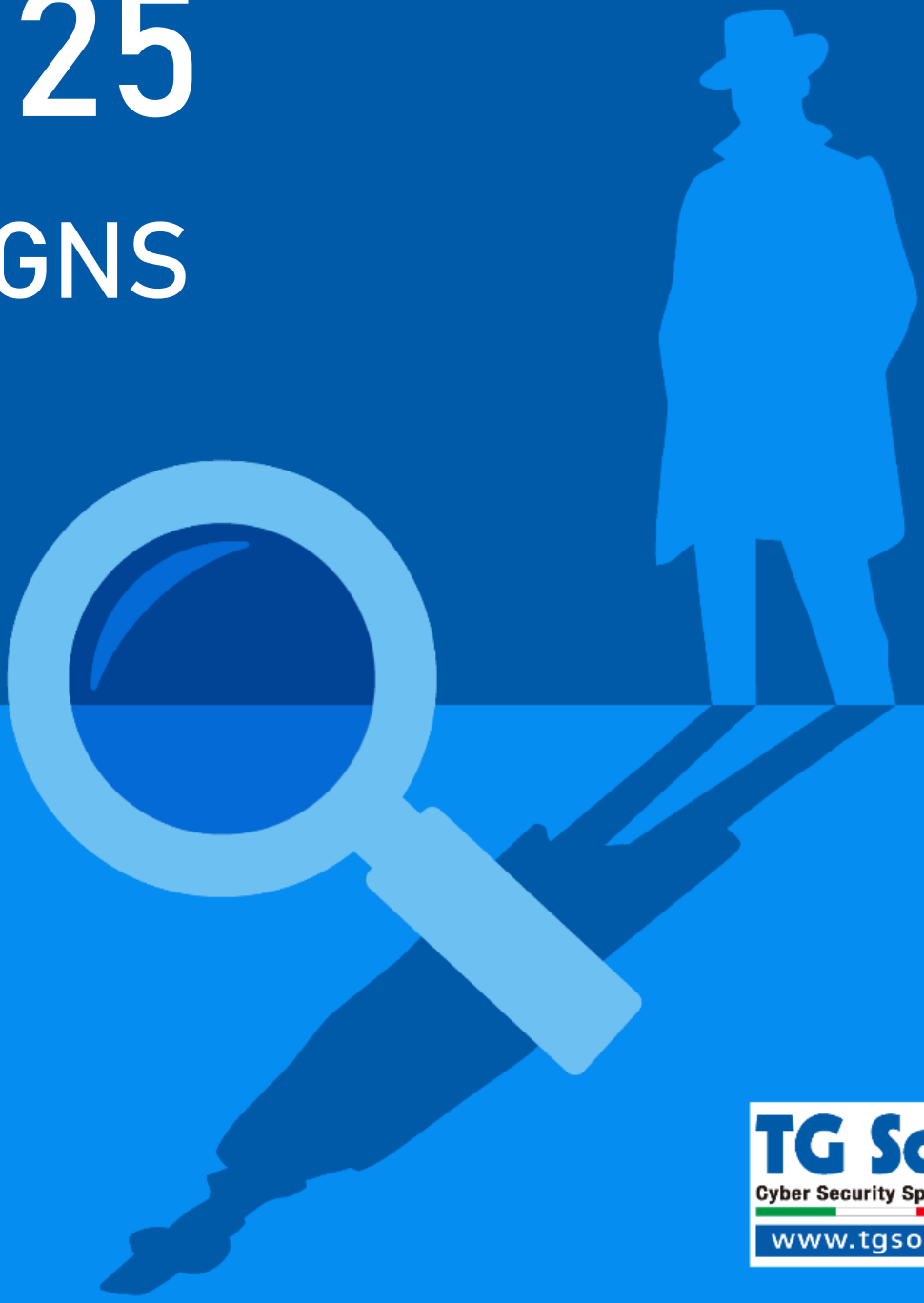
REPORT 2025

MALWARE CAMPAIGNS



TG Soft
Cyber Security Specialist
www.tgsoft.it

REPORT 2025

MALWARE CAMPAIGNS

Authors

Radu Breabin

Michele Zuin

Nicola Miotti

Samuele Callegaro

Gianfranco Tonello

Enrico Tonello

Index

Introduction

The following report, drawn up by the C.R.A.M. of TG Soft, summarises all the MalSpam campaigns sent via email that were analysed during the year 2024.

The TG Soft C.R.A.M. releases a weekly analysis of MalSpam campaigns spread in Italy and makes them available in the News section of TG Soft website.

In the year 2024, the majority of malware used belong to the **Info/Password Stealer** and **RAT** families with rare and sporadic exceptions.

This growing trend in the use of these types of malware is dictated both by the ease of access to these tools by cybercriminals who purchase these services on the dark web as MaaS (Malware as-a-Service) at easily accessible prices and by the actual dangerousness of this type of Malware which in certain families are particularly sophisticated.

The use of such Malware allows preliminary access to the affected machines/services, leading to an evolution of the attack that extends to the entire network/company, often culminating in the distribution of Ransomware CryptoMalware or with the hijacking of bank transfers via MITM attacks for the theft of money, etc.

Ransomware in particular, if not mitigated with effective technologies such as those present in the Vir.IT eXplorer PRO suite (see Vir.IT AntiRansomware protezione CryptoMalware) they can bring the entire company to its knees for days/weeks/months, also leading to serious economic consequences in terms of lost production and recovery costs.

Numerically, the number of campaigns follows the trend of the country's production activities, with an increase in campaigns in the initial part of the year to stabilize and then decrease in the final part. The trend of campaigns also reflects the main holidays with a decrease in the Christmas, Easter and summer holiday periods.

Malware that have historically hit Italy such as **Ursnif** was not spread in the year analyzed, as well as **Emotet** which has hit Italian users since 2020 through campaigns that use the “reply-chain” technique to make messages much more credible and therefore increase the effectiveness of the attack, carried out only a few weeks of MalSpam activity in 2023 to move to a period of definitive absence.

