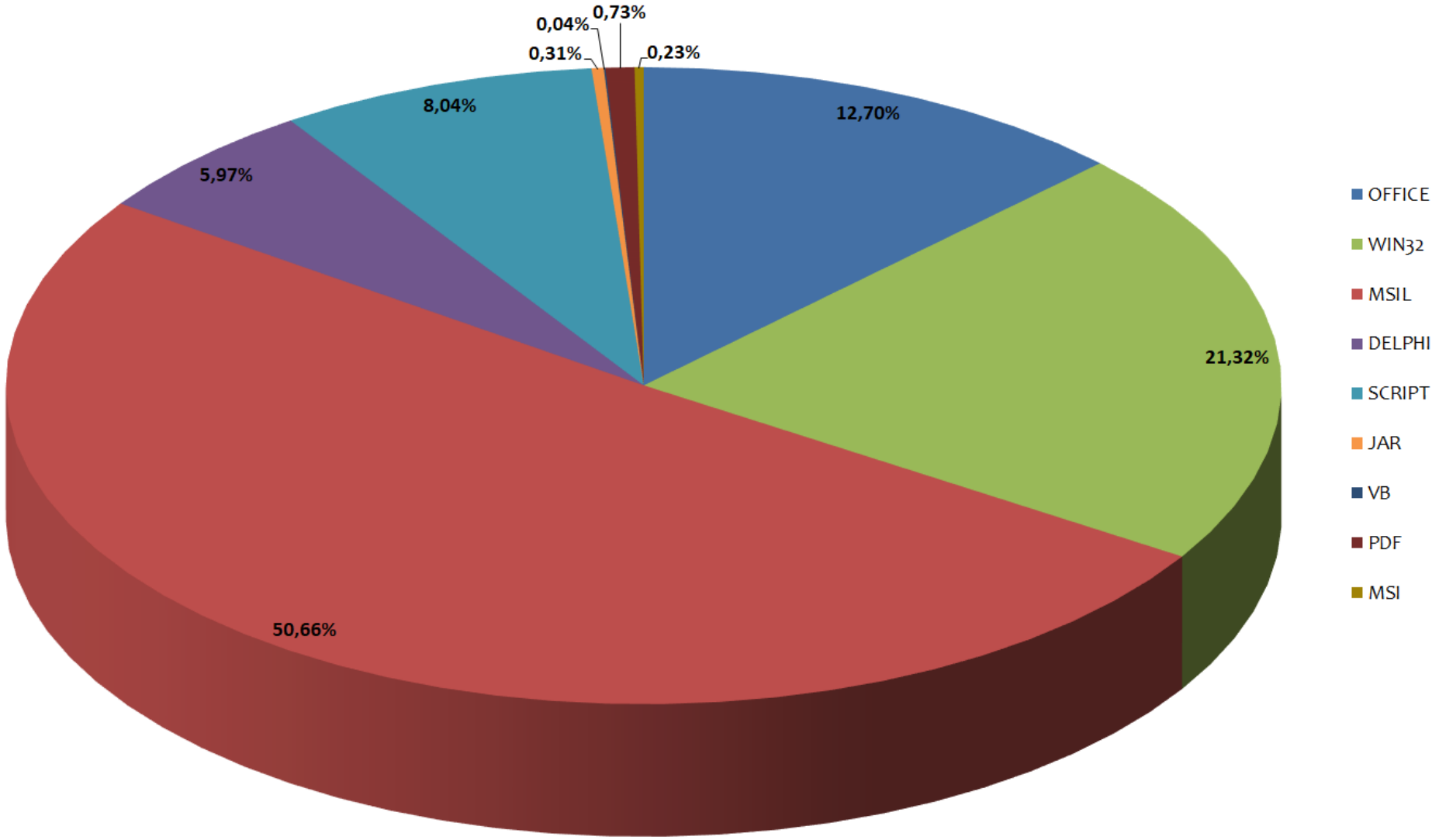
Il trend generale mostra una quantità maggiore di campagne nella parte iniziale dell'anno con un assestamento nella parte centrale ed una tendenza alla riduzione nella parte finale dell'anno.

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 6 che ha registrato **99** campagne, mente la settimana che ha registrato il maggior numero di campagne scritte in italiano è stata la Week 12 con **31** campagne.

La media generale calcolata sull'intero anno sulle campagne globali è di circa **50** campagne settimanali mentre quella delle campagne scritte in italiano è di circa **10** campagne.