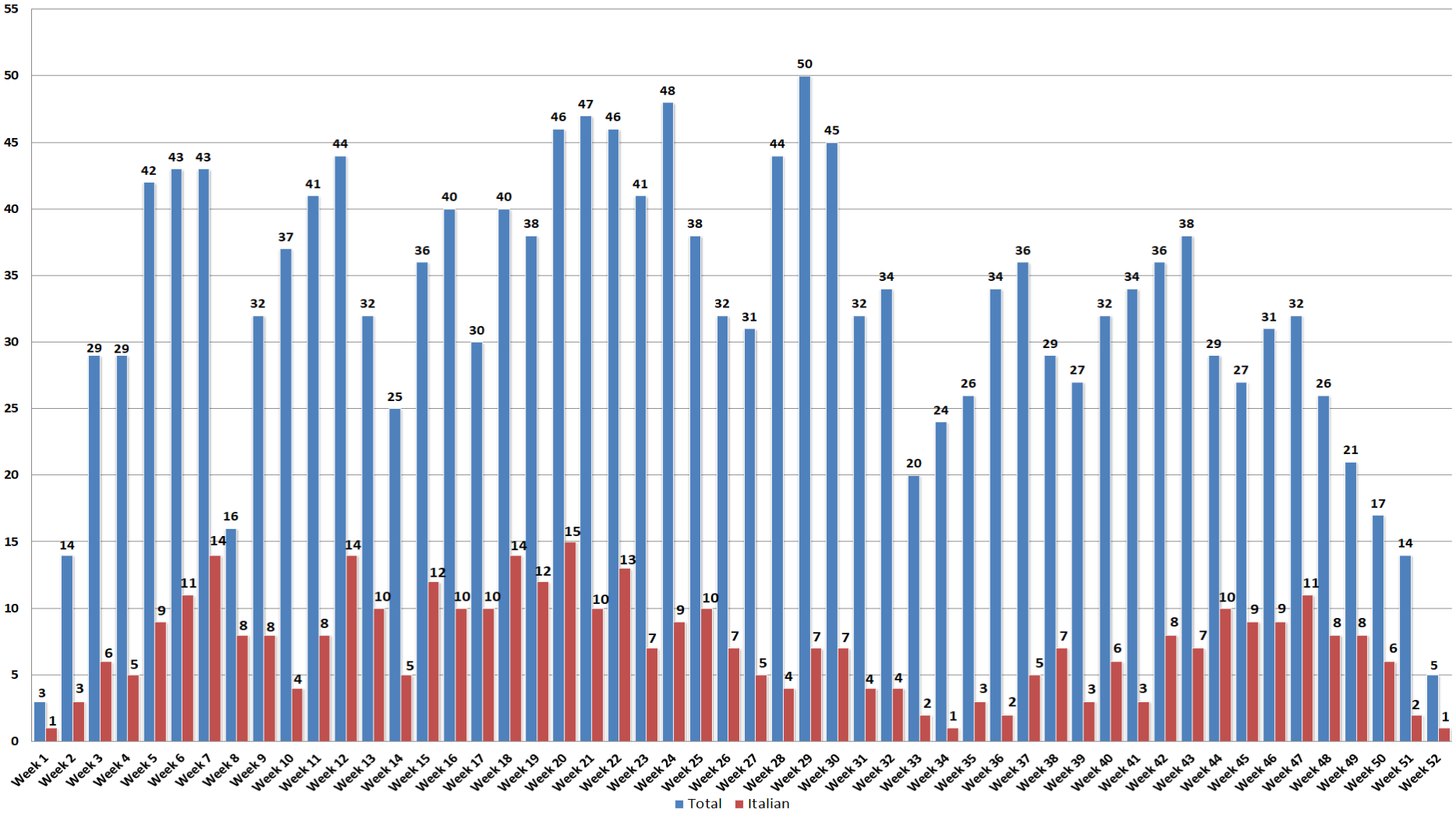
One of the novelties of this year was the interception of two targeted attacks on Italian companies and government entities by a Chinese cyber-actor that exploit a variant of the **Rat 9002** in diskless mode. Other variants have been called over time as **Rat 3102**. The two variants are notoriously linked to **APT17**, a Chinese cyber-criminal group known for: "Operation Aurora (attributed to the Chinese government)", "Operation Ephemeral Hydra" and for targeted attacks on companies and government entities.

In general, the malware that was mainly used to hit both through global campaigns and those written in Italian was **AgentTesla**, an easily available Info/Password Stealer that exfiltrates data and passwords from the affected machines. Generally, the collected data is exfiltrated via email but the malware also provides exfiltration functionality via FTP and Telegram channels.

Let's see in a small summary table the year 2024 in brief, in the following pages instead we will analyze in more detail the trend of the campaigns spread in Italy via email:

NUMBER OF GLOBAL CAMPAIGNS SPREAD IN ITALY ANALYSED	**1687**
NUMBER OF CAMPAIGNS IN ITALIAN (written in Italian) ANALYSED	**377 – 22,34%** compared to global campaigns
WEEKLY GLOBAL CAMPAIGNS PEAK	**50 – Week 29**
WEEKLY MAXIMUM PEAK OF ITALIAN CAMPAIGNS	**15 – Week 20**
MOST USED LANGUAGE	**MSIL (C# .NET) – 36,22%** of the total
MOST USED MALWARE FAMILY GLOBALLY	**AgentTesla**
MOST USED MALWARE FAMILY IN ITALIAN CAMPAIGNS	**AgentTesla**
TOTAL NUMBER OF TOPICS	**24**
MOST USED THEME IN ITALIAN CAMPAIGNS	**Orders (in italian “Ordini”)**

Weekly campaign performance chart in 2024



From the graph you can see the trend of the campaigns divided into the various weeks (Weeks) of the year 2024.

The blue bar indicates the total number of campaigns sent via email in Italy each week, while the red bar refers to campaigns written in Italian language (targeting Italy).

To understand how the various weeks (Weeks) are divided, below we report a small example table that indicates the division of the periods taken into consideration:

Week	from	to
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 total, **1687** global campaigns were monitored in 2024, while **377** campaigns were written in Italian.

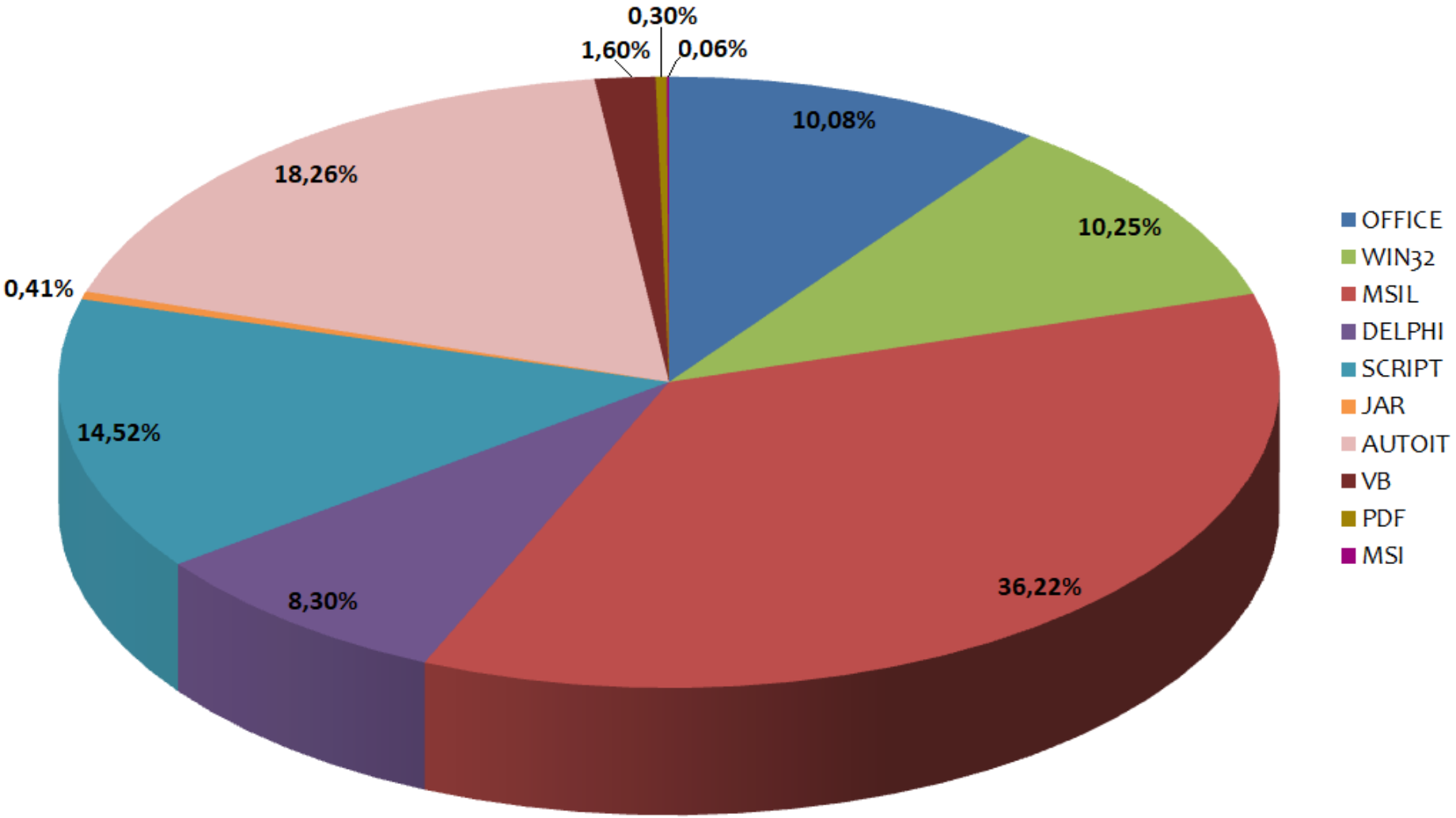
The general trend shows a greater amount of campaigns in the early part of the year with a reduction in the later part.

From the graph, it can be noted that MalSpam campaigns also follow the trend of the regular activities of the average user with a decrease during the holidays and a strong increase in periods of greater productivity where users are more easily targeted by malicious campaigns.

The week with the highest number of global campaigns was Week 29 which recorded **50** campaigns, while the week with the highest number of campaigns written in Italian was Week 20 with **15** campaigns.

The general average calculated over the entire year on global campaigns is approximately **32** weekly campaigns while that of campaigns written in Italian is approximately **7** campaigns.

Graph of the types of language used in 2024



From the graph we analyze the types of language used to develop malware spread in the year 2024.

As you can see, the **MSIL** language (C# .NET) is the most used language to create malware spread during the year with 36.22%.

In second place we find **AutoIT** executable files which represent 18.26%.

In third place are scripting languages with 14.52%, this family includes scripts such as JavaScript, VBScript, PowerShell, links, WSF, BAT, etc.

In fourth place we find the Win32 files which group all the executable samples with various compiled languages such as C, C++, etc. which represent 10.25%.

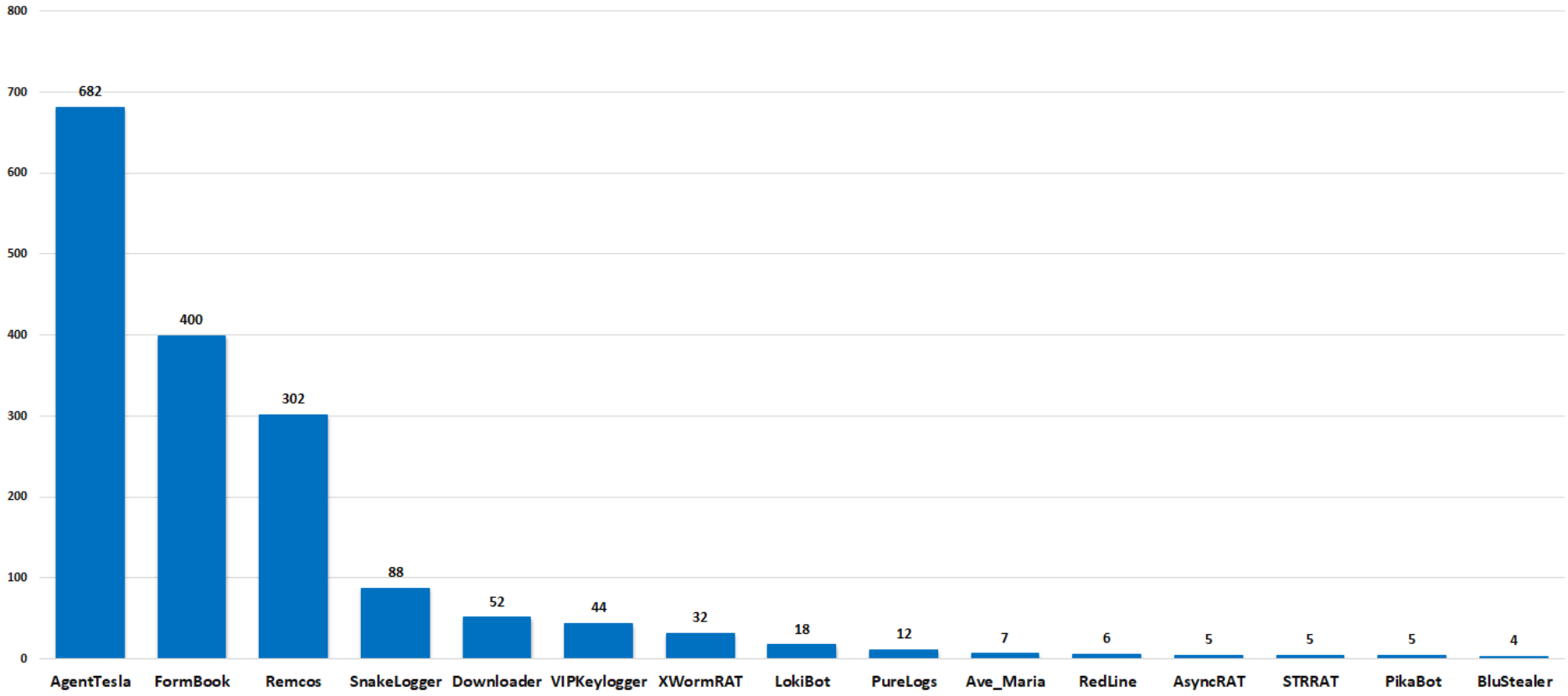
10.08% of malware spreads through Microsoft Office documents (Word, Excel, PowerPoint, etc.), Office documents generally use malicious macros to infect the victim's PC.