Grafico sulle tipologie di linguaggio utilizzate nel 2023



Dal grafico analizziamo le tipologie di linguaggio utilizzate per sviluppare i malware veicolati nell'anno 2023.

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 50,66%.

Al secondo posto troviamo i file **Win32** che raggruppano tutti i sample eseguibili con vari linguaggi compilati come il C, C++, ecc. che rappresentano il 21,32%.

Il 12,70% 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.

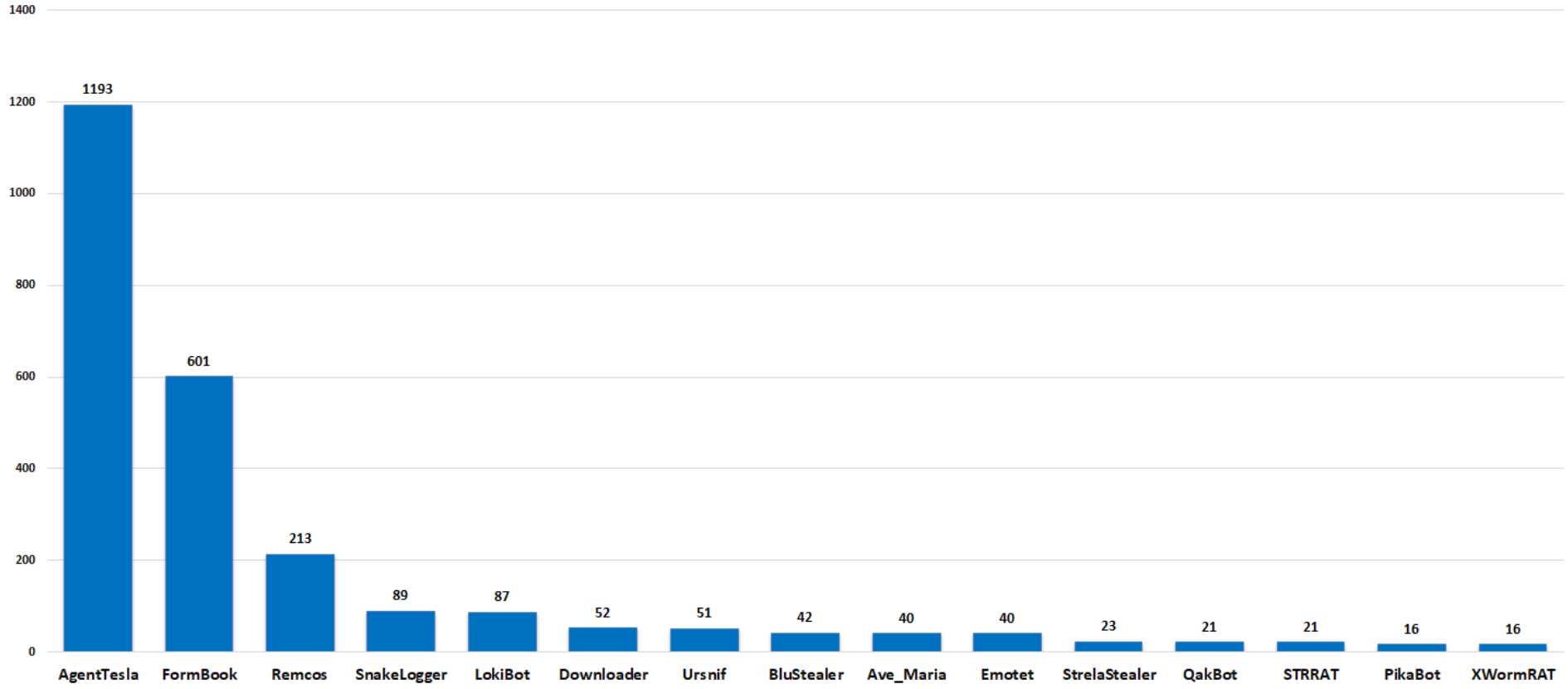
I linguaggi di scripting utilizzati sono l'8,04%, questa famiglia comprende gli script come JavaScript, VBScript, PowerShell, link, WSF, BAT, etc.

Il linguaggio di programmazione Delphi è utilizzato nel 5,97% 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	1316
WIN32	554
OFFICE	330
SCRIPT	209
DELPHI	155
PDF	19
JAR	8
MSI	6
VB	1

Famiglie malware globali analizzate nel 2023



Nel grafico vediamo le prime 15 famiglie malware veicolate globalmente nell'anno 2023, in totale sono state analizzate 41 famiglie di malware.