The Delphi programming language is used in 8.30% of the samples while the rest of the samples are represented in a minority by PDF, JAR (Java), MSI (installation packages) and VB (Visual Basic).

Below is a table with the number of campaigns divided by language:

LANGUAGE	NUMBER OF CAMPAIGNS
MSIL	611
AUTOIT	308
SCRIPT	245
WIN32	173
OFFICE	170
DELPHI	140
VB	27
JAR	7
PDF	5
MSI	1

Global Malware Families Analyzed in 2024



In the graph we see the top 15 malware families spread globally in the year 2024, in total 31 malware families were analyzed.

As you can see the most used malware was **AgentTesla** with **FormBook** in second place and **Remcos** in third.

We have detected a significant increase in a new malware family called **VIPKeylogger** which shares many features and concepts with the malware family called SnakeLogger. It is also an **Info/Password Stealer** which was first detected in the second half of the year 2024.

More generally, most of the malware used belongs to the macro family of **Info/Password Stealers**. This demonstrates a strong interest by cybercriminals towards the data and passwords of the victims.

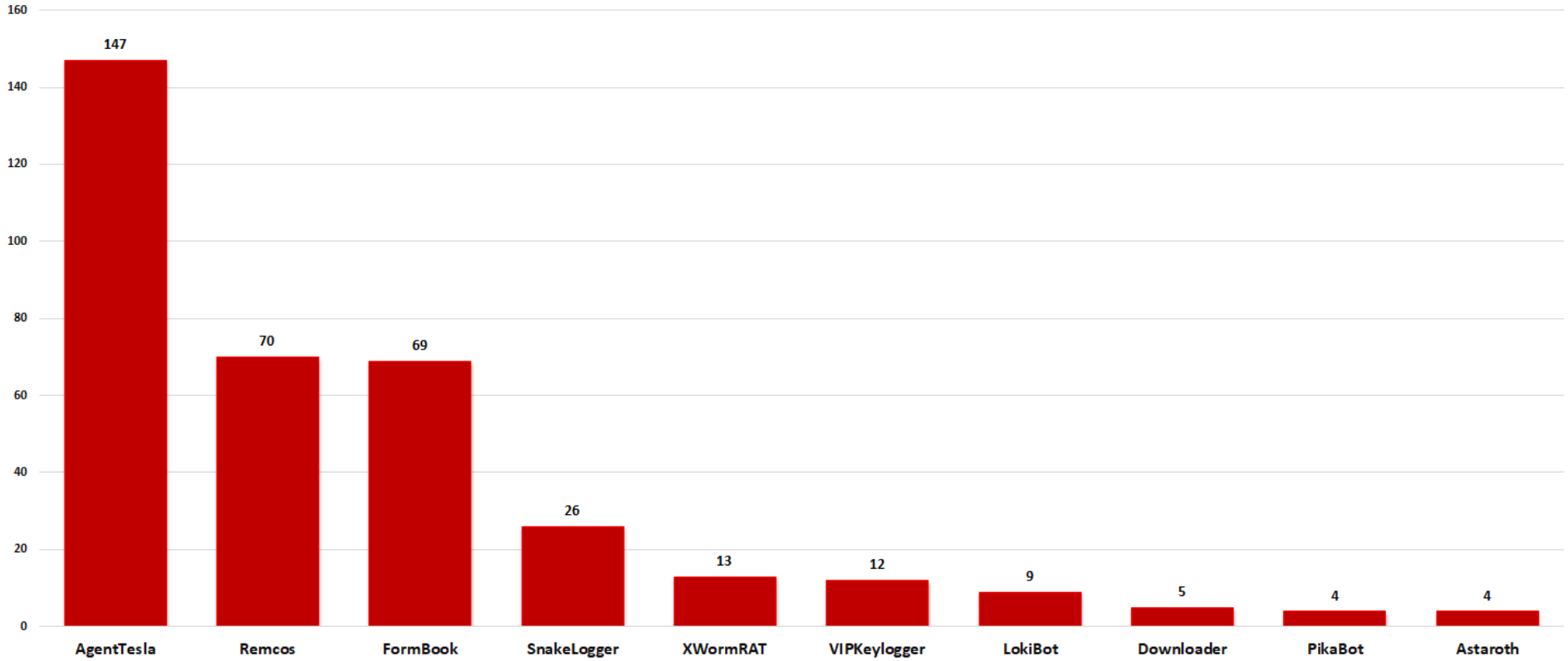
Info/Password Stealers are in fact a serious threat, as they are often the starting point of much more sophisticated attacks that involve the use of Ransomware/CryptoMalware to encrypt user data with subsequent ransom requests. These attacks, if not mitigated with specific technologies such as those present in the Vir.IT eXplorer PRO suite, can bring entire companies to their knees for weeks/months.

Another macro family that has been widely used during the year is that of **RATs** (Remote Access Trojans), these malware allow you to take complete control of the victim's PC, thus generating a dangerous access point from the outside to the victim's computer network.

Below is the summary table of all the families analyzed with the relative number of campaigns:

FAMILY	NUMBER OF CAMPAIGNS	FAMILY	NUMBER OF CAMPAIGNS
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		

Malware families in Italian analyzed in 2024



In the graph we see the first 10 malware families written in Italian that were analyzed in the year 2024, in total 20 malware families were detected.

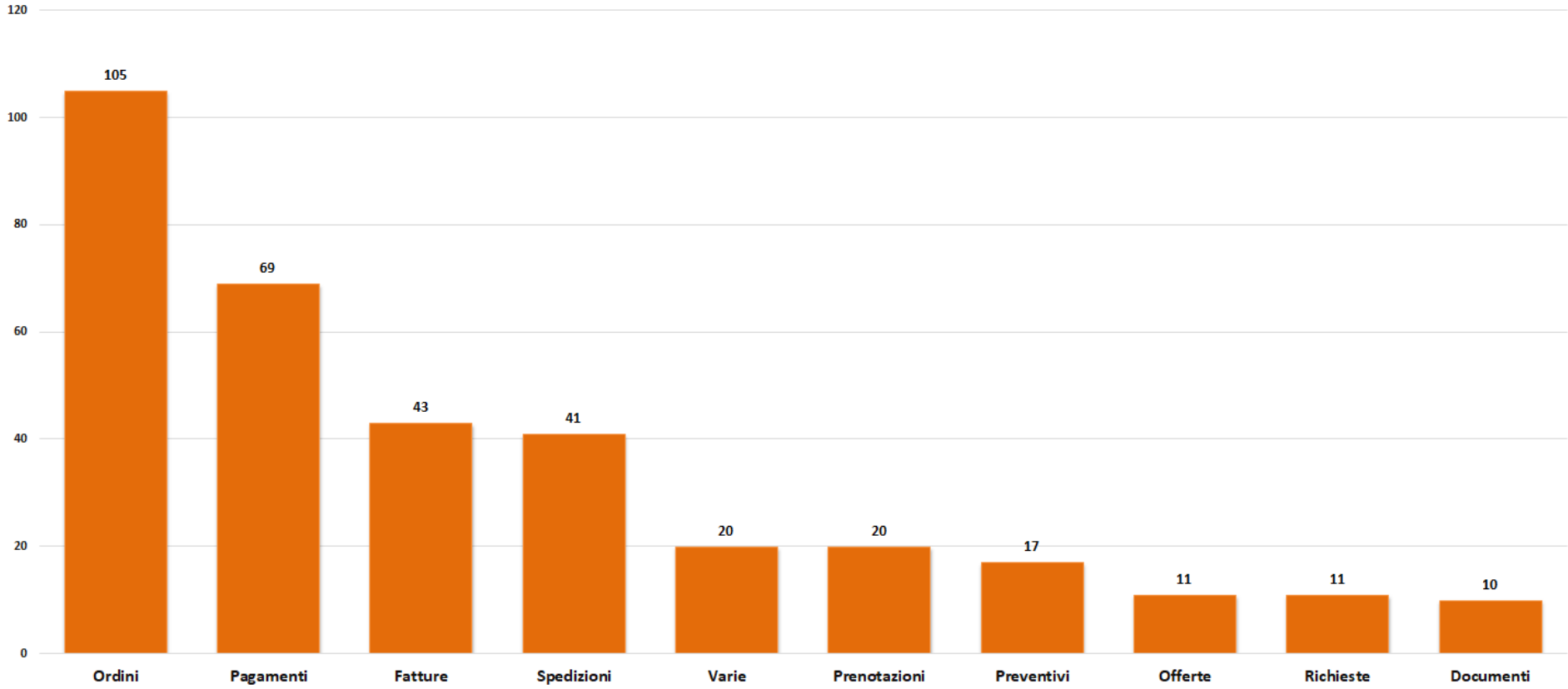
They also reflect global families in those written in Italian the most used malware is **AgentTesla** with **Remcos** in second place and **FormBook** in third.

Even in campaigns written in Italian, in general the majority of malware used belong to the macro family of **Info/Password Stealers** and **RATs**.

Below is the summary table of all the families analyzed with the relative number of campaigns:

FAMILY	NUMBER OF CAMPAIGNS	FAMILY	NUMBER OF CAMPAIGNS
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

Themes used in Italian malware campaigns analyzed in 2024



In the graph we analyze the first 10 themes used in MalSpam emails with an Italian target (written in Italian), in total 24 themes were detected.

In first place we find the theme "**Orders**" (“Ordini” in italian) with 105 campaigns, immediately in second place with 69 campaigns is the theme "**Payments**" (“Pagamenti” in italian), in third place more detached is the theme "Invoices" (“Fatture” in italian).

The “**Miscellaneous**” (“Varie” in italian) theme indicates emails replying to real conversations previously stolen and exploited by Cybercriminals to increase the credibility of the message sent and to deceive the victim more easily.

In general, the themes used cover a wide range of areas, starting from the more generic ones and arriving at more specific or governmental themes.

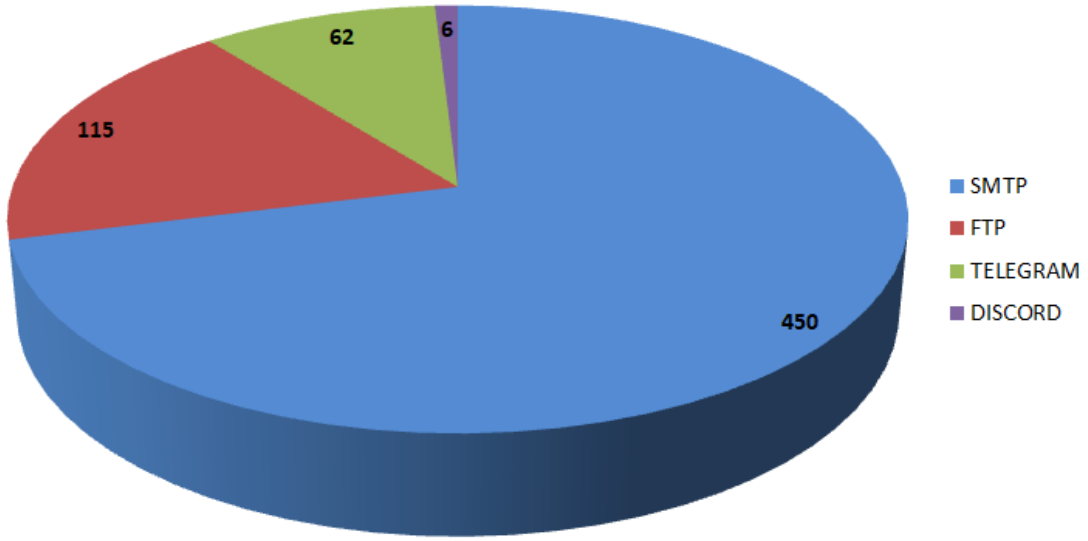
Below is the table with all the themes found and the relative quantity:

THEME (in italian)	NUMBER OF CAMPAIGNS	THEME (in italian)	NUMBER OF CAMPAIGNS
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