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

Il malware **Ursnif** ha visto una distribuzione abbastanza costante nei primi due quadrimestri dell'anno con un calo/assenza durante l'ultimo quadrimestre dell'anno.

Emotet non ha registrato una forte distribuzione con una presenza ridotta a poche settimane nei primi mesi dell'anno.

QakBot e **PikaBot** sono stati altalenanti con settimane di distribuzione e settimane di assenza.

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.

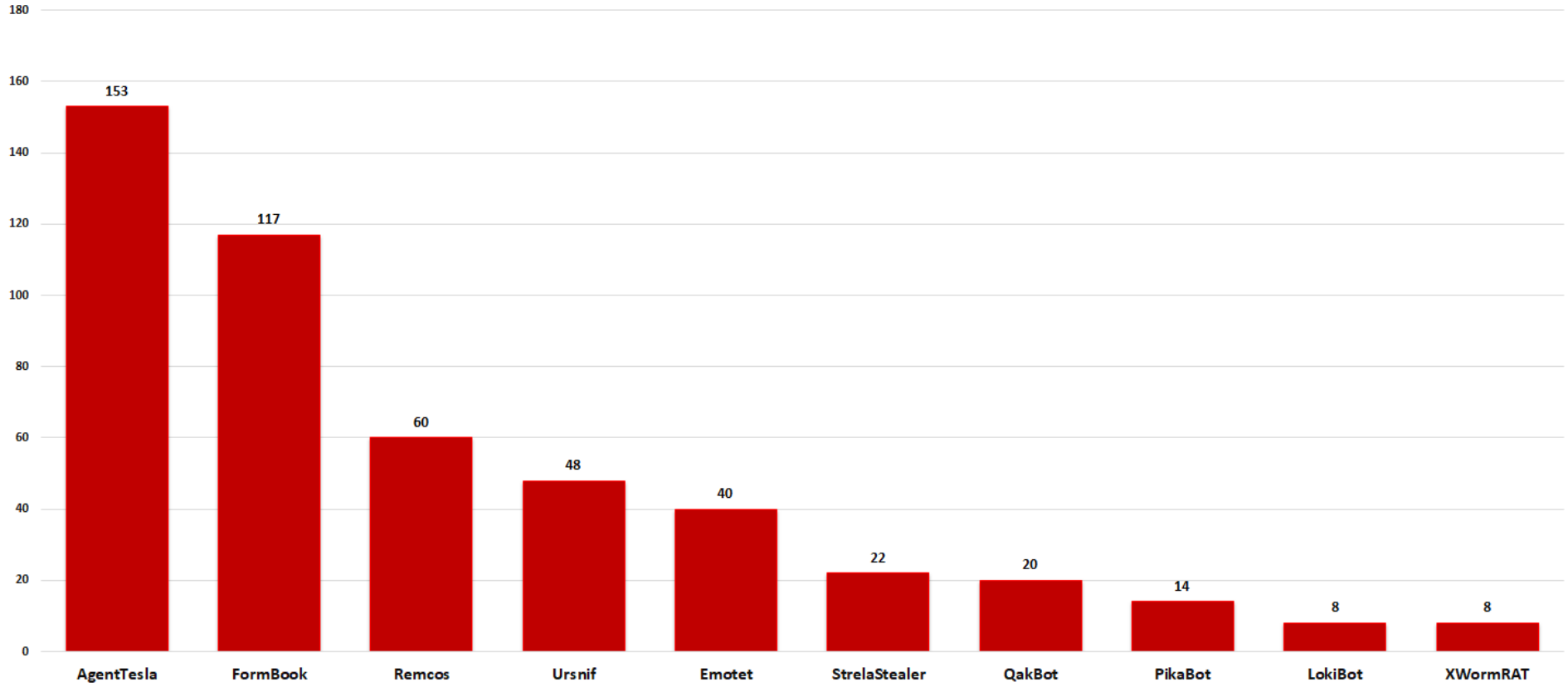
Gli **Info/Password Stealer** sono infatti una minaccia grave, in quanto sono spesso il punto iniziale di attacchi molto più sofisticati che prevedono l'utilizzo di Ransomware/CryptoMalware per la cifratura dei dati degli utenti con successiva richiesta di riscatto. Questi attacchi se non mitigati con 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	1193	WSHRAT	5
FormBook	601	Vjw0rm	4
Remcos	213	DCRAT	3
SnakeLogger	89	GomorrahStealer	3
LokiBot	87	NanoCore	3
Downloader	52	NetSupportRAT	3
Ursnif	51	Adwind	2
BluStealer	42	CoinMiner	2
Ave_Maria	40	NetWire	2
Emotet	40	QuasarRAT	2
StrelaStealer	23	RAT	2
QakBot	21	Chaos	1
STRRAT	21	DarkVisionRAT	1
PikaBot	16	HawkEye	1
XWormRAT	16	LaplasClipper	1
AzoRult	13	njRAT	1
Generic	10	PandoraRAT	1
AsyncRAT	9	PovertyStealer	1
Rhadamanthys	9	sLoad	1
Mekotio	7	VidarStealer	1
PureLogs	5		