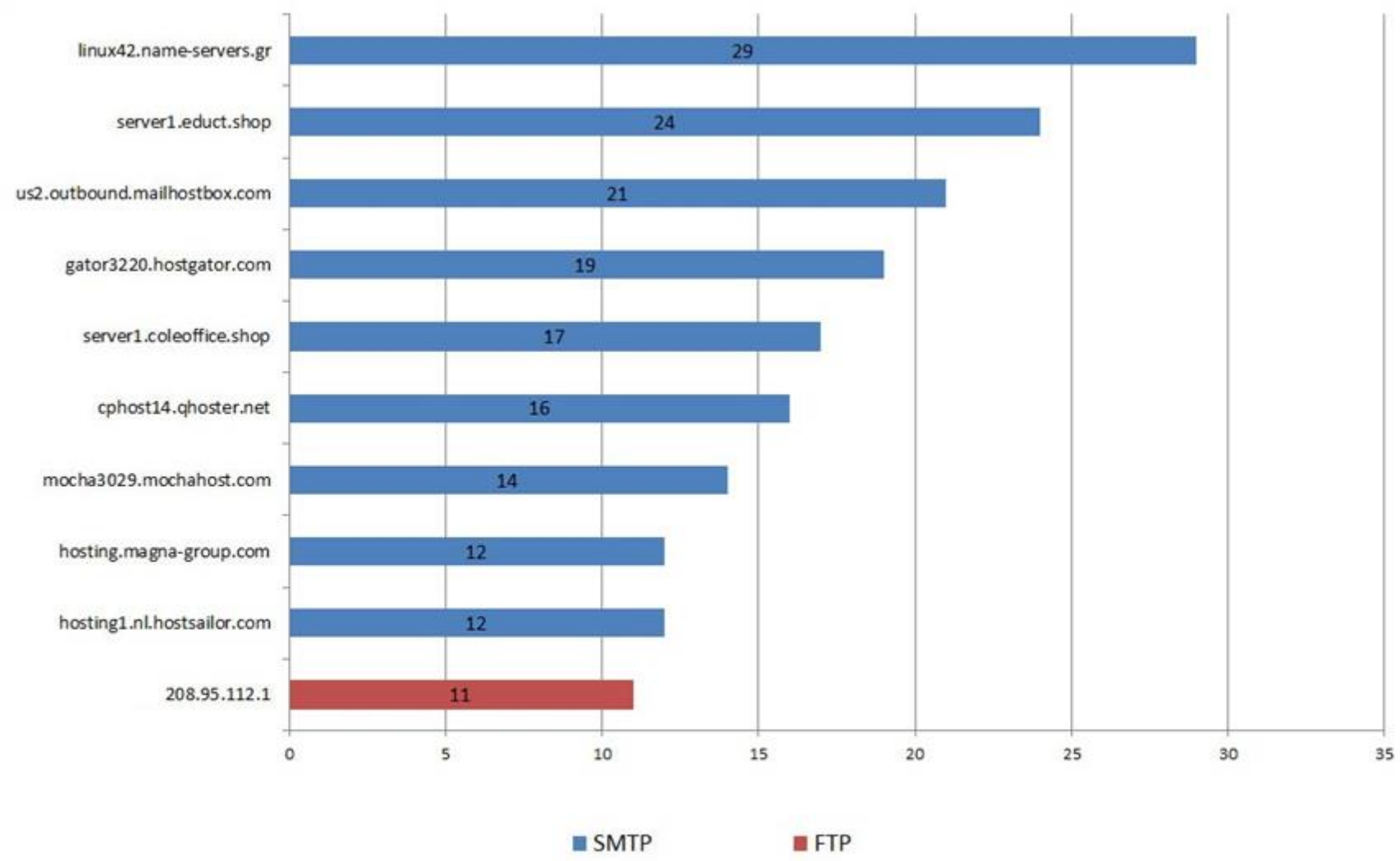
AgentTesla

We have conducted a deeper analysis of **AgentTesla**, the malware that belongs to the Info/Password Stealer family to better understand its main data exfiltration methods and the hosts that were used most frequently. The main data exfiltration methods that we detected in the year 2024 were the following 4:

- **SMTP** (Simple Mail Transfer Protocol) - which represents exfiltration through email servers and was the most widespread in the year 2024 with a total number of **450** samples.
- **FTP** (File Transfer Protocol) - It is the most famous protocol that is used to transfer files from a server to a client which has been detected for a total number of **115** samples.
- **Telegram** - one of the most well-known international messaging platforms used by malware to exfiltrate stolen data. In most cases, exfiltration occurs via a BOT created by the criminals, to which the data is sent in the form of a compressed archive. This method was detected for a total of **62** campaigns.
- **Discord** - it is always one of the most well-known international messaging and VoIP platforms which is also used as an exfiltration method through a BOT created by criminals, a method very similar to the one mentioned above for Telegram. In this case Discord was detected for a total number of **6** campaigns.

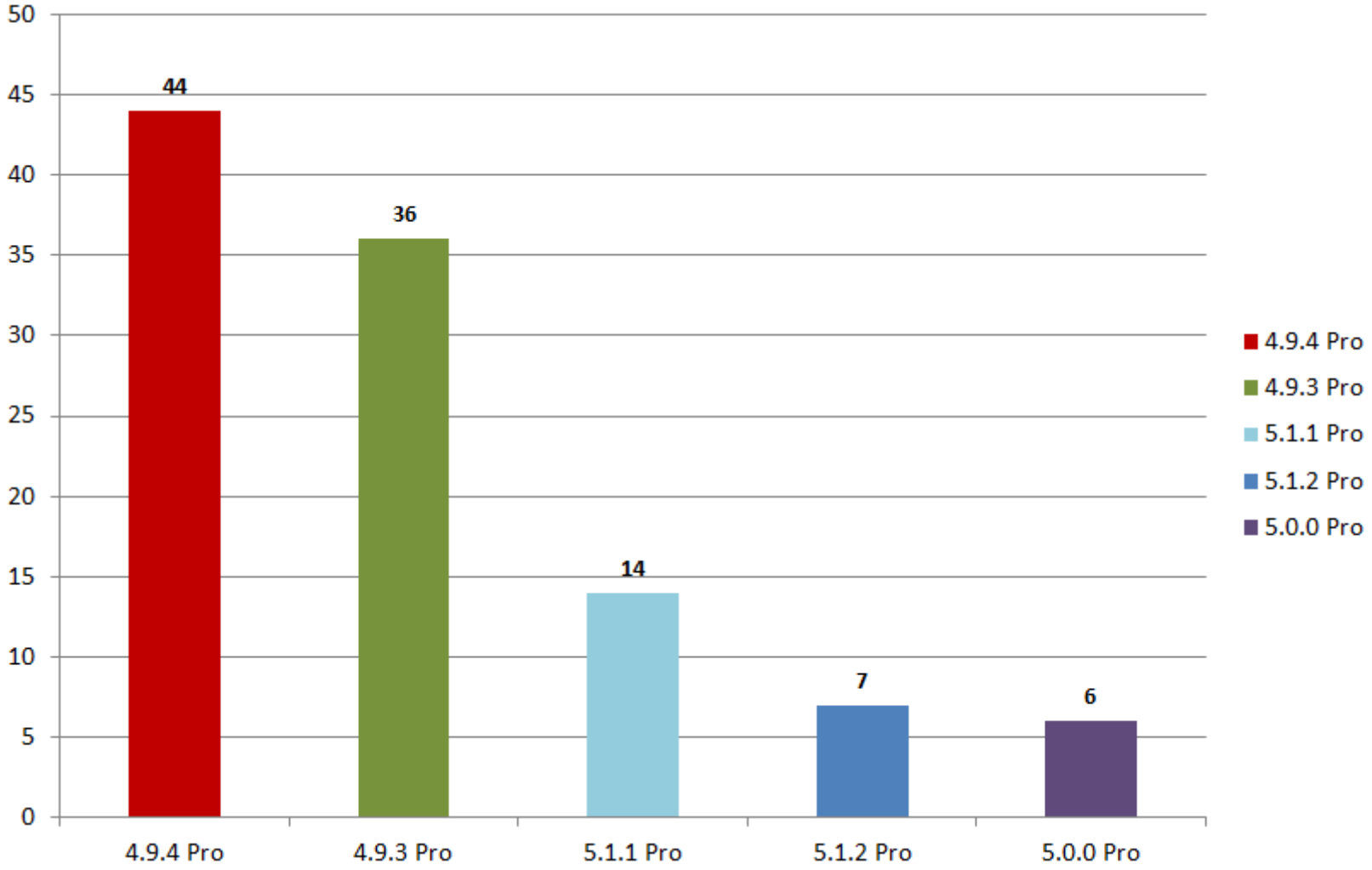


Below we see the **TOP10 SMTP/FTP** servers used by the AgentTesla malware:



Remcos

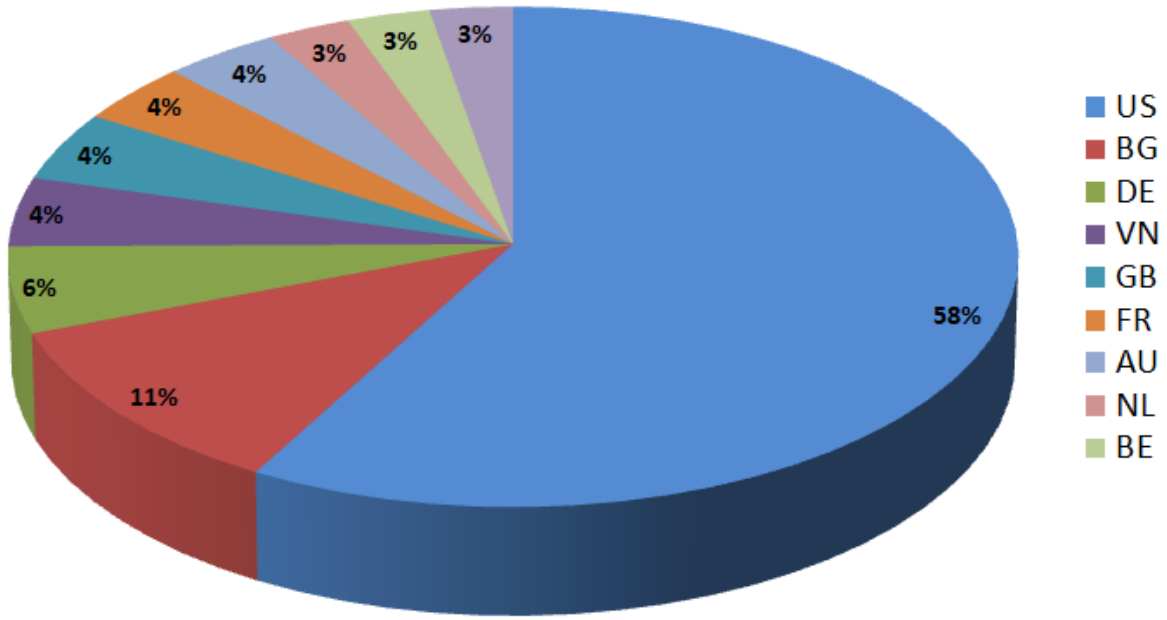
Another in-depth analysis was carried out on the **Remcos** malware which belongs to the macro-family of RATs (Remote Access Trojans), as we have already highlighted above, this malware has positioned itself in third place among the malware spread globally in the year 2024. The most widespread build was the 4.9.4 Pro version (by "Pro" we mean the professional version purchased with all the available features) with 44 campaigns detected.



During our analysis we also found that the most used Remcos license was: “**38CBE3E7CD1A6C11156346CAE4B39D90**” with 13 uses out of 207 campaigns analyzed.

It was also noted that the most spread mutexes in 2024 were "**Rmc-2OLA39**" and "**Rmc-999Z97**" with 6 appearances each, the “**MUTEX**” is the string that is assigned by the Threat Actor once the build configuration is finished, very often it is also used to trace the number of campaigns spread by a certain actor.

TOP 10 MUTEX	
MUTEX	**NUMBER OF CAMPAIGNS**
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