Famiglie malware in italiano analizzate nel 2023



Nel grafico vediamo le prime 10 famiglie malware scritte in italiano che sono state analizzate nell'anno 2023, in totale sono state rilevate 24 famiglie di malware.

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

Al quarto posto troviamo il famigerato **Ursnif** che colpisce l'Italia con campagne mirate ormai dal 2018.

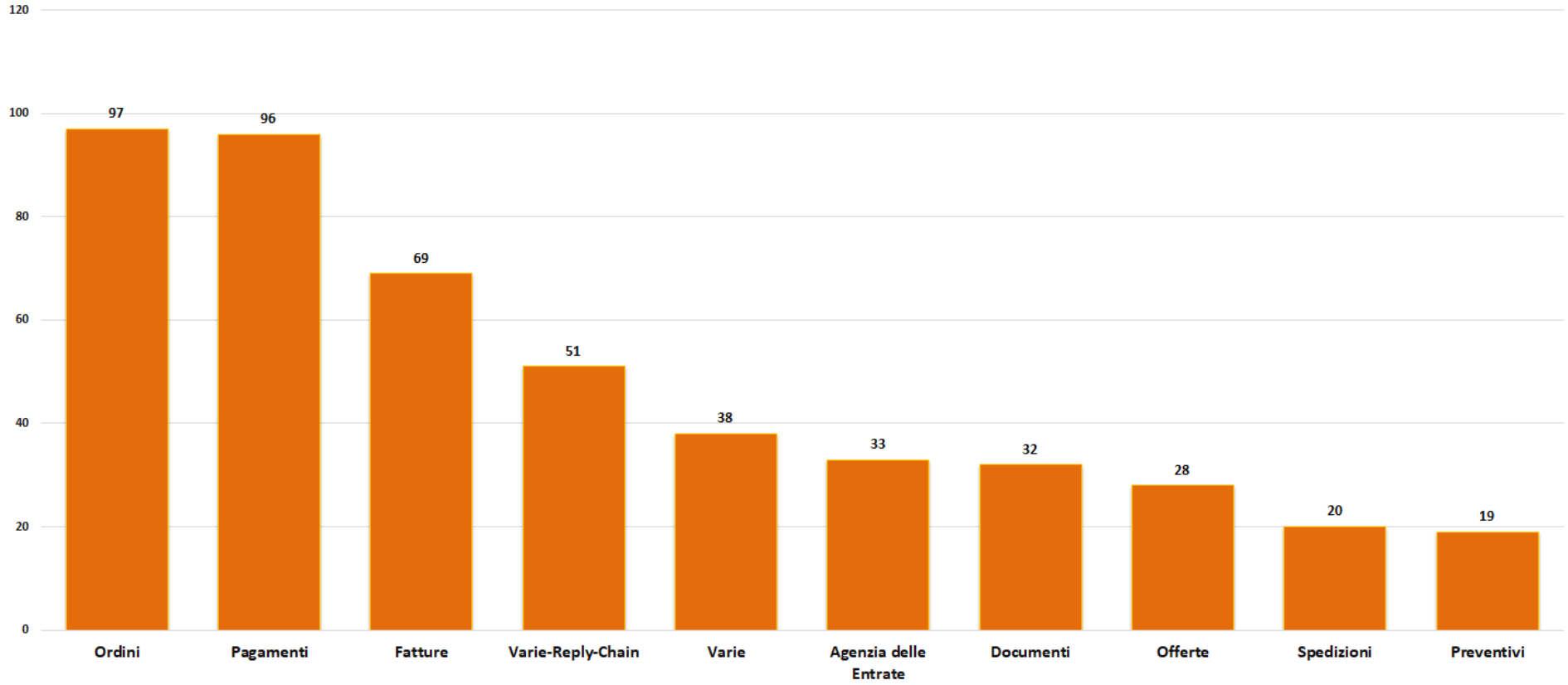
Emotet ha colpito nella parte iniziale dell'anno che campagne in reply-chain sfruttando messaggi email rubati alle vittime.

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	153	Rhadamanthys	4
FormBook	117	PureLogs	4
Remcos	60	SnakeLogger	3
Ursnif	48	STRRAT	3
Emotet	40	NanoCore	2
StrelaStealer	22	Adwind	2
QakBot	20	RAT	2
PikaBot	14	Downloader	1
LokiBot	8	WSHRAT	1
XWormRAT	8	DarkVisionRAT	1
Mekotio	8	VidarStealer	1
Ave_Maria	7	sLoad	1

Temi utilizzati nelle campagne malware in italiano analizzate nel 2023



Nel grafico analizziamo i primi 10 temi utilizzati nelle email di MalSpam con target italiano (scritte in lingua italiana), in totale sono stati rilevati 28 temi.

Al primo posto troviamo il tema "**Ordini**" con 97 campagne, subito al secondo posto con 96 campagne vi è il tema "**Pagamenti**", al terzo posto più distaccato vi è il tema "**Fatture**".

Il tema "**Agenzia delle Entrate**" è ancora molto utilizzato in particolar modo dal malware **Ursnif**.

Il tema "**Varie-Reply-Chain**" indica email di risposta a reali conversazioni precedentemente rubati e sfruttate dai CyberCriminali per aumentare la credibilità del messaggio inviato e per ingannare più facilmente la vittima, uno dei malware più noti per utilizzare questa tattica è il famigerato **Emotet**, ma non è il solo.

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	97	Corriere BRT	3
Pagamenti	96	Bonifico	3
Fatture	69	Prezzi	3
Varie-Reply-Chain	51	Ricevute	2
Varie	38	Ritiri	2
Agenzia delle Entrate	33	Ministero Sviluppo Economico	2
Documenti	32	Quotazione	1
Offerte	28	Consegne	1
Spedizioni	20	Prodotti	1
Preventivi	19	Cancellazioni	1
Prenotazioni	12	Giacenza	1
Corriere GLS	4	Trasferimento Fondi	1
Richieste	4	Ordinanze	1
Contratti	4	Acquisti	1

Conclusioni

L'anno 2023 ha riconfermato il trend di diffusione di **Info/Password Stealer** attraverso campagne di malspam (veicolate sia attraverso posta elettronica ordinaria sia in alcuni casi, sebbene ridotti, via PEC).

Tra le famiglie maggiormente veicolate troviamo **AgentTesla**, seguito a ruota da **FormBook** e **Remcos**. Queste tre famiglie hanno ottenuto il podio sia su quelle globali sia su quelle scritte in italiano.

Anche nel 2023 si è osservata l'attività da parte del threat actor che utilizza il malware **Ursnif** (ID 5050) per colpire l'utenza italiana con campagne mirate principalmente a tema governativo dell'Agenzia delle Entrate. Questo gruppo, che storicamente colpisce l'Italia dal 2018, verso la fine dell'anno sembra aver cambiato strategia utilizzando principalmente il malware **Remcos** al posto di Ursnif. Questo cambiamento potrebbe essere stato dettato da nuove necessità o da nuovi interessi verso i dati e le informazioni delle vittime italiane.

Per quanto riguarda i **ransomware**, veicolati attraverso l'email, si evidenzia solamente una campagna da parte della famiglia **Chaos**. Il vettore maggiormente utilizzato negli attacchi ransomware anche nell'anno 2023 è l'accesso tramite **Remote Desktop (RDP)** esposto verso internet, seguito da **VPN** (spesso tramite credenziali violate da password stealer) e vulnerabilità su **software/servizi/firewall** non regolarmente aggiornati.

I temi delle campagne malspam nel panorama italiano seguono le attività lavorative/produttive del Paese come ad esempio: **ordini, pagamenti e fatture**.

Il linguaggio di compilazione di malware più utilizzato nell'anno 2023 è stato il **C# (MSIL/.Net)**, questo linguaggio di alto livello permette una più facile implementazione di codice a differenza di altri linguaggi che richiedono capacità di programmazione più avanzate.

TG Soft
Cyber Security Specialist
www.tgsoft.it