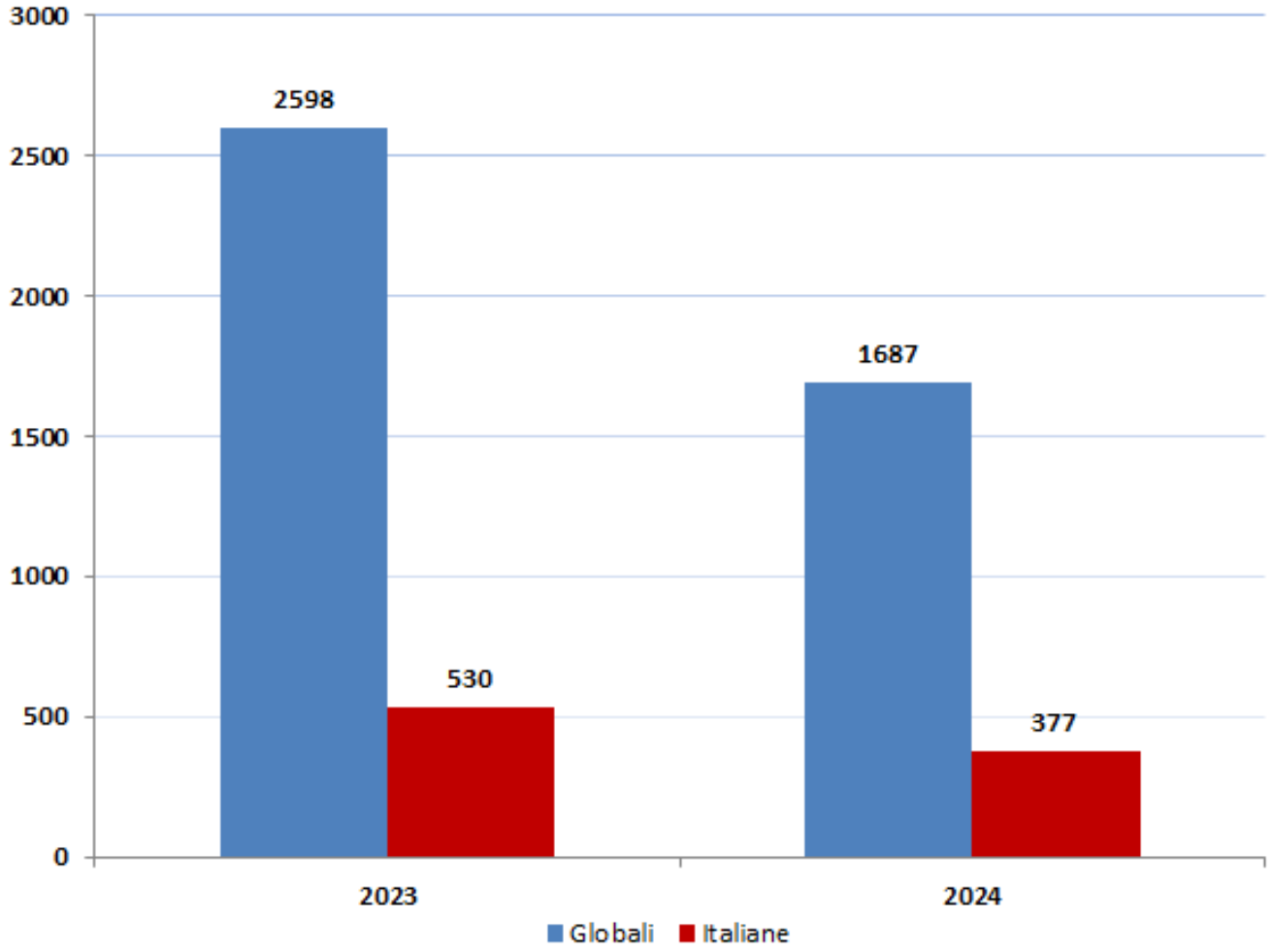


TOP10 C2

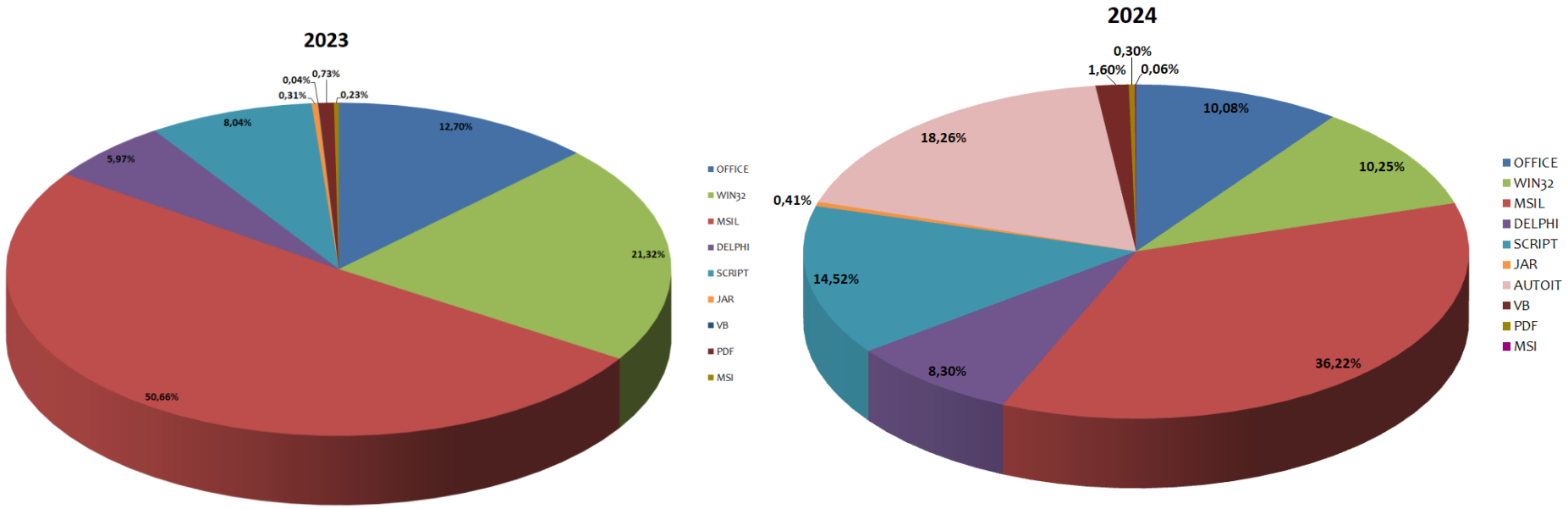
From the analysis of the malware and its traffic activities, the 10 most used countries to host Command and Control (C2) servers have been identified. As we can see from the pie chart, the highest percentage is that of the United States of America, it is the country where we have the highest number of C2 servers with 46 different IP addresses out of 105 in total. In second place we find Bulgaria with 15 different addresses out of a total of 20. As for the third place, it is Germany (abbreviation DE) with 6 different IP addresses out of a total of 10.

Comparison of malware campaigns analyzed in 2023/2024

Making a comparison with the year 2023, we can note that 2024 had a decrease of 911 global campaigns and 153 Italian campaigns (written in Italian) less than the year 2023.



In terms of the types of languages used, in 2024 we observed a strong decrease in the MSIL language (C# .NET) of approximately 14.44% compared to the year 2023, and a significant increase of 18.26% in the AutoIT programming language, which however in 2023 was incorporated into the Win32 family.



The first 3 families that dominated in both years remain unchanged, more precisely those of the macro families of Info/Password Stealer which are **AgentTesla**, **FormBook** and those of the macro families of RAT which is **Remcos**.

Another important similarity concerns the themes used in MalSpam emails with an Italian target (written in Italian), and the common predominance of the following themes: Orders, Payments and Invoices (Ordini, Pagamenti and Fatture in italian). This fact is explained by the simple reason that most of the emails sent by customers and suppliers concern the work and relational sphere, where in most cases it is precisely about orders and the activities that are carried out on them, mainly payments and invoices.

In the table below we can see the comparison of the families, as you can see some malware families were present both in 2023 and 2024 (light blue color), some were not present in 2024 (red color) while others are families that were not present in 2023 (green color).

Historical malware such as **Ursnif**, **Emotet** and **sLoad** were not detected in 2024 replaced by new families such as **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

Conclusions

The year 2024, although down compared to 2023, was characterized by the families of **Info/Password Stealers** and **RATs** mainly spread through ordinary electronic mail (**PEO**) and in some cases through certified electronic mail (**PEC**).

Following the trend of recent years, even in 2024 the most widespread malware was **AgentTesla**, demonstrating the interest of Cybercriminals in data and information present on the victims' devices.

The most used malware compilation language in the year 2024 was **C# (MSIL/.Net)**, this language is more high-level and therefore allows easier implementation of code with less specific knowledge, unlike other languages that require more advanced programming skills.

As for ransomware, the most used vector in ransomware attacks even in the year 2024 is access via **Remote Desktop (RDP)** exposed to the internet, showing how RDP is still a weak point in many corporate networks and that if poorly configured/exposed it can lead to very serious consequences.

The predominant themes were Orders, Payments and Invoices (Ordini, Pagamenti and Fatture in italian), all three linked to the country's production factor.

In terms of **APTs**, two targeted attacks on Italian companies and government entities by a Chinese cyber actor were observed on June 24 and July 2, 2024, using a diskless variant of the **Rat 9002**. These activities are associated with the APT17 group also known as "DeputyDog".

The first campaign on June 24, 2024, exploited an Office document, while the second campaign contained a link.

Both campaigns invited the victim to install a Skype for Business package from a link in an Italian government-like domain to deliver a variant of **Rat 9002**.

More information can be found in the dedicated article: Italian government agencies and companies in the target of a Chinese APT

TG Soft

Cyber Security Specialist

www.tgsoft.it